Microsoft.MS-102.vOct-2024.by.Unomoto.150q

Number: MS-102
Passing Score: 800
Time Limit: 120
File Version: 31.0

Exam Code: MS-102

Exam Name: Microsoft 365 Administrator

Case 01

Case Study

This is a case study. Case studies are not timed separately. You can use as much exam time as you on this exam in the time provided.

To answer the questions included in a case study, you will need to reference information that is provided in the case study. Case studies might contain exhibits and other resources that provide more information about the scenario that is described in the case study. Each question is independent of the other questions in this case study.

At the end of this case study, a review screen will appear. This screen allows you to review your answers and to make changes before you move to the next section of the exam. After you begin a new section, you cannot return to this section.

To start the case study

To display the first question in this case study, click the Next button. Use the buttons in the left pane to explore the content of the case study before you answer the questions. Clicking these buttons displays information such as business requirements, existing environment, and problem statements.

If the case study has an All Information tab, note that the information displayed is identical to the information displayed on the subsequent tabs. When you are ready to answer a question, click the Question button to return to the question.

Overview

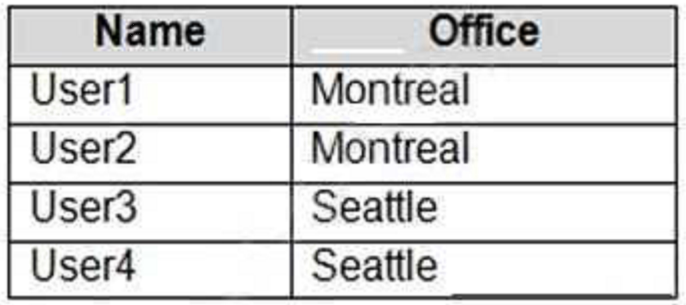
General Overviews

Litware, Inc. is a technology research company. The company has a main office in Montreal and a branch office in Seattle.

Environment

Existing Environment

The network contains an on-premises Active Directory domain named litware.com. The domain contains the users shown in the following table.

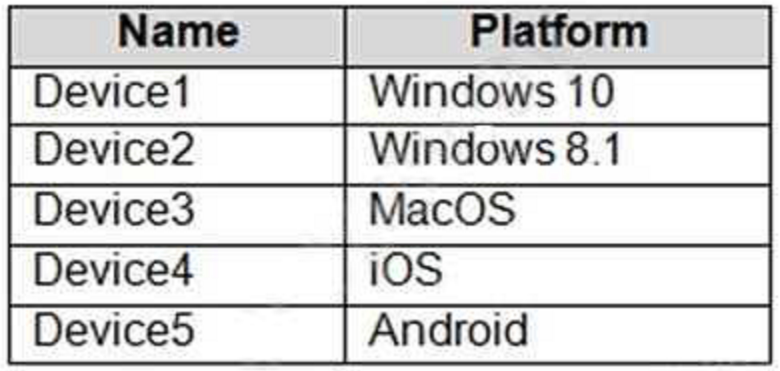


Name	Office
User1	Montreal
User2	Montreal
User3	Seattle
User4	Seattle

Microsoft Cloud Environment

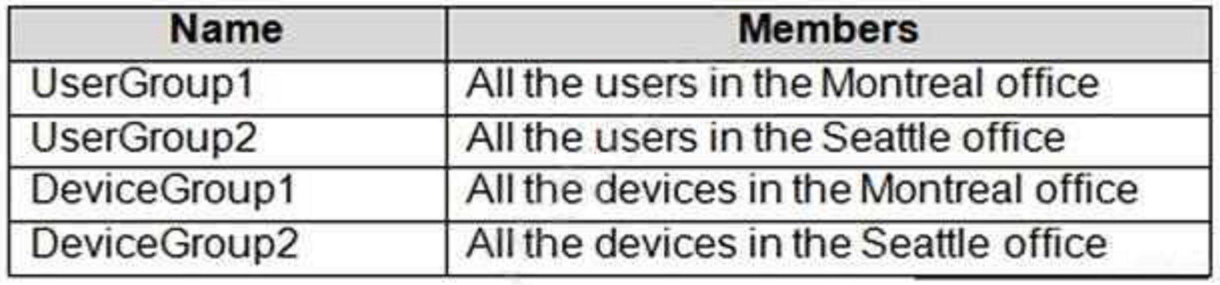
Litware has a Microsoft 365 subscription that contains a verified domain named litware.com. The subscription syncs to the on-premises domain.

Litware uses Microsoft Intune for device management and has the enrolled devices shown in the following table.



Name	Platform
Device1	Windows 10
Device2	Windows 8.1
Device3	MacOS
Device4	iOS
Device5	Android

Litware.com contains the security groups shown in the following table.



Name	Members
UserGroup1	All the users in the Montreal office
UserGroup2	All the users in the Seattle office
DeviceGroup1	All the devices in the Montreal office
DeviceGroup2	All the devices in the Seattle office

Litware uses Microsoft SharePoint Online and Microsoft Teams for collaboration.

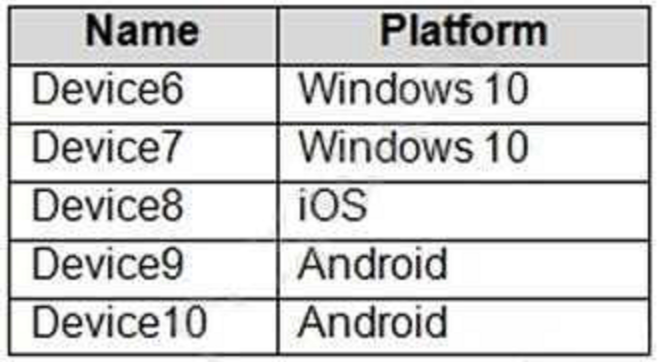
The verified domain is linked to an Azure Active Directory (Azure AD) tenant named litware.com.

Audit log search is turned on for the litware.com tenant.

Problem Statements

Litware identifies the following issues:

Users open email attachments that contain malicious content.
Devices without an assigned compliance policy show a status of Compliant.
User1 reports that the Sensitivity option in Microsoft Office for the web fails to appear.
Internal product codes and confidential supplier ID numbers are often shared during Microsoft Teams meetings and chat sessions that include guest users and external users.
Requirements
Planned Changes
Litware plans to implement the following changes:
Implement device configuration profiles that will configure the endpoint protection template settings for supported devices.
Configure information governance for Microsoft OneDrive, SharePoint Online, and Microsoft Teams.
Implement data loss prevention (DLP) policies to protect confidential information.
Grant User2 permissions to review the audit logs of he litware.com tenant.
Deploy new devices to the Seattle office as shown in the following table.



Name	Platform
Device6	Windows 10
Device7	Windows 10
Device8	iOS
Device9	Android
Device10	Android

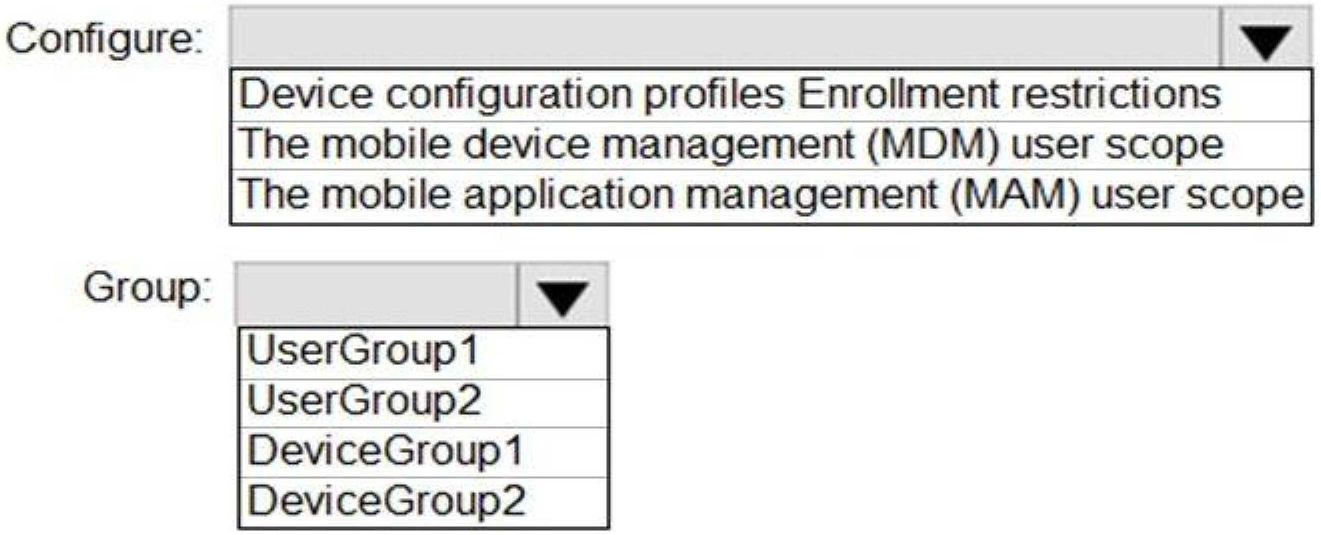
Implement a notification system for when DLP policies are triggered.
Configure a Safe Attachments policy for the litware.com tenant.
Technical Requirements
Litware identifies the following technical requirements:
Retention settings must be applied automatically to all the data stored in SharePoint Online sites,
OneDrive accounts, and Microsoft Teams channel messages, and the data must be retained for five years.
Emails messages that contain attachments must be delivered immediately, and placeholder must be provided for the attachments until scanning is complete.
All the Windows 10 devices in the Seattle office must be enrolled in Intune automatically when the devices are joined to or registered with Azure AD.
Devices without an assigned compliance policy must show a status of Not Compliant in the Microsoft Endpoint Manager admin center.
A notification must appear in the Microsoft 365 compliance center when a DLP policy is triggered.
User2 must be granted the permissions to review audit logs for the following activities:
- Admin activities in Microsoft Exchange Online
- Admin activities in SharePoint Online
- Admin activities in Azure AD
Users must be able to apply sensitivity labels to documents by using Office for the web.
Windows Autopilot must be used for device provisioning, whenever possible.
A DLP policy must be created to meet the following requirements:
- Confidential information must not be shared in Microsoft Teams chat sessions, meetings, or channel messages.

- Messages that contain internal product codes or supplier ID numbers must be blocked and deleted.
The principle of least privilege must be used.

QUESTION 1

HOTSPOT
You need to configure automatic enrollment in Intune. The solution must meet the technical requirements.
What should you configure, and to which group should you assign the configurations? To answer, select the appropriate options in the answer area.
NOTE: Each correct selection is worth one point.

Hot Area:



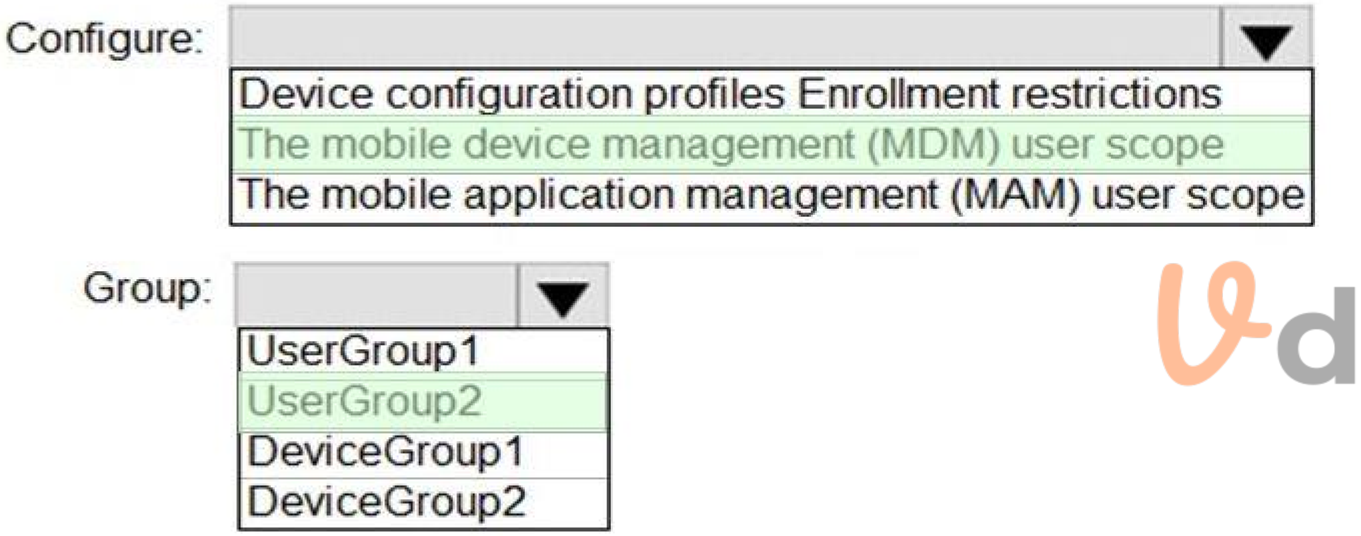
Configure:

- Device configuration profiles Enrollment restrictions
- The mobile device management (MDM) user scope
- The mobile application management (MAM) user scope

Group:

- UserGroup1
- UserGroup2
- DeviceGroup1
- DeviceGroup2

Answer Area:



Configure:

- Device configuration profiles Enrollment restrictions
- [✓ The mobile device management (MDM) user scope]
- The mobile application management (MAM) user scope

Group:

- UserGroup1
- [✓ UserGroup2]
- DeviceGroup1
- DeviceGroup2

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

QUESTION 2
You need to create the Safe Attachments policy to meet the technical requirements.
Which option should you select?

A. Replace
B. Enable redirect
C. Block
D. Dynamic Delivery

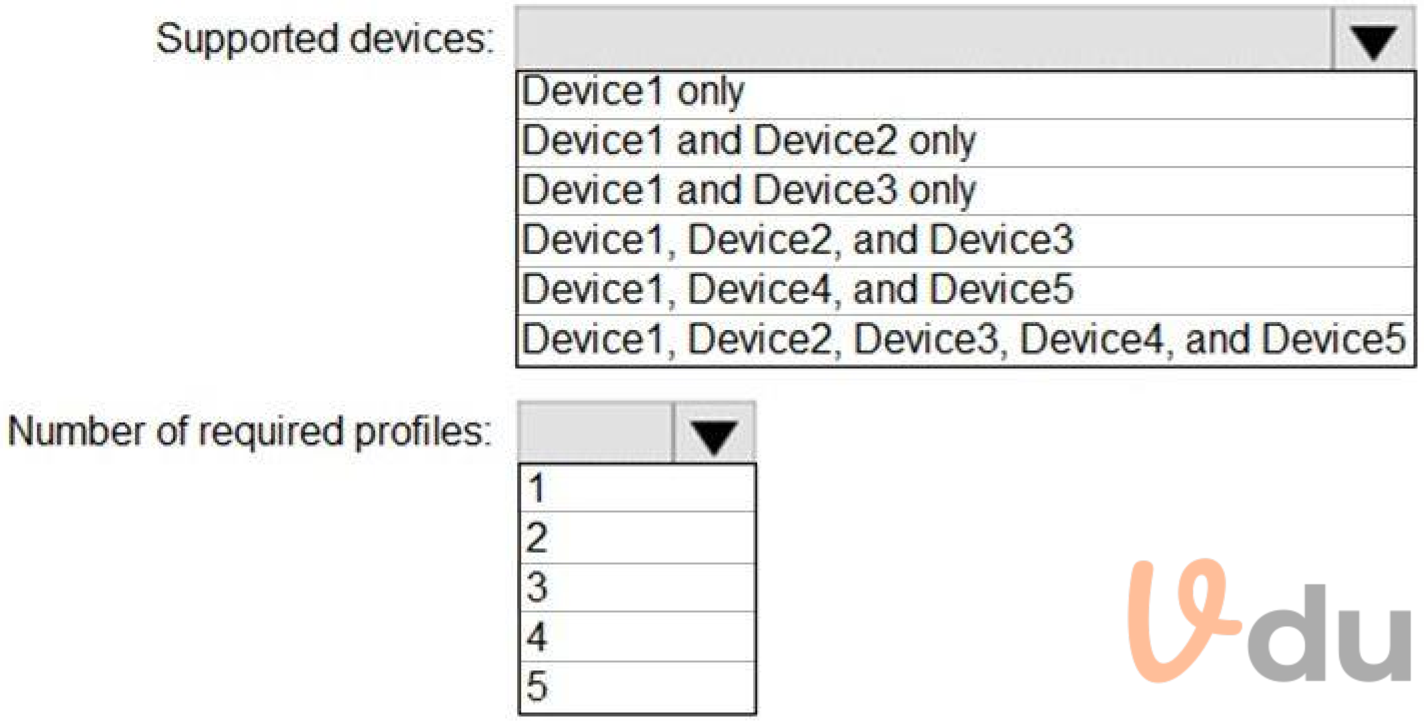
Correct Answer: D
Section:
Explanation:
https://github.com/MicrosoftDocs/microsoft-365-docs/blob/public/microsoft-365/security/office-365-security/safe-attachments.md

QUESTION 3

HOTSPOT

You plan to implement the endpoint protection device configuration profiles to support the planned changes.
You need to identify which devices will be supported, and how many profiles you should implement.
What should you identify? To answer, select the appropriate options in the answer area.
NOTE: Each correct selection is worth one point.

Hot Area:



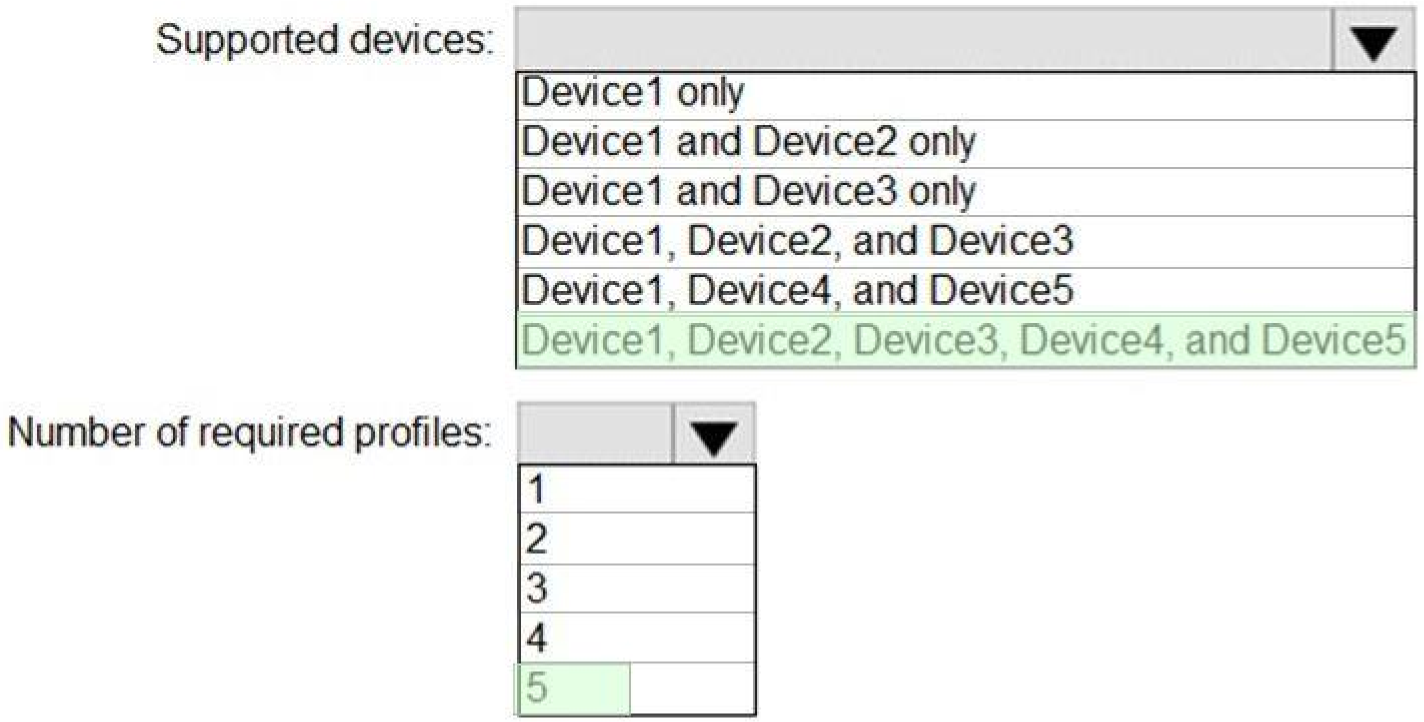
Supported devices:

Device1 only
Device1 and Device2 only
Device1 and Device3 only
Device1, Device2, and Device3
Device1, Device4, and Device5
Device1, Device2, Device3, Device4, and Device5

Number of required profiles:

1
2
3
4
5

Answer Area:



Supported devices:

Device1 only
Device1 and Device2 only
Device1 and Device3 only
Device1, Device2, and Device3
Device1, Device4, and Device5
[✓ Device1, Device2, Device3, Device4, and Device5]

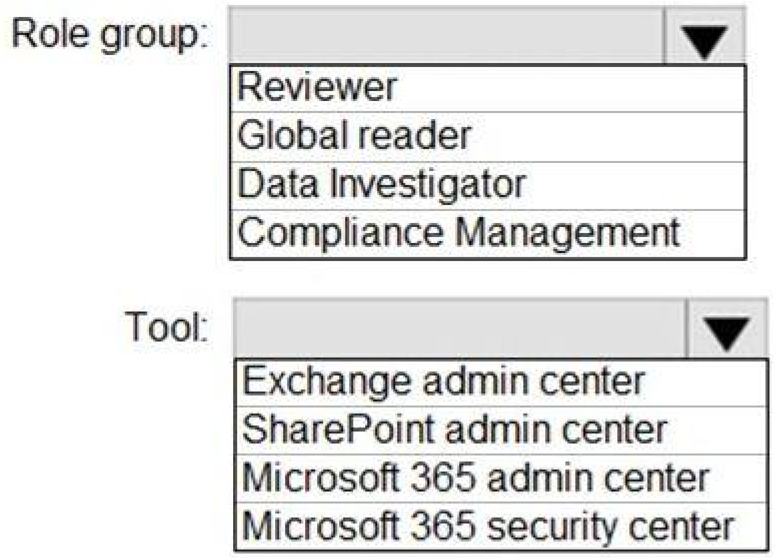
Number of required profiles:

1
2
3
4
[✓ 5]

Section:
Explanation:
https://docs.microsoft.com/en-us/mem/intune/configuration/device-profile-create

QUESTION 4
HOTSPOT
You need to ensure that User2 can review the audit logs. The solutions must meet the technical requirements.
To which role group should you add User2, and what should you use? To answer, select the appropriate options in the answer area.
NOTE: Each correct selection is worth one point.

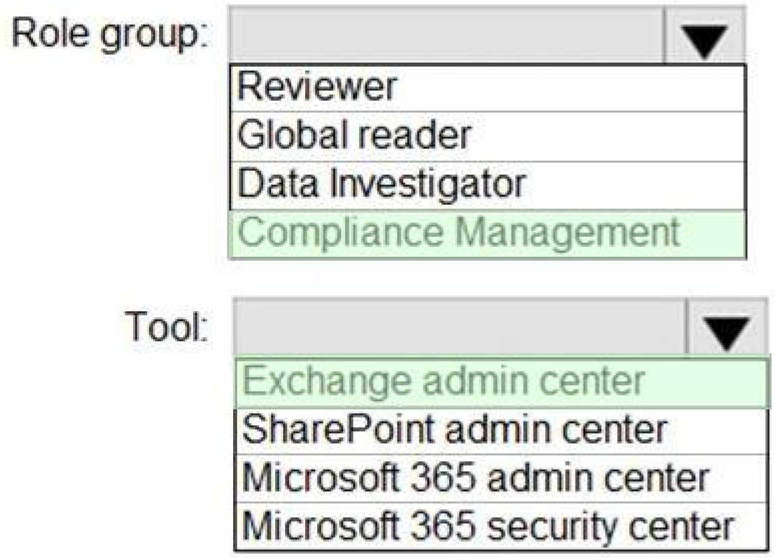
Hot Area:



Role group: ▼
- Reviewer
- Global reader
- Data Investigator
- Compliance Management

Tool: ▼
- Exchange admin center
- SharePoint admin center
- Microsoft 365 admin center
- Microsoft 365 security center

Answer Area:



Role group: ▼
- Reviewer
- Global reader
- Data Investigator
- [✓ Compliance Management]

Tool: ▼
- [✓ Exchange admin center]
- SharePoint admin center
- Microsoft 365 admin center
- Microsoft 365 security center

Section:
Explanation:
https://docs.microsoft.com/en-us/microsoft-365/compliance/search-the-audit-log-in-security-and-compliance?view=o365-worldwide

QUESTION 5
You need to configure Office on the web to meet the technical requirements.

What should you do?

A. Assign the Global reader role to User1.
B. Enable sensitivity labels for Office files in SharePoint Online and OneDrive.
C. Configure an auto-labeling policy to apply the sensitivity labels.
D. Assign the Office apps admin role to User1.

Correct Answer: B
Section:
Explanation:
https://docs.microsoft.com/en-us/microsoft-365/compliance/sensitivity-labels-sharepoint-onedrive-files?view=o365-worldwide

QUESTION 6
You create the planned DLP policies.
You need to configure notifications to meet the technical requirements.
What should you do?

A. From the Microsoft 365 security center, configure an alert policy.
B. From the Microsoft Endpoint Manager admin center, configure a custom notification.
C. From the Microsoft 365 admin center, configure a Briefing email.
D. From the Microsoft 365 compliance center, configure the Endpoint DLP settings.

Correct Answer: D
Section:
Explanation:
https://docs.microsoft.com/en-us/microsoft-365/compliance/dlp-configure-view-alerts-policies?view=o365-worldwide

QUESTION 7
You need to configure the compliance settings to meet the technical requirements.
What should you do in the Microsoft Endpoint Manager admin center?

A. From Compliance policies, modify the Notifications settings.
B. From Locations, create a new location for noncompliant devices.
C. From Retire Noncompliant Devices, select Clear All Devices Retire State.
D. Modify the Compliance policy settings.

Correct Answer: D
Section:
Explanation:
https://docs.microsoft.com/en-us/mem/intune/protect/device-compliance-get-started

QUESTION 8
You need to create the DLP policy to meet the technical requirements.
What should you configure first?

A. sensitive info types
B. the Insider risk management settings

C. the event types

D. the sensitivity labels

Correct Answer: A
Section:
Explanation:
https://docs.microsoft.com/en-us/microsoft-365/compliance/create-test-tune-dlp-policy?view=o365-worldwide

QUESTION 9

HOTSPOT

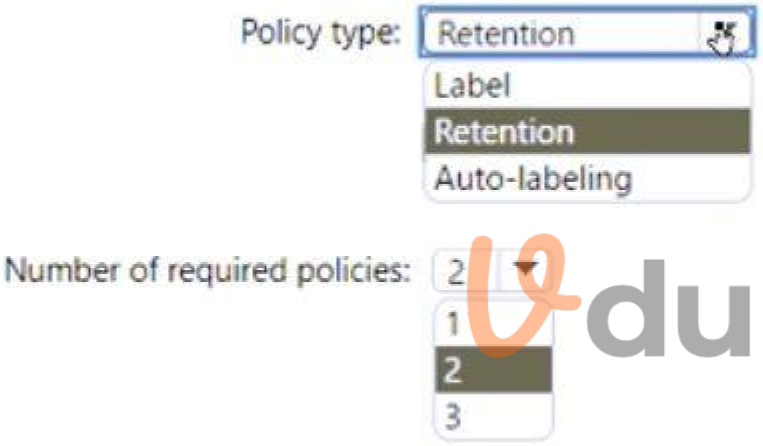
You need to configure the information governance settings to meet the technical requirements.

Which type of policy should you configure, and how many policies should you configure? To answer, select the appropriate options in the answer area.

NOTE: Each correct selection is worth one point.

Hot Area:

Answer Area

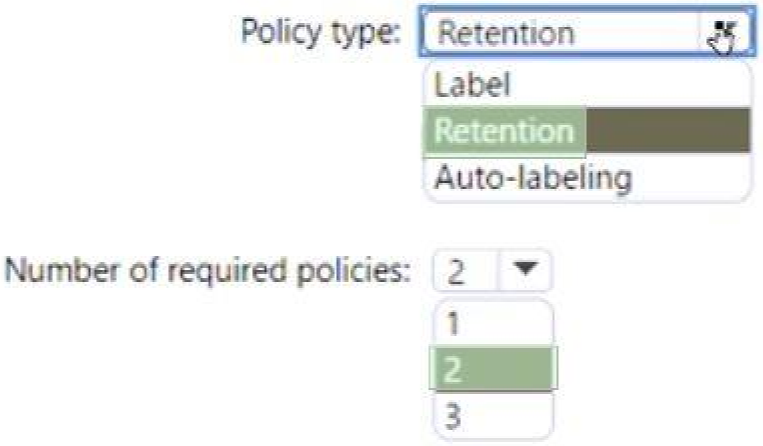


Policy type: Retention

Number of required policies: 2

Answer Area:

Answer Area



Policy type: Retention

Number of required policies: 2

Section:
Explanation:

Case 02

Case Study:
Overview

Existing Environment

This is a case study Case studies are not timed separately. You can use as much exam time as you would like to complete each case. However, there may be additional case studies and sections on this exam. You must manage your time to ensure that you are able to complete all questions included on this exam in the time provided.

To answer the questions included in a case study, you will need to reference information that is provided in the case study. Case studies might contain exhibits and other resources that provide more information about the scenario that is described in the case study. Each question is independent of the other questions in this case study.

At the end of this case study, a review screen will appear. This screen allows you to review your answers and to make changes before you move to the next section of the exam. After you begin a new section, you cannot return to this section.

To start the case study

To display the first question in this case study, click the Next button. Use the buttons in the left pane to explore the content of the case study before you answer the questions. Clicking these buttons displays information such as business requirements, existing environment, and problem statements.

When you are ready to answer a question, click the Question button to return to the question.

Current Infrastructure

A. Datum 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.ad3tum.com.

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

A. Datum uses and processes Personally Identifiable Information (PII).

Problem Statements

Requirements

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

Business Goals

A. Datum warns to be fully compliant with all the relevant data privacy laws in the regions where it operates.

A. Datum wants to minimize the cost of hardware and software whenever possible.

Technical Requirements

A. Datum 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 shows which Microsoft 36S 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 US.

PII data to other New York office users. 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 the EU PII data.

What should you create?

A. a retention policy from the Security & Compliance admin center.

B. a retention policy from the Exchange admin center

C. a data loss prevention (DLP) policy from the Exchange admin center

D. a data loss prevention (DLP) policy from the Security & Compliance admin center

Correct Answer: A

Section:

Explanation:

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

EU PII wants both documents and email message to be preserved so S&C Admin Center for Retention. If this was for Email only, this probably could have been done in EAC.

QUESTION 2

You need to meet the technical requirement for large-volume document retrieval. What should you create?

A. a data loss prevention (DLP) policy from the Security & Compliance admin center

B. an alert policy from the Security & Compliance admin center

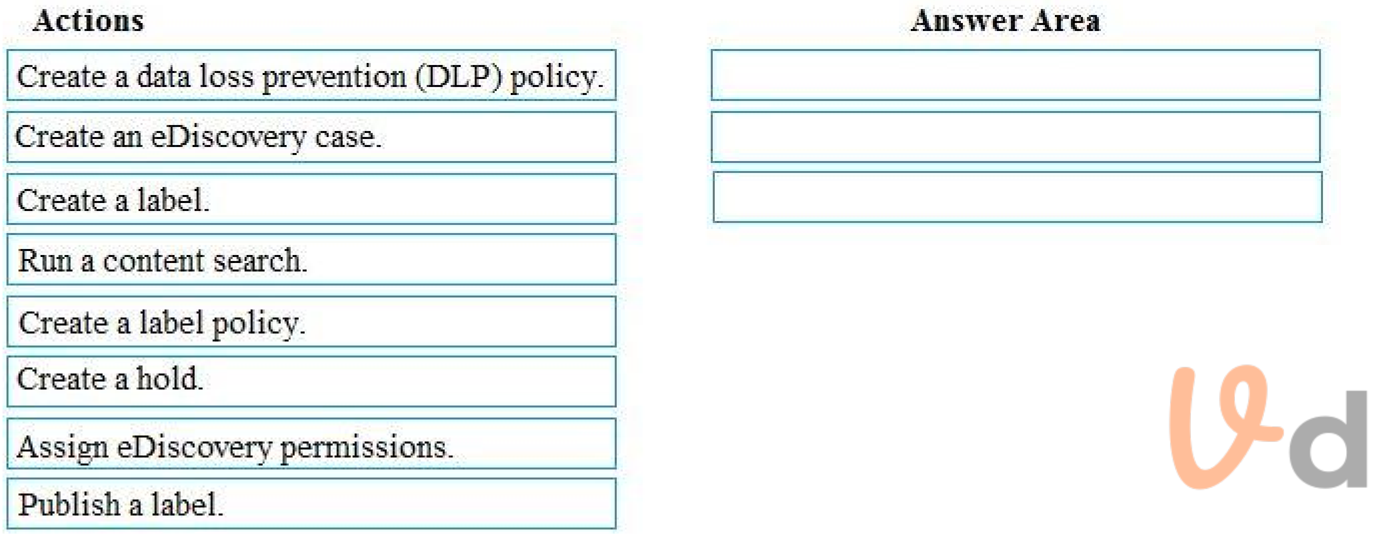
C. a file policy from Microsoft Cloud App Security

D. an activity policy from Microsoft Cloud App Security

Correct Answer: D
Section:
Explanation:
https://docs.microsoft.com/en-us/office365/securitycompliance/activity-policies-and-alerts

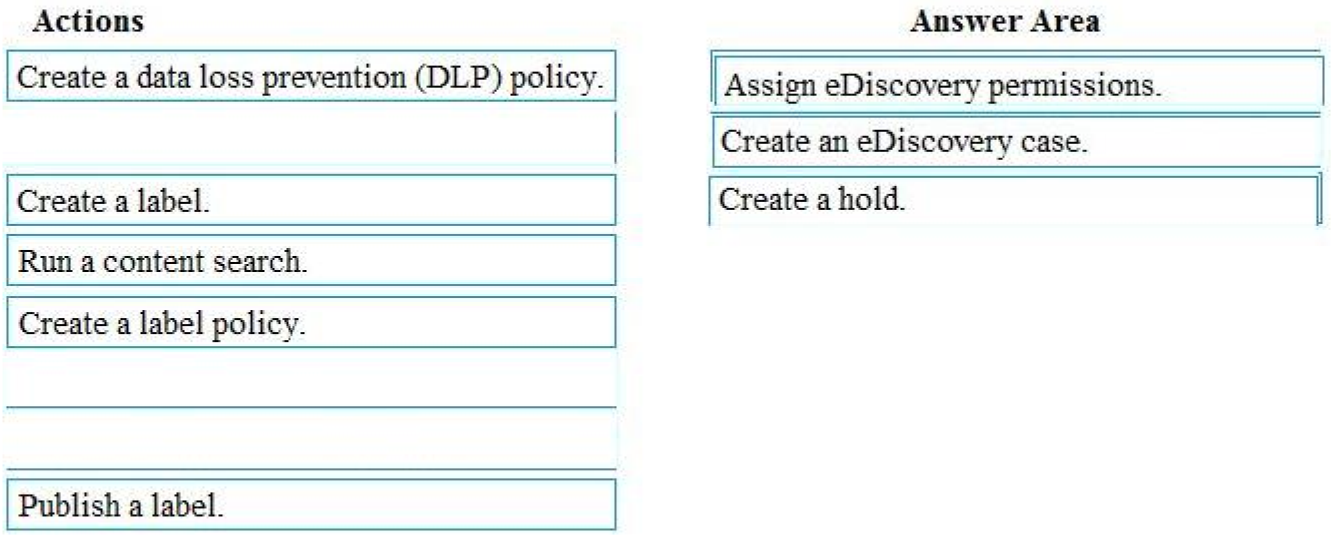
QUESTION 3
DRAG DROP
You need to meet the requirement for the legal department.
Which three actions should you perform in sequence from the Security & Compliance admin center? To answer, move the appropriate actions from the list of actions to the answer area and arrange them in the correct order.

Select and Place:



Actions	Answer Area
Create a data loss prevention (DLP) policy.	
Create an eDiscovery case.	
Create a label.	
Run a content search.	
Create a label policy.	
Create a hold.	
Assign eDiscovery permissions.	
Publish a label.	

Correct Answer:



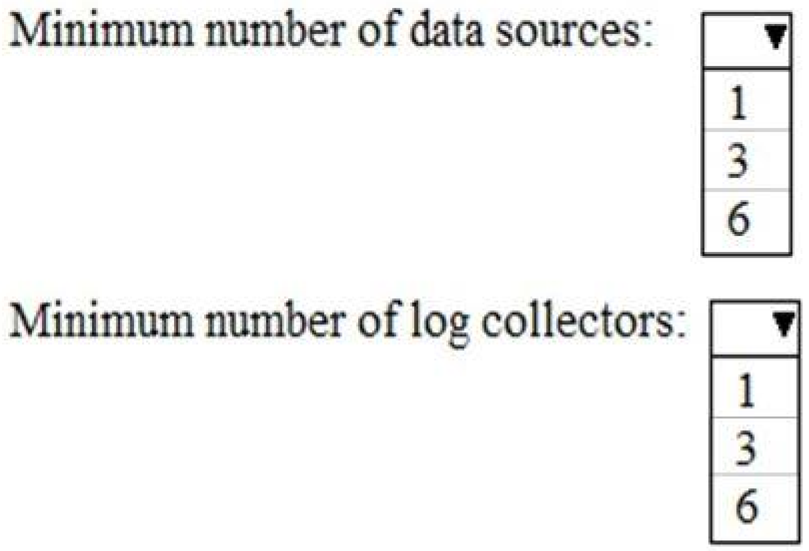
Actions	Answer Area
Create a data loss prevention (DLP) policy.	Assign eDiscovery permissions.
	Create an eDiscovery case.
Create a label.	Create a hold.
Run a content search.	
Create a label policy.	
Publish a label.	

Section:
Explanation:
https://www.sherweb.com/blog/ediscovery-office-365/

QUESTION 4
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:



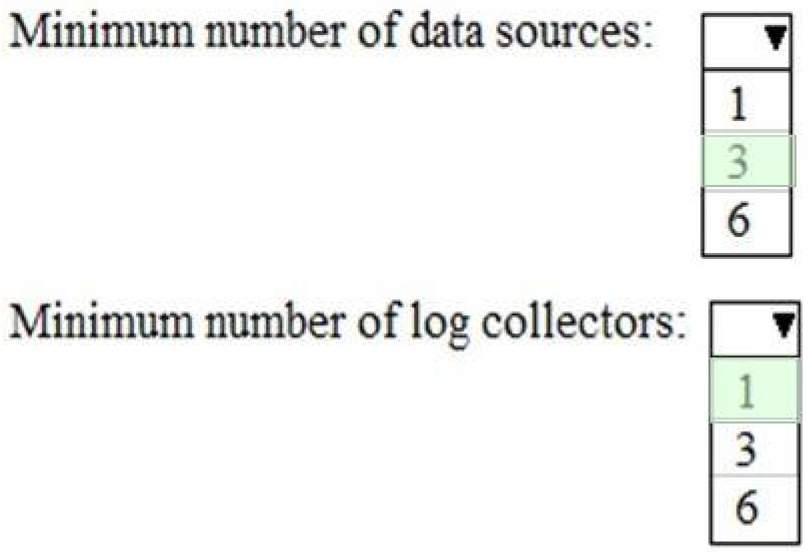
Minimum number of data sources: ▼

1
3
6

Minimum number of log collectors: ▼

1
3
6

Answer Area:



Minimum number of data sources: ▼

1
[✓ 3]
6

Minimum number of log collectors: ▼

[✓ 1]
3
6

Section:
Explanation:
https://docs.microsoft.com/en-us/cloud-app-security/discovery-docker

QUESTION 5
Which report should the New York office auditors view?

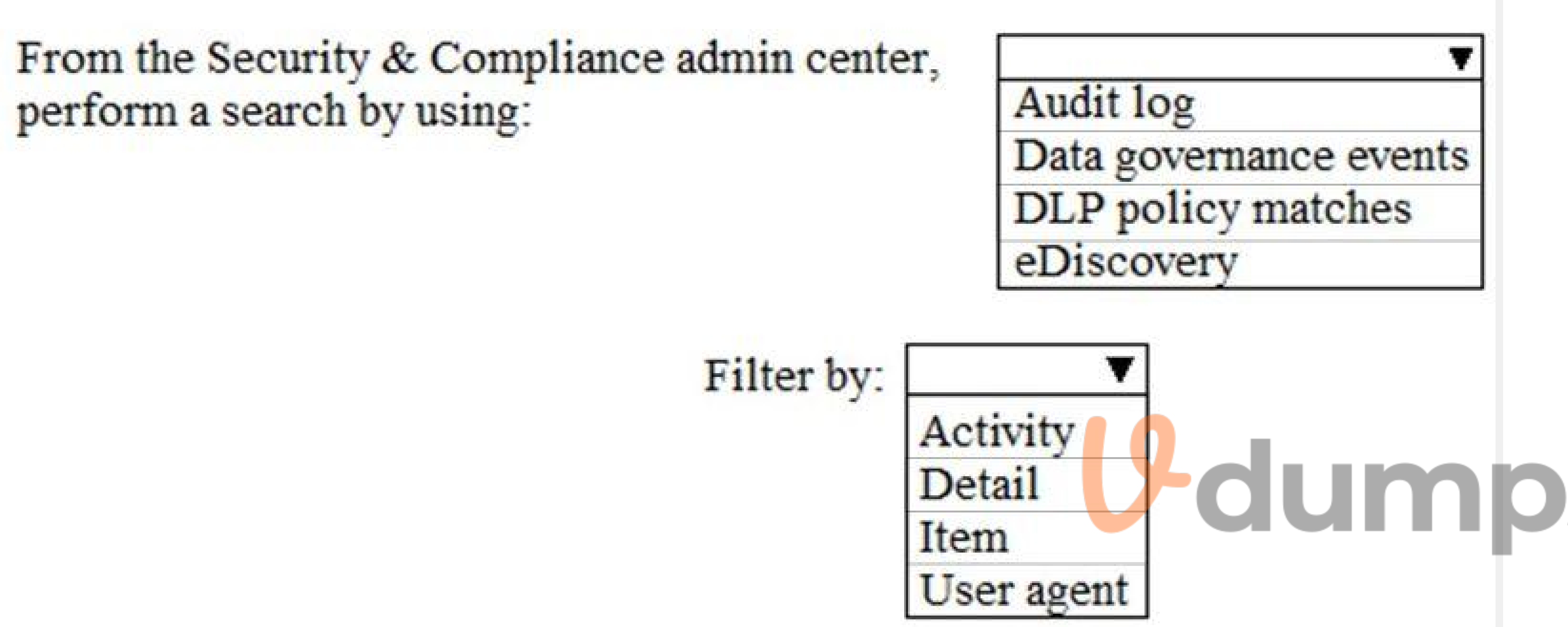
A. DLP policy matches
B. DLP false positives and overrides
C. DLP incidents
D. Top Senders and Recipients

Correct Answer: C

Section:
Explanation:
https://docs.microsoft.com/en-us/office365/securitycompliance/data-loss-prevention-policies
This report also shows policy matches over time, like the policy matches report. However, the policy matches report shows matches at a rule level; for example, if an email matched three different rules, the policy matches report shows three different line items. By contrast, the incidents report shows matches at an item level; for example, if an email matched three different rules, the incidents report shows a single line item for that piece of content. Because the report counts are aggregated differently, the policy matches report is better for identifying matches with specific rules and fine tuning DLP policies. The incidents report is better for identifying specific pieces of content that are problematic for your DLP policies.

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:



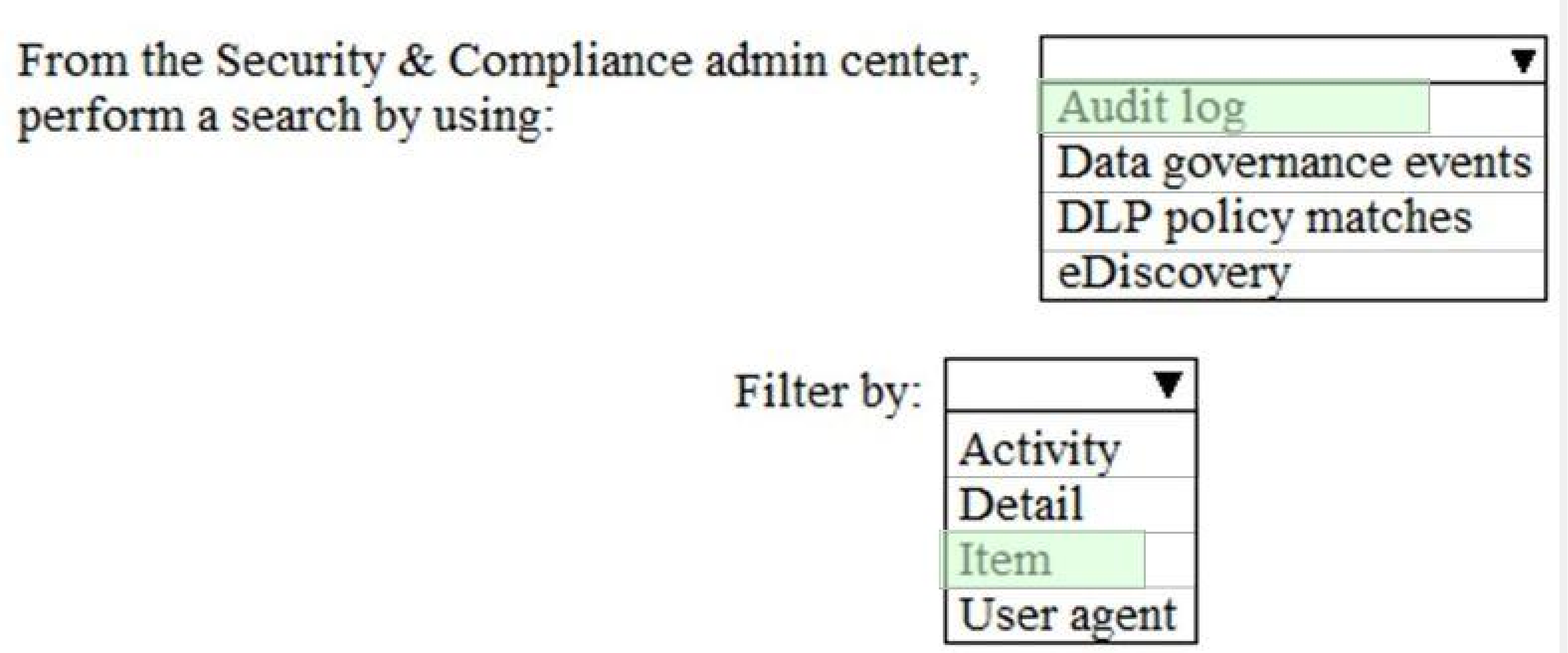
From the Security & Compliance admin center, perform a search by using:

▼
- Audit log
- Data governance events
- DLP policy matches
- eDiscovery

Filter by:

▼
- Activity
- Detail
- Item
- User agent

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:
Explanation:

https://docs.microsoft.com/en-us/office365/securitycompliance/search-the-audit-log-in-security-and-compliance#step-3-filter-the-search-results

QUESTION 7
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: B
Section:
Explanation:
https://docs.microsoft.com/en-us/azure/active-directory/conditional-access/concept-conditional-access-conditions#sign-in-risk states clearly that Sign-in risk

QUESTION 8
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: A
Section:
Explanation:
This is a case study. Case studies are not timed separately. You can use as much exam time as you would like to complete each case. However, there may be additional case studies and sections on this exam. You must manage your time to ensure that you are able to complete all questions included on this exam in the time provided.
To answer the questions included in a case study, you will need to reference information that is provided in the case study. Case studies might contain exhibits and other resources that provide more information about the scenario that is described in the case study. Each question is independent of the other questions in this case study.
At the end of this case study, a review screen will appear. This screen allows you to review your answers and to make changes before you move to the next section of the exam. After you begin a new section, you cannot return to this section.

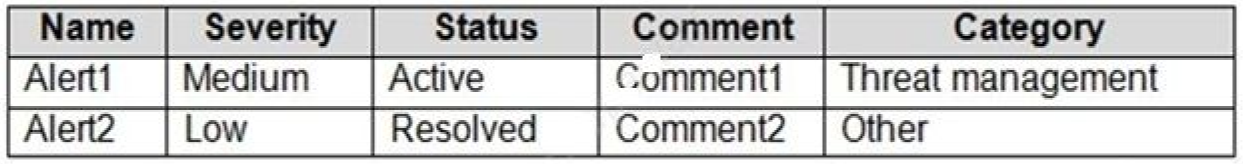
Exam A

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 computer that runs Windows 10.
You need to verify which version of Windows 10 is installed.
Solution: From the Settings app, you select System, and then you select About to view information about the system.
Does this meet the goal?

A. Yes
B. No

Correct Answer: A
Section:
Explanation:
https://support.microsoft.com/en-us/windows/which-version-of-windows-operating-system-am-i-running-628bec99-476a-2c13-5296-9dd081cdd808

QUESTION 2
You have a Microsoft 365 subscription that contains the alerts shown in the following table.



Name	Severity	Status	Comment	Category
Alert1	Medium	Active	Comment1	Threat management
Alert2	Low	Resolved	Comment2	Other

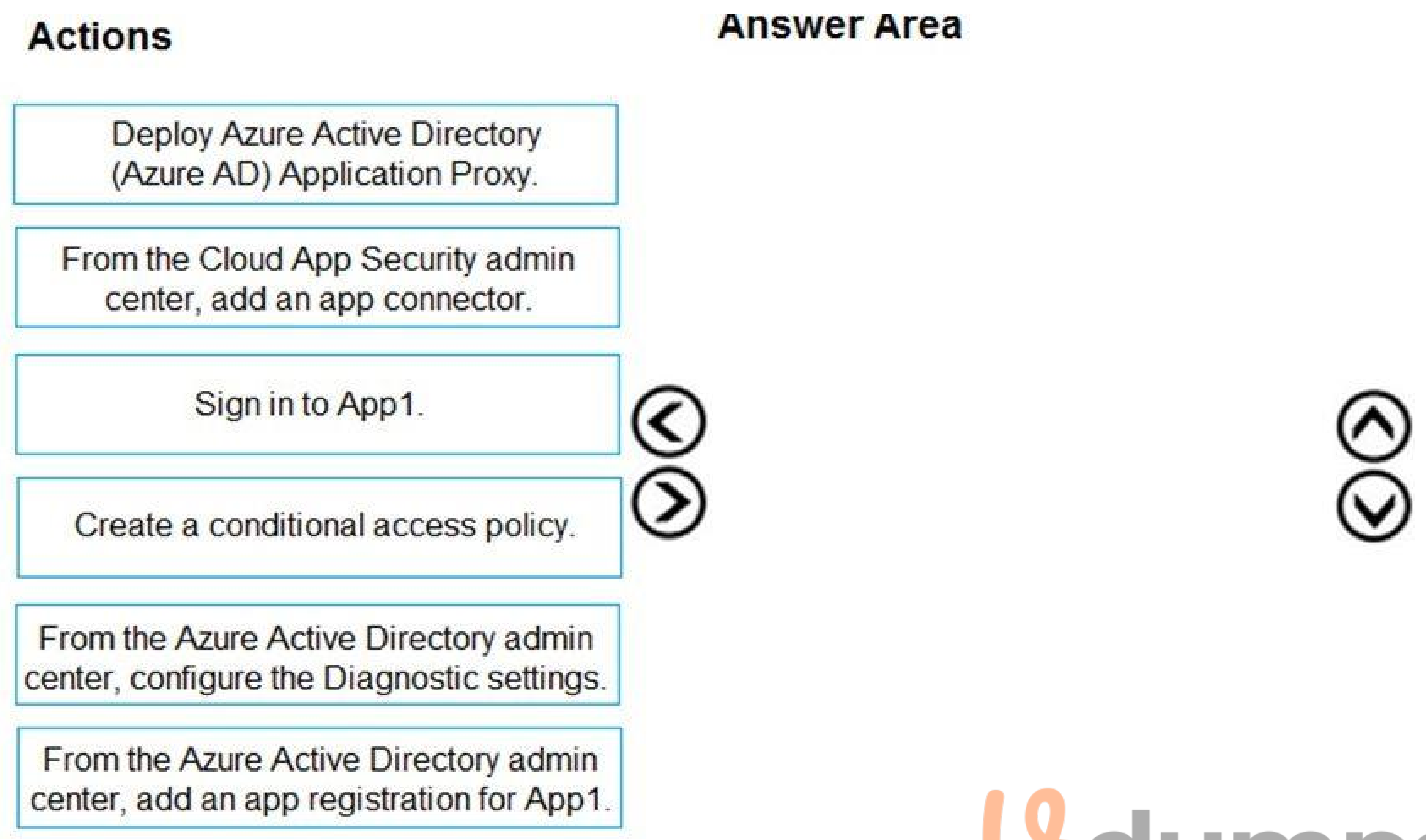
Which properties of the alerts can you modify?

A. Status only
B. Status and Comment only
C. Status and Severity only
D. Status, Severity, and Comment only
E. Status, Severity, Comment and Category

Correct Answer: B
Section:
Explanation:
https://docs.microsoft.com/en-us/microsoft-365/security/defender-endpoint/update-alert?view=o365-worldwide#limitations

QUESTION 3
DRAG DROP
Your company purchases a cloud app named App1.
You need to ensure that you can use Microsoft Cloud App Security to block downloads in App1. App1 supports session controls.
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.
https://docs.microsoft.com/en-us/cloud-app-security/getting-started-with-cloud-app-security

Select and Place:

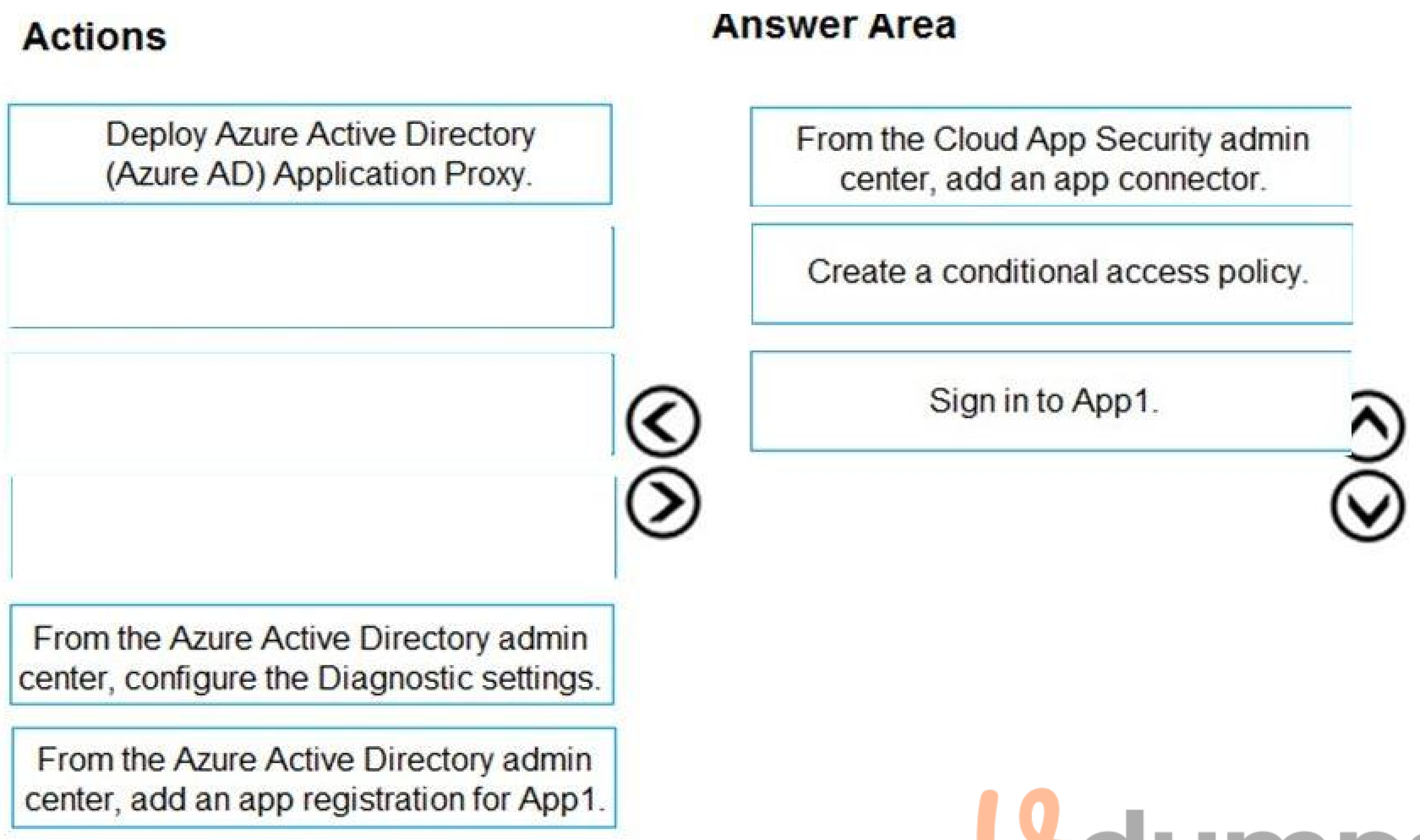


Actions

Answer Area

- Deploy Azure Active Directory (Azure AD) Application Proxy.
- From the Cloud App Security admin center, add an app connector.
- Sign in to App1.
- Create a conditional access policy.
- From the Azure Active Directory admin center, configure the Diagnostic settings.
- From the Azure Active Directory admin center, add an app registration for App1.

Correct Answer:



Actions

Deploy Azure Active Directory (Azure AD) Application Proxy.

From the Azure Active Directory admin center, configure the Diagnostic settings.

From the Azure Active Directory admin center, add an app registration for App1.

Answer Area

From the Cloud App Security admin center, add an app connector.

Create a conditional access policy.

Sign in to App1.

Section:
Explanation:
https://docs.microsoft.com/en-us/cloud-app-security/getting-started-with-cloud-app-security

QUESTION 4
You have a Microsoft 365 E5 subscription that has Microsoft Defender for Endpoint integrated with Microsoft Endpoint Manager.
Devices are onboarded by using Microsoft Defender for Endpoint.
You plan to block devices based on the results of the machine risk score calculated by Microsoft Defender for Endpoint.
What should you create first?

A. a device configuration policy
B. a device compliance policy
C. a conditional access policy
D. an endpoint detection and response policy

Correct Answer: B
Section:
Explanation:
https://docs.microsoft.com/en-us/mem/intune/protect/advanced-threat-protection-configure

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 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:

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 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:

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.
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?

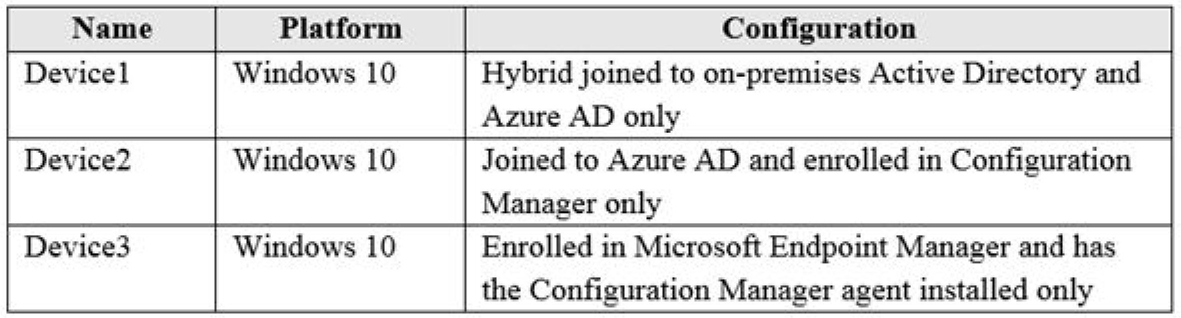
A. yes
B. No

Correct Answer: A
Section:

QUESTION 8

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

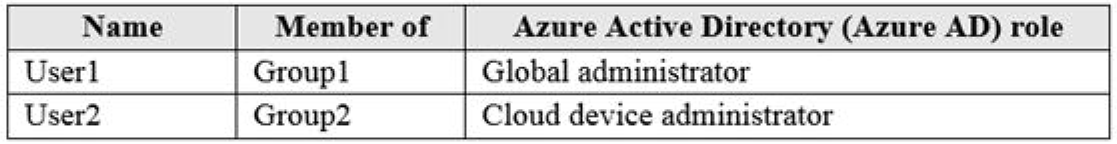
Correct Answer: D

Section:

QUESTION 9

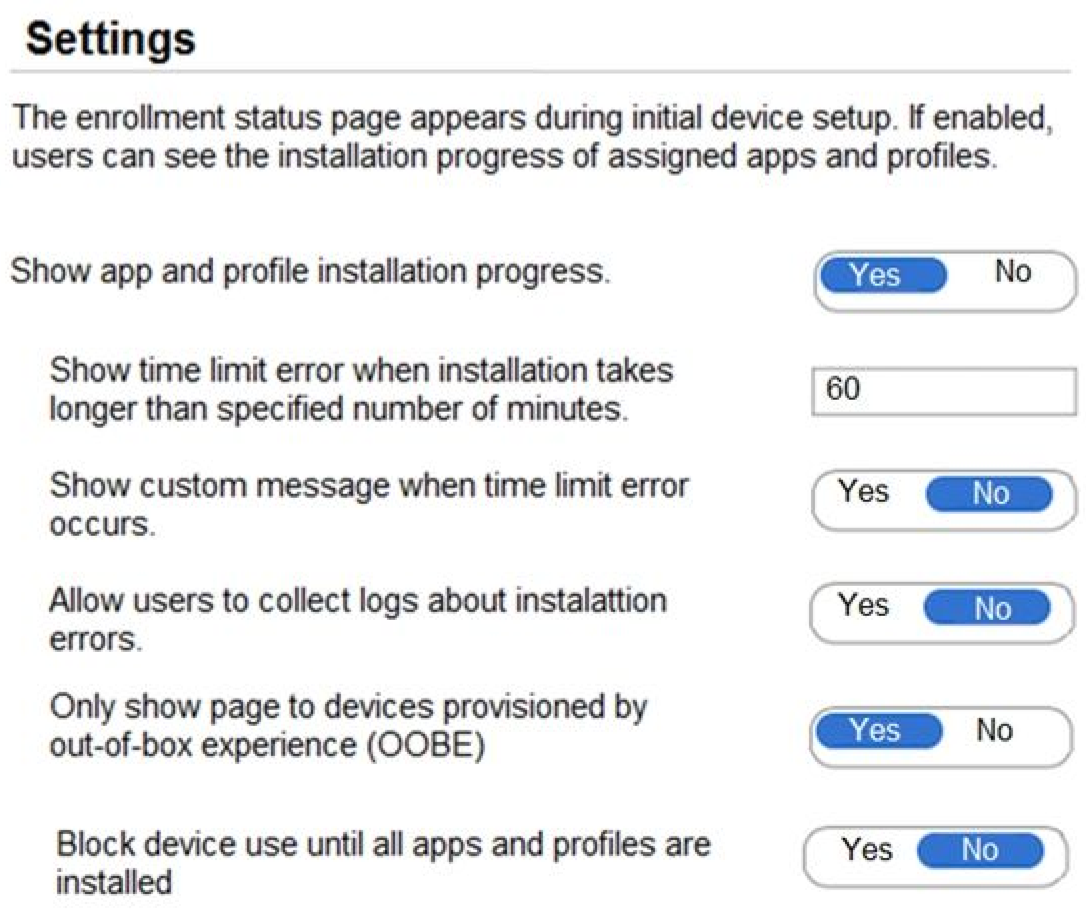
HOTSPOT

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

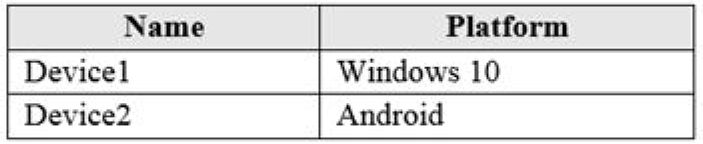
Show custom message when time limit error occurs. Yes [✓ No]

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]

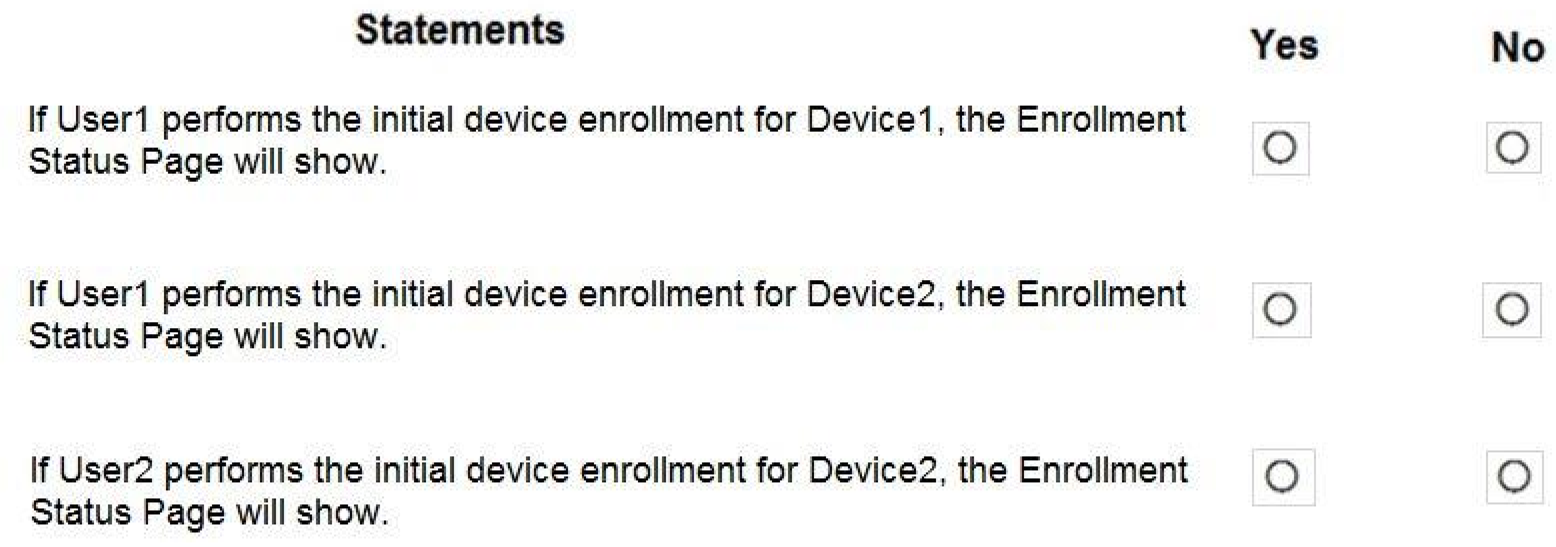
You assign the policy to Group1.
You purchase the devices shown in the following table.



Name	Platform
Device1	Windows 10
Device2	Android

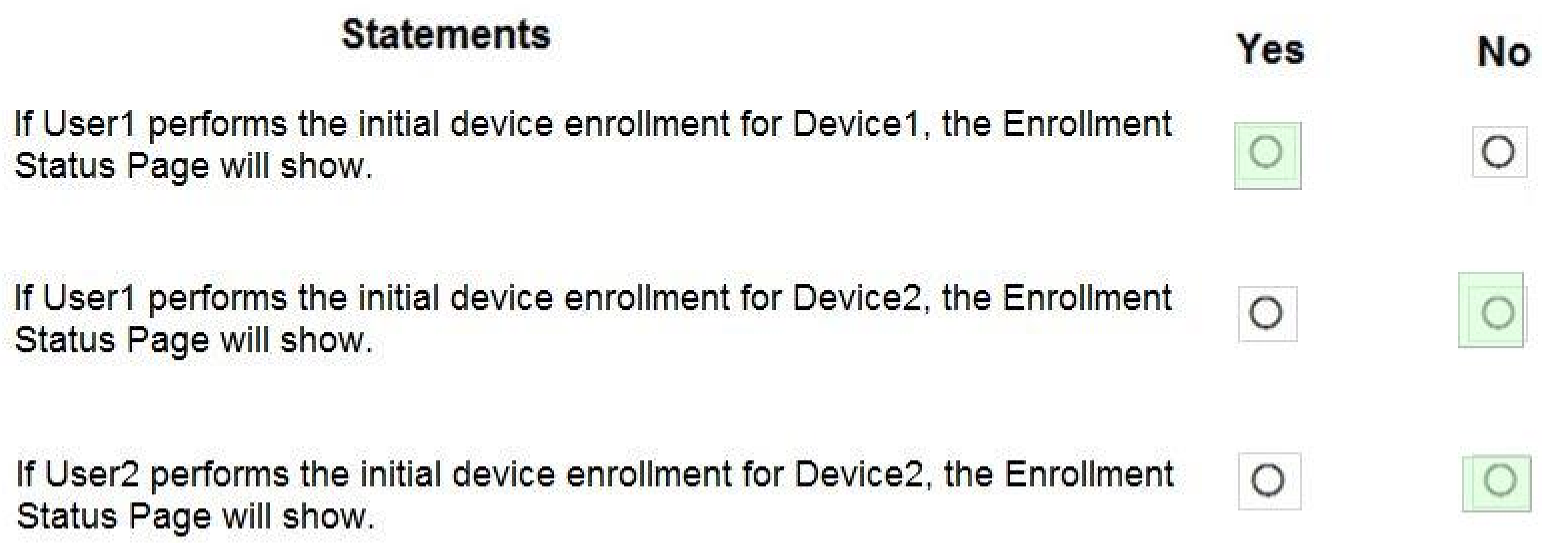
For each of the following statements, select Yes if the statement is true. Otherwise, select No.
NOTE: Each correct selection is worth one point.

Hot Area:



Statements	Yes	No
If User1 performs the initial device enrollment for Device1, the Enrollment Status Page will show.	○	○
If User1 performs the initial device enrollment for Device2, the Enrollment Status Page will show.	○	○
If User2 performs the initial device enrollment for Device2, the Enrollment Status Page will show.	○	○

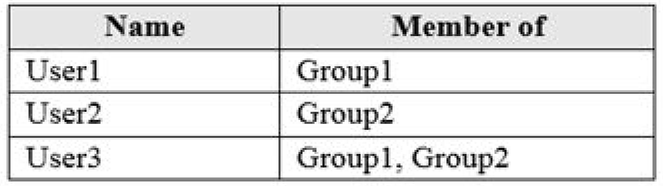
Answer Area:



Statements	Yes	No
If User1 performs the initial device enrollment for Device1, the Enrollment Status Page will show.	[✓ ○]	○
If User1 performs the initial device enrollment for Device2, the Enrollment Status Page will show.	○	[✓ ○]
If User2 performs the initial device enrollment for Device2, the Enrollment Status Page will show.	○	[✓ ○]

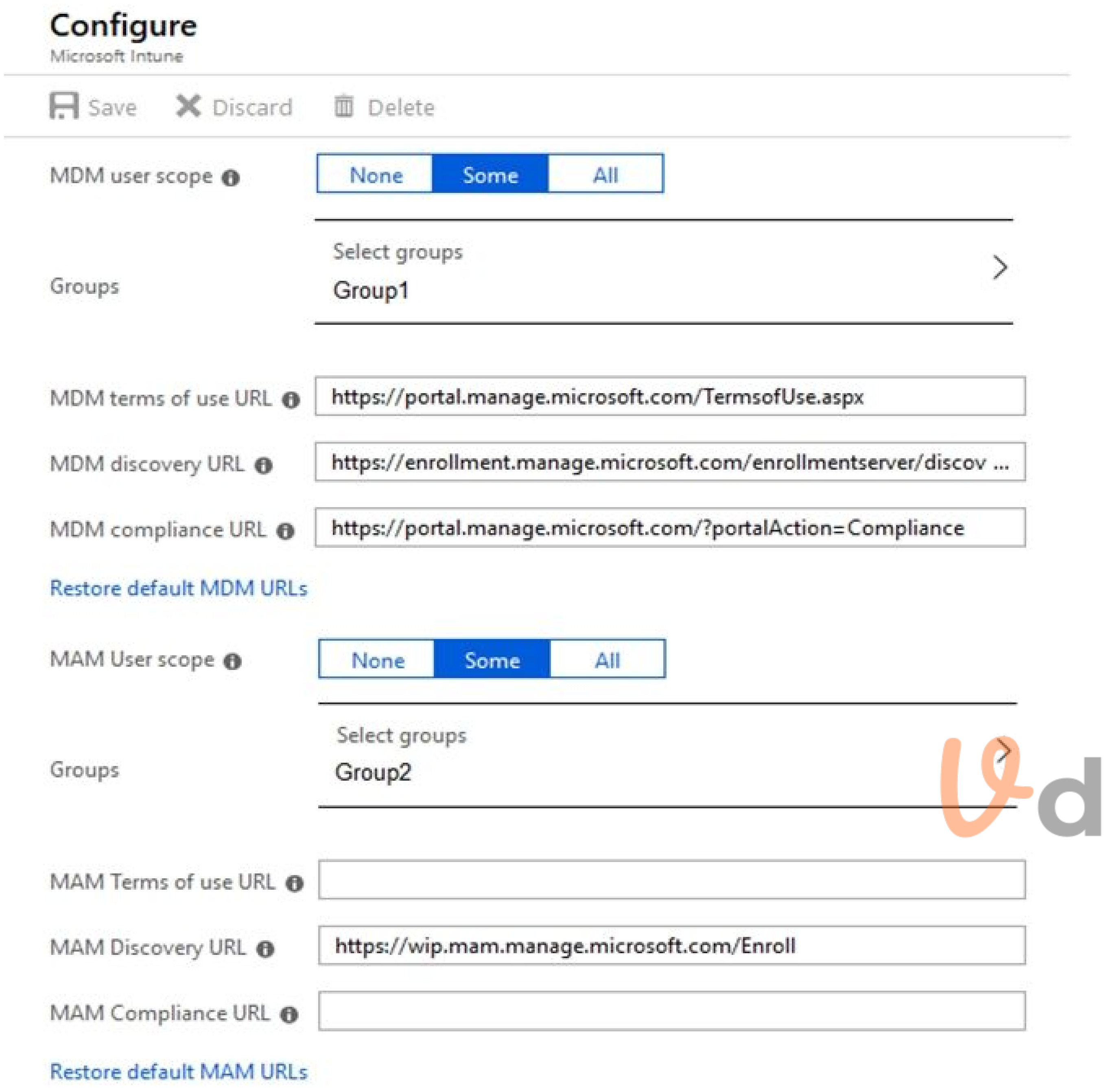
Section:
Explanation:
https://docs.microsoft.com/en-us/mem/intune/enrollment/windows-enrollment-status

QUESTION 10
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

Restore default MDM URLs

MAM User scope: None [✓ Some] All

Groups: Select groups — Group2

MAM Terms of use URL:

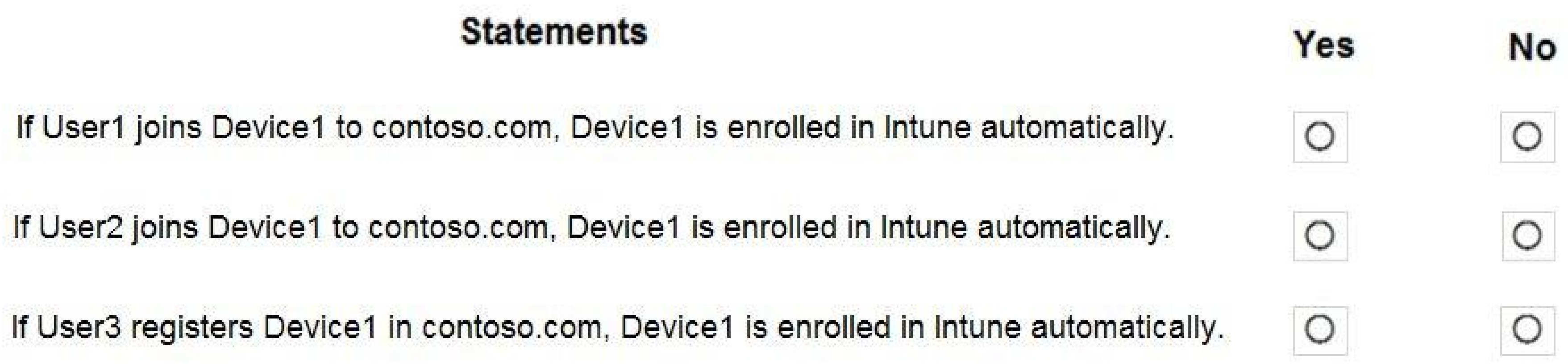
MAM Discovery URL: https://wip.mam.manage.microsoft.com/Enroll

MAM Compliance URL:

Restore default MAM URLs

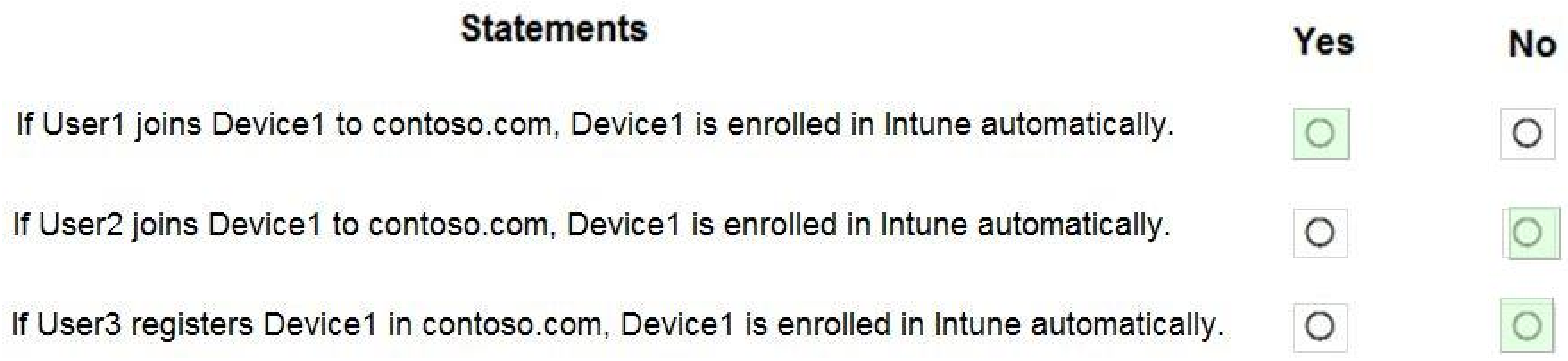
You purchase a Windows 10 device named Device1.
For each of the following statements, select Yes if the statement is true. Otherwise, select No.
NOTE: Each correct selection is worth one point.

Hot Area:



Statements	Yes	No
If User1 joins Device1 to contoso.com, Device1 is enrolled in Intune automatically.	○	○
If User2 joins Device1 to contoso.com, Device1 is enrolled in Intune automatically.	○	○
If User3 registers Device1 in contoso.com, Device1 is enrolled in Intune automatically.	○	○

Answer Area:



Statements	Yes	No
If User1 joins Device1 to contoso.com, Device1 is enrolled in Intune automatically.	●	○
If User2 joins Device1 to contoso.com, Device1 is enrolled in Intune automatically.	○	●
If User3 registers Device1 in contoso.com, Device1 is enrolled in Intune automatically.	○	●

Section:

Explanation:

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

QUESTION 11

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

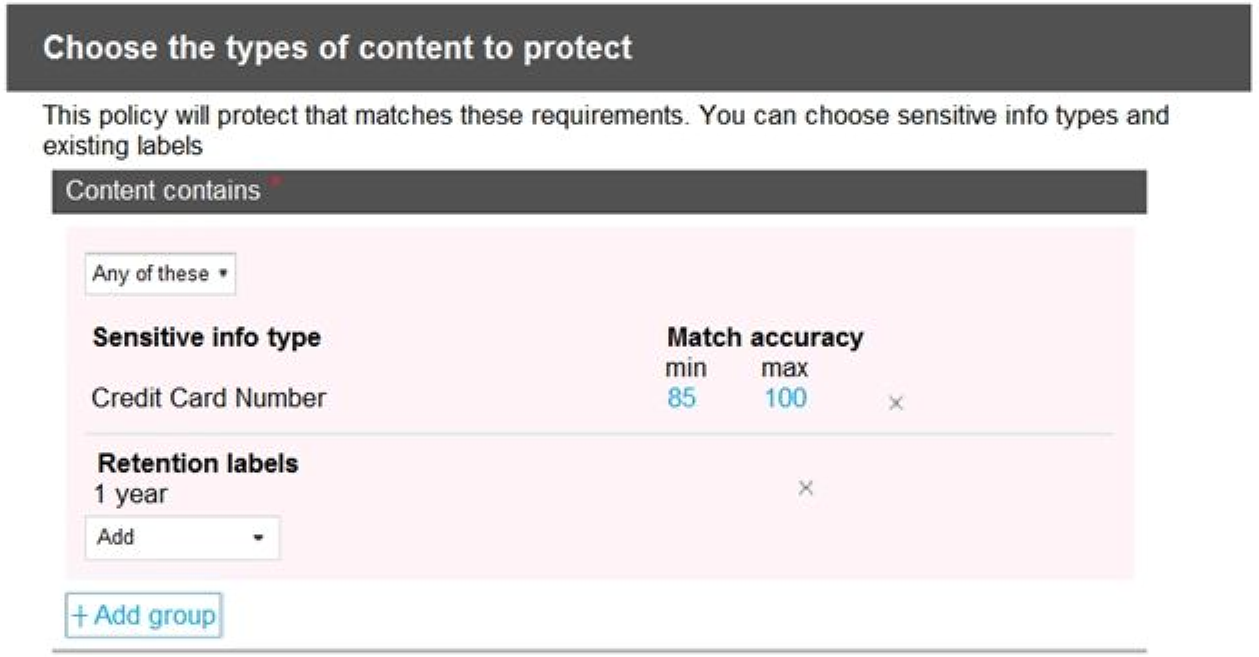
Correct Answer: D

Section:

QUESTION 12

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

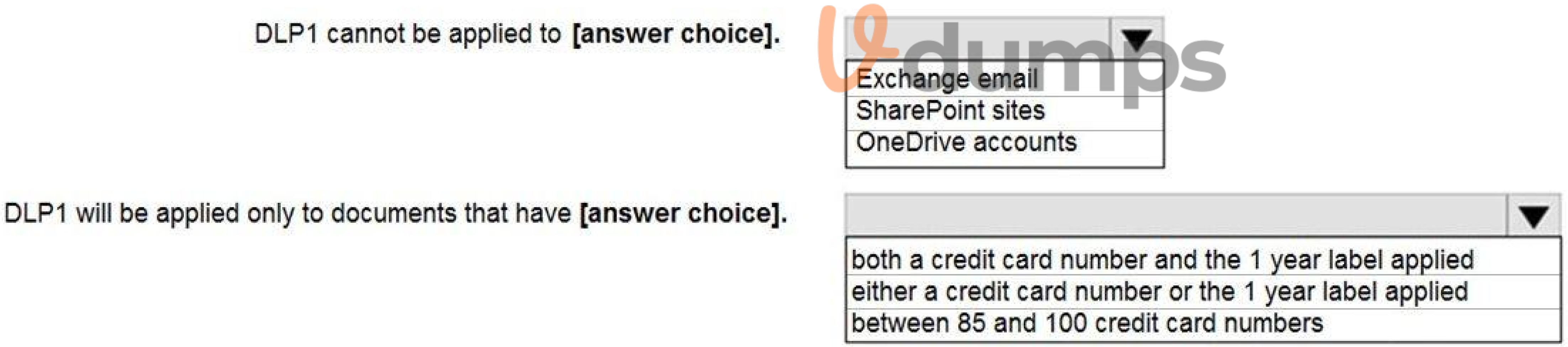
1 year ×

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:



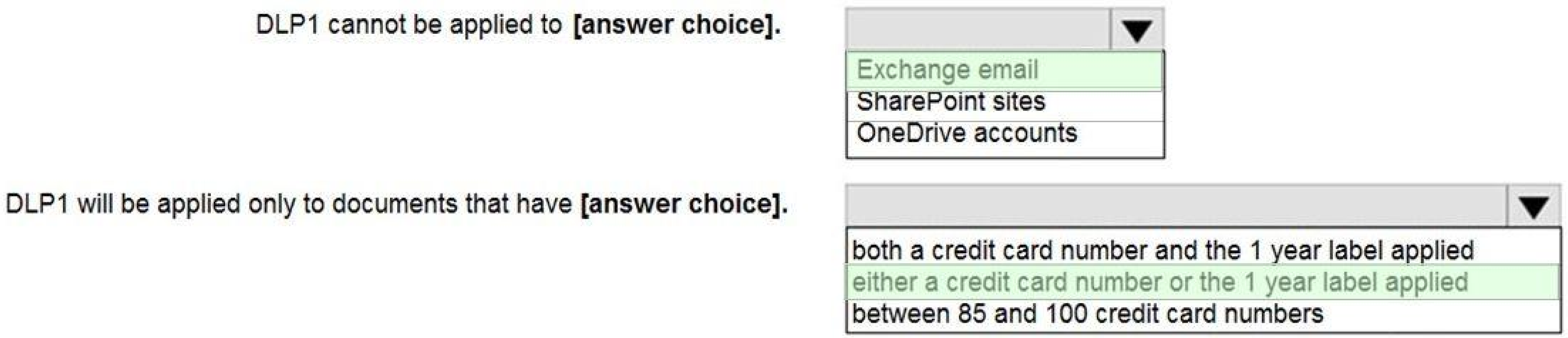
DLP1 cannot be applied to **[answer choice].**

- 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

Answer Area:



DLP1 cannot be applied to **[answer choice].** ▼

[✓ Exchange email]
SharePoint sites
OneDrive accounts

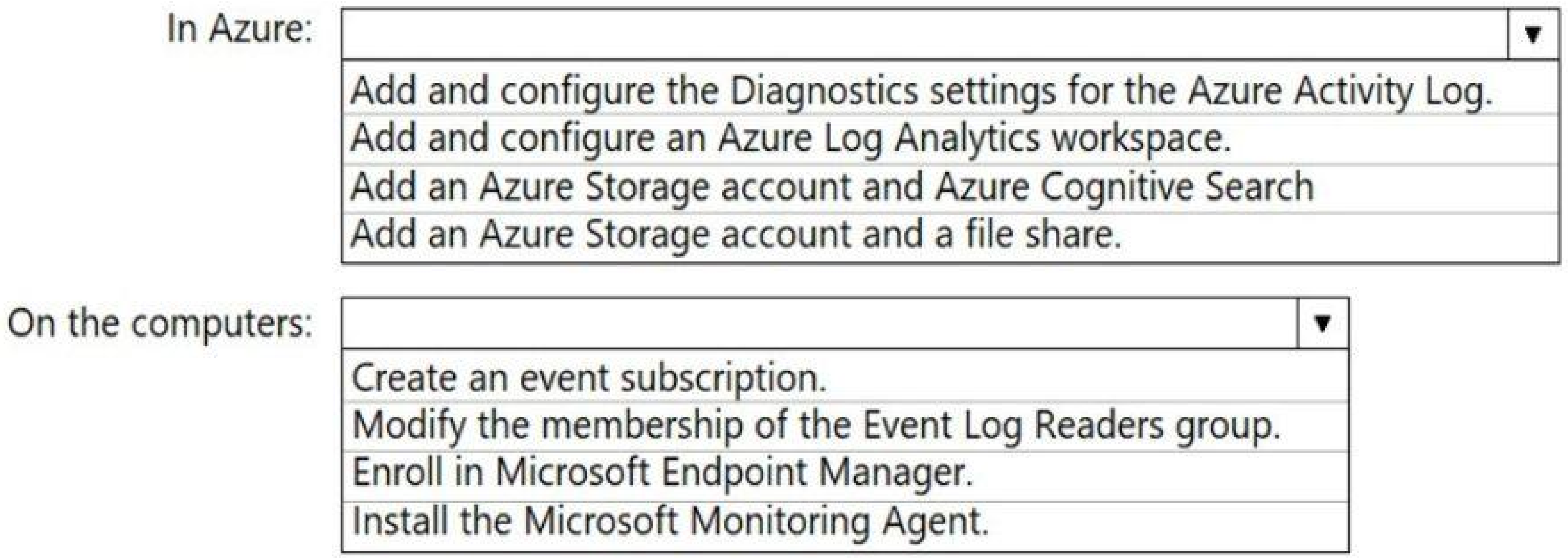
DLP1 will be applied only to documents that have **[answer choice].** ▼

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:
Explanation:
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 13
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:



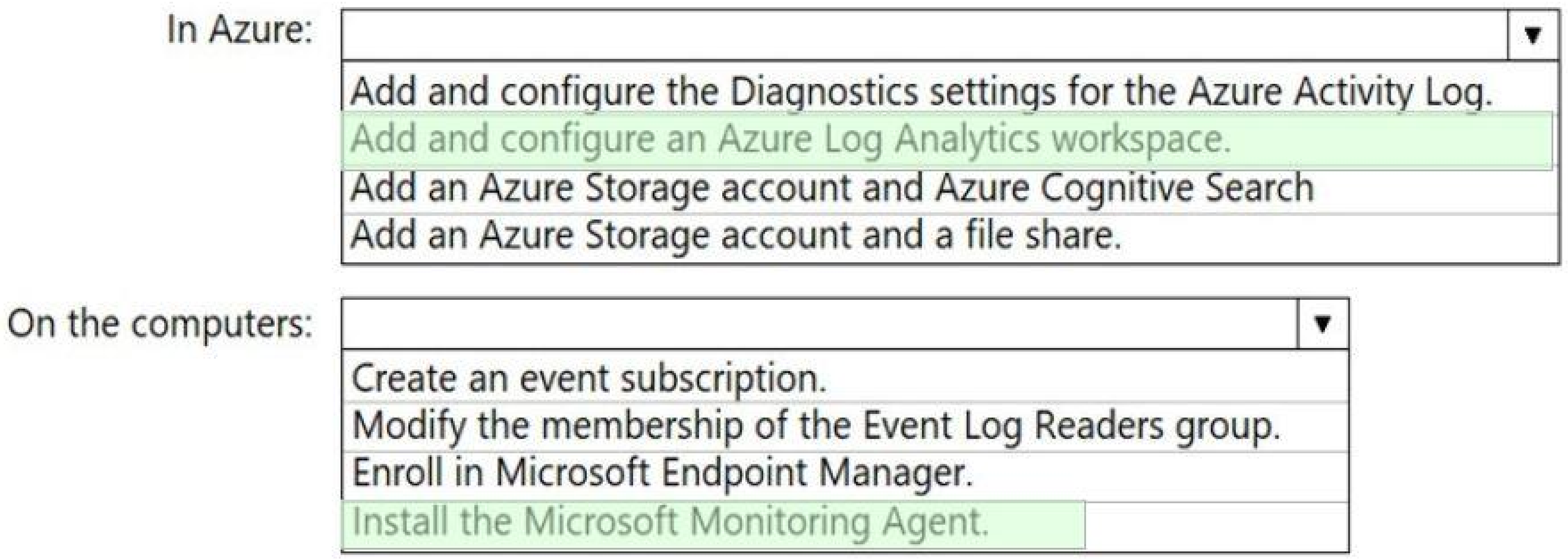
In Azure: ▼

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.

Answer Area:



In Azure: ▼

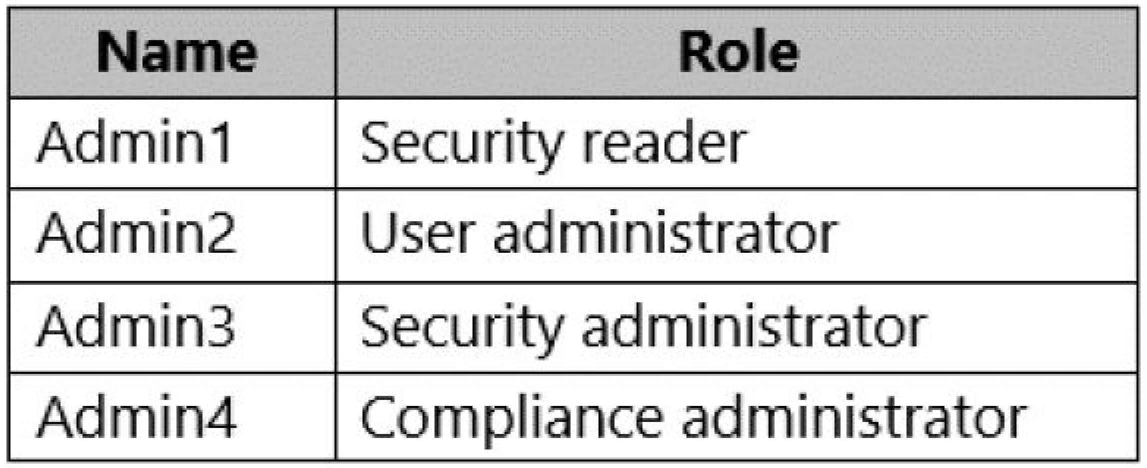
- Add and configure the Diagnostics settings for the Azure Activity Log.
- [✓ Add and configure an Azure Log Analytics workspace.]
- Add an Azure Storage account and Azure Cognitive Search
- Add an Azure Storage account and a file share.

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

QUESTION 14
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:
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 15

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?

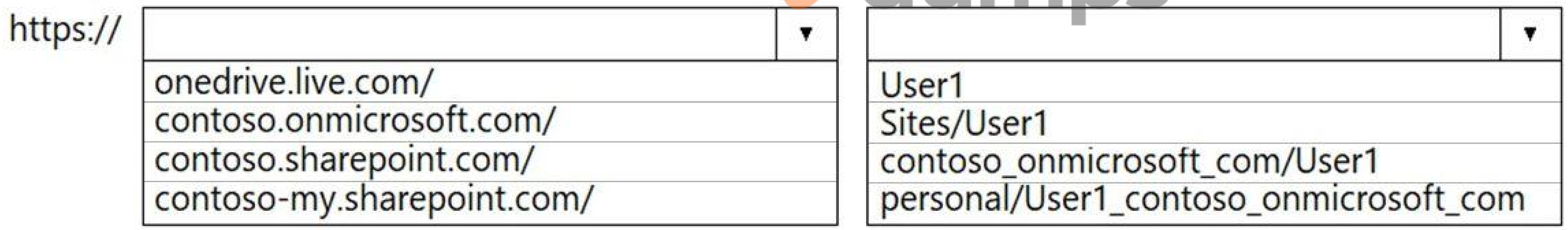
A. OneDrive accounts
B. Exchange email
C. Teams chat and channel messages
D. SharePoint sites

Correct Answer: B
Section:

QUESTION 16

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:

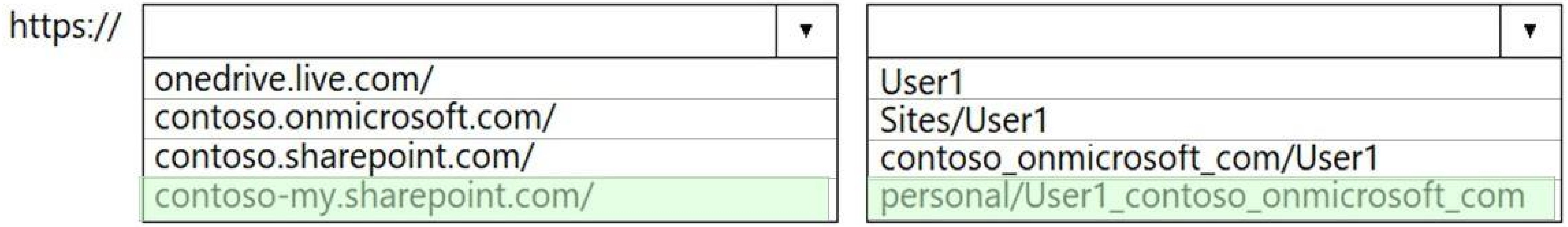


https://

- 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

Answer Area:



https://

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

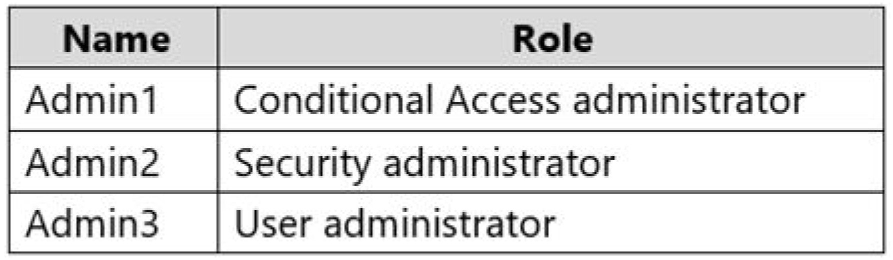
- User1
- Sites/User1
- contoso_onmicrosoft_com/User1
- [✓ personal/User1_contoso_onmicrosoft_com]

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

QUESTION 17

HOTSPOT

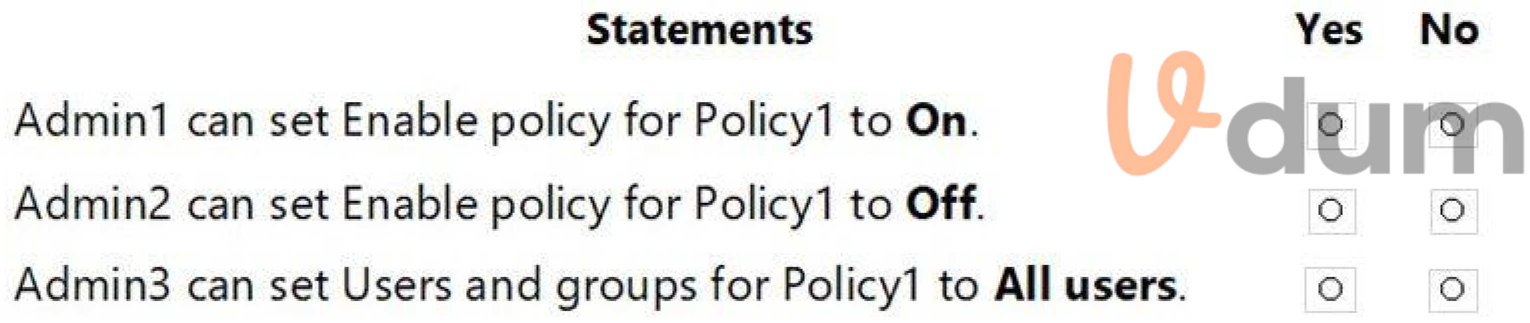
You have a Microsoft 365 E5 subscription linked to an Azure Active Directory (Azure AD) tenant. The tenant contains a group named Group1 and the users shown in the following table:



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

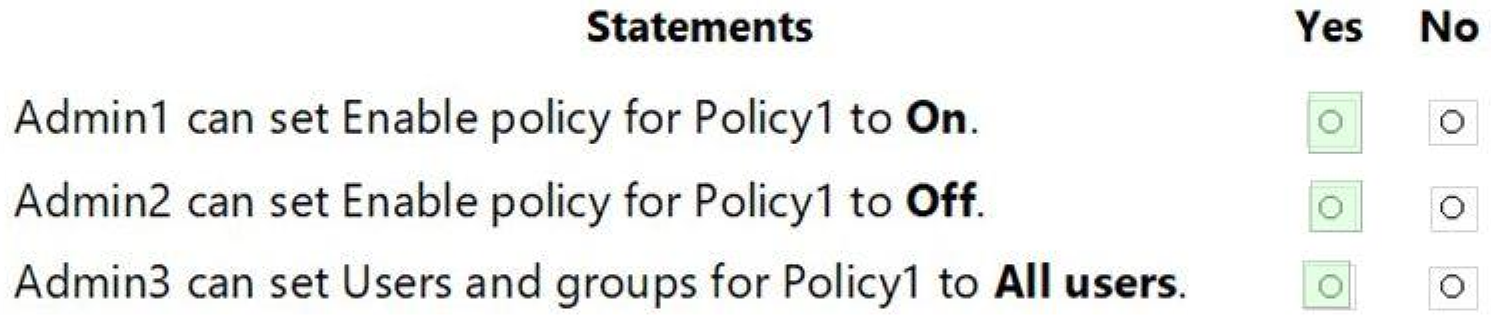
The tenant has a conditional access policy that has the following configurations:
Name: Policy1
Assignments:
- Users and groups: Group1
- Cloud aps or actions: All cloud apps
Access controls:
Grant, require multi-factor authentication
Enable policy: Report-only
You set Enabled Security defaults to Yes 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:



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**.	○	○

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:

Explanation:

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

QUESTION 18

DRAG DROP

You have a Microsoft 365 subscription.

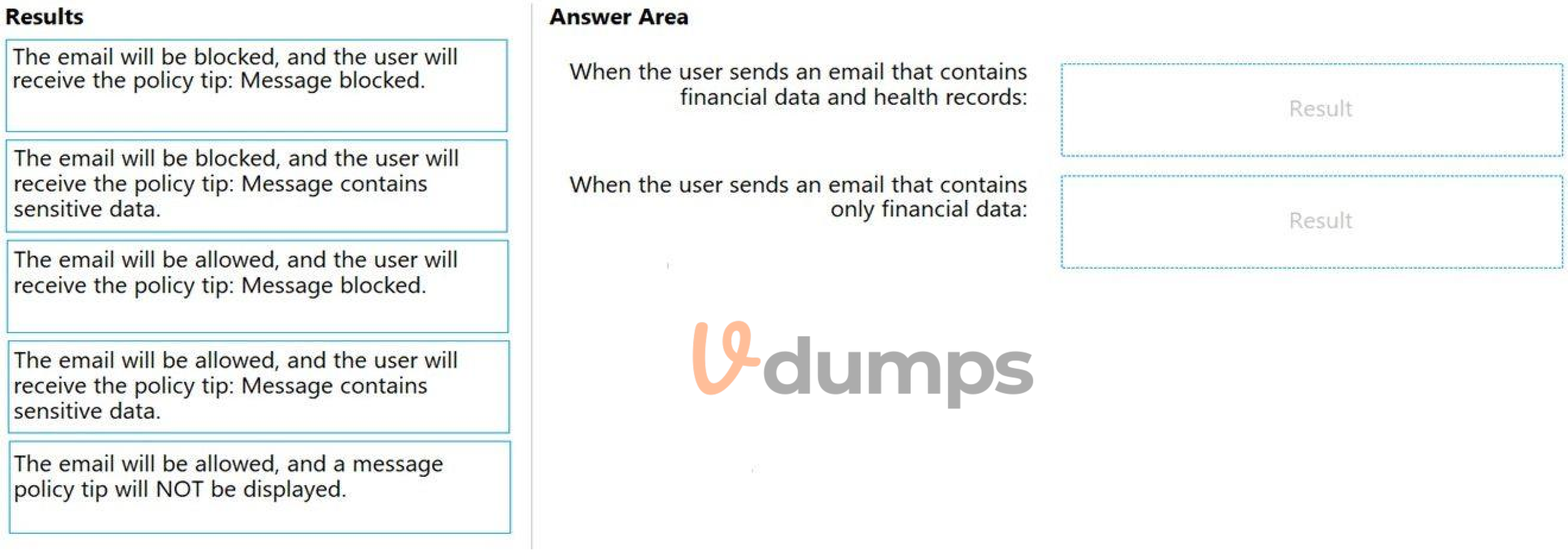
In the Exchange admin center, you have a data loss prevention (DLP) policy named Policy1 that has the following configurations:

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

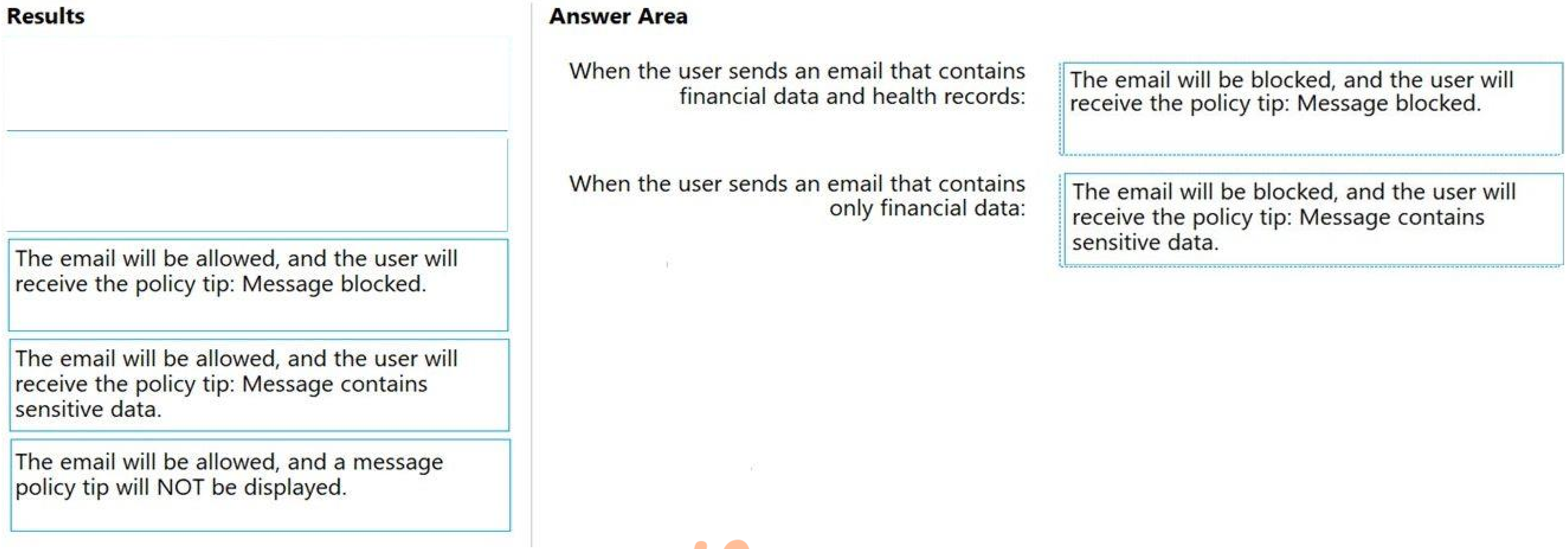
- The email will be blocked, and the user will receive the policy tip: Message blocked.
- The email will be blocked, and the user will receive the policy tip: Message contains sensitive data.
- The email will be allowed, and the user will receive the policy tip: Message blocked.
- The email will be allowed, 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 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.

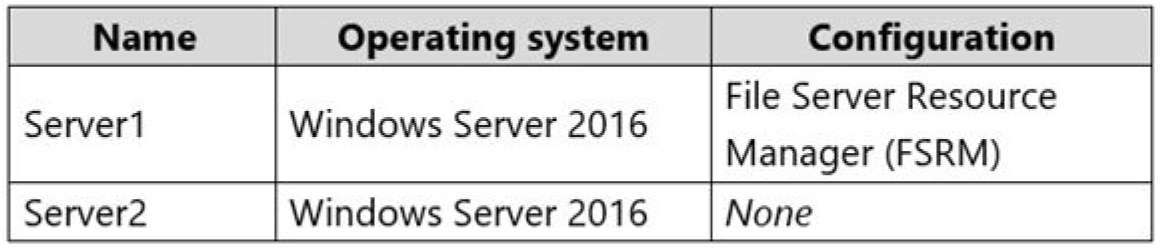
Answer Area

When the user sends an email that contains financial data and health records: 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 blocked, and the user will receive the policy tip: Message contains sensitive data.

Section:
Explanation:
https://docs.microsoft.com/en-us/microsoft-365/compliance/how-dlp-works-between-admin-centers

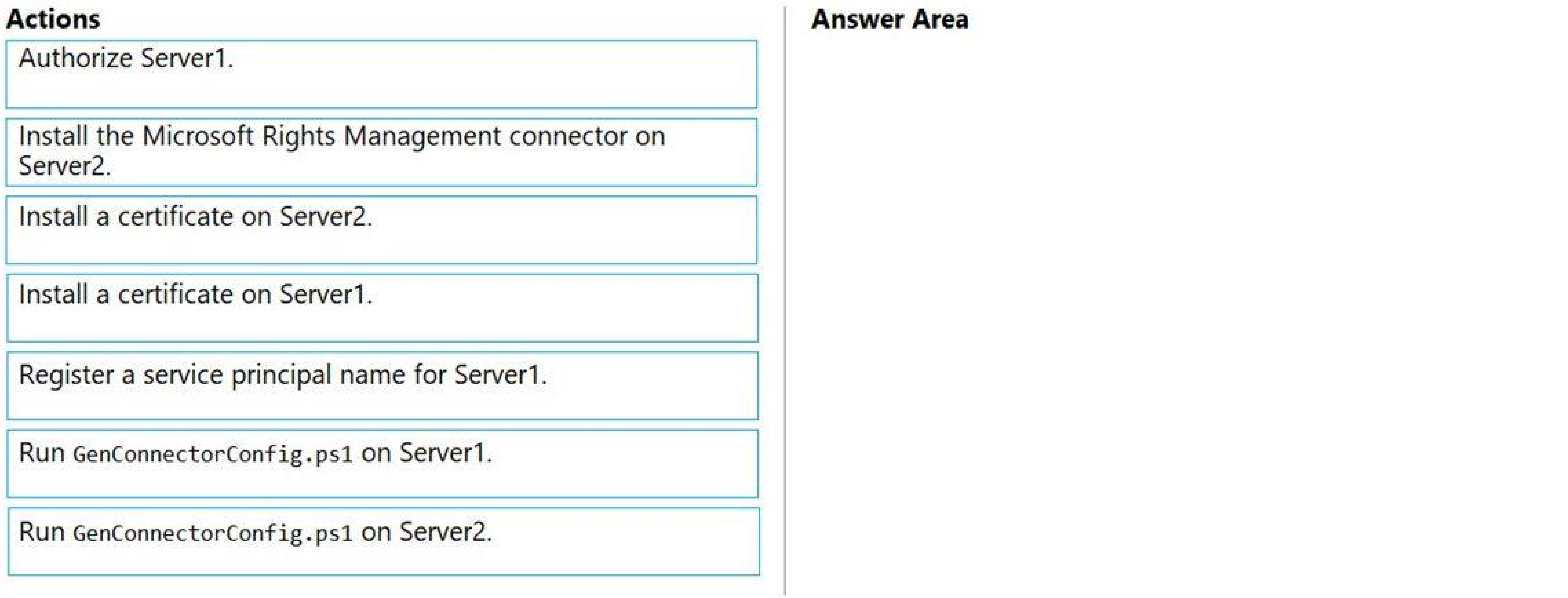
QUESTION 19
DRAG DROP
Your network contains an on-premises Active Directory domain that syncs to Azure Active Directory (Azure AD). The domain contains the servers shown in the following table.



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:

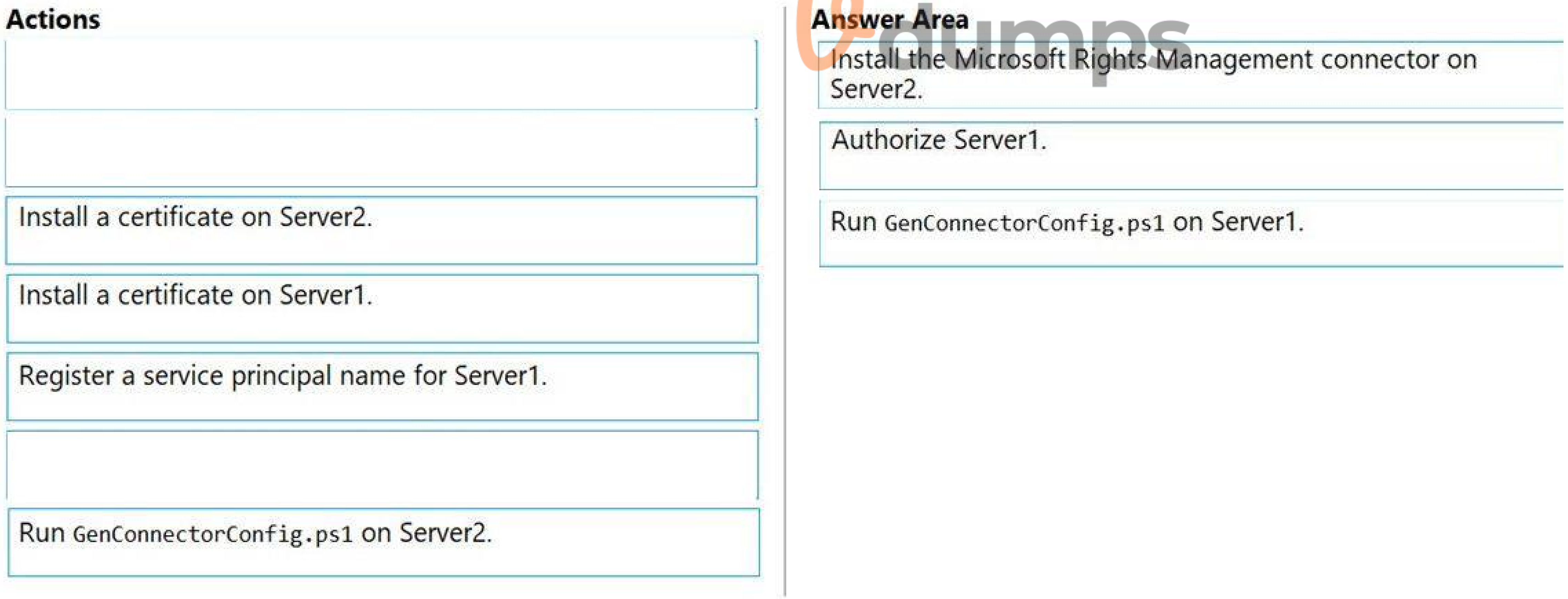


Actions

- 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:

Explanation:

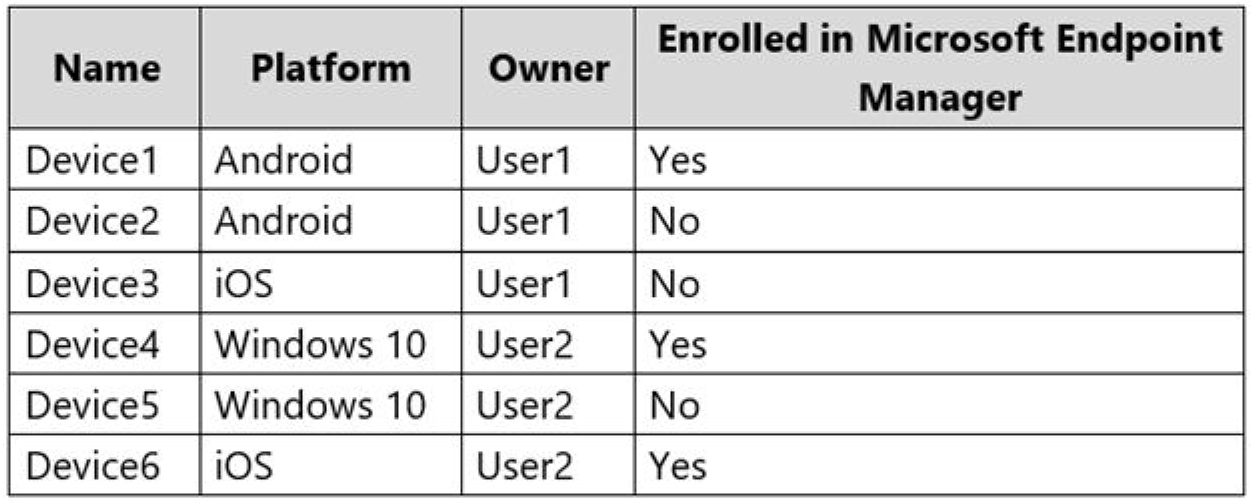
https://docs.microsoft.com/en-us/azure/information-protection/install-configure-rms-connector

https://docs.microsoft.com/en-us/azure/information-protection/configure-servers-rms-connector

QUESTION 20

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:

Explanation:

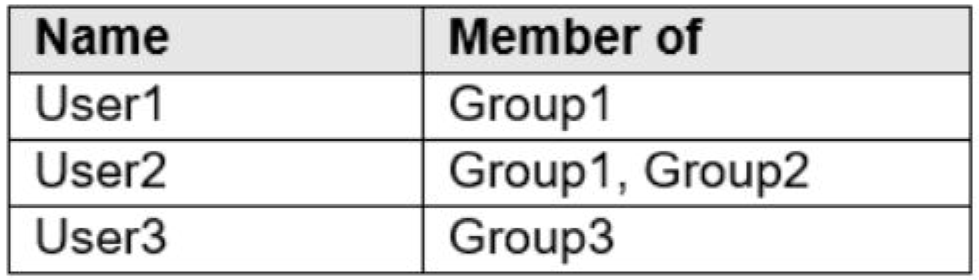
You can create and use app configuration policies to provide configuration settings for both iOS/iPadOS or Android apps on devices that are and are not enrolled in Microsoft Endpoint Manager.

https://docs.microsoft.com/en-us/mem/intune/apps/app-configuration-policies-overview

QUESTION 21

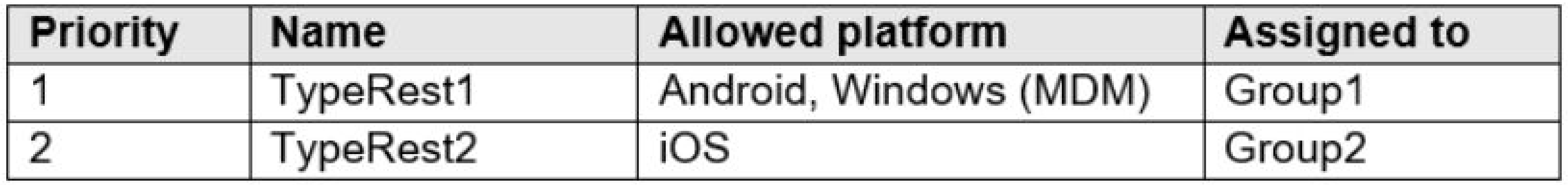
HOTSPOT

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



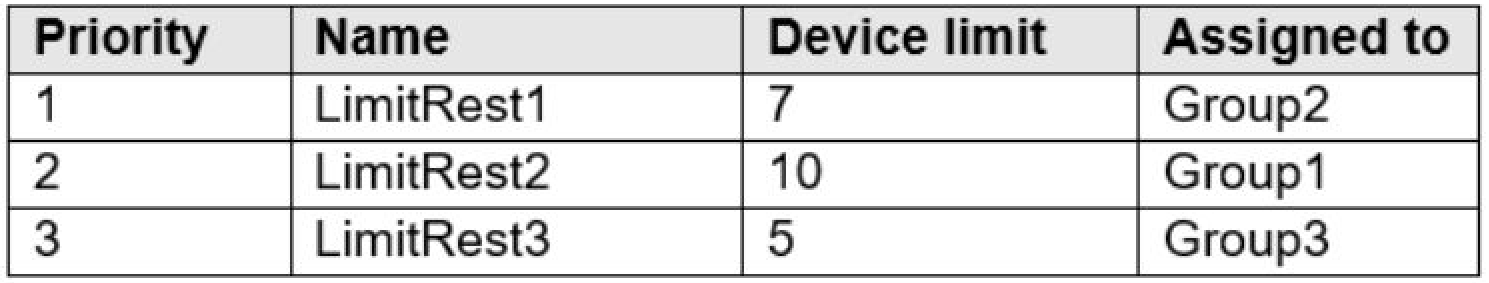
Name	Member of
User1	Group1
User2	Group1, Group2
User3	Group3

In Microsoft Endpoint Manager, you create two device type restrictions that have the settings shown in the following table.



Priority	Name	Allowed platform	Assigned to
1	TypeRest1	Android, Windows (MDM)	Group1
2	TypeRest2	iOS	Group2

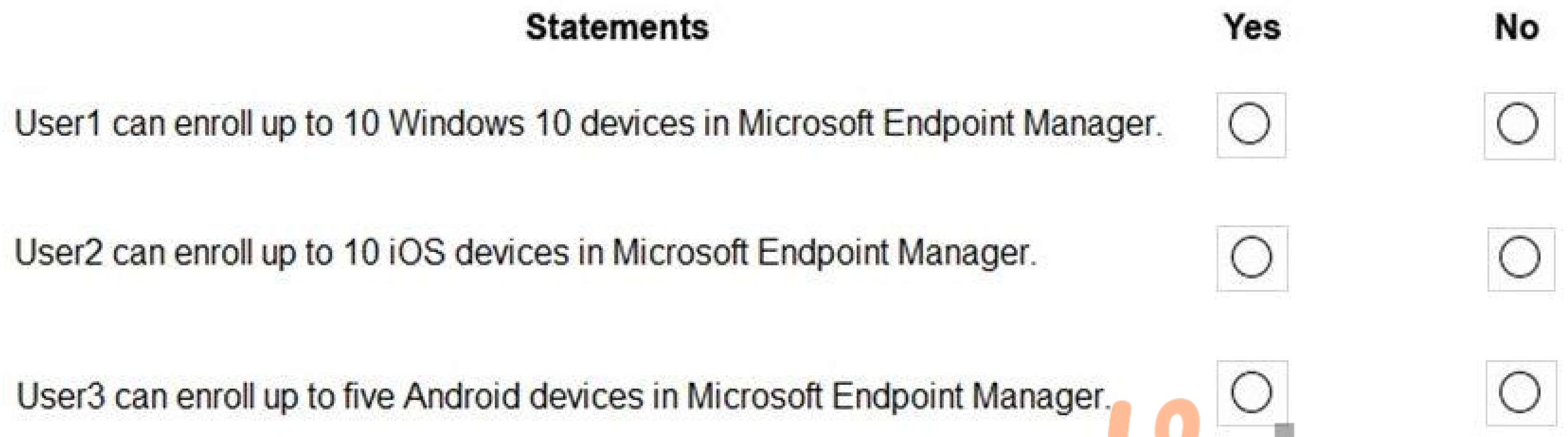
In Microsoft Endpoint Manager, you create three device limit restrictions that have the settings shown in the following table.



Priority	Name	Device limit	Assigned to
1	LimitRest1	7	Group2
2	LimitRest2	10	Group1
3	LimitRest3	5	Group3

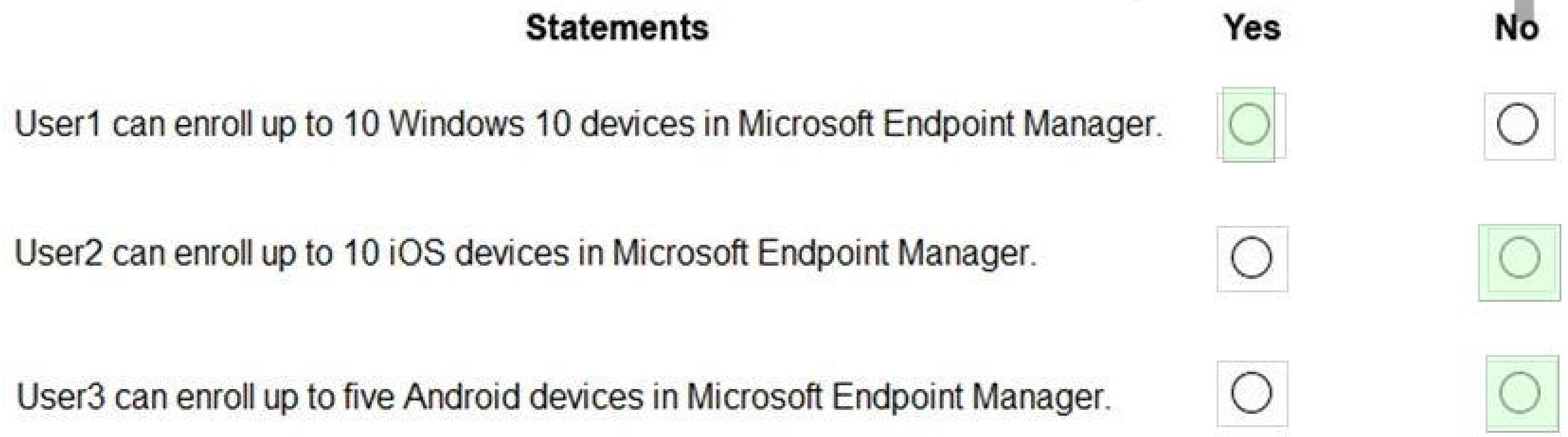
For each of the following statements, select Yes if the statement is true. Otherwise, select No.
NOTE: Each correct selection is worth one point.

Hot Area:



Statements	Yes	No
User1 can enroll up to 10 Windows 10 devices in Microsoft Endpoint Manager.	○	○
User2 can enroll up to 10 iOS devices in Microsoft Endpoint Manager.	○	○
User3 can enroll up to five Android devices in Microsoft Endpoint Manager.	○	○

Answer Area:



Statements	Yes	No
User1 can enroll up to 10 Windows 10 devices in Microsoft Endpoint Manager.	[✓ ○]	○
User2 can enroll up to 10 iOS devices in Microsoft Endpoint Manager.	○	[✓ ○]
User3 can enroll up to five Android devices in Microsoft Endpoint Manager.	○	[✓ ○]

Section:
Explanation:

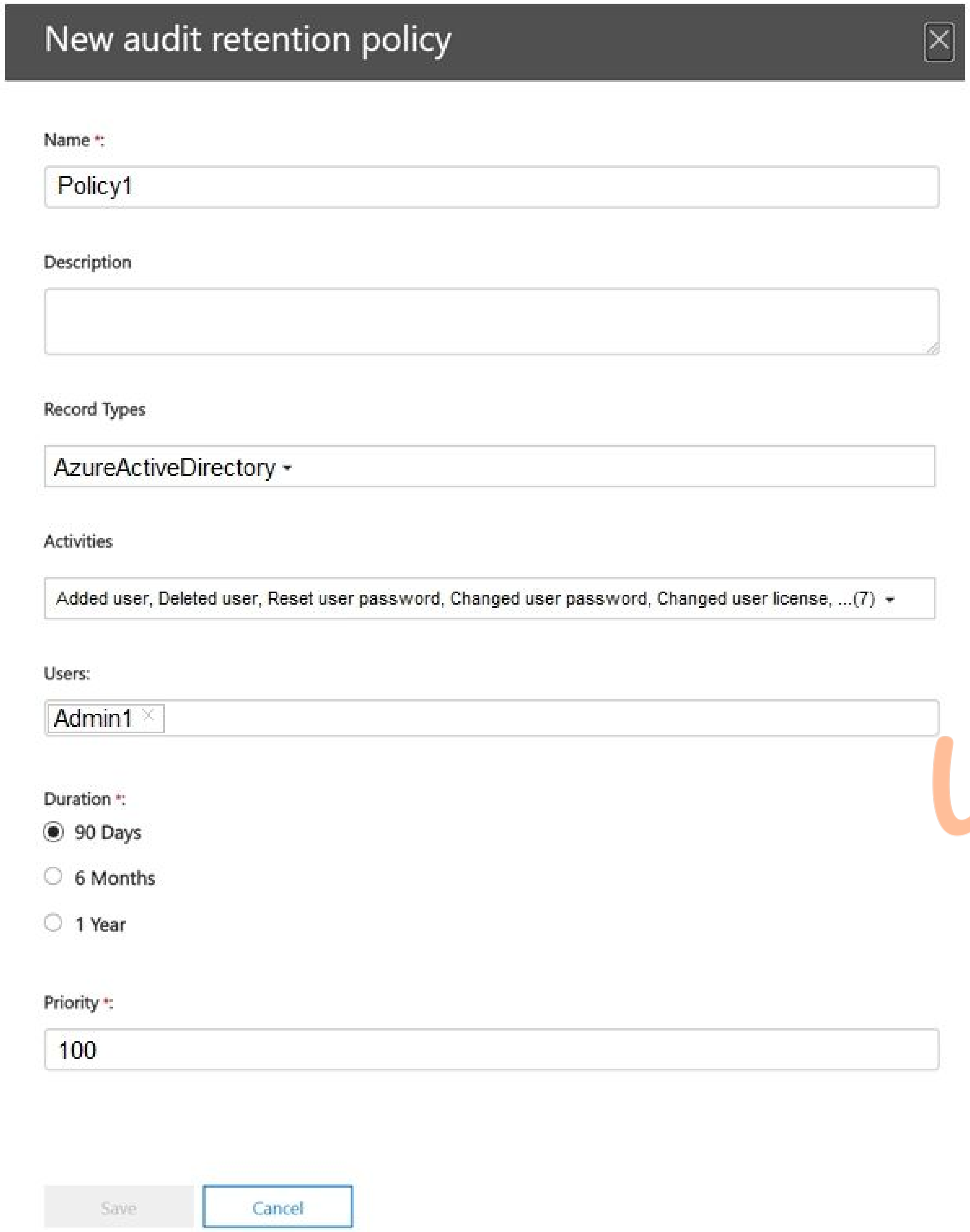
QUESTION 22
Your company has digitally signed applications.
You need to ensure that Microsoft Defender Advanced Threat Protection (Microsoft Defender ATP) considers the digitally signed applications safe and never analyzes them.
What should you create in the Microsoft Defender Security Center?

A. a custom detection rule
B. an allowed/blocked list rule
C. an alert suppression rule

D. an indicator

Correct Answer: D
Section:
Explanation:
https://docs.microsoft.com/en-us/windows/security/threat-protection/microsoft-defender-atp/manage-indicators

QUESTION 23
HOTSPOT
You have a Microsoft 365 E5 subscription that contains two users named Admin1 and Admin2.
All users are assigned a Microsoft 365 Enterprise E5 license and auditing is turned on.
You create the audit retention policy shown in the exhibit. (Click the Exhibit tab.)



New audit retention policy

Name *:

Policy1

Description

Record Types

AzureActiveDirectory

Activities

Added user, Deleted user, Reset user password, Changed user password, Changed user license, ...(7)

Users:

Admin1

Duration *:

● 90 Days

○ 6 Months

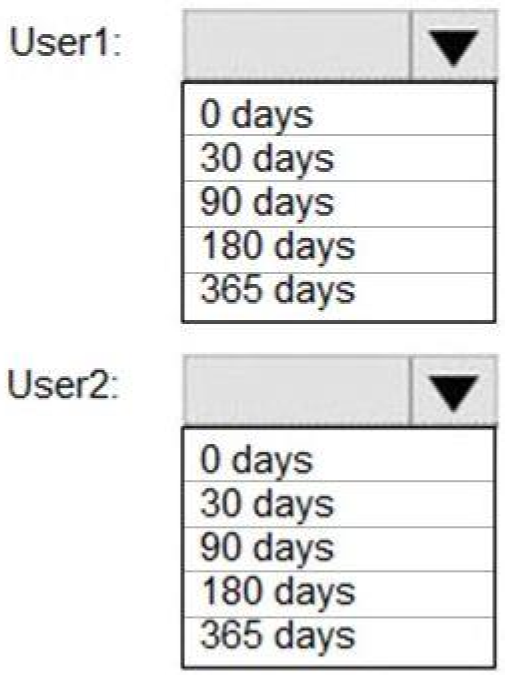
○ 1 Year

Priority *:

100

After Policy1 is created, the following actions are performed:
Admin1 creates a user named User1.
Admin2 creates a user named User2.
How long will the audit events for the creation of User1 and User2 be retained? To answer, select the appropriate options in the answer area.
NOTE: Each correct selection is worth one point.

Hot Area:



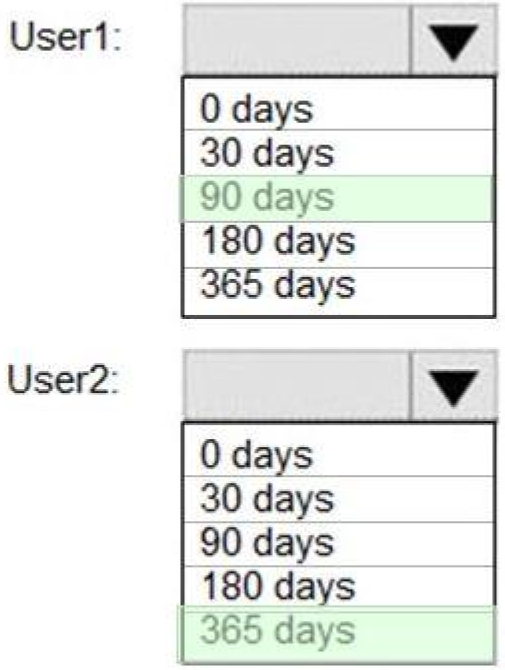
User1:

- 0 days
- 30 days
- 90 days
- 180 days
- 365 days

User2:

- 0 days
- 30 days
- 90 days
- 180 days
- 365 days

Answer Area:



User1:

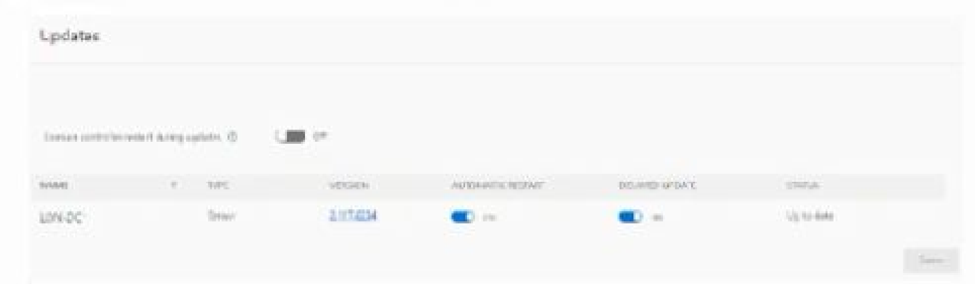
- 0 days
- 30 days
- [✓ 90 days]
- 180 days
- 365 days

User2:

- 0 days
- 30 days
- 90 days
- 180 days
- [✓ 365 days]

Section:
Explanation:
https://docs.microsoft.com/en-us/microsoft-365/compliance/audit-log-retention-policies?view=o365-worldwide

QUESTION 24
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 UPDATE	STATUS
LON-DC	Sensor	2.117.6234	On	On	Up to date

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

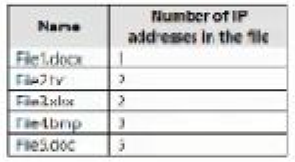
A. 20 hours
B. 12 hours
C. 7 hours
D. 48 hours

Correct Answer: B
Section:

QUESTION 25

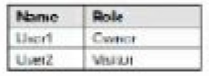
HOTSPOT

You have a Microsoft 365 subscription that contains a Microsoft SharePoint Online site named Site1. Site1 has he files in the following table.



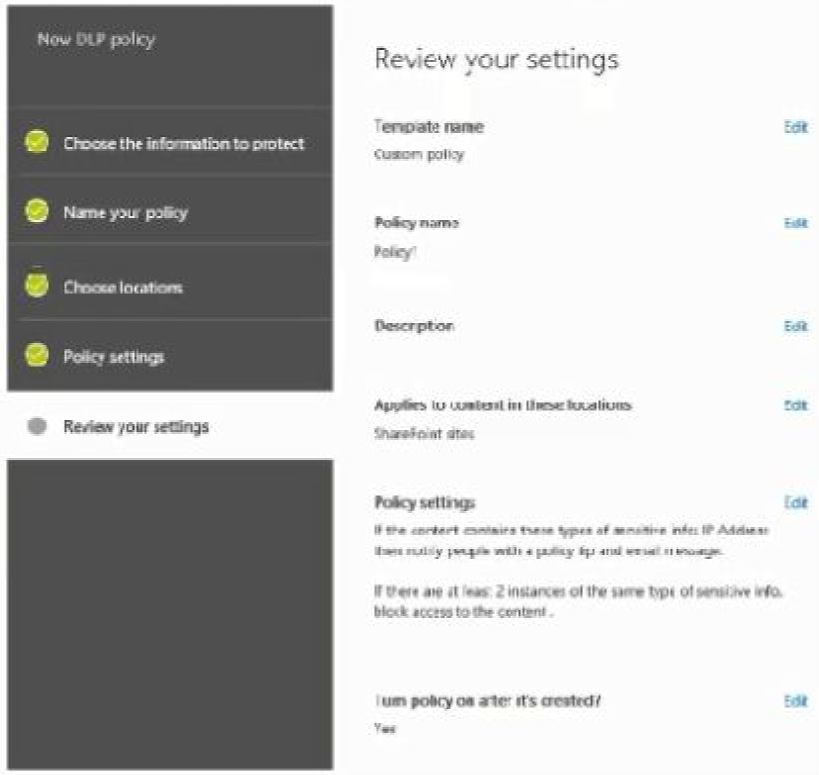
Name	Number of IP addresses in the file
File1.docx	1
File2.tv	2
File3.xlsx	2
File4.bmp	3
File5.doc	3

The Site1 users are assigned the roles shown in the following table.



Name	Role
User1	Owner
User2	Visitor

You create a data less prevention (DLP) policy names Policy1 as shown in the following exhibit.



Review your settings

Template name
Custom policy

Policy name
Policy1

Description

Applies to content in these locations
SharePoint sites

Policy settings
If the content contains these types of sensitive info: IP Address then notify people with a policy tip and email message.

If there are at least 2 instances of the same type of sensitive info, block access to the content .

Turn policy on after it's created?
Yes

How many files will be visible to user1 and User2 after Policy' is applied to answer, selected select the appropriate options in the answer area.

NOTE: Each correct selection is worth one point.

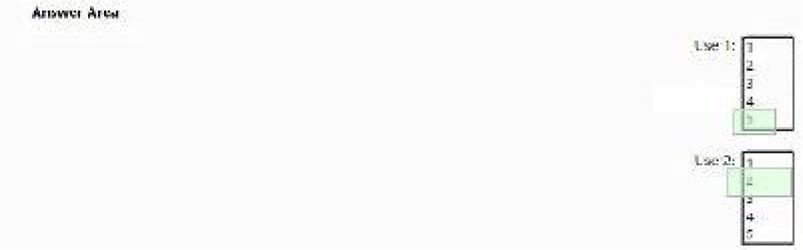
Hot Area:

Answer Area

Use 1: 1 2 3 4 5

Use 2: 1 2 3 4 5

Answer Area:



Answer Area

Use 1: 1 2 3 4 5

Use 2: 1 2 3 4 5

Section:
Explanation:

QUESTION 26
You have a Microsoft 365 F5 subscription.
You plan to deploy 100 new Windows 10 devices.
You need to order the appropriate version of Windows 10 for the new devices. The version must
Meet the following requirements.
Be serviced for a minimum of 24 moths.
Support Microsoft Application Virtualization (App-V)
Which version should you identify?

A. Window 10 Pro, version 1909
B. Window 10 Pro, version 2004
C. Window 10 Pro, version 1909
D. Window 10 Enterprise, version 2004

Correct Answer: D
Section:
Explanation:
https://docs.microsoft.com/en-us/windows/release-health/release-information
https://docs.microsoft.com/en-us/windows/application-management/app-v/appv-supported-configurations

QUESTION 27
You have a Microsoft 365 subscription.
You discover that some external users accessed center for 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: B
Section:

QUESTION 28

HOTSPOT

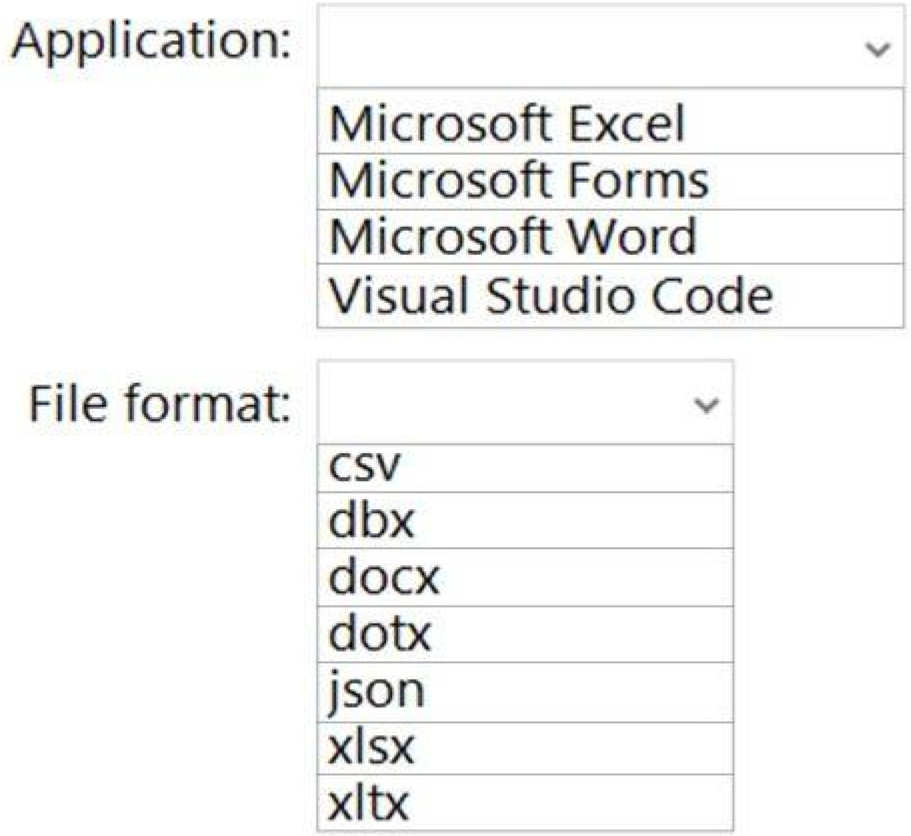
You have a Microsoft 365 tenant.

You need to create a custom Compliance Manager assessment template.

Which application should you use to create the template, and in which file format should the template be saved? To answer, select the appropriate options in the answer area.

NOTE: Each correct selection is worth one point.

Hot Area:



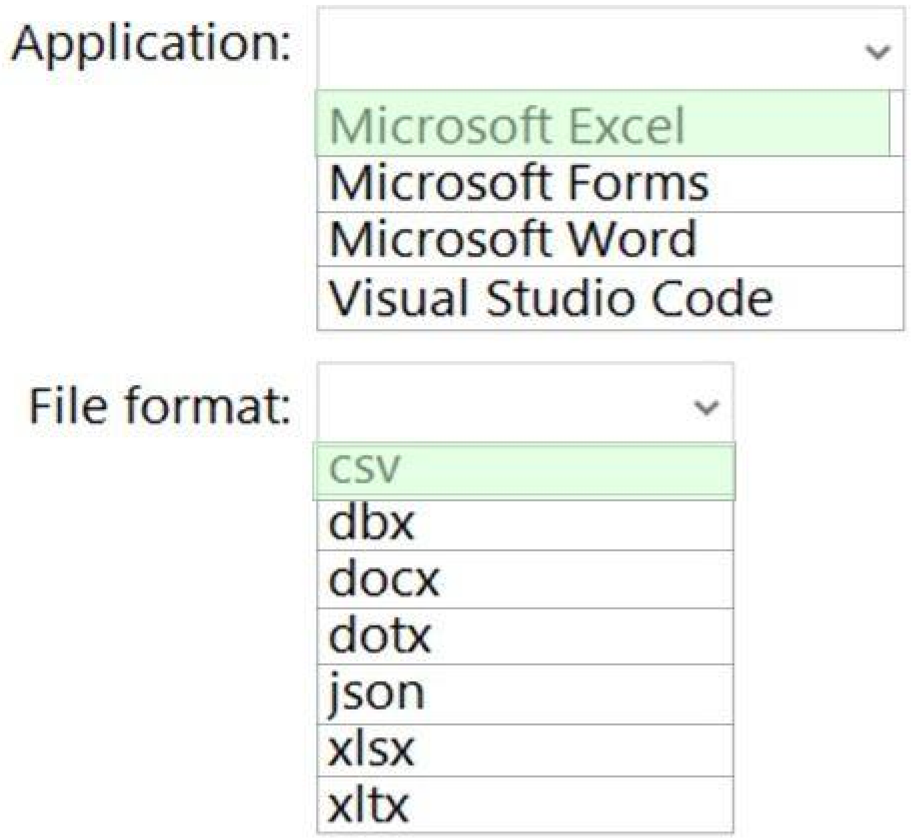
Application:

- Microsoft Excel
- Microsoft Forms
- Microsoft Word
- Visual Studio Code

File format:

- csv
- dbx
- docx
- dotx
- json
- xlsx
- xltx

Answer Area:

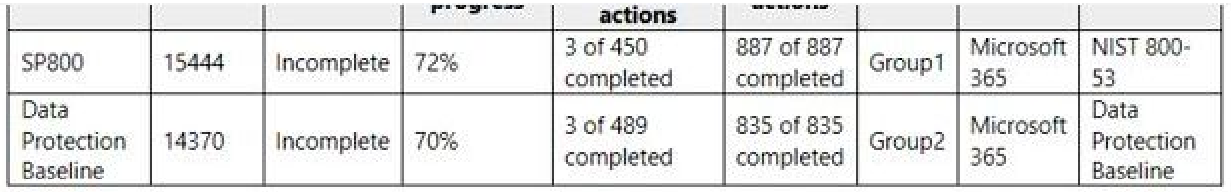


Application:
- Microsoft Excel
- Microsoft Forms
- Microsoft Word
- Visual Studio Code

File format:
- csv
- dbx
- docx
- dotx
- json
- xlsx
- xltx

Section:
Explanation:
https://docs.microsoft.com/en-us/microsoft-365/compliance/compliance-manager-templates-create?view=o365-worldwide

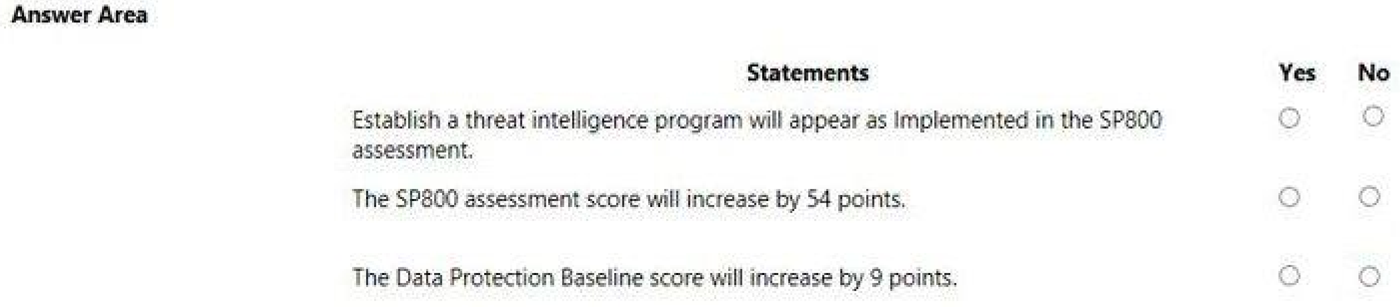
QUESTION 29
HOTSPOT



			progress	actions	actions			
SP800	15444	Incomplete	72%	3 of 450 completed	887 of 887 completed	Group1	Microsoft 365	NIST 800-53
Data Protection Baseline	14370	Incomplete	70%	3 of 489 completed	835 of 835 completed	Group2	Microsoft 365	Data Protection Baseline

The SP800 assessment has the improvement actions shown in the following table.

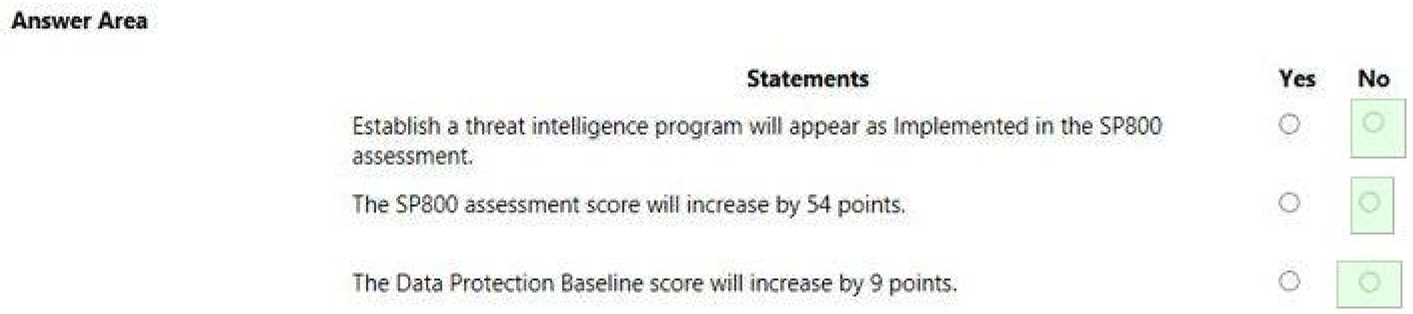
Hot Area:



Answer Area

Statements	Yes	No
Establish a threat intelligence program will appear as Implemented in the SP800 assessment.	○	○
The SP800 assessment score will increase by 54 points.	○	○
The Data Protection Baseline score will increase by 9 points.	○	○

Answer Area:



Answer Area

Statements	Yes	No
Establish a threat intelligence program will appear as Implemented in the SP800 assessment.	○	[✓ ○]
The SP800 assessment score will increase by 54 points.	○	[✓ ○]
The Data Protection Baseline score will increase by 9 points.	○	[✓ ○]

Section:
Explanation:

QUESTION 30

DRAG DROP

You have a Microsoft 365 E5 tenant.

You need to implement compliance solutions that meet the following requirements:

* Use a file plan to manage retention labels.

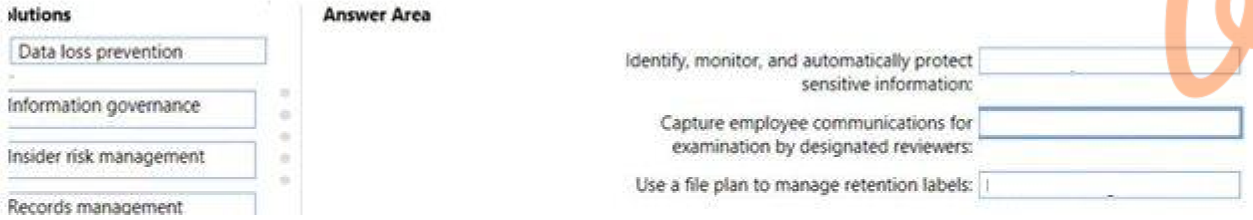
* Identify, monitor, and automatically protect sensitive information.

* Capture employee communications for examination by designated reviewers.

Which solution should you use for each requirement? To answer, drag the appropriate solutions to the correct requirements. Each solution may be used once, more than once, or not at all. You may need to drag the split bat between panes or scroll to view content.

NOTE: Each correct selection is worth one point.

Select and Place:



lutions

Data loss prevention

Information governance

Insider risk management

Records management

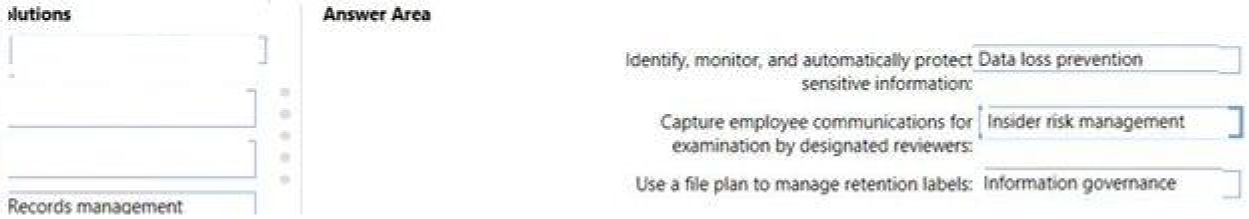
Answer Area

Identify, monitor, and automatically protect sensitive information:

Capture employee communications for examination by designated reviewers:

Use a file plan to manage retention labels:

Correct Answer:



lutions

Records management

Answer Area

Identify, monitor, and automatically protect sensitive information: Data loss prevention

Capture employee communications for examination by designated reviewers: Insider risk management

Use a file plan to manage retention labels: Information governance

Section:
Explanation:

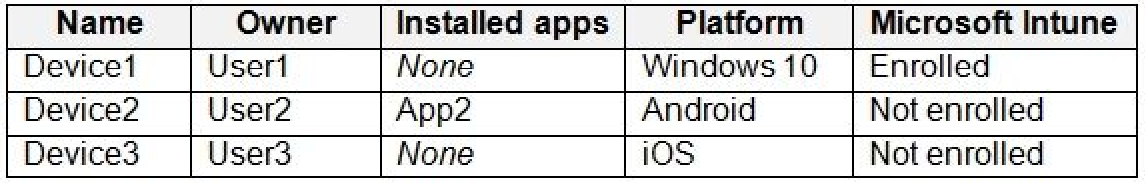
QUESTION 31

HOTSPOT

You have a Microsoft 365 E5 tenant that contains the users shown in the following table.

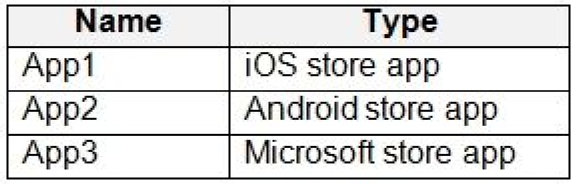
Name	Member of
User1	UserGroup1
User2	UserGroup2
User3	UserGroup3

The tenant contains the devices shown in the following table.



Name	Owner	Installed apps	Platform	Microsoft Intune
Device1	User1	*None*	Windows 10	Enrolled
Device2	User2	App2	Android	Not enrolled
Device3	User3	*None*	iOS	Not enrolled

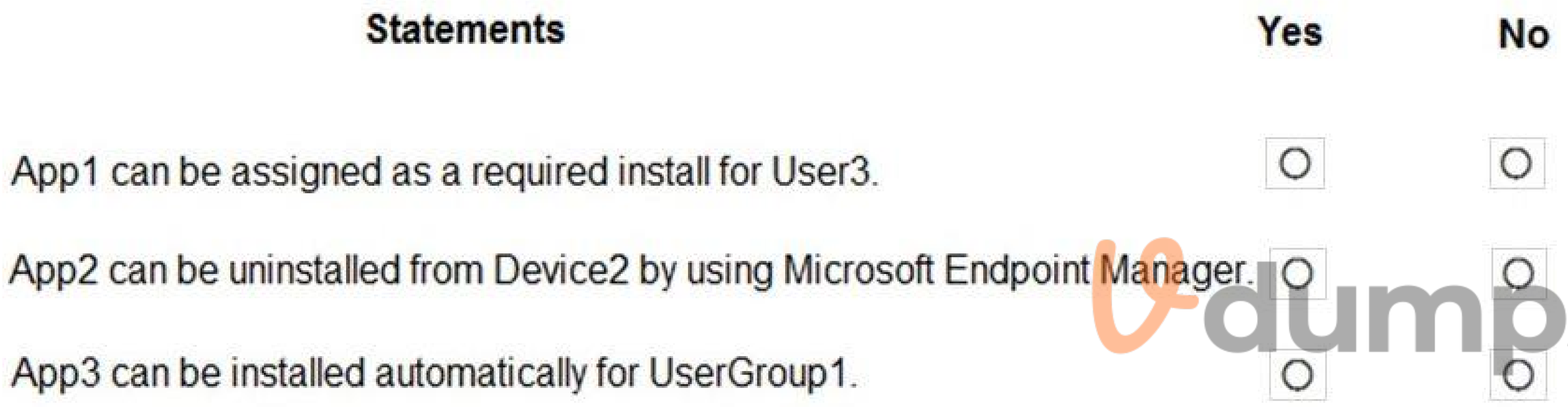
You have the apps shown in the following table.



Name	Type
App1	iOS store app
App2	Android store app
App3	Microsoft store app

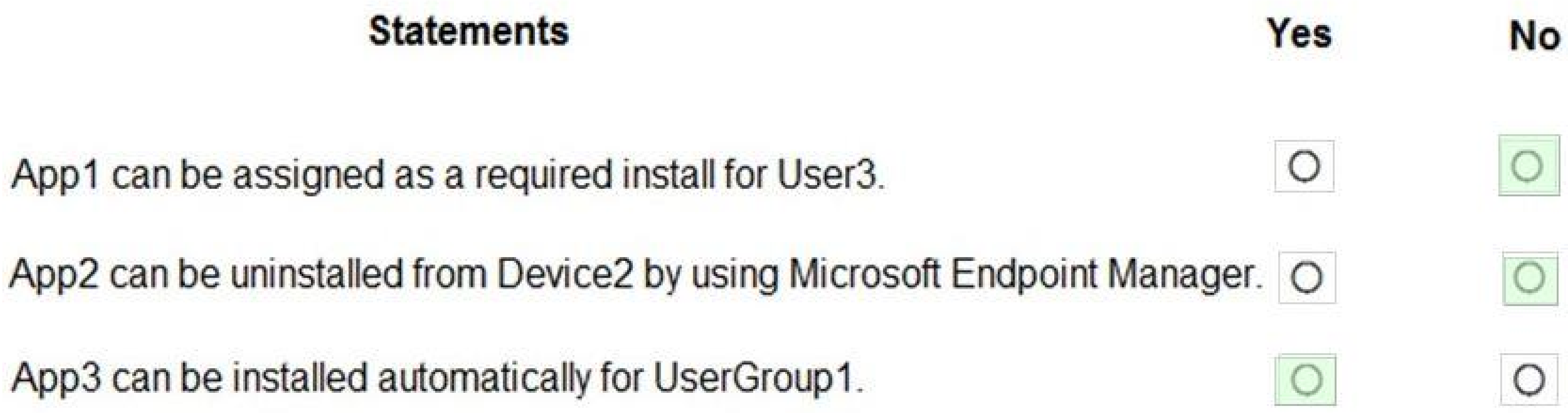
You plan to use Microsoft Endpoint Manager to manage the apps for the users.
For each of the following statements, select Yes if the statement is true. Otherwise, select No.
NOTE: Each correct selection is worth one point.

Hot Area:



Statements	Yes	No
App1 can be assigned as a required install for User3.	○	○
App2 can be uninstalled from Device2 by using Microsoft Endpoint Manager.	○	○
App3 can be installed automatically for UserGroup1.	○	○

Answer Area:



Statements	Yes	No
App1 can be assigned as a required install for User3.	○	[✓ ○]
App2 can be uninstalled from Device2 by using Microsoft Endpoint Manager.	○	[✓ ○]
App3 can be installed automatically for UserGroup1.	[✓ ○]	○

Section:
Explanation:
https://docs.microsoft.com/en-us/mem/intune/apps/apps-deploy
https://docs.microsoft.com/en-us/mem/intune/apps/apps-windows-10-app-deploy

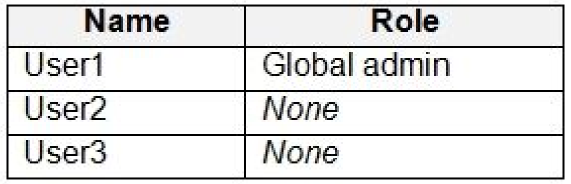
QUESTION 32
You have Windows 10 devices that are managed by using Microsoft Endpoint Manager.
You need to configure the security settings in Microsoft Edge.

What should you create in Microsoft Endpoint Manager?

A. an app configuration policy
B. an app
C. a device configuration profile
D. a device compliance policy

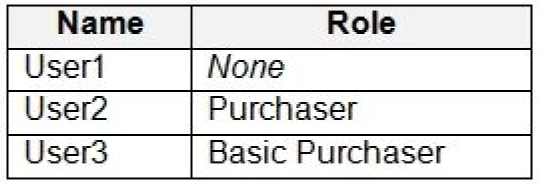
Correct Answer: C
Section:
Explanation:
https://docs.microsoft.com/en-us/deployedge/configure-edge-with-intune

QUESTION 33
HOTSPOT
You have a Microsoft 365 E5 tenant that contains the users shown in the following table.



Name	Role
User1	Global admin
User2	*None*
User3	*None*

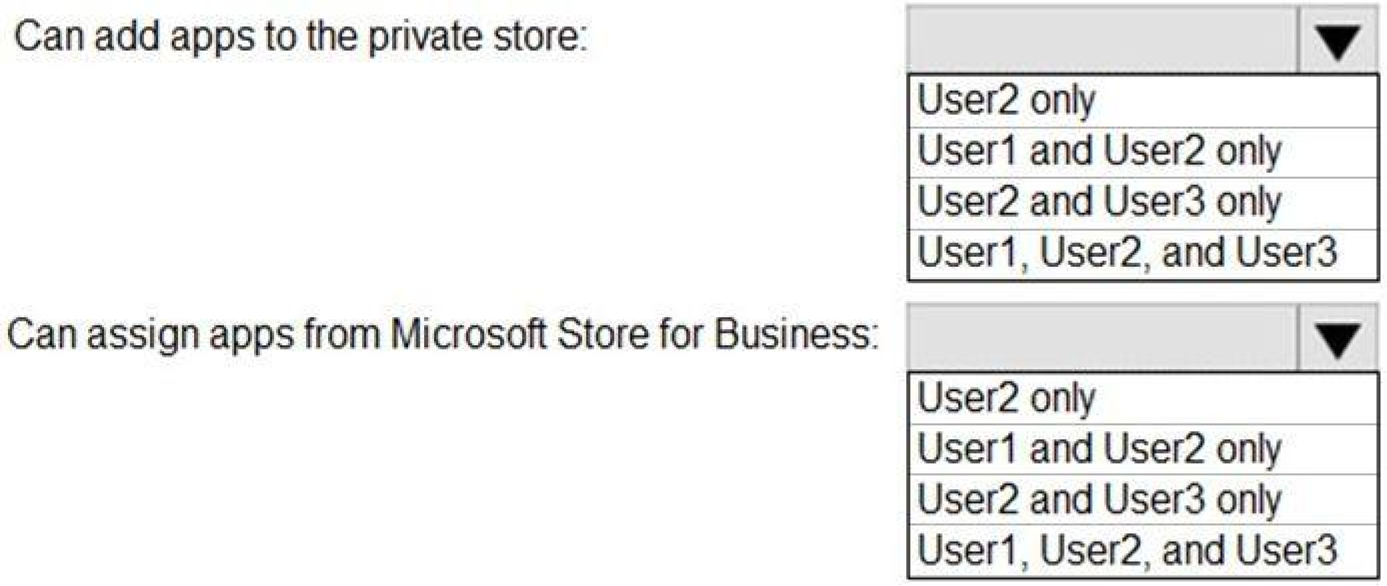
You provision the private store in Microsoft Store for Business.
You assign Microsoft Store for Business roles to the users as shown in the following table.



Name	Role
User1	*None*
User2	Purchaser
User3	Basic Purchaser

You need to identify which users can add apps to the private store, and which users can assign apps from Microsoft Store for Business.
Which users should you identify? To answer, select the appropriate options in the answer area.
NOTE: Each correct selection is worth one point.

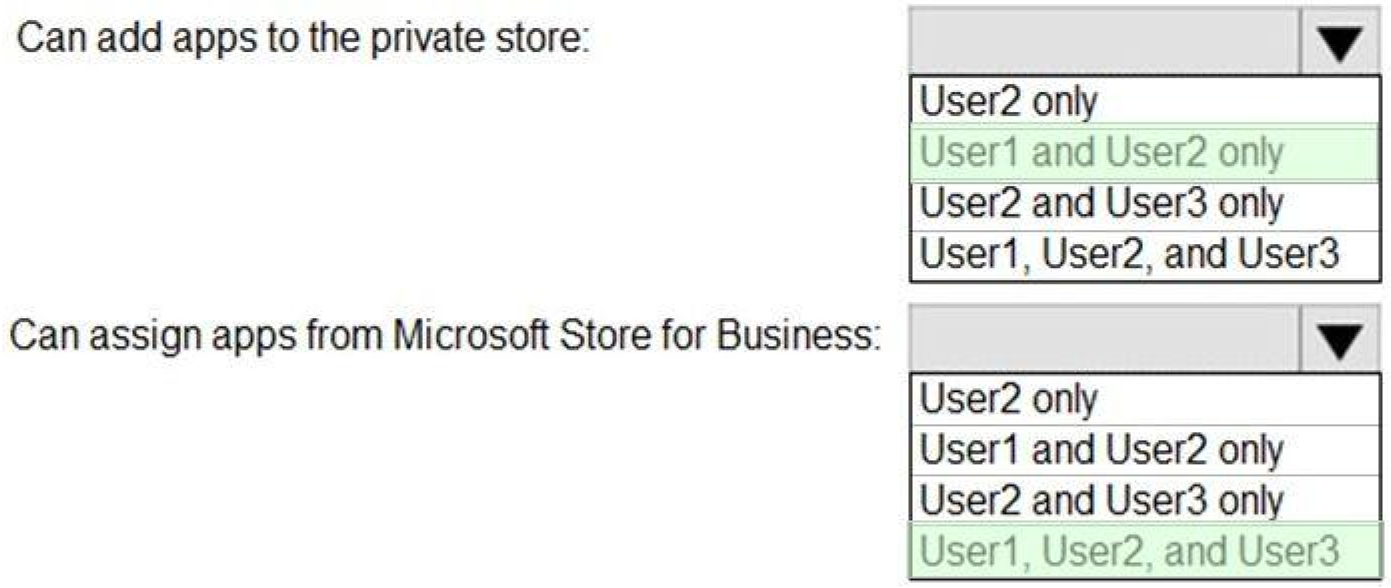
Hot Area:



Can add apps to the private store:
- User2 only
- User1 and User2 only
- User2 and User3 only
- User1, User2, and User3

Can assign apps from Microsoft Store for Business:
- User2 only
- User1 and User2 only
- User2 and User3 only
- User1, User2, and User3

Answer Area:



Can add apps to the private store:

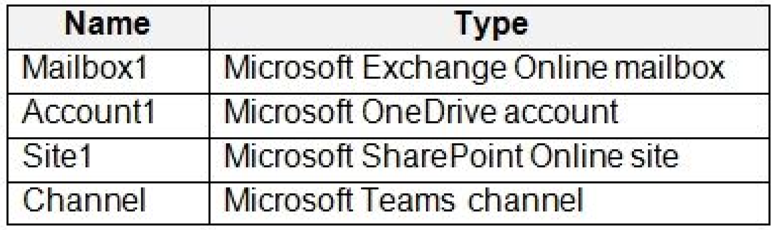
- User2 only
- [✓ User1 and User2 only]
- User2 and User3 only
- User1, User2, and User3

Can assign apps from Microsoft Store for Business:

- User2 only
- User1 and User2 only
- User2 and User3 only
- [✓ User1, User2, and User3]

Section:
Explanation:
https://docs.microsoft.com/en-us/microsoft-store/roles-and-permissions-microsoft-store-for-business
https://docs.microsoft.com/en-us/education/windows/education-scenarios-store-for-business#basic-purchaser-role

QUESTION 34
You have a Microsoft 365 E5 tenant that contains the resources shown in the following table.



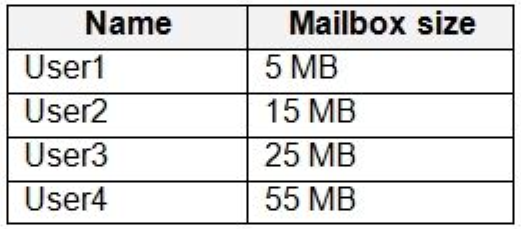
Name	Type
Mailbox1	Microsoft Exchange Online mailbox
Account1	Microsoft OneDrive account
Site1	Microsoft SharePoint Online site
Channel	Microsoft Teams channel

To which resources can you apply a sensitivity label by using an auto-labeling policy?

A. Mailbox1 and Site1 only
B. Mailbox1, Account1, and Site1 only
C. Account1 and Site1 only
D. Mailbox1, Account1, Site1, and Channel1
E. Account1, Site1, and Channel1 only

Correct Answer: E
Section:
Explanation:
https://docs.microsoft.com/en-us/microsoft-365/compliance/sensitivity-labels?view=o365-worldwide

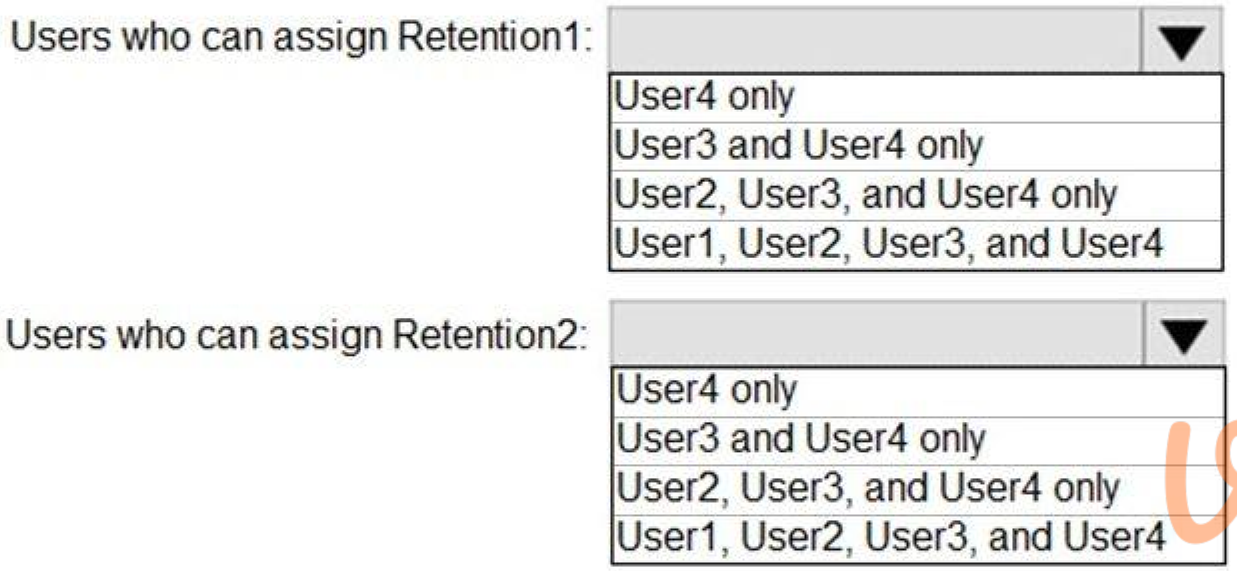
QUESTION 35
HOTSPOT
You have a Microsoft 365 E5 subscription that contains the users shown in the following table.



Name	Mailbox size
User1	5 MB
User2	15 MB
User3	25 MB
User4	55 MB

You have a Microsoft Office 365 retention label named Retention1 that is published to Exchange email.
You have a Microsoft Exchange Online retention policy that is applied to all mailboxes. The retention policy contains a retention tag named Retention2.
Which users can assign Retention1 and Retention2 to their emails? To answer, select the appropriate options in the answer area.
NOTE: Each correct selection is worth one point.

Hot Area:



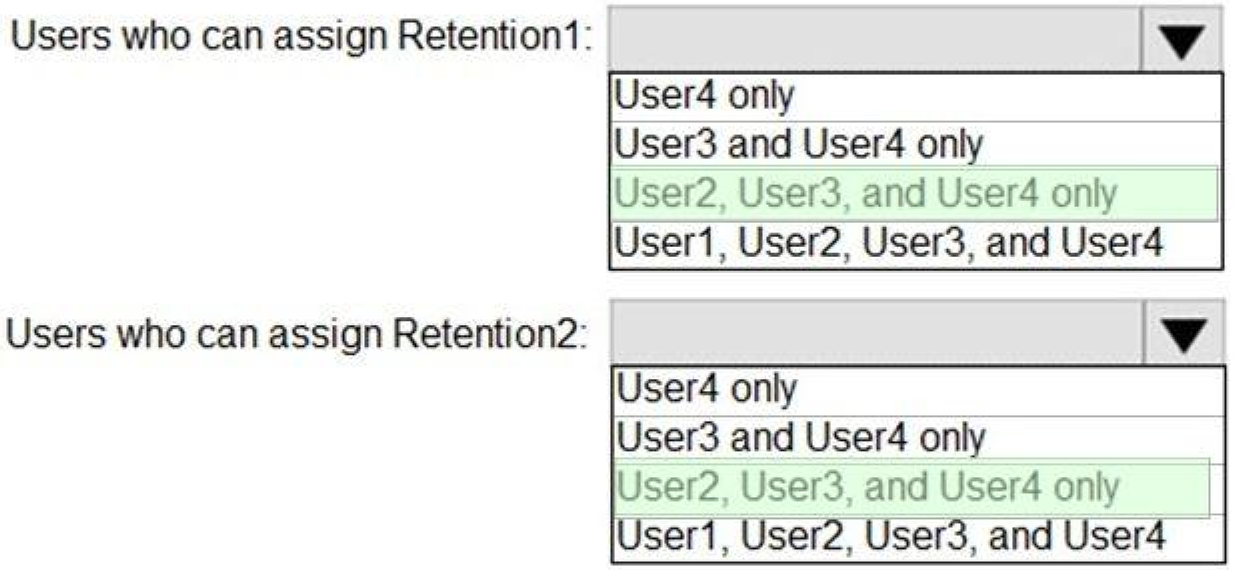
Users who can assign Retention1:

- User4 only
- User3 and User4 only
- User2, User3, and User4 only
- User1, User2, User3, and User4

Users who can assign Retention2:

- User4 only
- User3 and User4 only
- User2, User3, and User4 only
- User1, User2, User3, and User4

Answer Area:



Users who can assign Retention1:

- User4 only
- User3 and User4 only
- [✓ User2, User3, and User4 only]
- User1, User2, User3, and User4

Users who can assign Retention2:

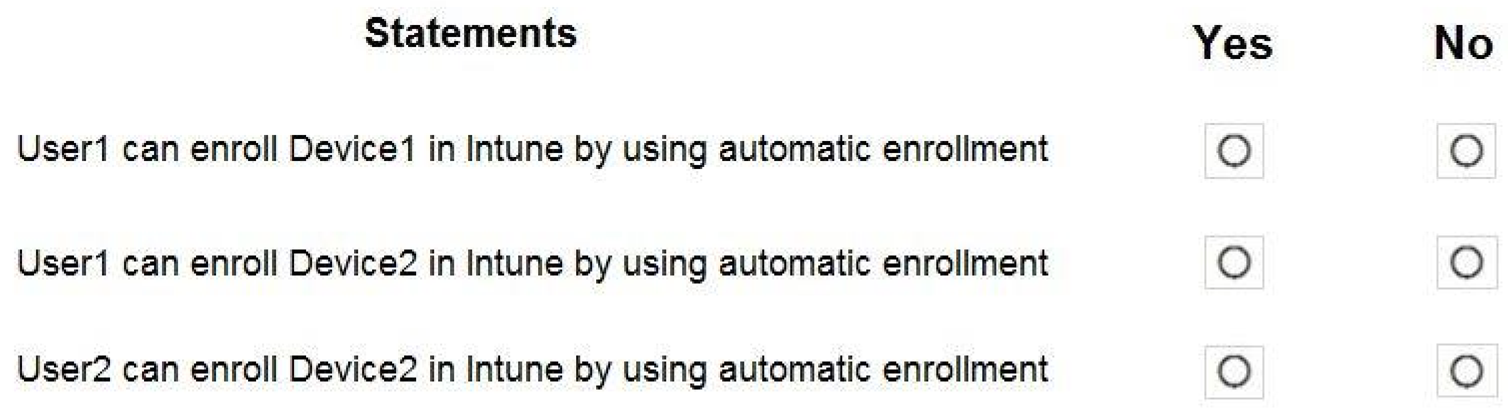
- User4 only
- User3 and User4 only
- [✓ User2, User3, and User4 only]
- User1, User2, User3, and User4

Section:
Explanation:
https://docs.microsoft.com/en-us/microsoft-365/compliance/retention-policies-exchange?view=o365-worldwide

QUESTION 36
HOTSPOT

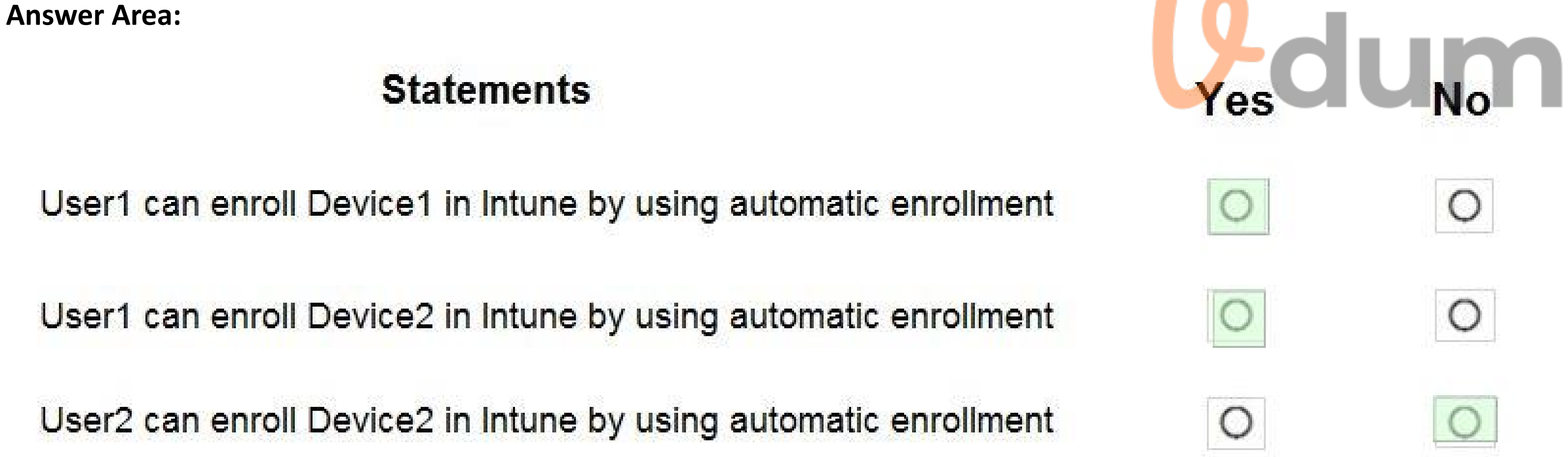
You have a Microsoft 365 E5 tenant that contains two users named User1 and User2 and the groups shown in the following table.
You have a Microsoft Intune enrollment policy that has the following settings:
MDM user scope: Some
Groups: Group1
MAM user scope: Some
Groups: Group2
You purchase the devices shown in the following table.
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:



Statements	Yes	No
User1 can enroll Device1 in Intune by using automatic enrollment	○	○
User1 can enroll Device2 in Intune by using automatic enrollment	○	○
User2 can enroll Device2 in Intune by using automatic enrollment	○	○

Answer Area:

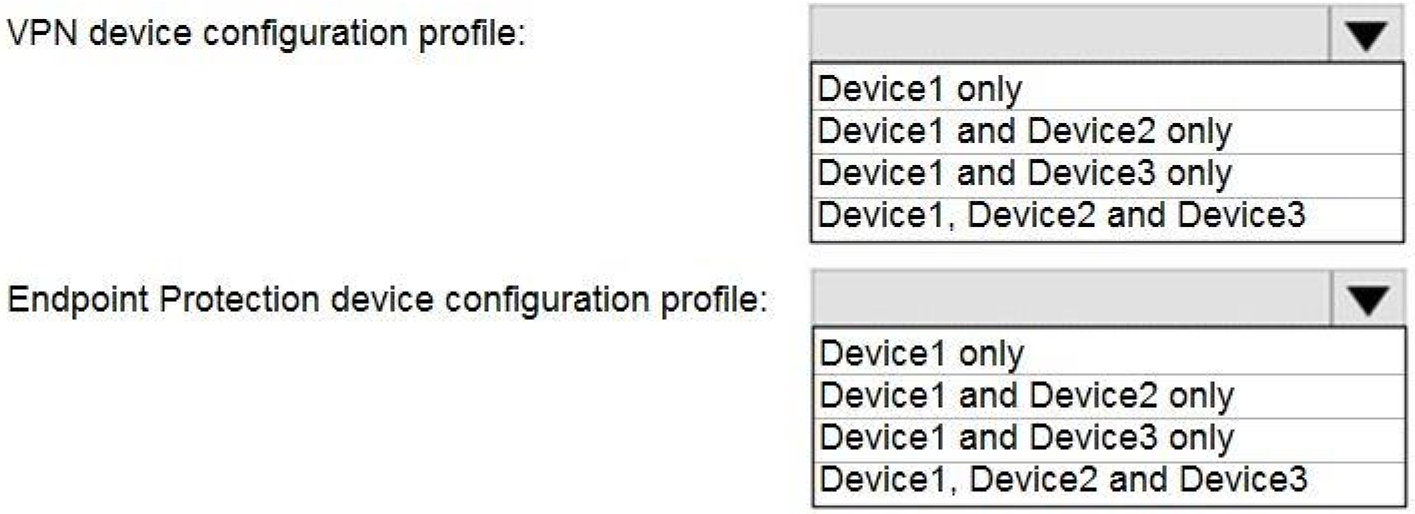


Statements	Yes	No
User1 can enroll Device1 in Intune by using automatic enrollment	[✓ ○]	○
User1 can enroll Device2 in Intune by using automatic enrollment	[✓ ○]	○
User2 can enroll Device2 in Intune by using automatic enrollment	○	[✓ ○]

Section:
Explanation:
https://docs.microsoft.com/en-us/mem/intune/enrollment/windows-enroll
https://docs.microsoft.com/en-us/mem/intune/enrollment/android-enroll-device-administrator

QUESTION 37
HOTSPOT
You have a Microsoft 365 tenant that contains devices enrolled in Microsoft Intune. The devices are configured as shown in the following table.
You plan to perform the following device management tasks in Microsoft Endpoint Manager:
Deploy a VPN connection by using a VPN device configuration profile.
Configure security settings by using an Endpoint Protection device configuration profile.
You support the management tasks.
What should you identify? To answer, select the appropriate options in the answer area.
NOTE: Each correct selection is worth one point.

Hot Area:



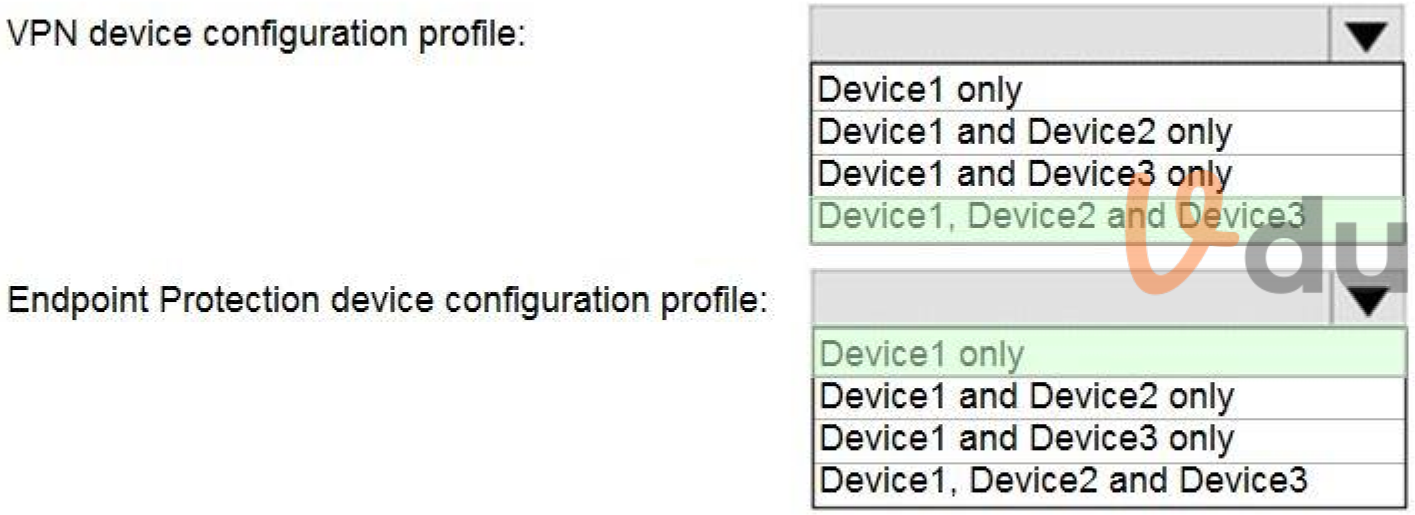
VPN device configuration profile:

- Device1 only
- Device1 and Device2 only
- Device1 and Device3 only
- Device1, Device2 and Device3

Endpoint Protection device configuration profile:

- Device1 only
- Device1 and Device2 only
- Device1 and Device3 only
- Device1, Device2 and Device3

Answer Area:



VPN device configuration profile:

- Device1 only
- Device1 and Device2 only
- Device1 and Device3 only
- [✓ Device1, Device2 and Device3]

Endpoint Protection device configuration profile:

- [✓ Device1 only]
- Device1 and Device2 only
- Device1 and Device3 only
- Device1, Device2 and Device3

Section:
Explanation:
https://docs.microsoft.com/en-us/mem/intune/configuration/vpn-settings-configure
https://docs.microsoft.com/en-us/mem/intune/protect/endpoint-protection-macos

QUESTION 38

DRAG DROP

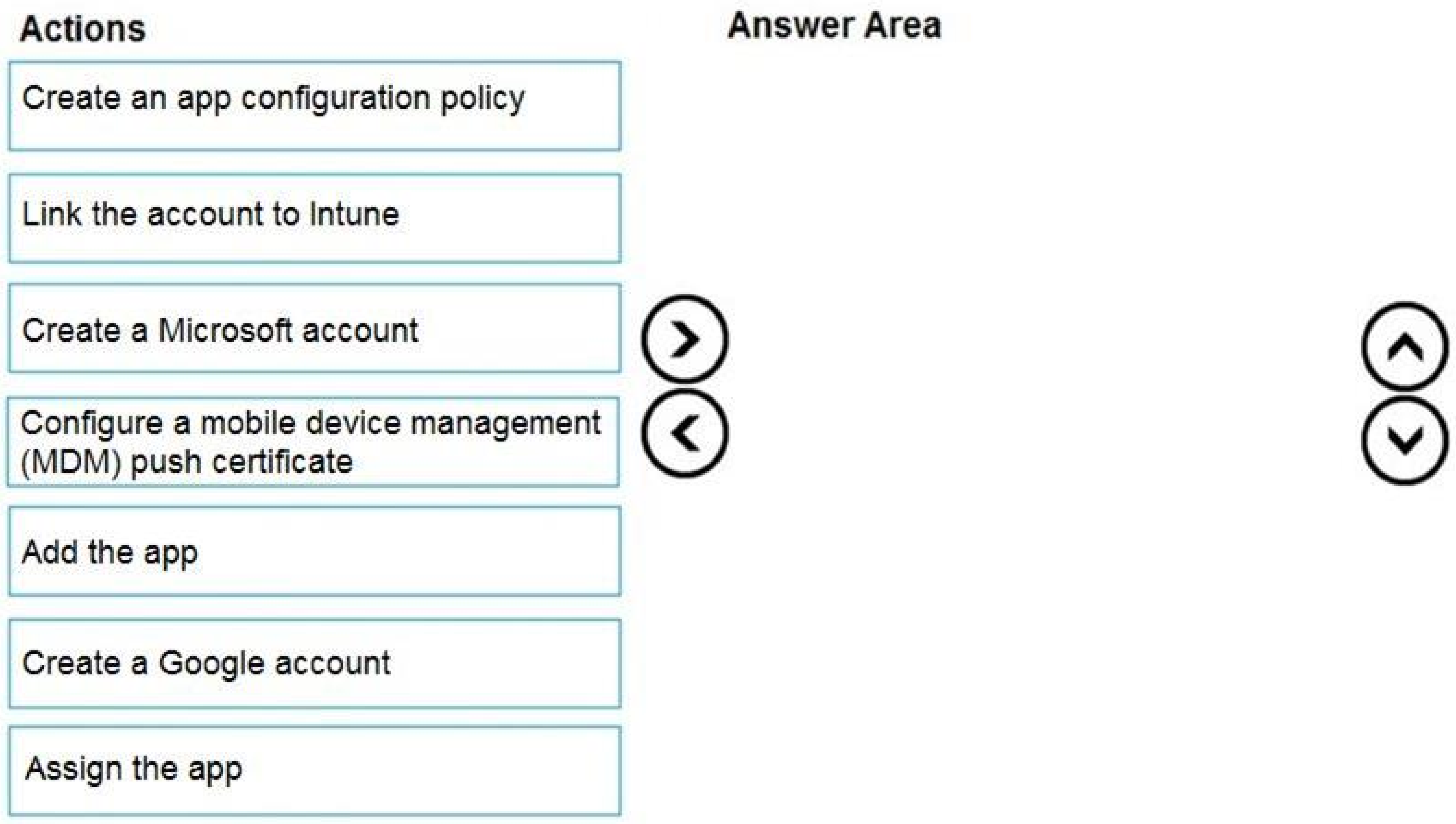
You have a Microsoft 365 E5 tenant that contains 500 Android devices enrolled in Microsoft Intune.

You need to use Microsoft Endpoint Manager to deploy a managed Google Play app to the devices.

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.

https://docs.microsoft.com/en-us/mem/intune/apps/apps-add-android-for-work#assign-a-managed-google-play-app-to-android-enterprise-fully-managed-devices

Select and Place:

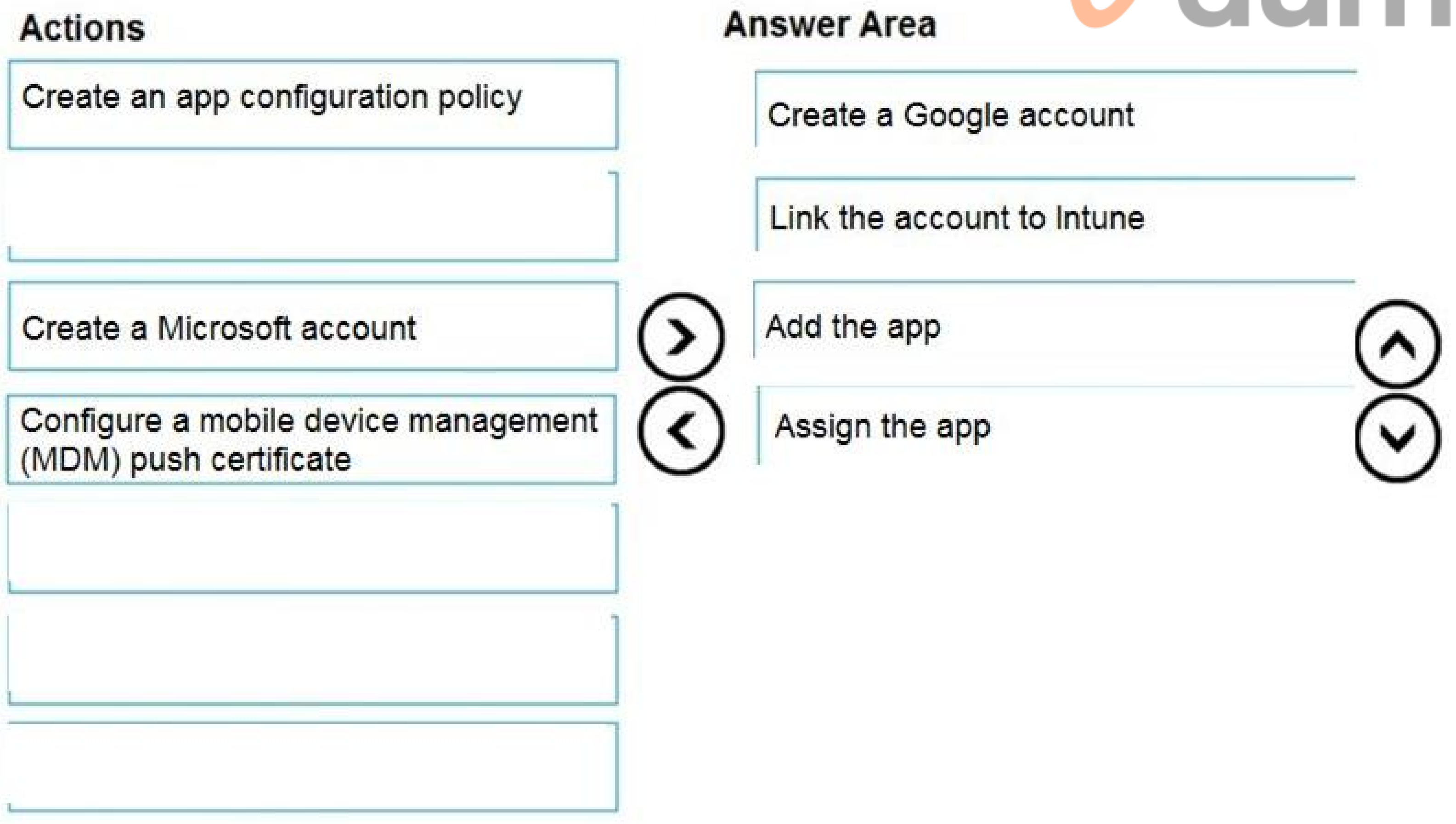


Actions

- Create an app configuration policy
- Link the account to Intune
- Create a Microsoft account
- Configure a mobile device management (MDM) push certificate
- Add the app
- Create a Google account
- Assign the app

Answer Area

Correct Answer:



Actions

- Create an app configuration policy
- Create a Microsoft account
- Configure a mobile device management (MDM) push certificate

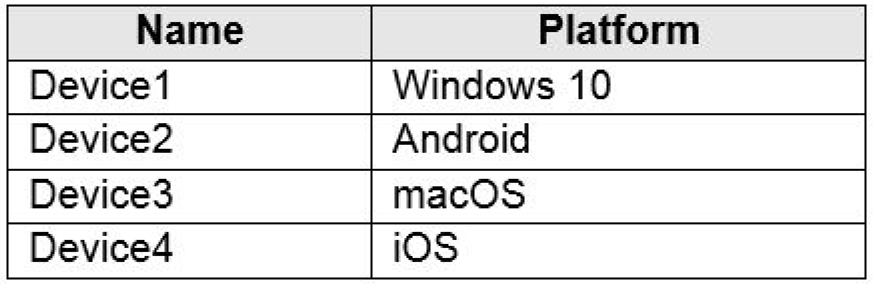
Answer Area

- Create a Google account
- Link the account to Intune
- Add the app
- Assign the app

Section:

Explanation:
https://docs.microsoft.com/en-us/mem/intune/apps/apps-add-android-for-work#assign-a-managed-google-play-app-to-android-enterprise-fully-managed-devices

QUESTION 39
You have a Microsoft 365 E5 tenant that contains four devices enrolled in Microsoft Intune as shown in the following table.



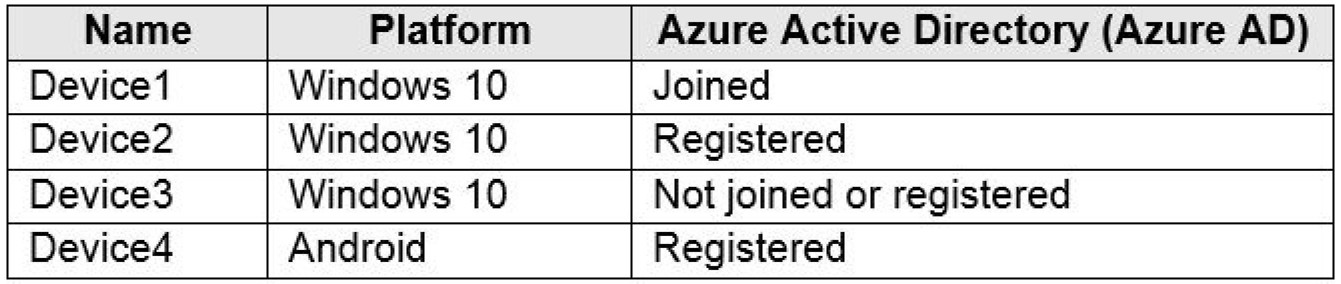
Name	Platform
Device1	Windows 10
Device2	Android
Device3	macOS
Device4	iOS

You plan to deploy Microsoft 365 Apps for enterprise by using Microsoft Endpoint Manager.
To which devices can you deploy Microsoft 365 Apps for enterprise?

A. Device1 only
B. Device1 and Device3 only
C. Device2 and Device4 only
D. Device1, Device2. and Device3 only
E. Device1, Device2, Device3, and Device4

Correct Answer: B
Section:
Explanation:
https://docs.microsoft.com/en-us/mem/intune/apps/apps-add

QUESTION 40
You have a Microsoft 365 E5 tenant that contains the devices shown in the following table.



Name	Platform	Azure Active Directory (Azure AD)
Device1	Windows 10	Joined
Device2	Windows 10	Registered
Device3	Windows 10	Not joined or registered
Device4	Android	Registered

You plan to review device startup performance issues by using Endpoint analytics.
Which devices can you monitor by using Endpoint analytics?

A. Device1 only
B. Device1 and Device2 only
C. Device1, Device2, and Device3 only
D. Device1, Device2, and Device4 only
E. Device1, Device2, Device3, and Device4

Correct Answer: A
Section:
Explanation:

https://docs.microsoft.com/en-us/mem/analytics/overview

QUESTION 41
You have a Microsoft 365 E5 tenant that contains 100 Windows 10 devices.
You plan to deploy a Windows 10 Security Baseline profile that will protect secrets stored in memory.
What should you configure in the profile?

A. Microsoft Defender Credential Guard
B. BitLocker Drive Encryption (BitLocker)
C. Microsoft Defender
D. Microsoft Defender Exploit Guard

Correct Answer: A
Section:

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.
You have a computer that runs Windows 10.
You need to verify which version of Windows 10 is installed.
Solution: From Device Manager, you view the computer properties.
Does this meet the goal?

A. Yes
B. No

Correct Answer: B
Section:
Explanation:
https://support.microsoft.com/en-us/windows/which-version-of-windows-operating-system-am-i-running-628bec99-476a-2c13-5296-9dd081cdd808

QUESTION 43
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 computer that runs Windows 10.
You need to verify which version of Windows 10 is installed.
Solution: At a command prompt, you run the winver.exe command.
Does this meet the goal?

A. Yes
B. No

Correct Answer: A
Section:
Explanation:
https://support.microsoft.com/en-us/windows/which-version-of-windows-operating-system-am-i-running-628bec99-476a-2c13-5296-9dd081cdd808

QUESTION 44

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 computer that runs Windows 10.

You need to verify which version of Windows 10 is installed.

Solution: From the Settings app, you select Update & Security to view the update history.

Does this meet the goal?

A. Yes

B. No

Correct Answer: B

Section:

QUESTION 45

DRAG DROP

Your company has a Microsoft 365 E5 tenant.

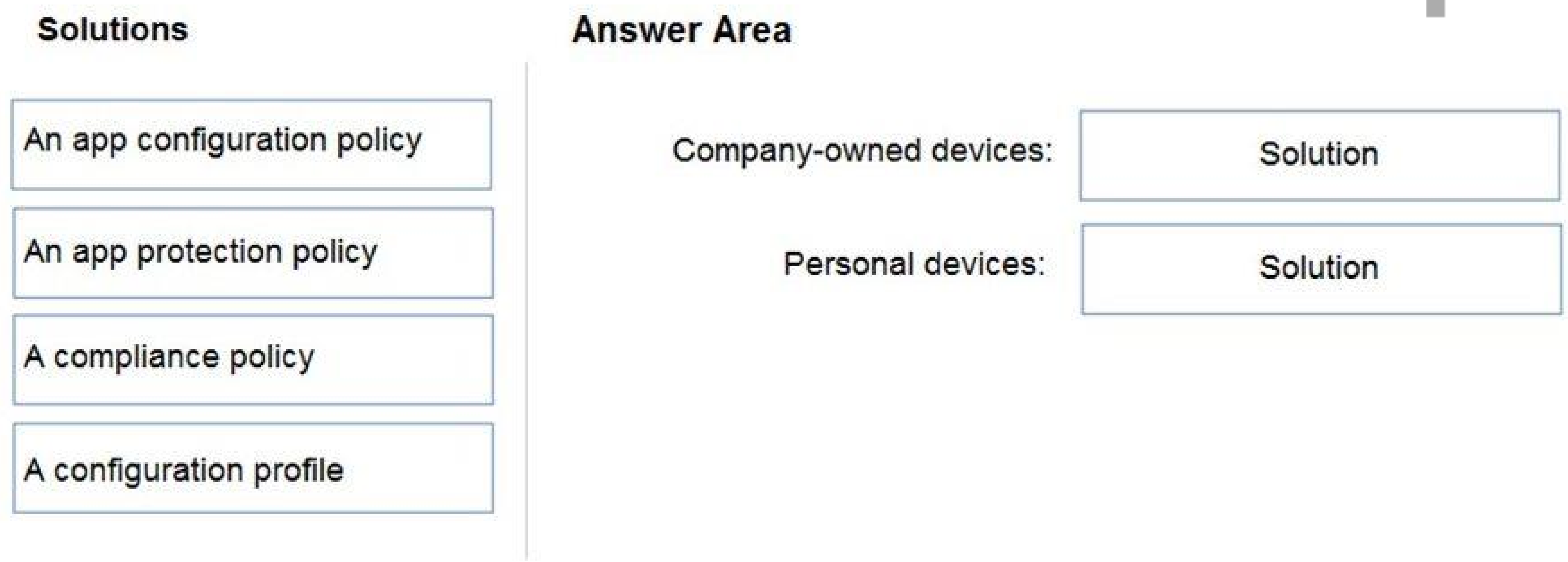
Users access resources in the tenant by using both personal and company-owned Android devices. Company policies requires that the devices have a threat level of medium or lower to access Microsoft Exchange Online mailboxes.

You need to recommend a solution to identify the threat level of the devices and to control access of the devices to the resources.

What should you include in the solution for each device type? To answer, drag the appropriate components to the correct devices. Each component 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:



Solutions

An app configuration policy

An app protection policy

A compliance policy

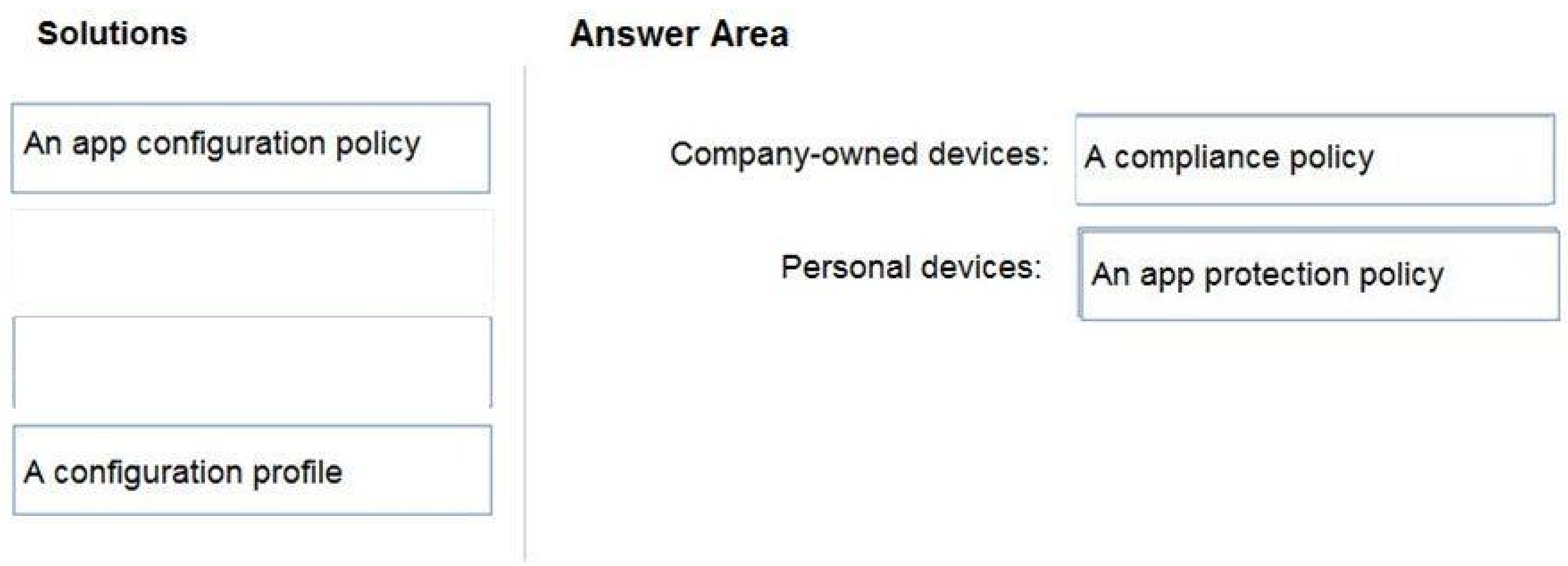
A configuration profile

Answer Area

Company-owned devices: Solution

Personal devices: Solution

Correct Answer:



Solutions

An app configuration policy

A configuration profile

Answer Area

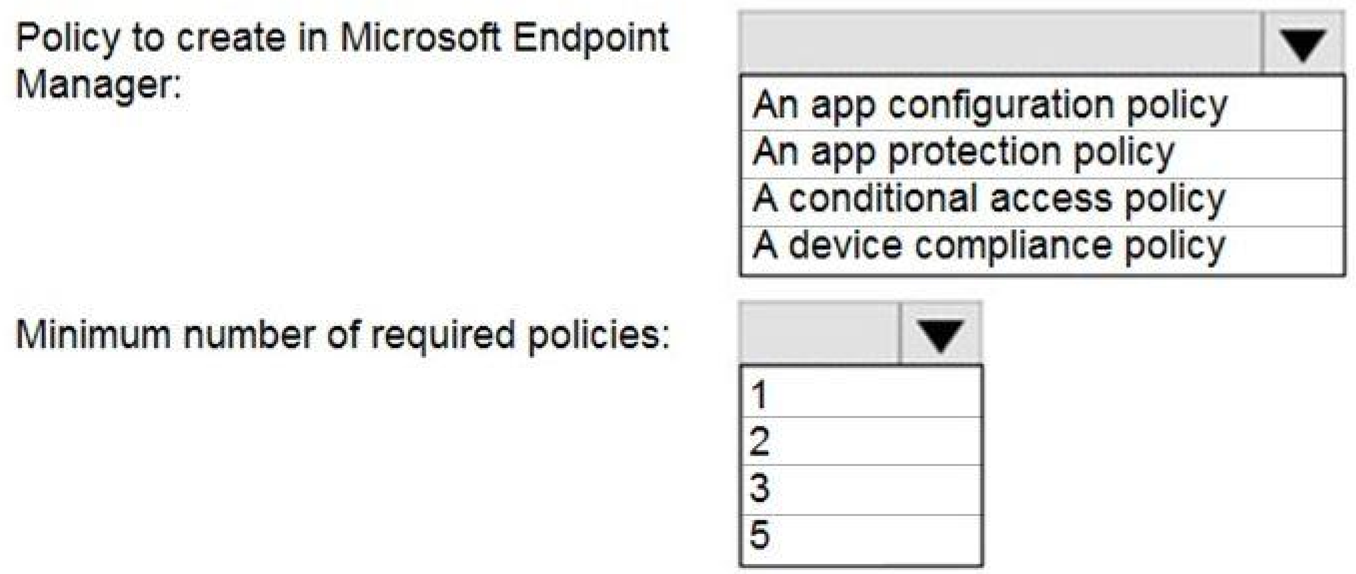
Company-owned devices: A compliance policy

Personal devices: An app protection policy

Section:
Explanation:

QUESTION 46
HOTSPOT
You have a Microsoft 365 E5 tenant that contains five devices enrolled in Microsoft Intune as shown in the following table.
All the devices have an app named App1 installed.
You need to prevent users from copying data from App1 and pasting the data into other apps.
Which policy should you create in Microsoft Endpoint Manager, and what is the minimum number of required policies? To answer, select the appropriate options in the answer area.
NOTE: Each correct selection is worth one point.

Hot Area:



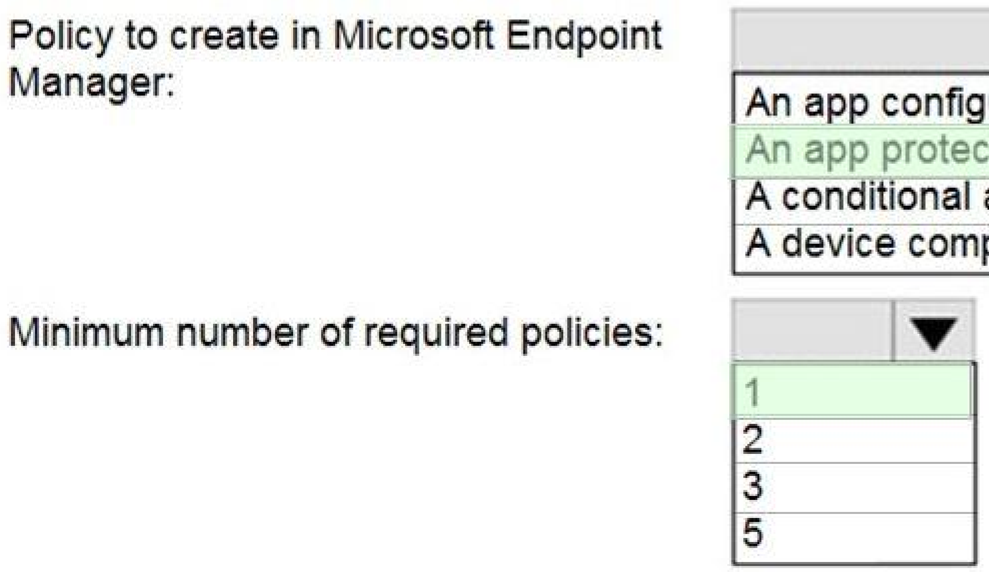
Policy to create in Microsoft Endpoint Manager:

- An app configuration policy
- An app protection policy
- A conditional access policy
- A device compliance policy

Minimum number of required policies:

- 1
- 2
- 3
- 5

Answer Area:



Policy to create in Microsoft Endpoint Manager:

- An app configuration policy
- [✓ An app protection policy]
- A conditional access policy
- A device compliance policy

Minimum number of required policies:

- [✓ 1]
- 2
- 3
- 5

Section:
Explanation:
https://docs.microsoft.com/en-us/mem/intune/apps/app-protection-policy

QUESTION 47
You have a Microsoft 365 tenant.
You plan to manage incidents in the tenant by using the Microsoft 365 security center.
Which Microsoft service source will appear on the Incidents page of the Microsoft 365 security center?

A. Microsoft Cloud App Security
B. Azure Sentinel
C. Azure Web Application Firewall
D. Azure Defender

Correct Answer: A
Section:
Explanation:
https://docs.microsoft.com/en-us/microsoft-365/security/defender/investigate-alerts?view=o365-worldwide

QUESTION 48
You have a Microsoft 365 tenant.
You plan to manage incidents in the tenant by using the Microsoft 365 security center.
Which Microsoft service source will appear on the Incidents page of the Microsoft 365 security center?

A. Microsoft Defender for CloudUse the
B. Microsoft Purview
C. Azure Arc
D. Microsoft Defender for Identity

Correct Answer: D
Section:
Explanation:

https://docs.microsoft.com/en-us/microsoft-365/security/defender/investigate-alerts?view=o365-worldwide

QUESTION 49
You have a Microsoft 365 E5 tenant.
You need to evaluate compliance with European Union privacy regulations for customer data.
What should you do in the Microsoft 365 compliance center?

A. Create a Data Subject Request (DSR)
B. Create a data loss prevention (DLP) policy for General Data Protection Regulation (GDPR) data
C. Create an assessment based on the EU GDPR assessment template
D. Create an assessment based on the Data Protection Baseline assessment template

Correct Answer: C
Section:
Explanation:
https://docs.microsoft.com/en-us/compliance/regulatory/gdpr-action-plan

QUESTION 50
You have a Microsoft 365 E5 tenant.
You need to be notified when emails with attachments that contain sensitive personal data are sent to external recipients.
Which two policies can you use? Each correct answer presents a complete solution.
NOTE: Each correct selection is worth one point.

A. a data loss prevention (DLP) policy
B. a sensitivity label policy
C. a Microsoft Cloud App Security file policy
D. a communication compliance policy
E. a retention label policy

Correct Answer: A, D
Section:

QUESTION 51
You have a Microsoft 365 E5 tenant.
You create an auto-labeling policy to encrypt emails that contain a sensitive info type. You specify the locations where the policy will be applied.
You need to deploy the policy.
What should you do first?

A. Review the sensitive information in Activity explorer
B. Turn on the policy
C. Run the policy in simulation mode
D. Configure Azure Information Protection analytics

Correct Answer: C
Section:
Explanation:
https://docs.microsoft.com/en-us/microsoft-365/compliance/apply-sensitivity-label-automatically?view=o365-worldwide

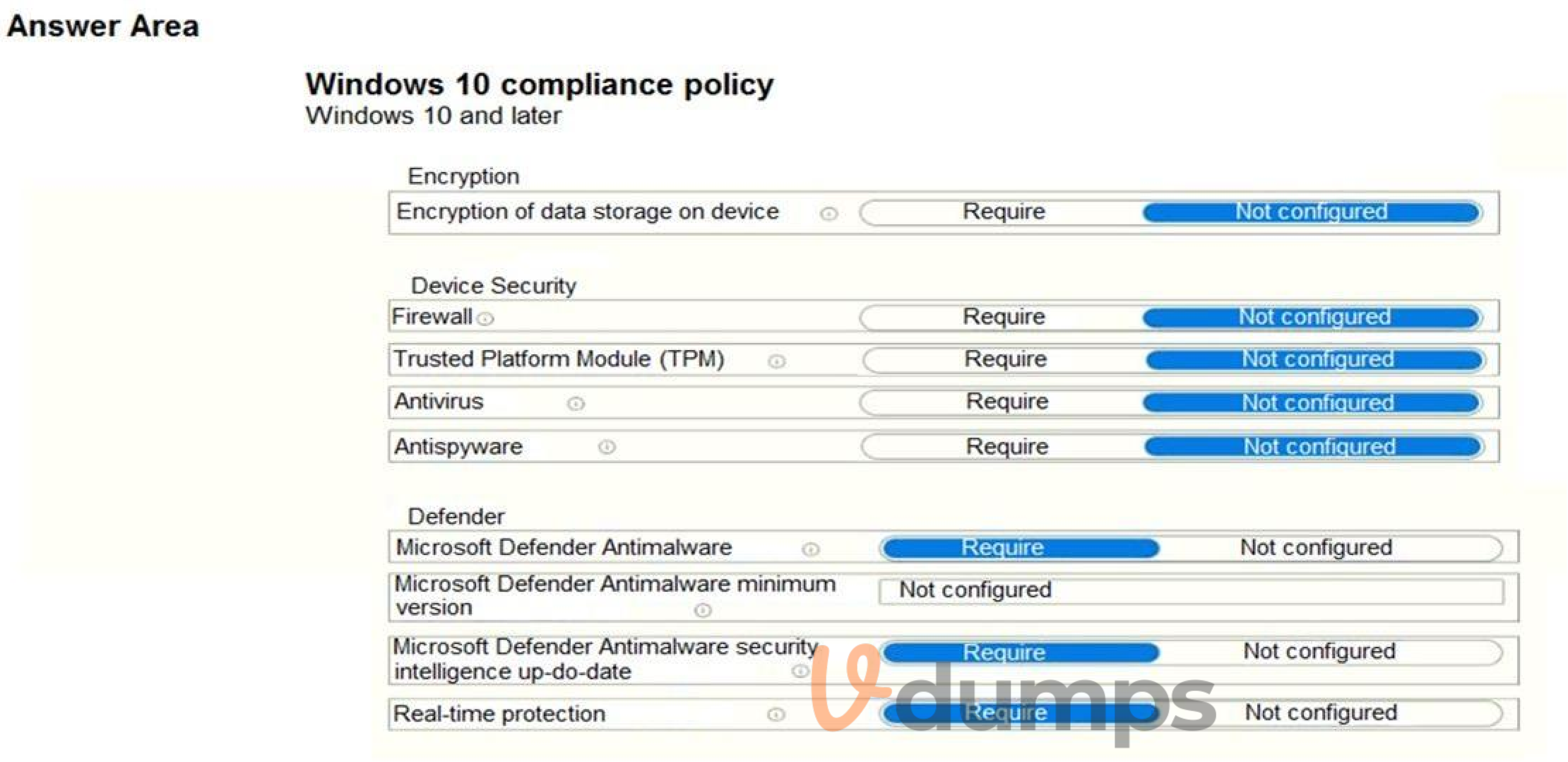
QUESTION 52
You have a Microsoft 365 tenant and a LinkedIn company page.
You plan to archive data from the LinkedIn page to Microsoft 365 by using the LinkedIn connector.
Where can you store data from the LinkedIn connector?

A. a Microsoft OneDrive for Business folder
B. a Microsoft SharePoint Online document library
C. a Microsoft 365 mailbox
D. Azure Files

Correct Answer: C
Section:
Explanation:
https://docs.microsoft.com/en-us/microsoft-365/compliance/archive-linkedin-data?view=o365-worldwide

QUESTION 53
HOTSPOT
You have a Microsoft 365 E5 tenant that contains 500 Windows 10 devices and a Windows 10 compliance policy.
You deploy a third-party antivirus solution to the devices.
You need to ensure that the devices are marked as compliant.
Which three settings should you modify in the compliance policy? To answer, select the appropriate settings in the answer area.
NOTE: Each correct selection is worth one point.

Hot Area:



Answer Area

Windows 10 compliance policy

Windows 10 and later

Encryption

Encryption of data storage on device	Require [✓ Not configured]

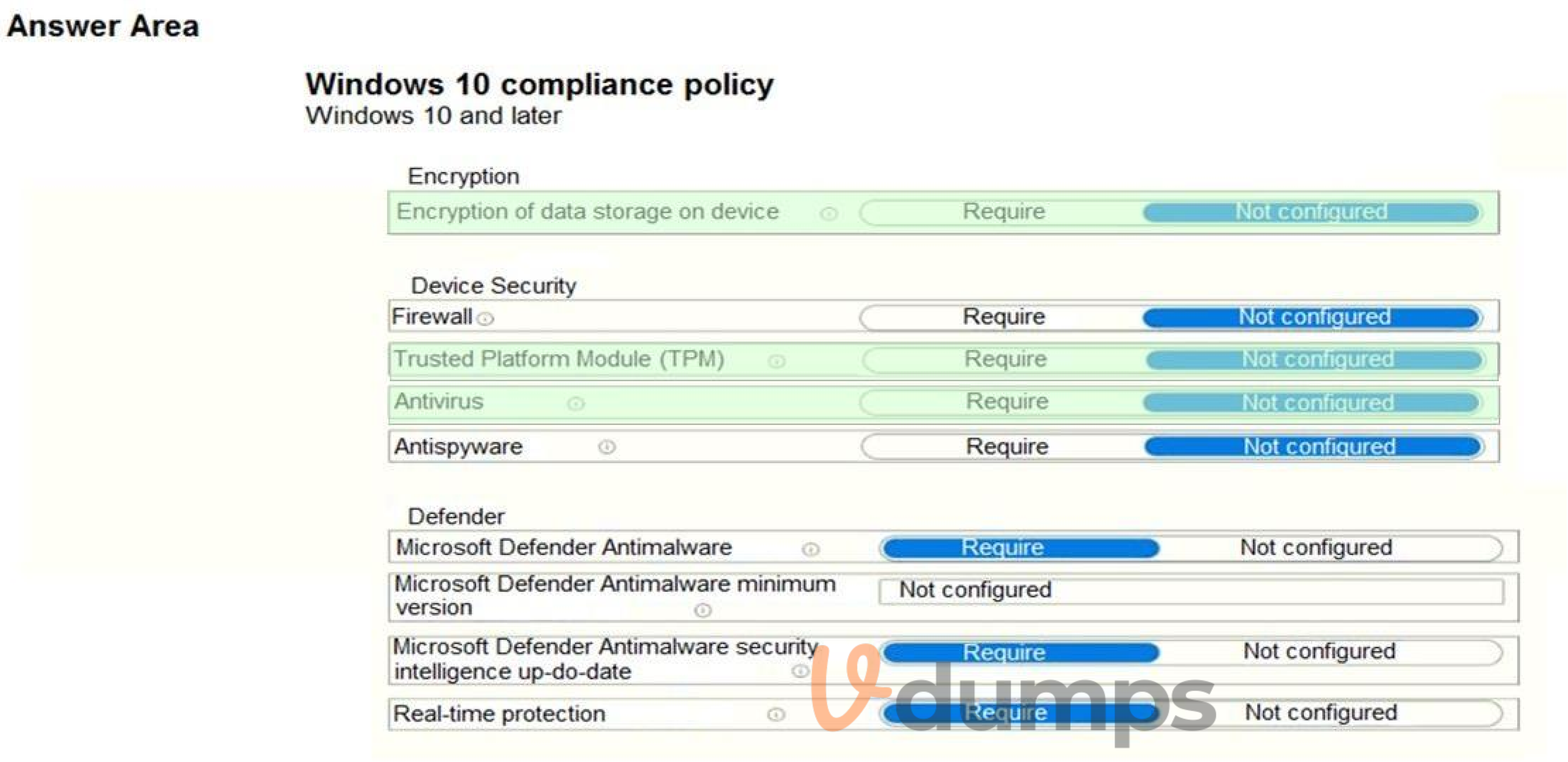
Device Security

Firewall	Require [✓ Not configured]
Trusted Platform Module (TPM)	Require [✓ Not configured]
Antivirus	Require [✓ Not configured]
Antispyware	Require [✓ Not configured]

Defender

Microsoft Defender Antimalware	[✓ Require] Not configured
Microsoft Defender Antimalware minimum version	Not configured
Microsoft Defender Antimalware security intelligence up-do-date	[✓ Require] Not configured
Real-time protection	[✓ Require] Not configured

Answer Area:



Answer Area

Windows 10 compliance policy

Windows 10 and later

Encryption

Encryption of data storage on device	Require [✓ Not configured]

Device Security

Firewall	Require [✓ Not configured]
Trusted Platform Module (TPM)	Require [✓ Not configured]
Antivirus	Require [✓ Not configured]
Antispyware	Require [✓ Not configured]

Defender

Microsoft Defender Antimalware	[✓ Require] Not configured
Microsoft Defender Antimalware minimum version	Not configured
Microsoft Defender Antimalware security intelligence up-do-date	[✓ Require] Not configured
Real-time protection	[✓ Require] Not configured

Section:

Explanation:

https://docs.microsoft.com/en-us/mem/intune/protect/compliance-policy-create-windows

QUESTION 54

You have an Azure AD tenant.

You have 1,000 computers that run Windows 10 Pro and are joined to Azure AD.

You purchase a Microsoft 365 E3 subscription.

You need to deploy Windows 10 Enterprise to the computers. The solution must minimize administrative effort.

What should you do?

A. From the Microsoft Endpoinf Manager admin center, create a Windows Autopilot deployment profile. Assign the profile to all the computers. Instruct users to restart their computer and perform a network restart.

B. Enroll the computers in Microsoft Intune. Create a configuration profile by using the Edition upgrade and mode switch template. From the Microsoft Endpoint Manager admin center, assign the profile to all the computers and instruct users to restart their computer.

C. From Windows Configuration Designer, create a provisioning package that has an EditionUpgrade configuration and upload the package to a Microsoft SharePoint Online site. Instruct users to run the provisioning package from SharePoint Online.

D. From the Azure Active Directory admin center, create a security group that has dynamic device membership. Assign licenses to the group and instruct users to sign in to their computer.

Correct Answer: B

Section:

QUESTION 55

HOTSPOT

Your company has a Microsoft 365 E5 tenant.

Users at the company use the following versions of Microsoft Office:

* Microsoft 365 Apps for enterprise

* Office for the web

* Office 2016

* Office 2019

The company currently uses the following Office file types:

* .docx

* .xlsx

* .doc

* xls

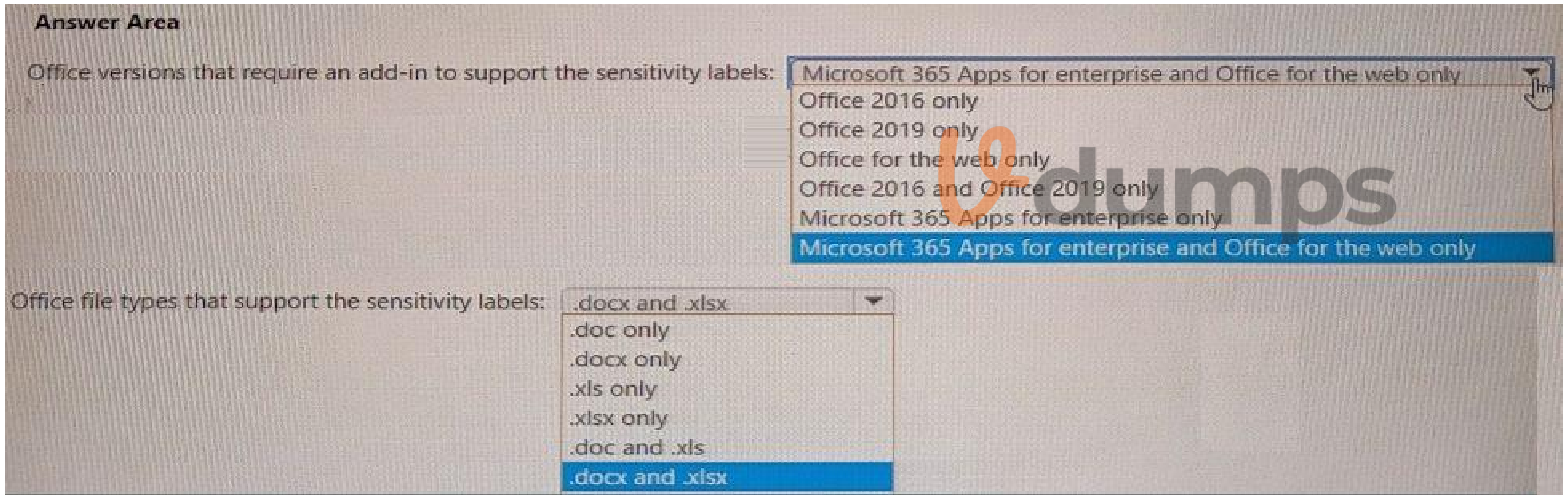
You plan to use sensitivity labels. You need to identify the following:

* Which versions of Office require an add-in to support the sensitivity labels.

* Which file types support the sensitivity labels.

What should you identify? To answer, select the appropriate options in the answer area, NOTE: Each correct selection is worth one point.

Hot Area:



Answer Area

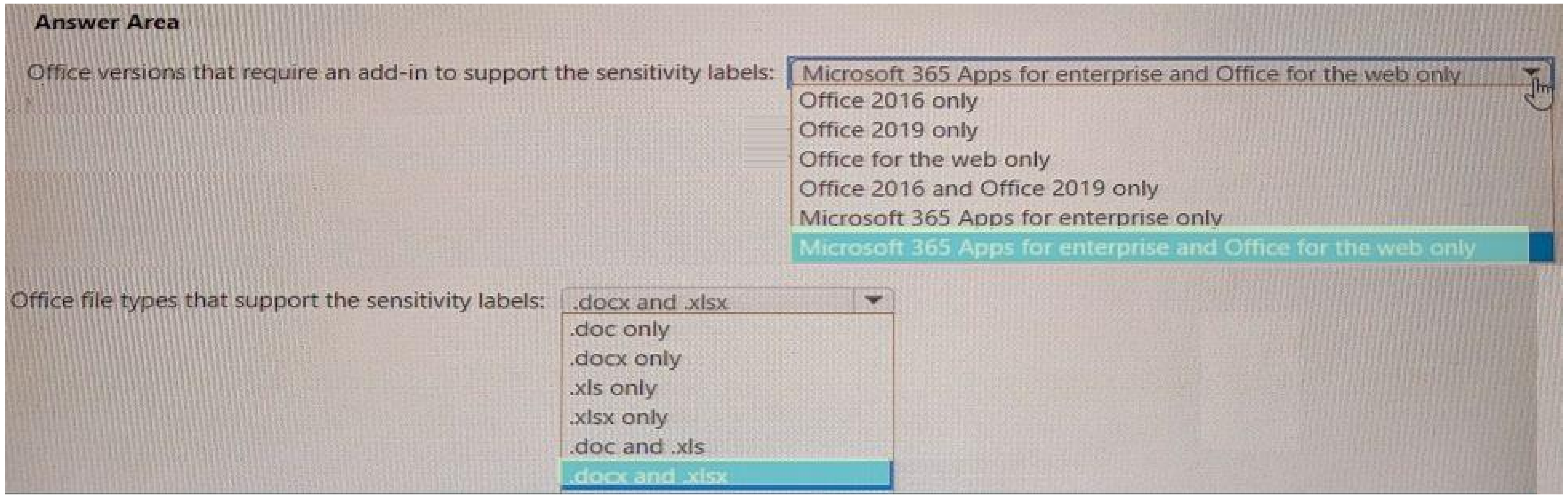
Office versions that require an add-in to support the sensitivity labels: Microsoft 365 Apps for enterprise and Office for the web only

Office 2016 only
Office 2019 only
Office for the web only
Office 2016 and Office 2019 only
Microsoft 365 Apps for enterprise only
Microsoft 365 Apps for enterprise and Office for the web only

Office file types that support the sensitivity labels: .docx and .xlsx

.doc only
.docx only
.xls only
.xlsx only
.doc and .xls
.docx and .xlsx

Answer Area:



Answer Area

Office versions that require an add-in to support the sensitivity labels: Microsoft 365 Apps for enterprise and Office for the web only

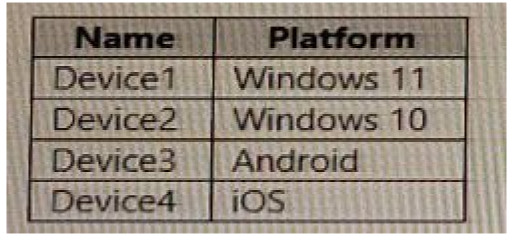
Office 2016 only
Office 2019 only
Office for the web only
Office 2016 and Office 2019 only
Microsoft 365 Apps for enterprise only
Microsoft 365 Apps for enterprise and Office for the web only

Office file types that support the sensitivity labels: .docx and .xlsx

.doc only
.docx only
.xls only
.xlsx only
.doc and .xls
.docx and .xlsx

Section:
Explanation:

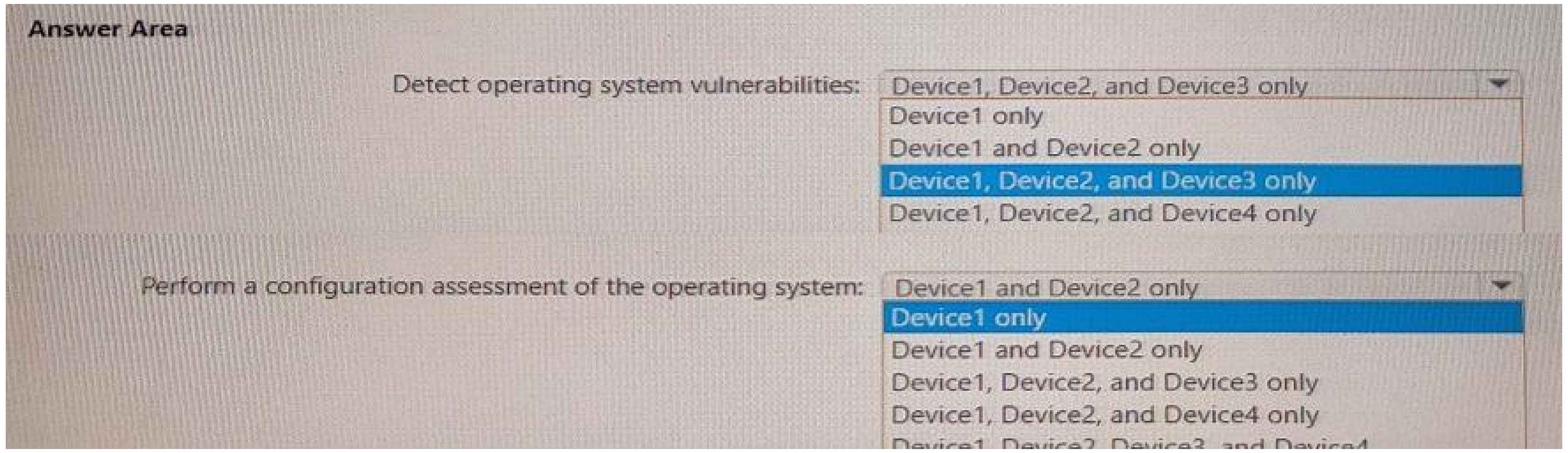
QUESTION 56
HOTSPOT
You have a Microsoft 365 E5 subscription that contains the devices shown in the following table.



Name	Platform
Device1	Windows 11
Device2	Windows 10
Device3	Android
Device4	iOS

All the devices are onboarded To Microsoft Defender for Endpoint
You plan to use Microsoft Defender Vulnerability Management to meet the following requirements:
* Detect operating system vulnerabilities.

Hot Area:



Answer Area

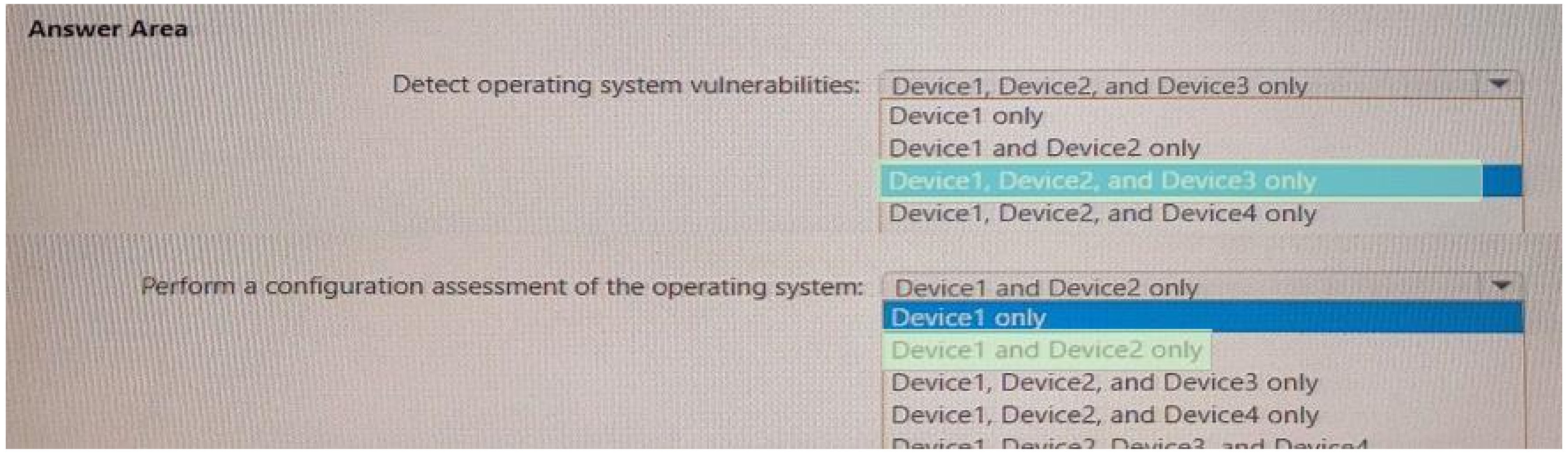
Detect operating system vulnerabilities: Device1, Device2, and Device3 only

Device1 only
Device1 and Device2 only
Device1, Device2, and Device3 only
Device1, Device2, and Device4 only

Perform a configuration assessment of the operating system: Device1 and Device2 only

Device1 only
Device1 and Device2 only
Device1, Device2, and Device3 only
Device1, Device2, and Device4 only
Device1, Device2, Device3, and Device4

Answer Area:



Answer Area

Detect operating system vulnerabilities: Device1, Device2, and Device3 only

- Device1 only
- Device1 and Device2 only
- Device1, Device2, and Device3 only
- Device1, Device2, and Device4 only

Perform a configuration assessment of the operating system: Device1 and Device2 only

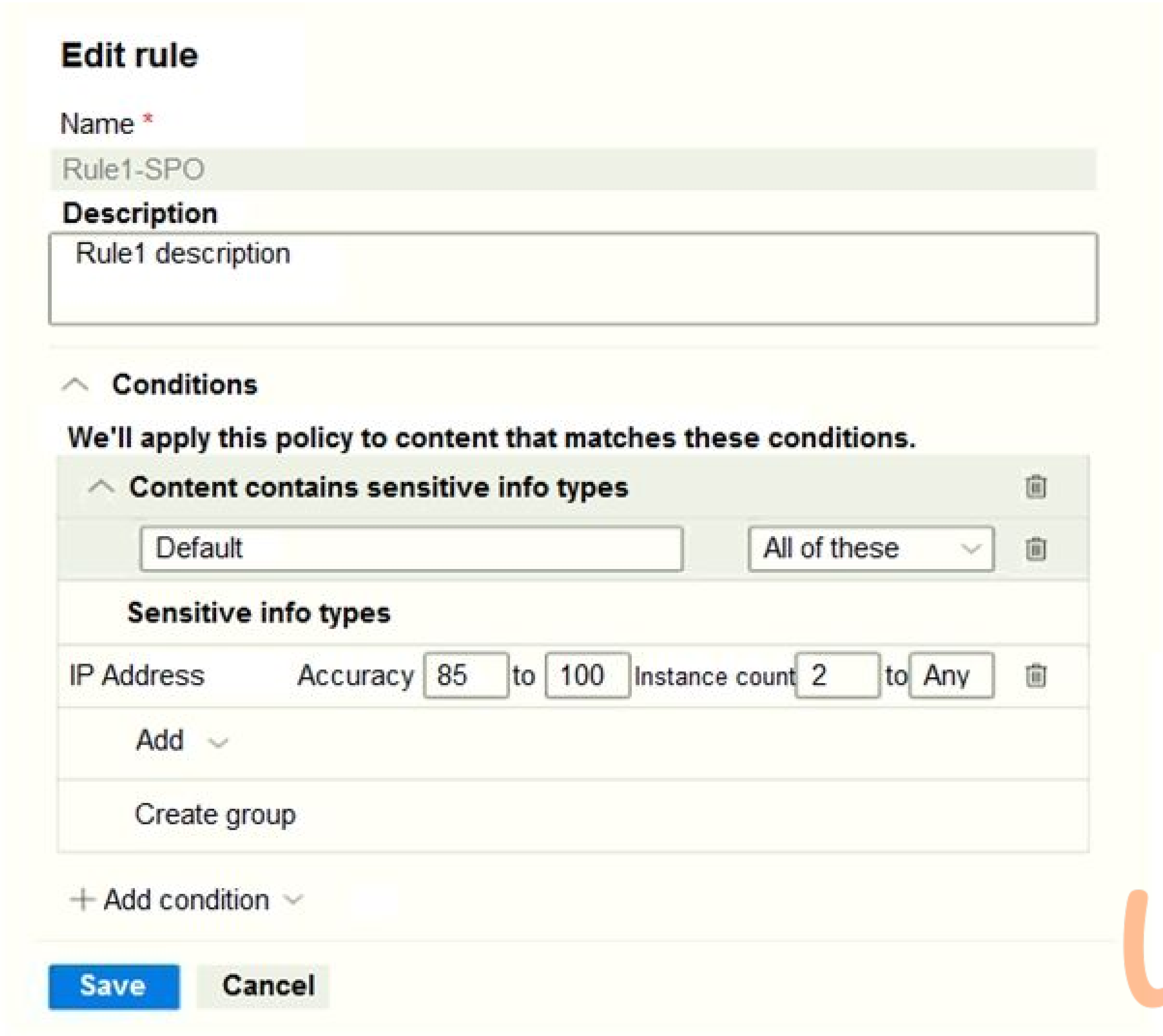
- Device1 only
- Device1 and Device2 only
- Device1, Device2, and Device3 only
- Device1, Device2, and Device4 only
- Device1, Device2, Device3, and Device4

Section:
Explanation:

QUESTION 57
HOTSPOT
You have a Microsoft 365 E5 tenant that contains a Microsoft SharePoint Online site named Site1. Site1 contains the files shown in the following table.

Name	Number of IP addresses in the file
File1.docx	1
File2.txt	2
File3.xlsx	5

You create a sensitivity label named Sensitivity1 and an auto-label policy that has the following configurations:
Name: AutoLabel1
Label to auto-apply: Sensitivity1
Rules for SharePoint Online sites: Rule1-SPO
Choose locations where you want to apply the label: Site1
Rule1-SPO is configured as shown in the following exhibit.



Edit rule

Name *

Rule1-SPO

Description

Rule1 description

Conditions

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

Content contains sensitive info types

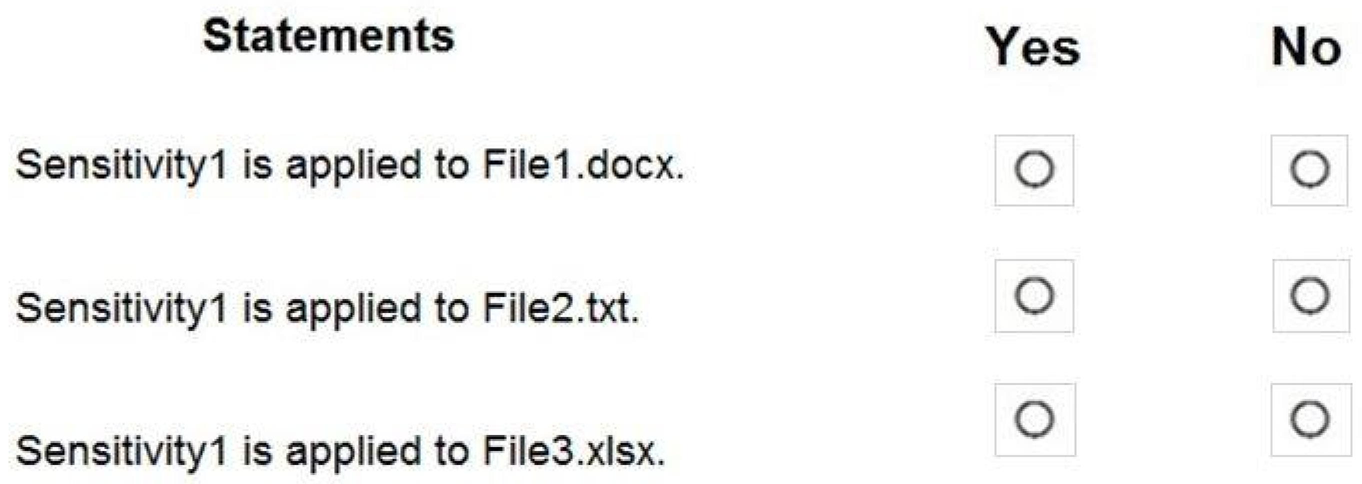
Default — All of these

Sensitive info types

IP Address Accuracy 85 to 100 Instance count 2 to Any

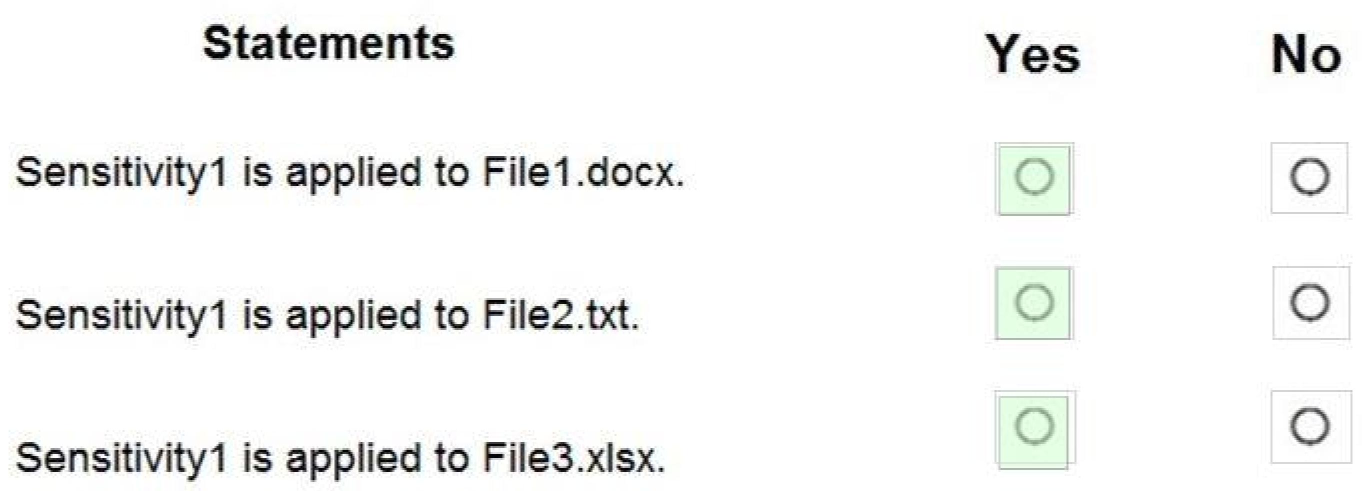
For each of the following statements, select Yes if the statement is true. Otherwise, select No.
NOTE: Each correct selection is worth one point.

Hot Area:



Statements	Yes	No
Sensitivity1 is applied to File1.docx.	○	○
Sensitivity1 is applied to File2.txt.	○	○
Sensitivity1 is applied to File3.xlsx.	○	○

Answer Area:



Statements	Yes	No
Sensitivity1 is applied to File1.docx.	[✓ ○]	○
Sensitivity1 is applied to File2.txt.	[✓ ○]	○
Sensitivity1 is applied to File3.xlsx.	[✓ ○]	○

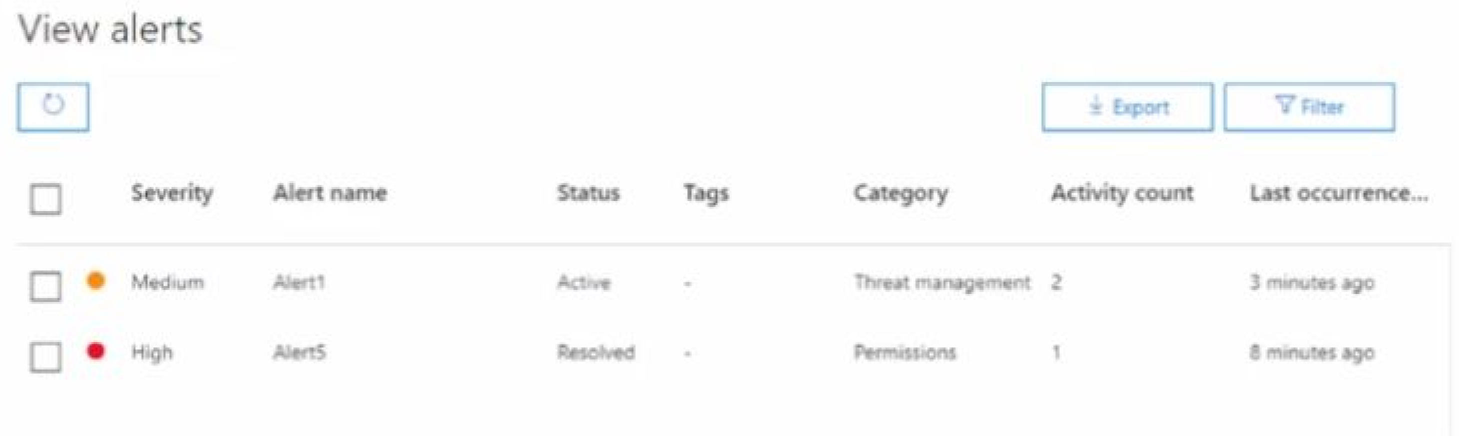
Section:
Explanation:
https://docs.microsoft.com/en-us/microsoft-365/compliance/apply-sensitivity-label-automatically?view=o365-worldwide
https://docs.microsoft.com/en-us/microsoft-365/compliance/sensitivity-labels?view=o365-worldwide

QUESTION 58
You plan to use Azure Sentinel and Microsoft Cloud App Security. You need to connect Cloud App Security to Azure Sentinel.
What should you do in the Cloud App Security admin center?

A. From Automatic log upload, add a log collector.
B. From Automatic log upload, add a data source.
C. From Connected apps, add an app connector.
D. From Security extension, add a SIEM agent.

Correct Answer: D
Section:

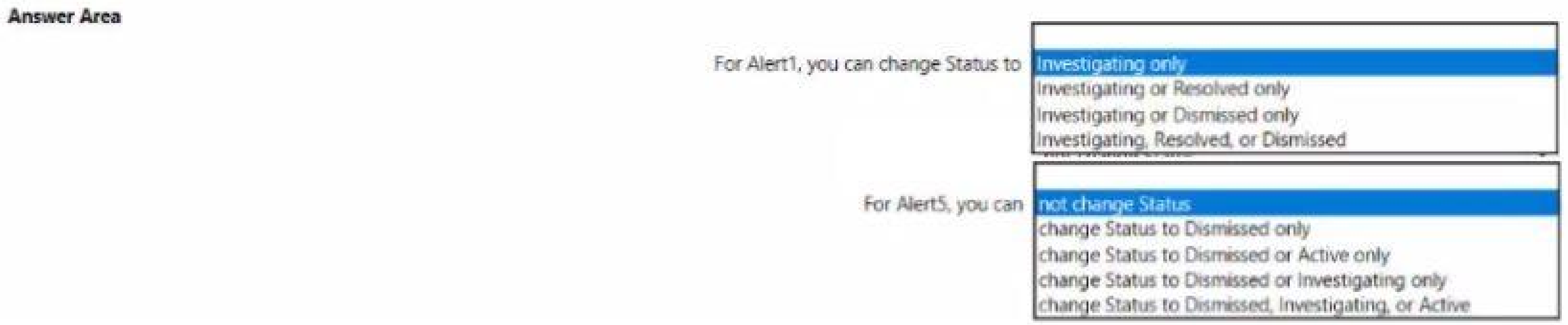
QUESTION 59
HOTSPOT
You have a Microsoft 365 ES tenant.
You have the alerts shown in the following exhibit.



□	Severity	Alert name	Status	Tags	Category	Activity count	Last occurrence...
□	● Medium	Alert1	Active	-	Threat management	2	3 minutes ago
□	● High	Alert5	Resolved	-	Permissions	1	8 minutes ago

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

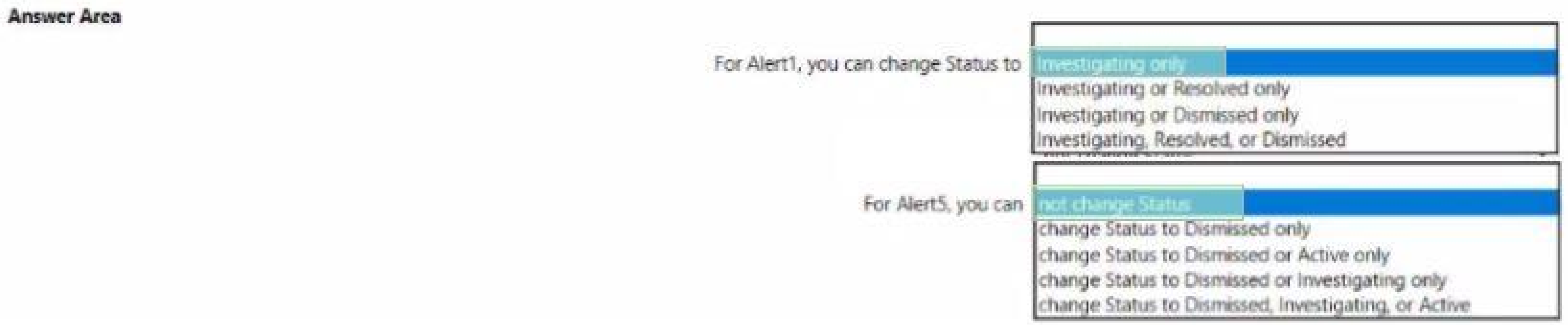
For Alert1, you can change Status to

- Investigating only
- Investigating or Resolved only
- Investigating or Dismissed only
- Investigating, Resolved, or Dismissed

For Alert5, you can

- not change Status
- change Status to Dismissed only
- change Status to Dismissed or Active only
- change Status to Dismissed or Investigating only
- change Status to Dismissed, Investigating, or Active

Answer Area:



Answer Area

For Alert1, you can change Status to

- Investigating only
- Investigating or Resolved only
- Investigating or Dismissed only
- Investigating, Resolved, or Dismissed

For Alert5, you can

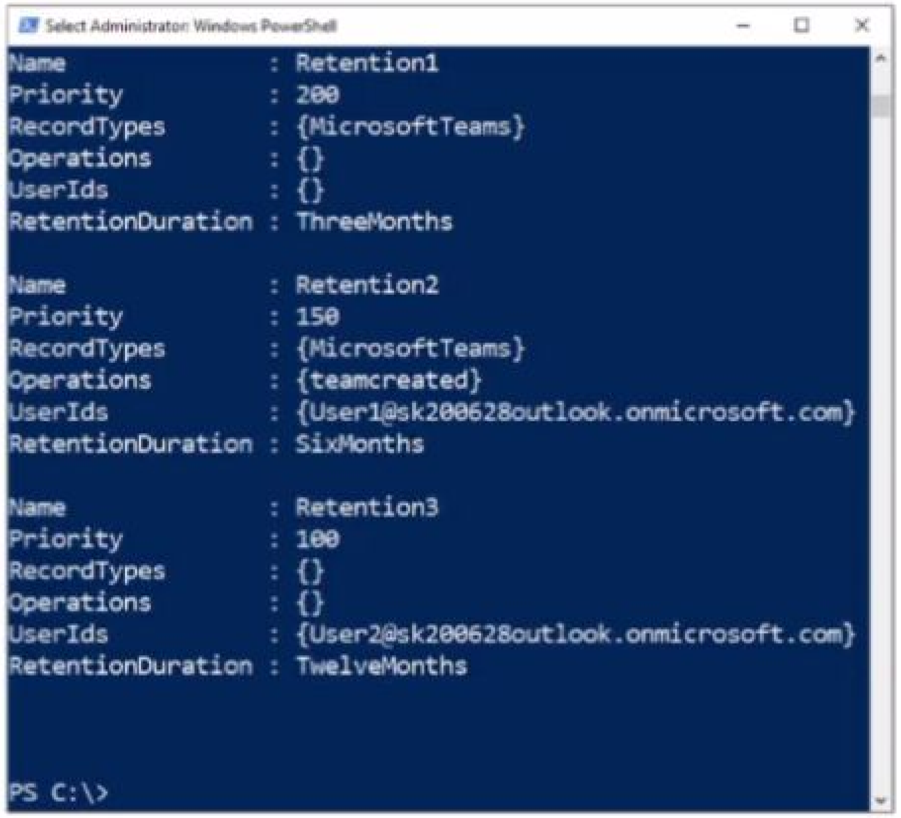
- not change Status
- change Status to Dismissed only
- change Status to Dismissed or Active only
- change Status to Dismissed or Investigating only
- change Status to Dismissed, Investigating, or Active

Section:
Explanation:

QUESTION 60

HOTSPOT

You have a Microsoft 365 ES subscription that has three auto retention policies as show in the following exhibit.

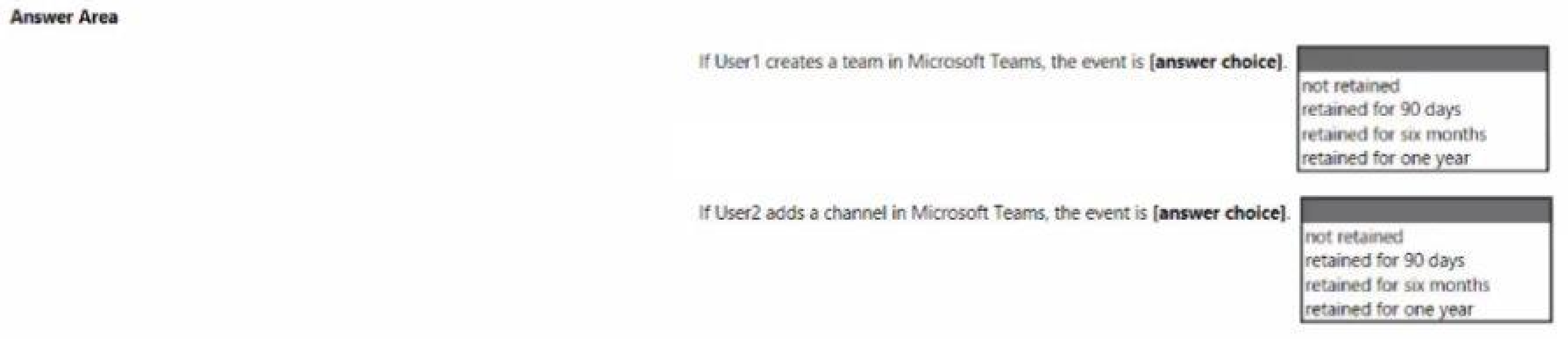


Select Administrator: Windows PowerShell

```
Name              : Retention1
Priority          : 200
RecordTypes       : {MicrosoftTeams}
Operations        : {}
UserIds           : {}
RetentionDuration : ThreeMonths

Name              : Retention2
Priority          : 150
RecordTypes       : {MicrosoftTeams}
Operations        : {teamcreated}
UserIds           : {User1@sk200628outlook.onmicrosoft.com}
RetentionDuration : SixMonths

Name              : Retention3
Priority          : 100
RecordTypes       : {}
Operations        : {}
UserIds           : {User2@sk200628outlook.onmicrosoft.com}
RetentionDuration : TwelveMonths


PS C:\>
```

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

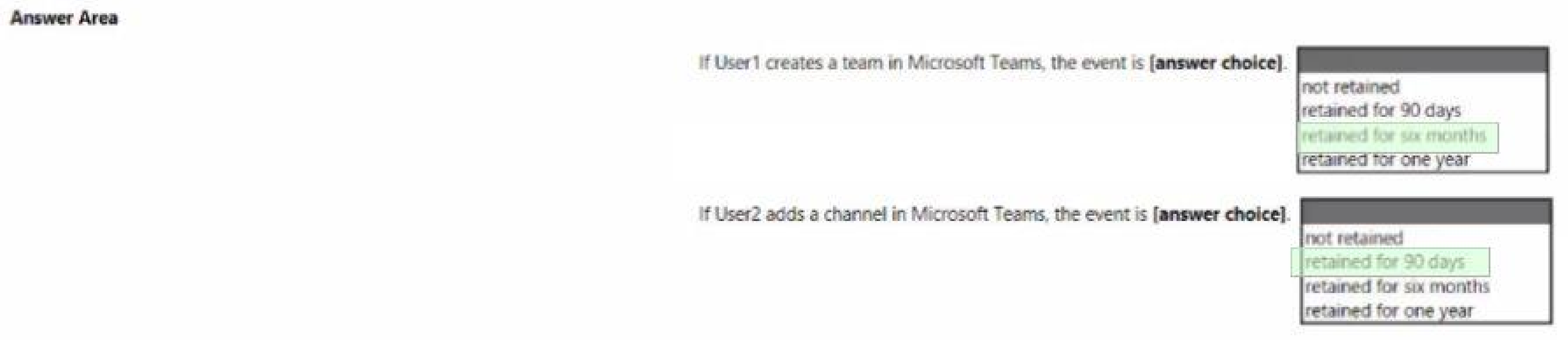
If User1 creates a team in Microsoft Teams, the event is **[answer choice]**.

- not retained
- retained for 90 days
- retained for six months
- retained for one year

If User2 adds a channel in Microsoft Teams, the event is **[answer choice]**.

- not retained
- retained for 90 days
- retained for six months
- retained for one year

Answer Area:



Answer Area

If User1 creates a team in Microsoft Teams, the event is **[answer choice]**.

- not retained
- retained for 90 days
- [✓ retained for six months]
- retained for one year

If User2 adds a channel in Microsoft Teams, the event is **[answer choice]**.

- not retained
- [✓ retained for 90 days]
- retained for six months
- retained for one year

Section:
Explanation:

QUESTION 61

HOTSPOT

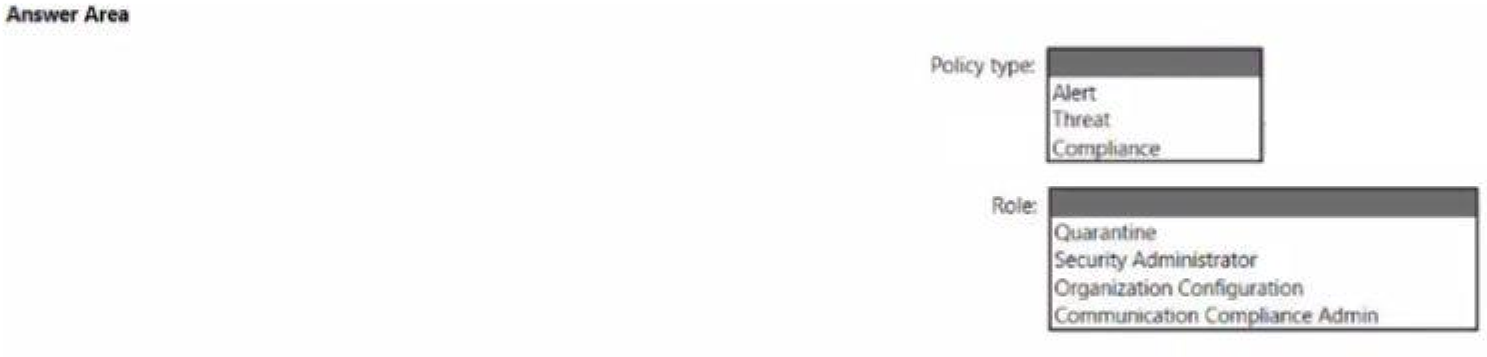
You have a Microsoft 365 E5 tenant.

You need to ensure that administrators are notified when a user receives an email message that contains malware. The solution must use the principle of least privilege.

Which type of policy should you create and which Microsoft 365 compliance center role is required to create the pokey? To answer, select the appropriate options in the answer area.

NOTE: Each correct selection is worth one point.

Hot Area:



Answer Area

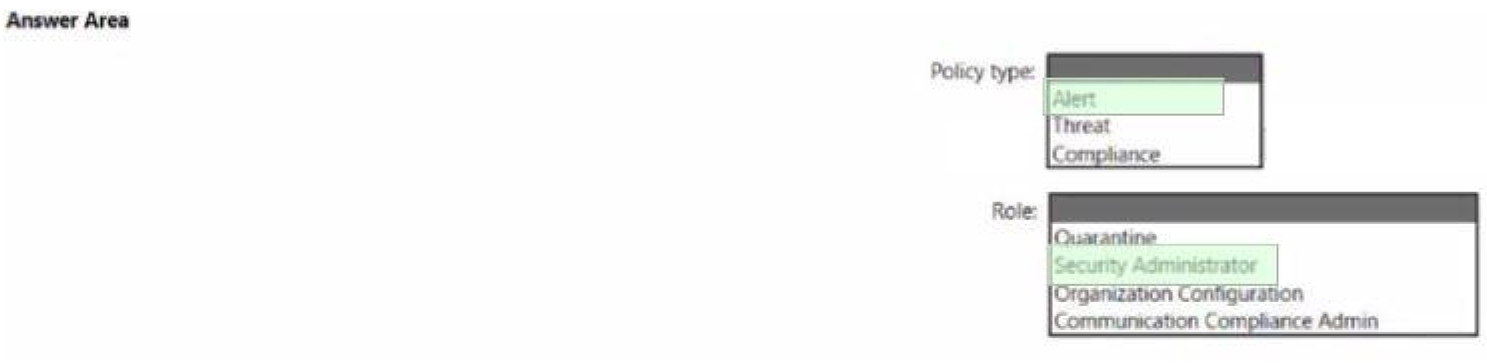
Policy type:

- Alert
- Threat
- Compliance

Role:

- Quarantine
- Security Administrator
- Organization Configuration
- Communication Compliance Admin

Answer Area:



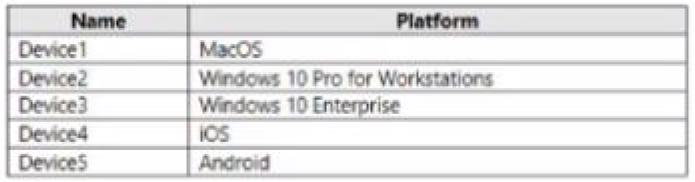
Answer Area

Policy type:
- [✓ Alert]
- Threat
- Compliance

Role:
- Quarantine
- [✓ Security Administrator]
- Organization Configuration
- Communication Compliance Admin

Section:
Explanation:

QUESTION 62
You have a Microsoft 365 tenant that contains devices registered for mobile device management. The devices are configured as shown in the following table.



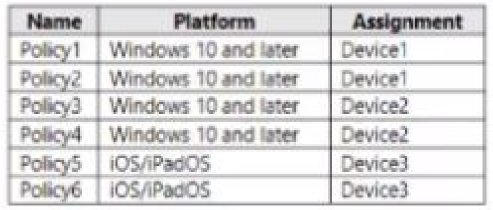
Name	Platform
Device1	MacOS
Device2	Windows 10 Pro for Workstations
Device3	Windows 10 Enterprise
Device4	iOS
Device5	Android

You plan to enable VPN access for the devices.
What is the minimum number of configuration policies required?

A. 3
B. 5
C. 4
D. 1

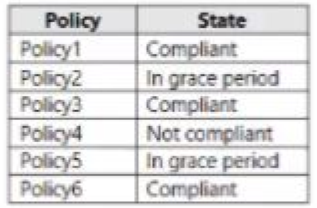
Correct Answer: D
Section:

QUESTION 63
HOTSPOT
You have device compliance policies shown in the following table.



Name	Platform	Assignment
Policy1	Windows 10 and later	Device1
Policy2	Windows 10 and later	Device1
Policy3	Windows 10 and later	Device2
Policy4	Windows 10 and later	Device2
Policy5	iOS/iPadOS	Device3
Policy6	iOS/iPadOS	Device3

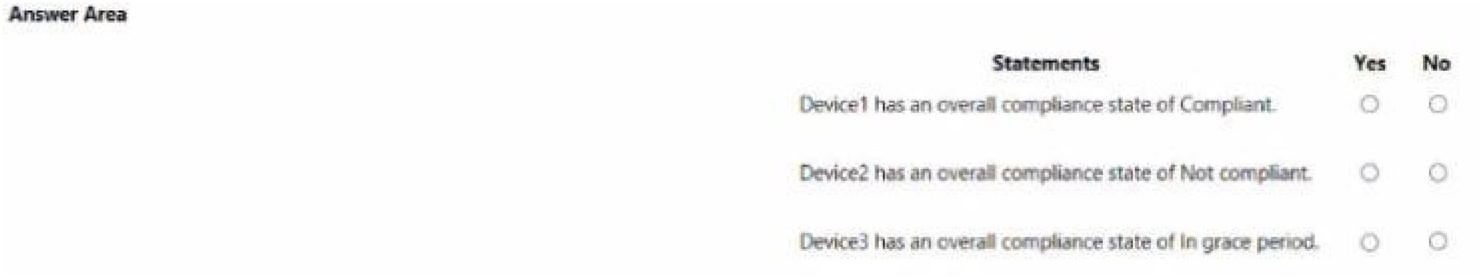
The device compliance state for each policy is shown in the following table.



Policy	State
Policy1	Compliant
Policy2	In grace period
Policy3	Compliant
Policy4	Not compliant
Policy5	In grace period
Policy6	Compliant

NOTE: Each correct selection is worth one point.

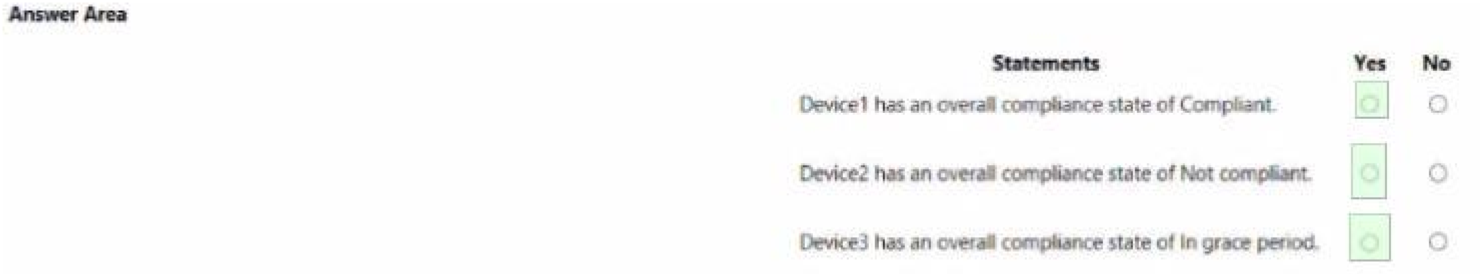
Hot Area:



Answer Area

Statements	Yes	No
Device1 has an overall compliance state of Compliant.	○	○
Device2 has an overall compliance state of Not compliant.	○	○
Device3 has an overall compliance state of In grace period.	○	○

Answer Area:



Answer Area

Statements	Yes	No
Device1 has an overall compliance state of Compliant.	☑	○
Device2 has an overall compliance state of Not compliant.	☑	○
Device3 has an overall compliance state of In grace period.	☑	○

Section:
Explanation:

QUESTION 64

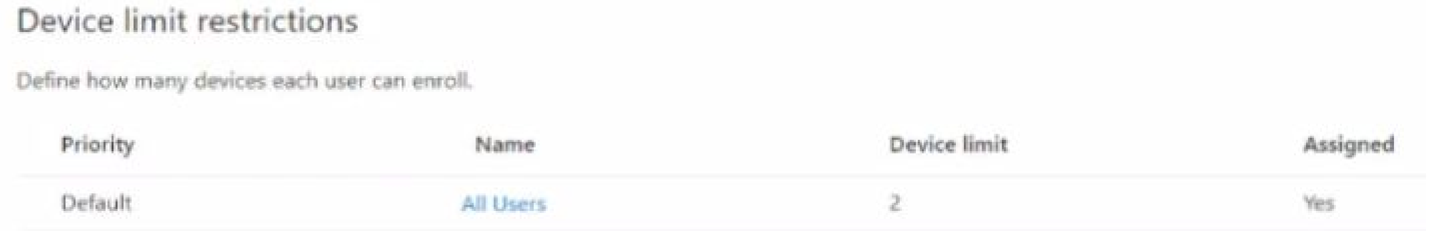
You have a Microsoft 365 E5 tenant that contains 500 Windows 10 devices. The devices are enrolled in Microsoft intune.
You plan to use Endpoint analytics to identify hardware issues.
You need to enable Window health monitoring on the devices to support Endpoint analytics
What should you do?

A. Configure the Endpoint analytics baseline regression threshold.
B. Create a configuration profile.
C. Create a Windows 10 Security Baseline profile
D. Create a compliance policy.

Correct Answer: B
Section:

QUESTION 65

HOTSPOT
You have 2,500 Windows 10 devices and a Microsoft 365 E5 tenant that contains two users named User1 and User2. The devices are not enrollment in Microsoft Intune.
In Microsoft Endpoint Manager, the Device limit restrictions are configured as shown in the following exhibit.

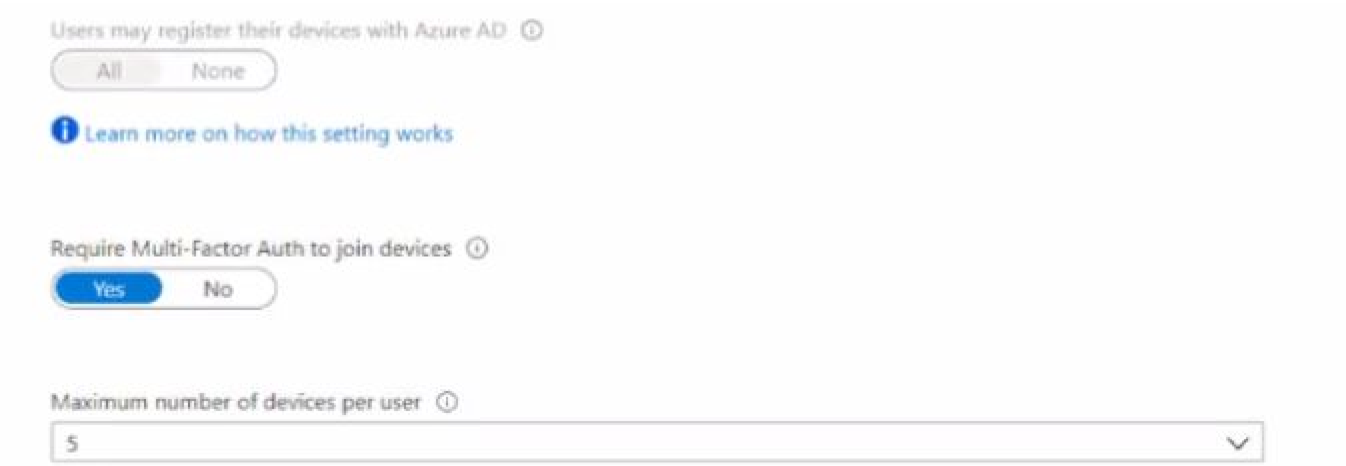


Device limit restrictions

Define how many devices each user can enroll.

Priority	Name	Device limit	Assigned
Default	All Users	2	Yes

In Azure Active Directory (Azure AD), the Device settings are configured as shown in the following exhibit.



Users may register their devices with Azure AD ⓘ

All None

Learn more on how this setting works

Require Multi-Factor Auth to join devices ⓘ

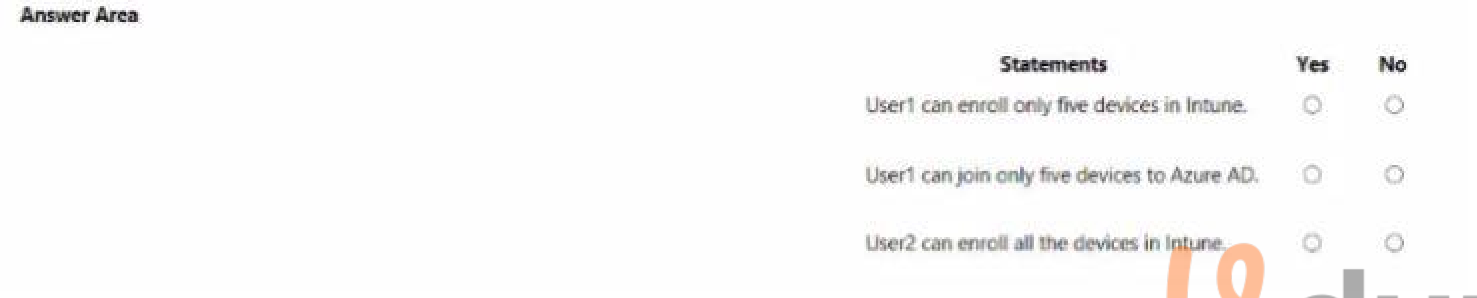
[✓ Yes] No

Maximum number of devices per user ⓘ

5

From Microsoft Endpoint Manager, you add User2 as a device enrollment manager (DEM).
For each of the following statement, select Yes if the statement is true. Otherwise, select No.
NOTE: Each correct selection is worth one point.

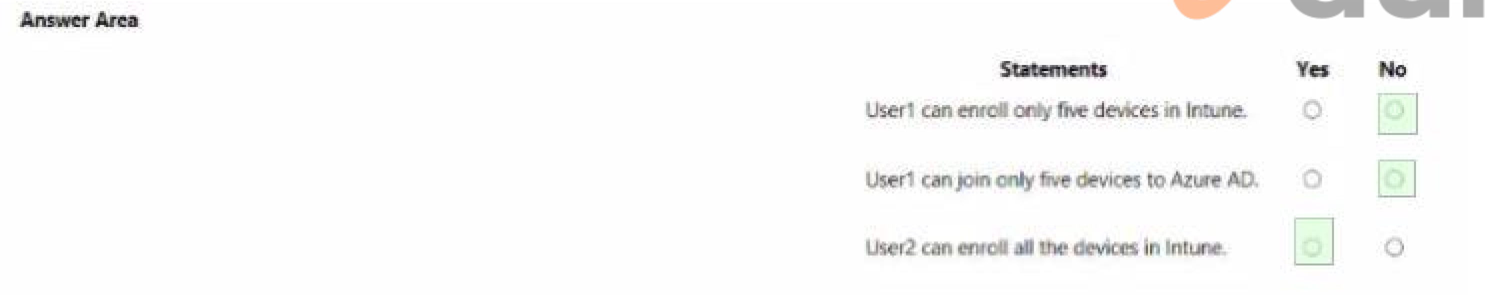
Hot Area:



Answer Area

Statements	Yes	No
User1 can enroll only five devices in Intune.	○	○
User1 can join only five devices to Azure AD.	○	○
User2 can enroll all the devices in Intune.	○	○

Answer Area:



Answer Area

Statements	Yes	No
User1 can enroll only five devices in Intune.	○	[✓ ○]
User1 can join only five devices to Azure AD.	○	[✓ ○]
User2 can enroll all the devices in Intune.	[✓ ○]	○

Section:
Explanation:

QUESTION 66
You have a Microsoft 365 tenant.
You plan to implement Endpoint Protection device configuration profiles.
Which platform can you manage by using the profile?

A. Android
B. CentOS Linux
C. iOS
D. Window 10

Correct Answer: D
Section:

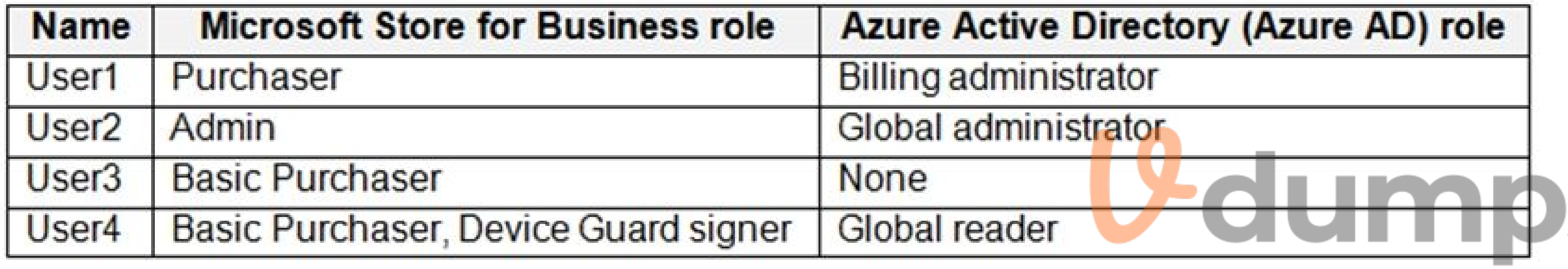
Explanation:
https://docs.microsoft.com/en-us/mem/intune/protect/endpoint-protection-configure

QUESTION 67
You purchase a new computer that has Windows 10, version 2004 preinstalled.
You need to ensure that the computer is up-to-date. The solution must minimize the number of updates installed.
What should you do on the computer?

A. Install all the feature updates released since version 2004 and all the quality updates released since version 2004 only.
B. install the West feature update and the latest quality update only.
C. install all the feature updates released since version 2004 and the latest quality update only.
D. install the latest feature update and all the quality updates released since version 2004.

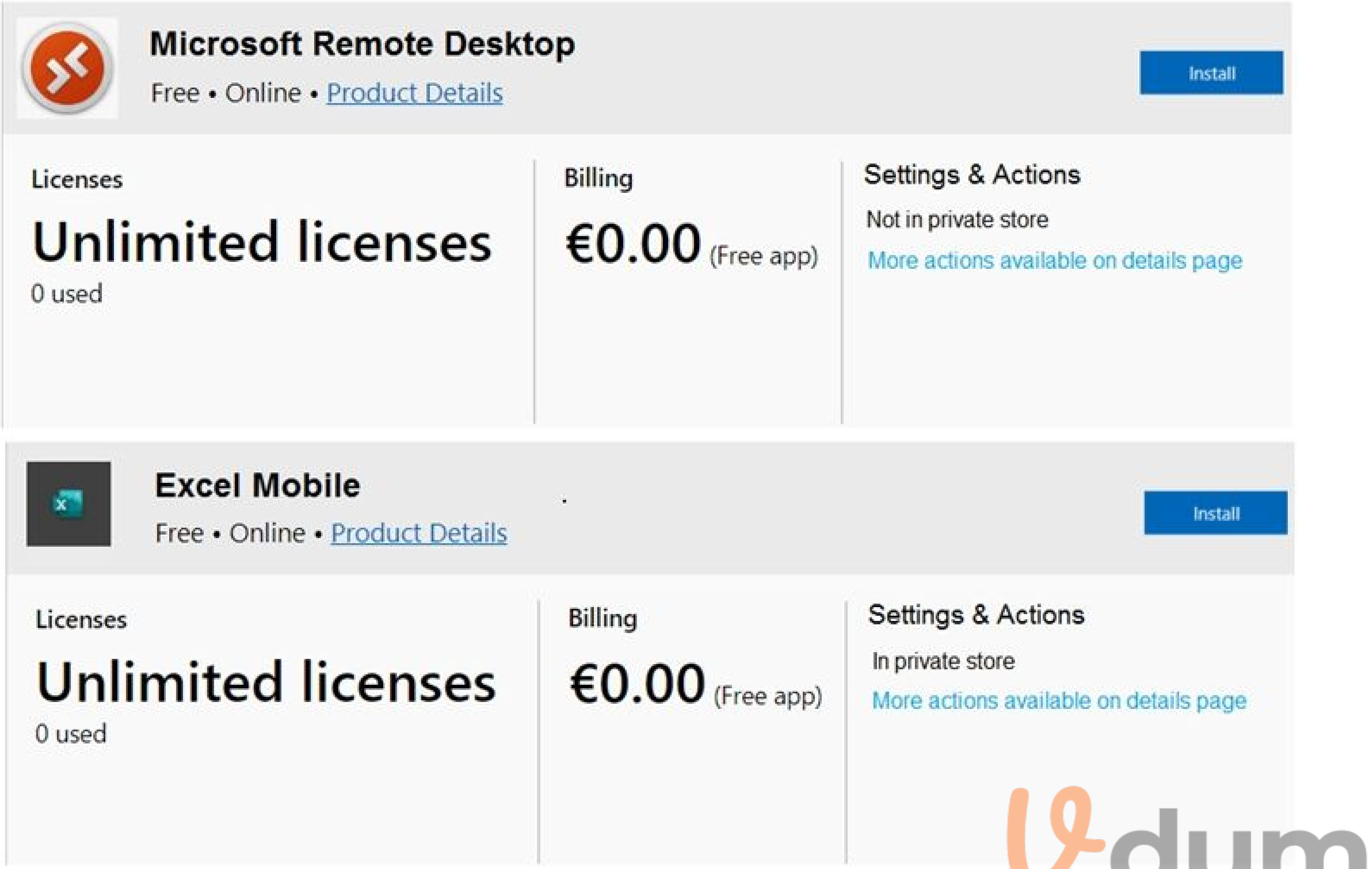
Correct Answer: B
Section:

QUESTION 68
HOTSPOT
You have a Microsoft 365 tenant that is signed up for Microsoft Store for Business and contains the users shown in the following table.



Name	Microsoft Store for Business role	Azure Active Directory (Azure AD) role
User1	Purchaser	Billing administrator
User2	Admin	Global administrator
User3	Basic Purchaser	None
User4	Basic Purchaser, Device Guard signer	Global reader

All users have Windows 10 Enterprise devices.
The Products & services settings in Microsoft Store for Business are shown in the following exhibit.



Microsoft Remote Desktop

Free • Online • Product Details

Licenses

Unlimited licenses

0 used

Billing

€0.00 (Free app)

Settings & Actions

Not in private store

More actions available on details page

Excel Mobile

Free • Online • Product Details

Licenses

Unlimited licenses

0 used

Billing

€0.00 (Free app)

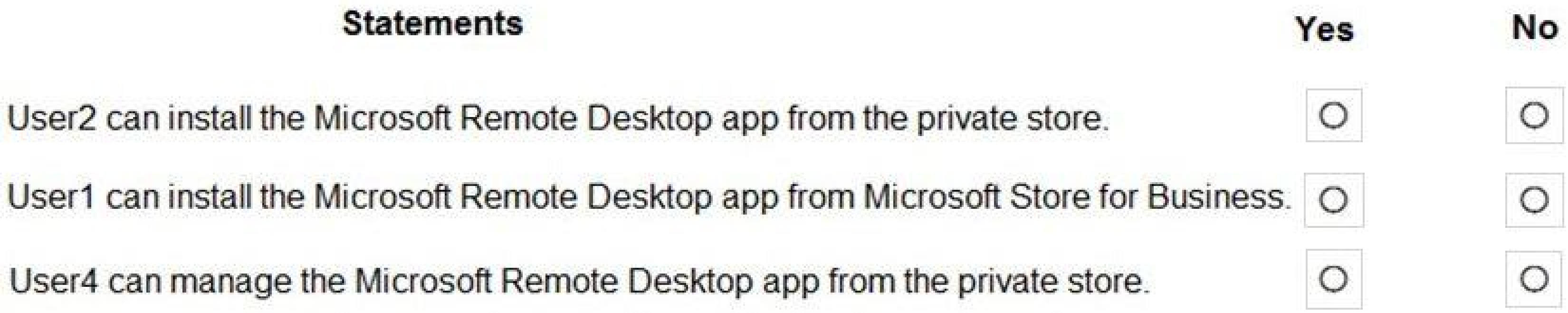
Settings & Actions

In private store

More actions available on details page

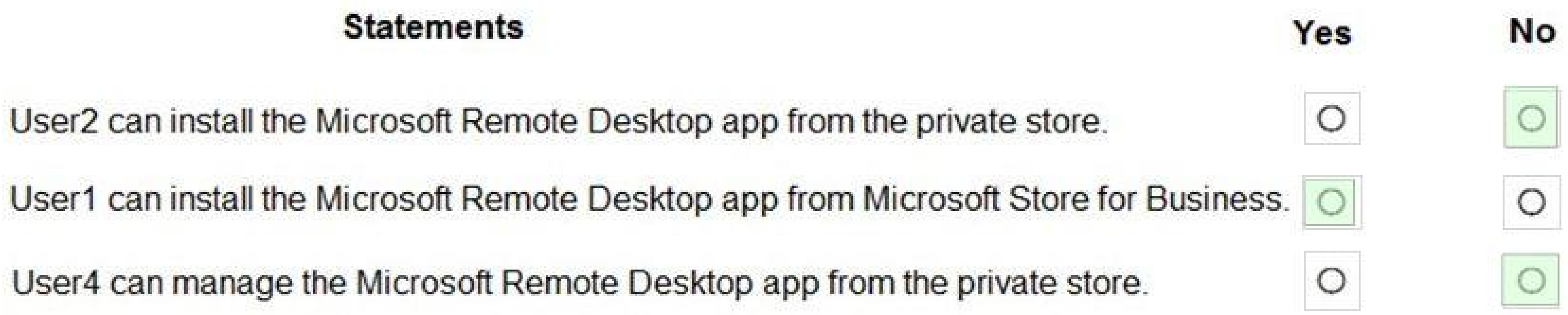
For each of the following statements, select Yes if the statement is true. Otherwise, select No.
NOTE: Each correct selection is worth one point.

Hot Area:



Statements	Yes	No
User2 can install the Microsoft Remote Desktop app from the private store.	○	○
User1 can install the Microsoft Remote Desktop app from Microsoft Store for Business.	○	○
User4 can manage the Microsoft Remote Desktop app from the private store.	○	○

Answer Area:



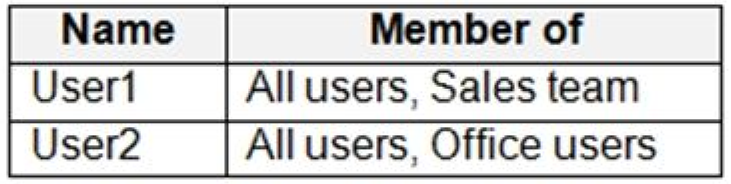
Statements	Yes	No
User2 can install the Microsoft Remote Desktop app from the private store.	○	[✓ ○]
User1 can install the Microsoft Remote Desktop app from Microsoft Store for Business.	[✓ ○]	○
User4 can manage the Microsoft Remote Desktop app from the private store.	○	[✓ ○]

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

QUESTION 69

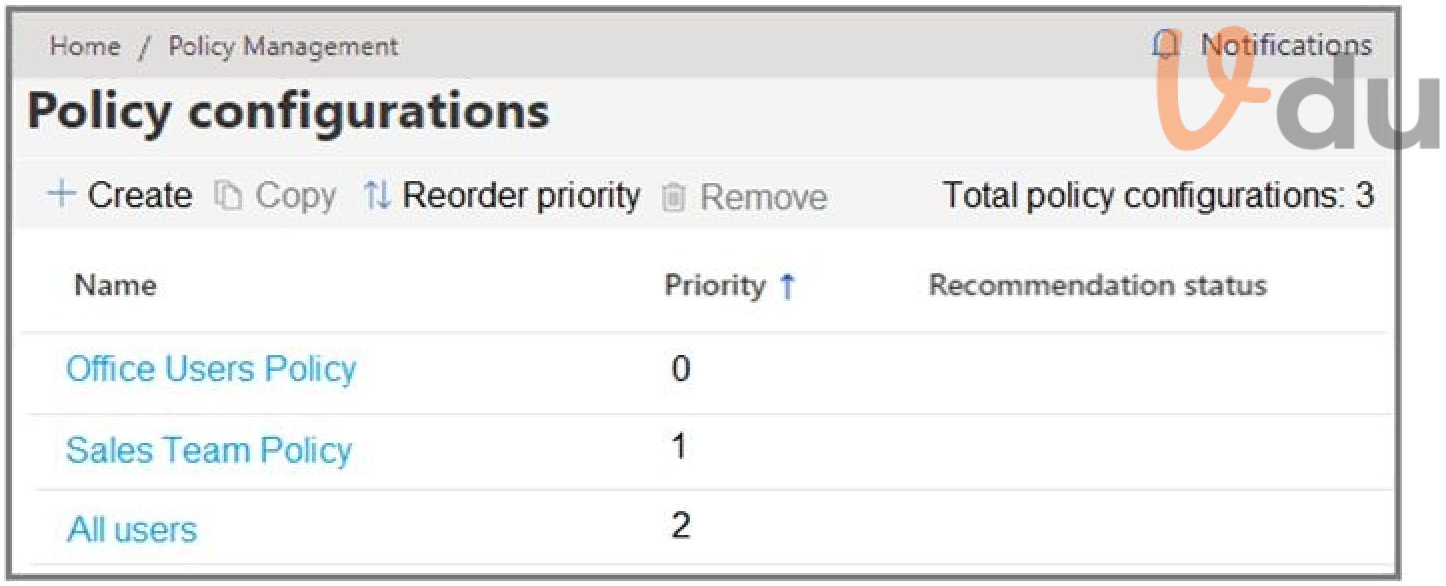
HOTSPOT

You have a Microsoft 365 subscription that contains three groups named All users, Sales team, and Office users, and two users shown in the following table.



Name	Member of
User1	All users, Sales team
User2	All users, Office users

In Microsoft Endpoint Manager, you have the Policies for Office apps settings shown in the following exhibit.



Home / Policy Management

Notifications

Policy configurations

+ Create Copy Reorder priority Remove Total policy configurations: 3

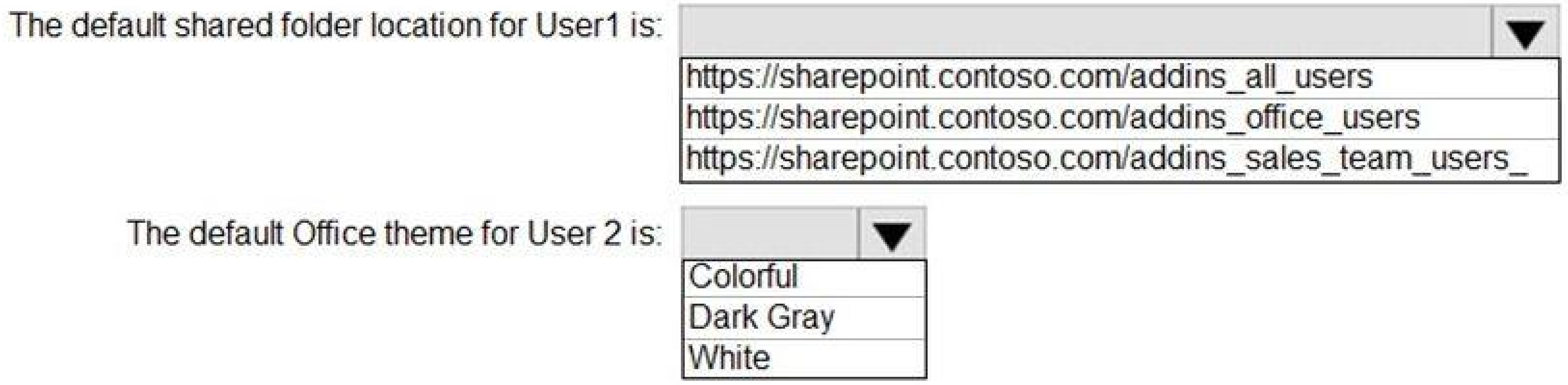
Name	Priority ↑	Recommendation status
Office Users Policy	0	
Sales Team Policy	1	
All users	2	

The policies use the settings shown in the following table.

What is the default share folder location for User1 and the default Office theme for User2? To answer, select the appropriate options in the answer area.

NOTE: Each correct selection is worth one point.

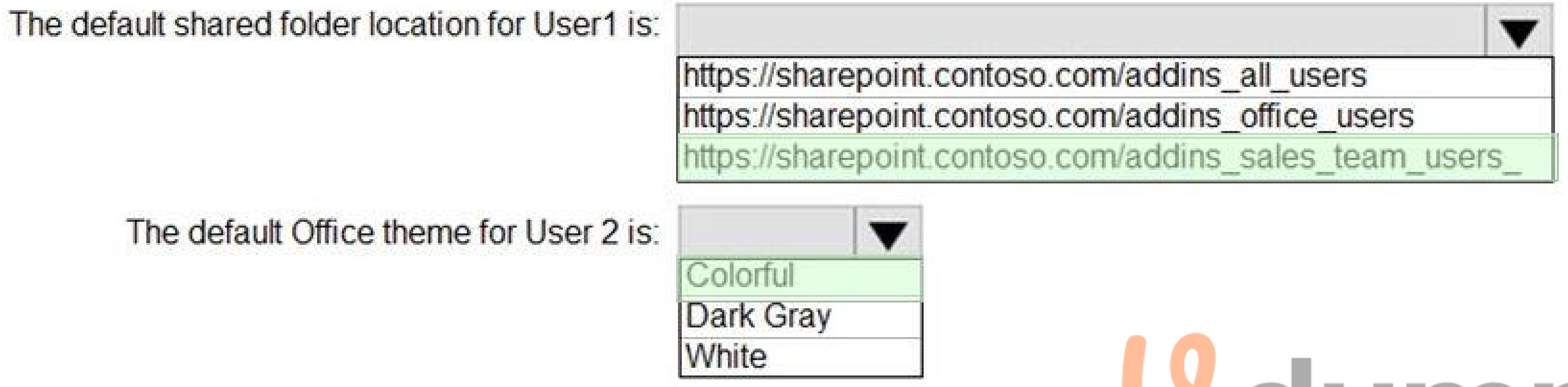
Hot Area:



The default shared folder location for User1 is: ▼
https://sharepoint.contoso.com/addins_all_users
https://sharepoint.contoso.com/addins_office_users
https://sharepoint.contoso.com/addins_sales_team_users_

The default Office theme for User 2 is: ▼
Colorful
Dark Gray
White

Answer Area:



The default shared folder location for User1 is: ▼
https://sharepoint.contoso.com/addins_all_users
https://sharepoint.contoso.com/addins_office_users
[✓ https://sharepoint.contoso.com/addins_sales_team_users_]

The default Office theme for User 2 is: ▼
[✓ Colorful]
Dark Gray
White

Section:
Explanation:
https://docs.microsoft.com/en-us/deployoffice/overview-office-cloud-policy-service

QUESTION 70
You have a Microsoft 365 tenant that contains a Windows 10 device. The device is onboarded to Microsoft Defender for Endpoint.
From Microsoft Defender Security Center, you perform a security investigation.
You need to run a PowerShell script on the device to collect forensic information.
Which action should you select on the device page?

A. Initiate Live Response Session
B. Initiate Automated Investigation
C. Collect investigation package
D. Go hunt

Correct Answer: A
Section:
Explanation:
https://docs.microsoft.com/en-us/microsoft-365/security/defender-endpoint/live-response?view=o365-worldwide

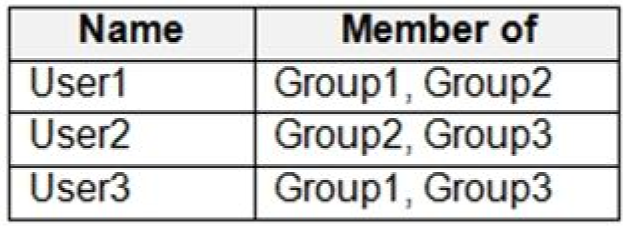
QUESTION 71
You have a Microsoft 365 E5 subscription.
You plan to implement Microsoft 365 compliance policies to meet the following requirements:
Identify documents that are stored in Microsoft Teams and SharePoint Online that contain Personally Identifiable Information (PII).

Report on shared documents that contain PII.
What should you create?

A. an alert policy
B. a data loss prevention (DLP) policy
C. a retention policy
D. a Microsoft Cloud App Security policy

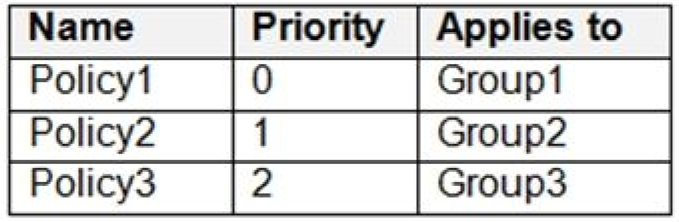
Correct Answer: B
Section:
Explanation:
https://docs.microsoft.com/en-us/microsoft-365/compliance/dlp-learn-about-dlp?view=o365-worldwide

QUESTION 72
HOTSPOT
You have a Microsoft 365 E5 subscription that contains the users shown in the following table.



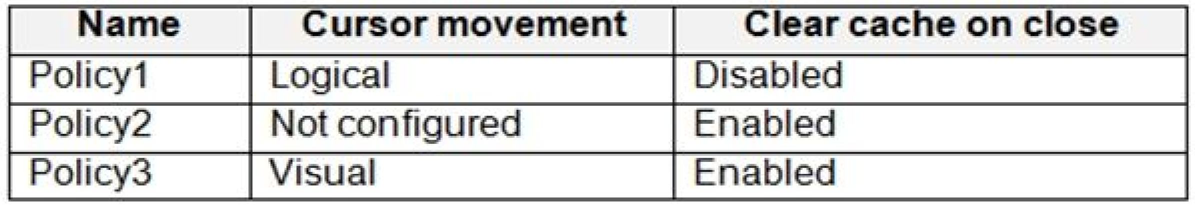
Name	Member of
User1	Group1, Group2
User2	Group2, Group3
User3	Group1, Group3

In Microsoft Endpoint Manager, you have the Policies for Office apps settings shown in the following table.



Name	Priority	Applies to
Policy1	0	Group1
Policy2	1	Group2
Policy3	2	Group3

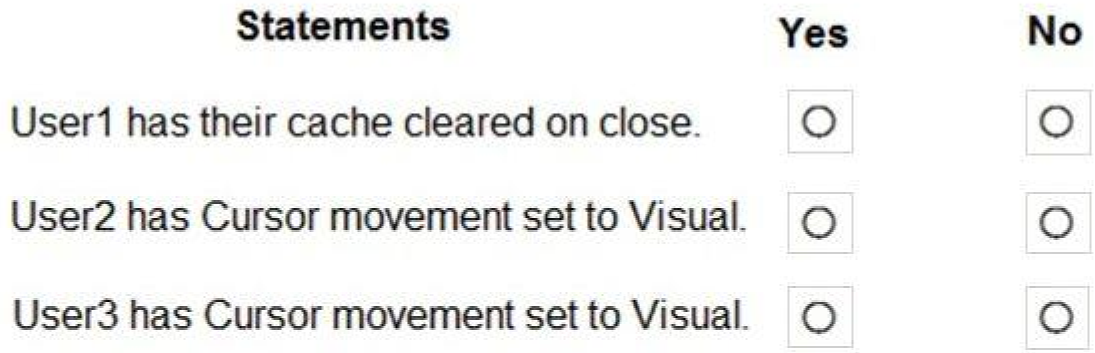
The policies use the settings shown in the following table.



Name	Cursor movement	Clear cache on close
Policy1	Logical	Disabled
Policy2	Not configured	Enabled
Policy3	Visual	Enabled

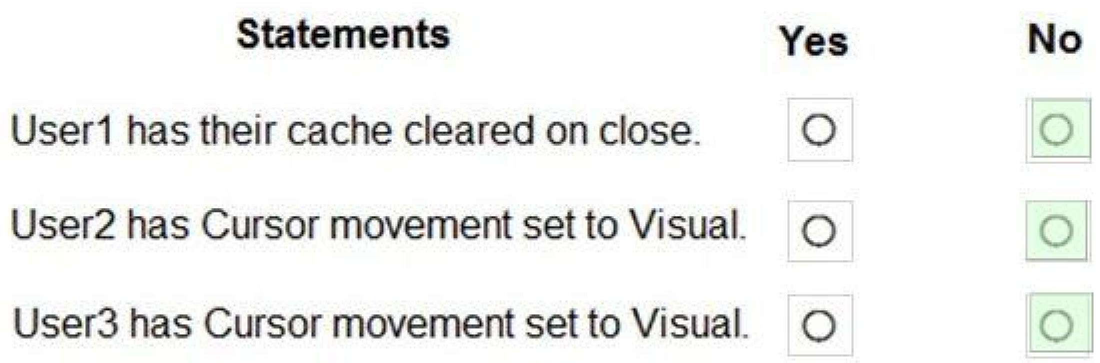
For each of the following statements, select Yes if the statement is true. Otherwise, select No.
NOTE: Each correct selection is worth one point.

Hot Area:



Statements	Yes	No
User1 has their cache cleared on close.	○	○
User2 has Cursor movement set to Visual.	○	○
User3 has Cursor movement set to Visual.	○	○

Answer Area:



Statements	Yes	No
User1 has their cache cleared on close.	○	[✓ ○]
User2 has Cursor movement set to Visual.	○	[✓ ○]
User3 has Cursor movement set to Visual.	○	[✓ ○]

Section:
Explanation:
https://docs.microsoft.com/en-us/deployoffice/overview-office-cloud-policy-service

QUESTION 73
You have a Microsoft 365 tenant.
You plan to enable BitLocker Disk Encryption (BitLocker) automatically for all Windows 10 devices that enroll in Microsoft Intune.
What should you use?

A. an attack surface reduction (ASR) policy
B. an app configuration policy
C. a device compliance policy
D. a device configuration profile

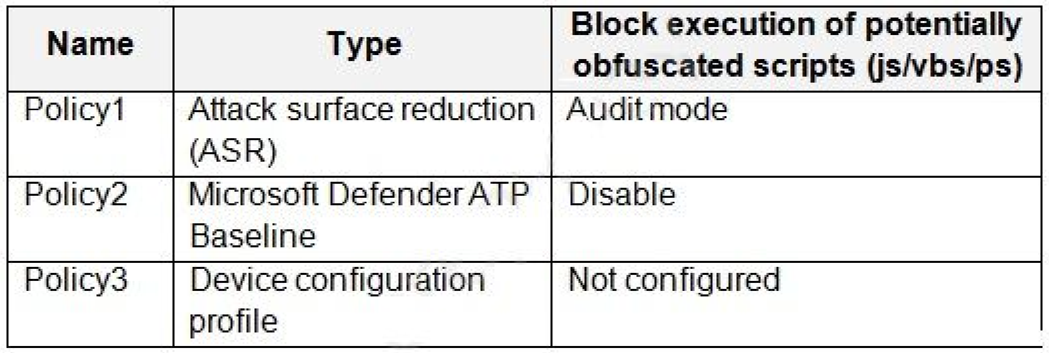
Correct Answer: D
Section:
Explanation:
https://docs.microsoft.com/en-us/mem/intune/protect/encrypt-devices

QUESTION 74
You have a Microsoft 365 tenant that contains 500 Windows 10 devices and a Microsoft Endpoint Manager device compliance policy.
You need to ensure that only devices marked as compliant can access Microsoft Office 365 apps.
Which policy type should you configure?

A. conditional access
B. account protection
C. attack surface reduction (ASR)
D. Endpoint detection and response

Correct Answer: A
Section:
Explanation:
https://docs.microsoft.com/en-us/mem/intune/protect/device-compliance-get-started

QUESTION 75
You have a Microsoft 365 tenant that contains a Windows 10 device named Device1 and the Microsoft Endpoint Manager policies shown in the following table.



Name	Type	Block execution of potentially obfuscated scripts (js/vbs/ps)
Policy1	Attack surface reduction (ASR)	Audit mode
Policy2	Microsoft Defender ATP Baseline	Disable
Policy3	Device configuration profile	Not configured

The policies are assigned to Device1.
Which policy settings will be applied to Device1?

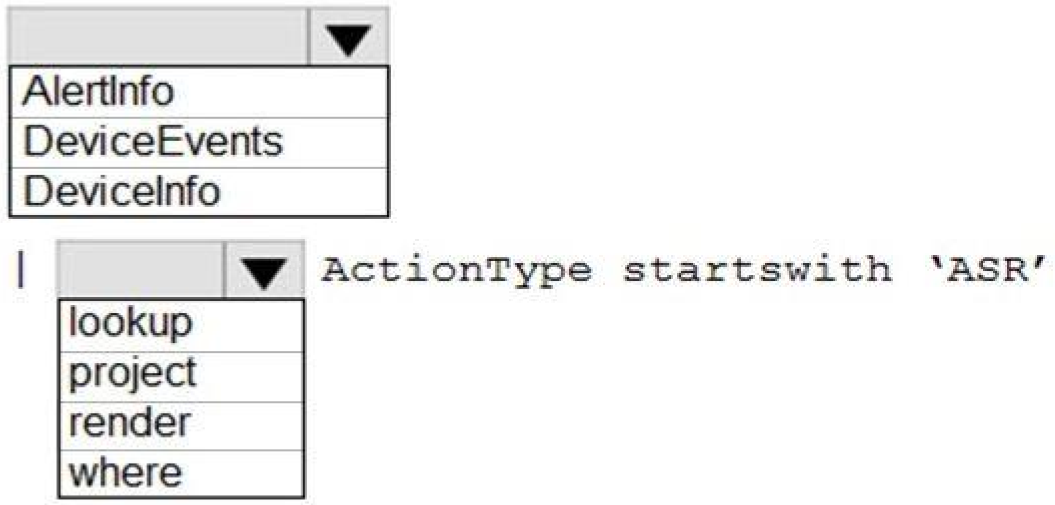
A. only the settings of Policy1
B. only the settings of Policy2
C. only the settings of Policy3
D. no settings

Correct Answer: D
Section:

QUESTION 76

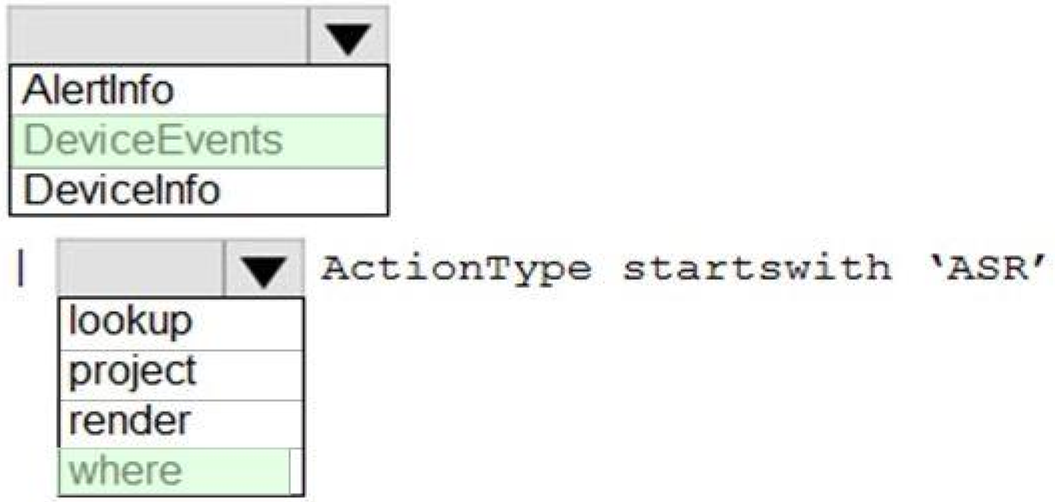
HOTSPOT
You have a Microsoft 365 E5 tenant that contains 100 Windows 10 devices.
You plan to attack surface reduction (ASR) rules for the Windows 10 devices.
You configure the ASR rules in audit mode and collect audit data in a Log Analytics workspace.
You need to find the ASR rules that match the activities on the devices.
How should you complete the Kusto query? To answer, select the appropriate options in the answer area.
NOTE: Each correct selection is worth one point.

Hot Area:



```
| [ ▼ ] ActionType startswith 'ASR'
```

Answer Area:

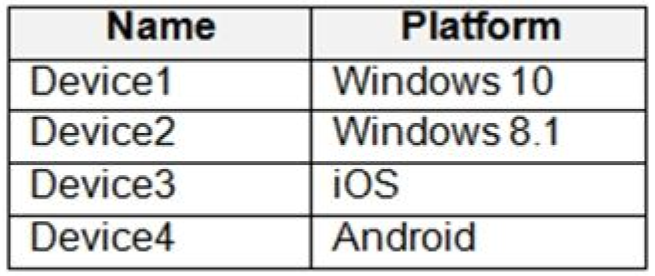


▼
AlertInfo
[✓ DeviceEvents]
DeviceInfo

| ▼ ActionType startswith 'ASR'
lookup
project
render
[✓ where]

Section:
Explanation:
https://techcommunity.microsoft.com/t5/microsoft-defender-for-endpoint/demystifying-attack-surface-reduction-rules-part-3/ba-p/1360968

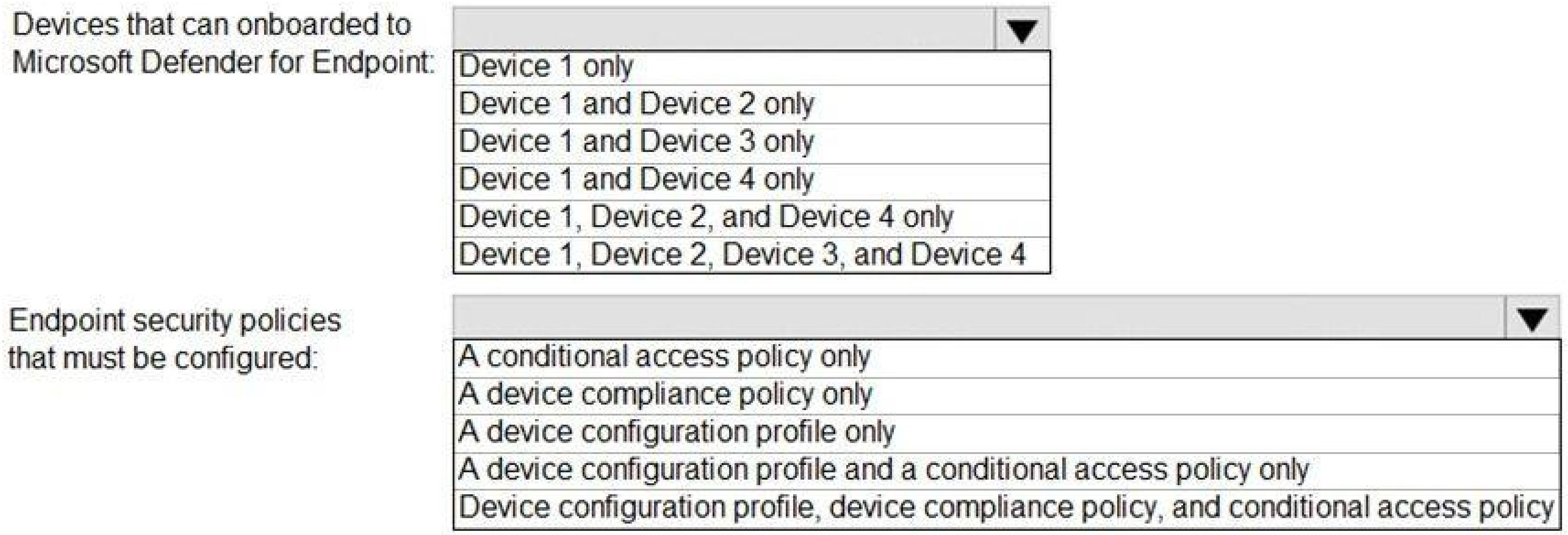
QUESTION 77
HOTSPOT
You have a Microsoft 365 E5 tenant that connects to Microsoft Defender for Endpoint.
You have devices enrolled in Microsoft Intune as shown in the following table.



Name	Platform
Device1	Windows 10
Device2	Windows 8.1
Device3	iOS
Device4	Android

You plan to use risk levels in Microsoft Defender for Endpoint to identify whether a device is compliant. Noncompliant devices must be blocked from accessing corporate resources.
You need to identify which devices can be onboarded to Microsoft Defender for Endpoint, and which Endpoint security policies must be configured.
What should you identify? To answer, select the appropriate options in the answer area.
NOTE: Each correct selection is worth one point.

Hot Area:



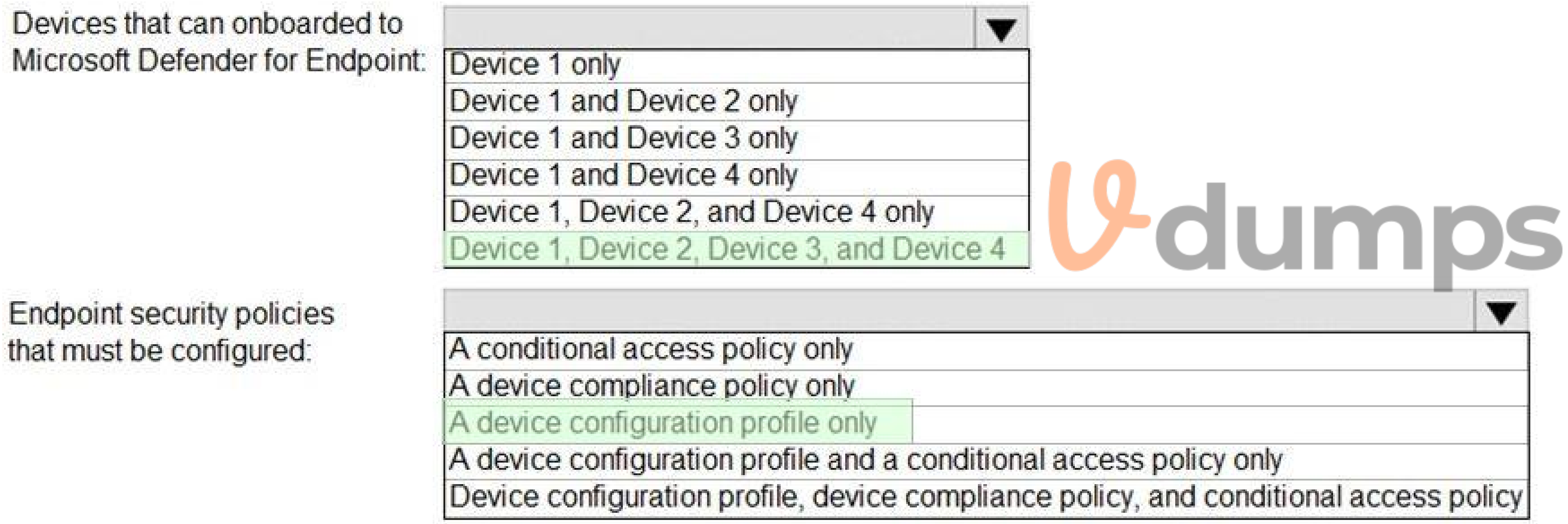
Devices that can onboarded to Microsoft Defender for Endpoint:

- Device 1 only
- Device 1 and Device 2 only
- Device 1 and Device 3 only
- Device 1 and Device 4 only
- Device 1, Device 2, and Device 4 only
- Device 1, Device 2, Device 3, and Device 4

Endpoint security policies that must be configured:

- A conditional access policy only
- A device compliance policy only
- A device configuration profile only
- A device configuration profile and a conditional access policy only
- Device configuration profile, device compliance policy, and conditional access policy

Answer Area:



Devices that can onboarded to Microsoft Defender for Endpoint:

- Device 1 only
- Device 1 and Device 2 only
- Device 1 and Device 3 only
- Device 1 and Device 4 only
- Device 1, Device 2, and Device 4 only
- [✓ Device 1, Device 2, Device 3, and Device 4]

Endpoint security policies that must be configured:

- A conditional access policy only
- A device compliance policy only
- [✓ A device configuration profile only]
- A device configuration profile and a conditional access policy only
- Device configuration profile, device compliance policy, and conditional access policy

Section:
Explanation:
https://docs.microsoft.com/en-us/microsoft-365/security/defender-endpoint/configure-machines-onboarding?view=o365-worldwide

QUESTION 78
You have a Microsoft 365 E5 tenant that contains a user named User1.
You plan to implement insider risk management.
You need to ensure that User1 can perform the following tasks:
Review alerts.
Manage cases.
Create notice templates.
Review user emails by using Content explorer.
The solution must use the principle of least privilege.
To which role group should you add User1?

A. Insider Risk Management

B. Insider Risk Management Analysts
C. Insider Risk Management Investigators
D. Insider Risk Management Admin

Correct Answer: C
Section:
Explanation:
https://docs.microsoft.com/en-us/microsoft-365/compliance/insider-risk-management-configure?view=o365-worldwide

QUESTION 79
Your company has a Microsoft 365 E5 tenant that contains a user named User1.
You review the company's compliance score.
You need to assign the following improvement action to User1:Enable self-service password reset.
What should you do first?

A. From Compliance Manager, turn off automated testing.
B. From the Azure Active Directory admin center, enable self-service password reset (SSPR).
C. From the Microsoft 365 admin center, modify the self-service password reset (SSPR) settings.
D. From the Azure Active Directory admin center, add User1 to the Compliance administrator role.

Correct Answer: D
Section:
Explanation:
https://docs.microsoft.com/en-us/microsoft-365/compliance/compliance-manager-improvement-actions?view=o365-worldwide
https://docs.microsoft.com/en-us/azure/active-directory/fundamentals/active-directory-users-assign-role-azure-portal

QUESTION 80
Your company has a Microsoft E5 tenant.
The company must meet the requirements of the ISO/IEC 27001:2013 standard.
You need to assess the company's current state of compliance.
What should you use?

A. eDiscovery
B. Information governance
C. Compliance Manager
D. Data Subject Requests (DSRs)

Correct Answer: C
Section:
Explanation:
https://docs.microsoft.com/en-us/compliance/regulatory/offering-iso-27001

QUESTION 81
You have a Microsoft 365 E5 tenant.
Users store data in the following locations:
Microsoft Teams
Microsoft OneDrive
Microsoft Exchange Online

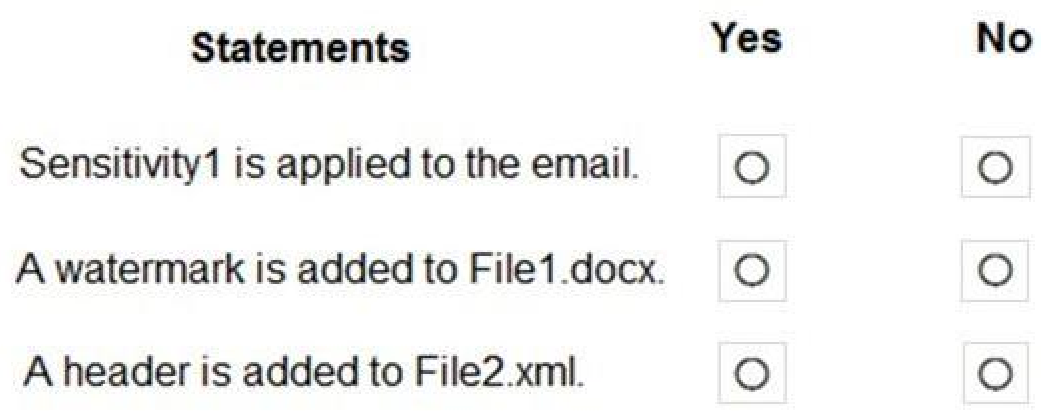
Microsoft SharePoint Online
You need to retain Microsoft 365 data for two years.
What is the minimum number of retention policies that you should create?

A. 1
B. 2
C. 3
D. 4

Correct Answer: C
Section:
Explanation:
https://docs.microsoft.com/en-us/microsoft-365/compliance/create-retention-policies?view=o365-worldwide

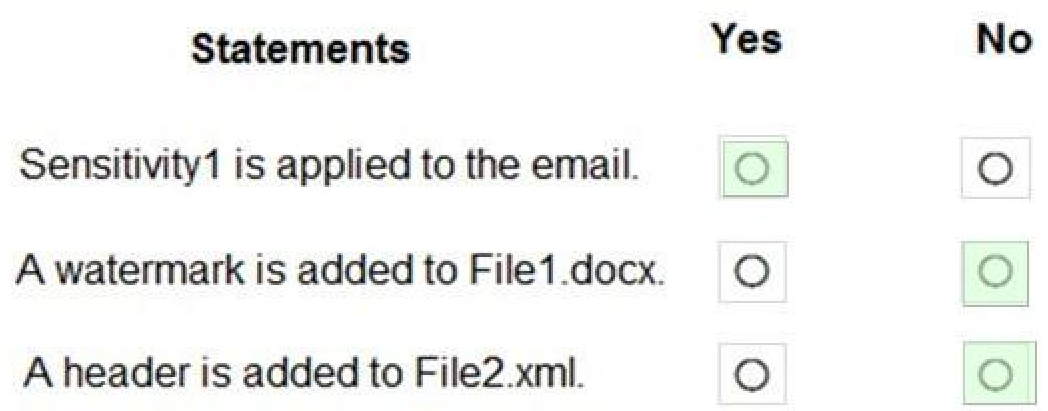
QUESTION 82
HOTSPOT
You have a Microsoft 365 E5 tenant.
You have a sensitivity label configured as shown in the Sensitivity label exhibit. (Click the Sensitivity label tab.)
You have an auto-labeling policy as shown in the Auto-labeling policy exhibit. (Click the Auto-labeling policy tab.)
A user sends an email that contains the components shown in the following table.
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:



Statements	Yes	No
Sensitivity1 is applied to the email.	○	○
A watermark is added to File1.docx.	○	○
A header is added to File2.xml.	○	○

Answer Area:



Statements	Yes	No
Sensitivity1 is applied to the email.	[✓ ○]	○
A watermark is added to File1.docx.	○	[✓ ○]
A header is added to File2.xml.	○	[✓ ○]

Section:

Explanation:
https://docs.microsoft.com/en-us/microsoft-365/compliance/apply-sensitivity-label-automatically?view=o365-worldwide

QUESTION 83
You have a Microsoft 365 E5 tenant.
You plan to create a custom Compliance Manager assessment template based on the ISO 27001:2013 template.
You need to export the existing template.
Which file format should you use for the exported template?

A. CSV
B. XLSX
C. JSON
D. XML

Correct Answer: B
Section:
Explanation:
https://docs.microsoft.com/en-us/microsoft-365/compliance/compliance-manager-templates?view=o365-worldwide#export-a-template

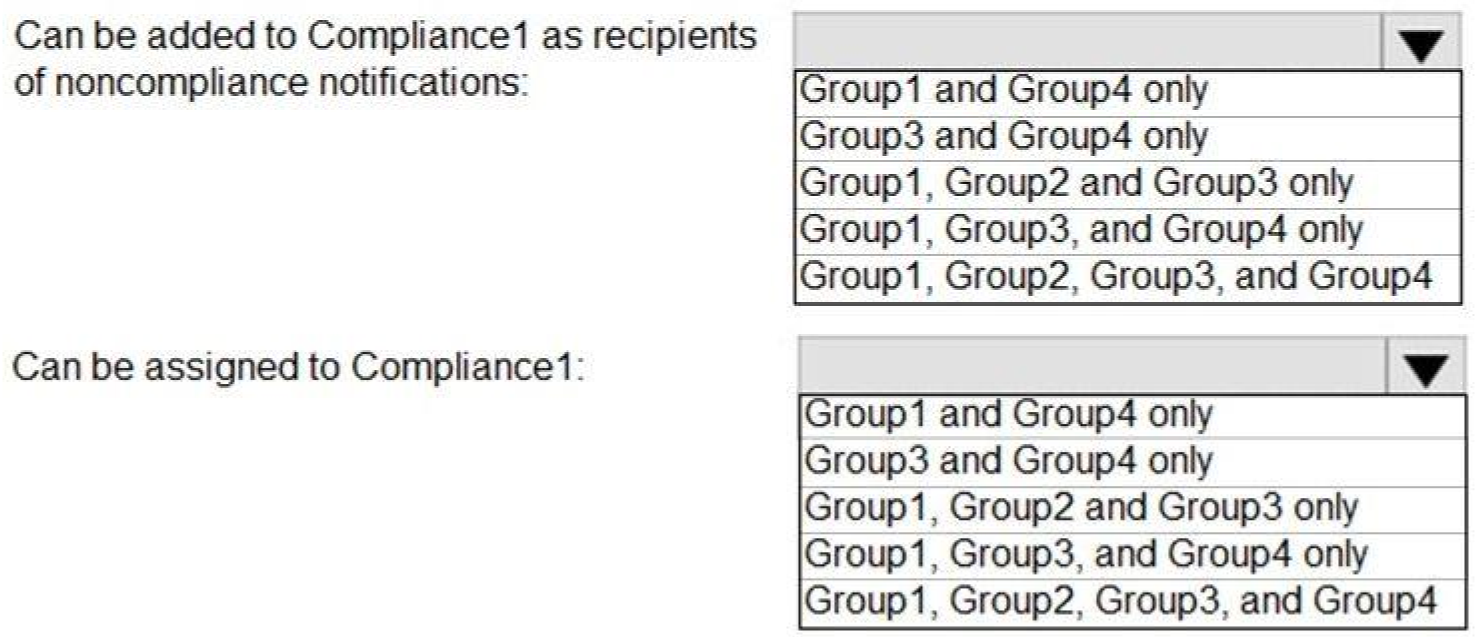
QUESTION 84
You have a Microsoft 365 tenant that contains 1,000 Windows 10 devices. The devices are enrolled in Microsoft Intune.
Company policy requires that the devices have the following configurations:
Require complex passwords.
Require the encryption of removable data storage devices.
Have Microsoft Defender Antivirus real-time protection enabled.
You need to configure the devices to meet the requirements.
What should you use?

A. an app configuration policy
B. a compliance policy C a security baseline profile D a conditional access policy

Correct Answer: B
Section:
Explanation:
https://docs.microsoft.com/en-us/mem/intune/protect/device-compliance-get-started

QUESTION 85
HOTSPOT
You have a Microsoft 365 tenant that contains the groups shown in the following table.
You plan to create a compliance policy named Compliance1.
You need to identify the groups that meet the following requirements:
Can be added to Compliance1 as recipients of noncompliance notifications
Can be assigned to Compliance1
To answer, select the appropriate options in the answer area.
NOTE: Each correct selection is worth one point.

Hot Area:



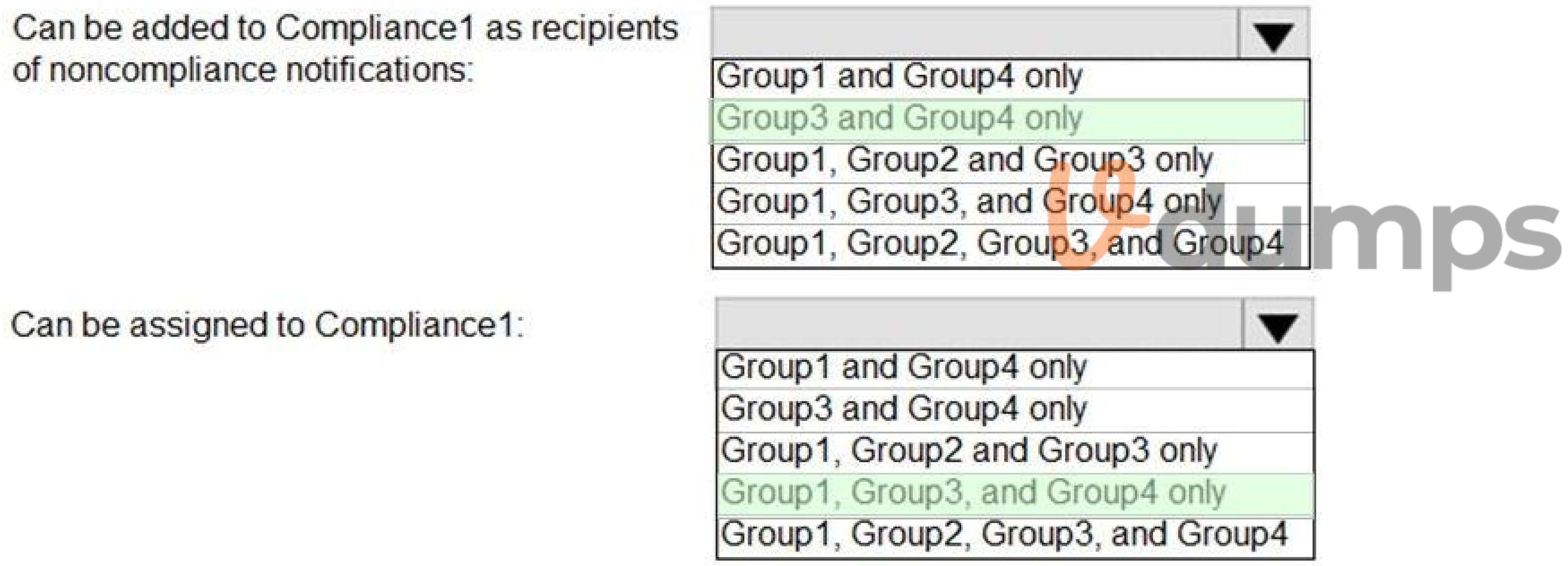
Can be added to Compliance1 as recipients of noncompliance notifications:

- Group1 and Group4 only
- Group3 and Group4 only
- Group1, Group2 and Group3 only
- Group1, Group3, and Group4 only
- Group1, Group2, Group3, and Group4

Can be assigned to Compliance1:

- Group1 and Group4 only
- Group3 and Group4 only
- Group1, Group2 and Group3 only
- Group1, Group3, and Group4 only
- Group1, Group2, Group3, and Group4

Answer Area:



Can be added to Compliance1 as recipients of noncompliance notifications:

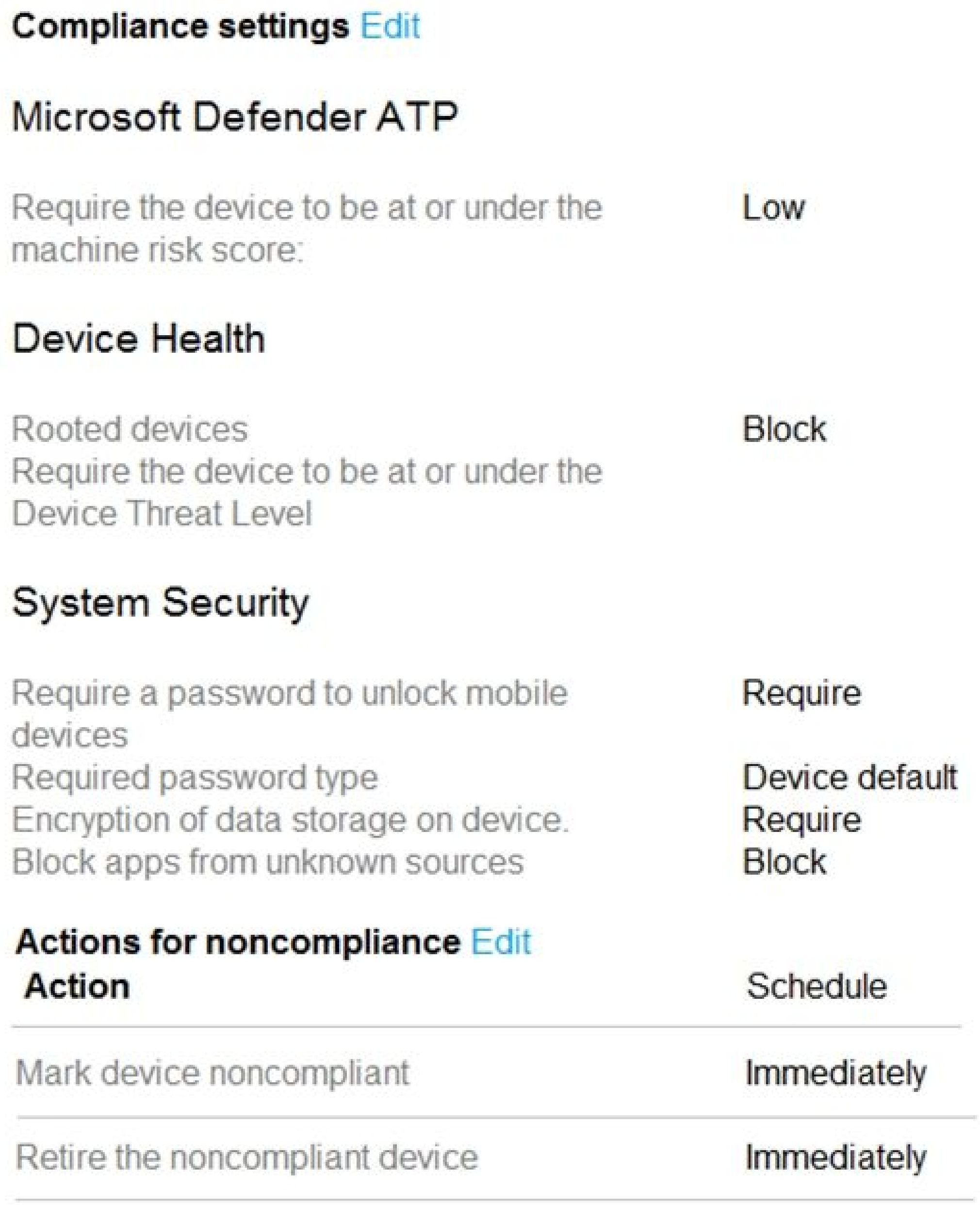
- Group1 and Group4 only
- [✓ Group3 and Group4 only]
- Group1, Group2 and Group3 only
- Group1, Group3, and Group4 only
- Group1, Group2, Group3, and Group4

Can be assigned to Compliance1:

- Group1 and Group4 only
- Group3 and Group4 only
- Group1, Group2 and Group3 only
- [✓ Group1, Group3, and Group4 only]
- Group1, Group2, Group3, and Group4

Section:
Explanation:
https://www.itpromentor.com/devices-or-users-when-to-target-which-policy-type-in-microsoft-endpoint-manager-intune/

QUESTION 86
HOTSPOT
You have a Microsoft 365 E5 tenant.
You configure a device compliance policy as shown in the following exhibit.



Compliance settings Edit

Microsoft Defender ATP

Require the device to be at or under the machine risk score:	Low

Device Health

Rooted devices	Block
Require the device to be at or under the Device Threat Level	

System Security

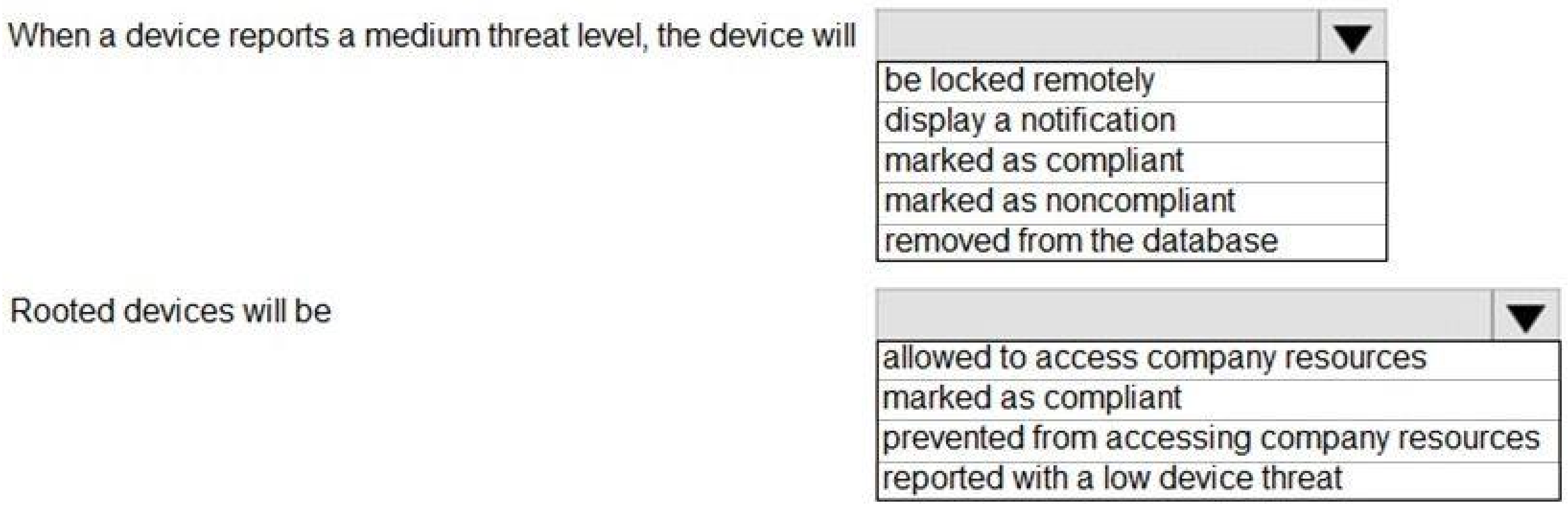
Require a password to unlock mobile devices	Require
Required password type	Device default
Encryption of data storage on device.	Require
Block apps from unknown sources	Block

Actions for noncompliance Edit

Action	Schedule
Mark device noncompliant	Immediately
Retire the noncompliant device	Immediately

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:



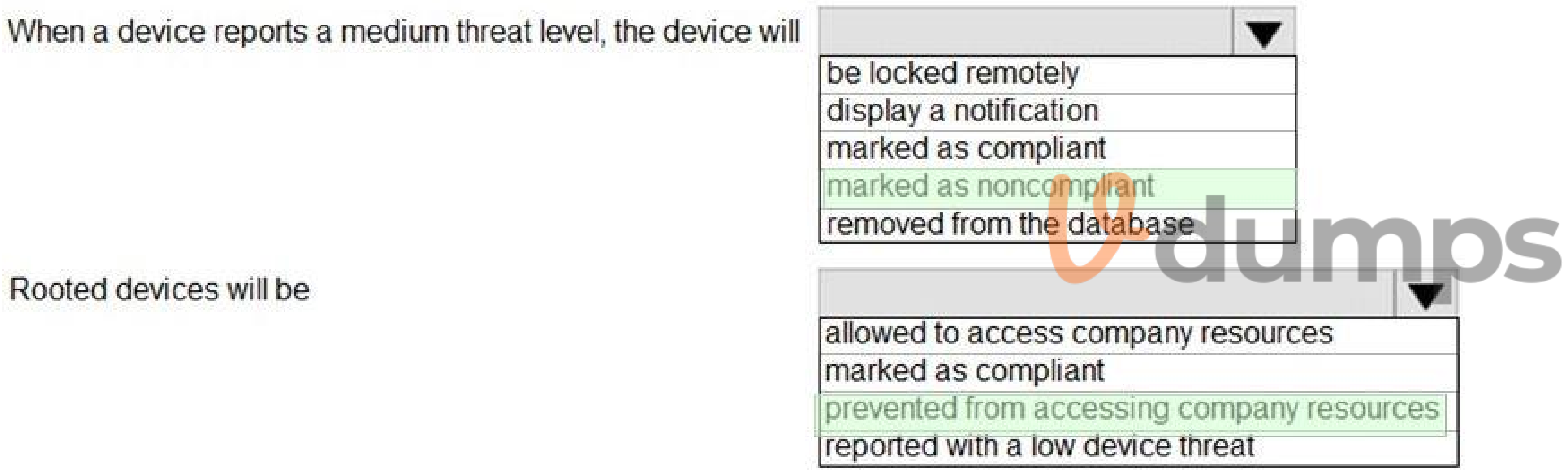
When a device reports a medium threat level, the device will ▼

- be locked remotely
- display a notification
- marked as compliant
- marked as noncompliant
- removed from the database

Rooted devices will be ▼

- allowed to access company resources
- marked as compliant
- prevented from accessing company resources
- reported with a low device threat

Answer Area:



When a device reports a medium threat level, the device will ▼

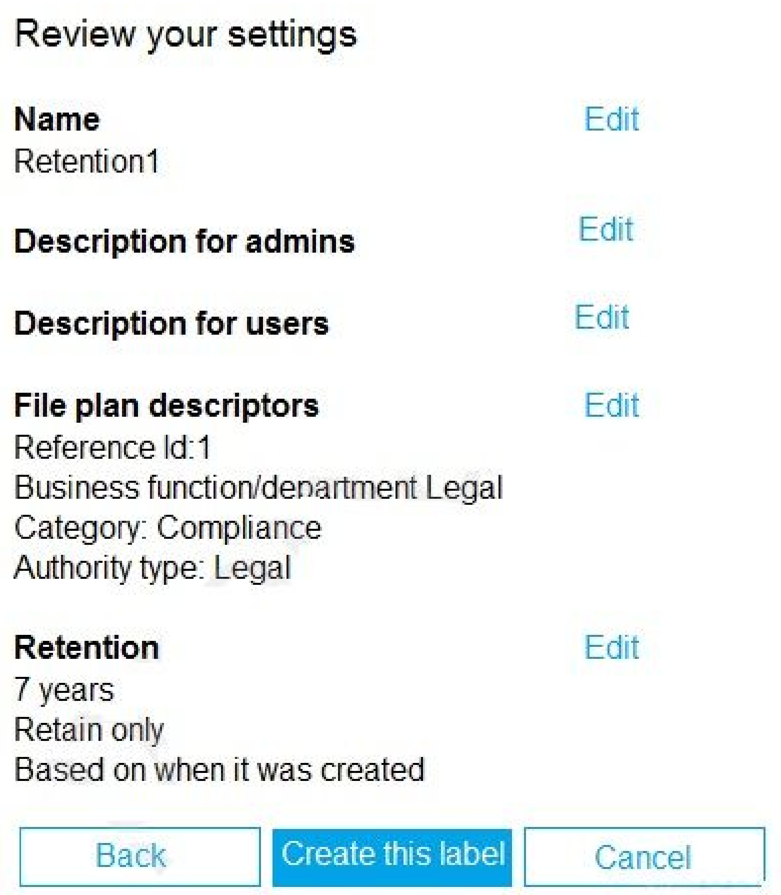
- be locked remotely
- display a notification
- marked as compliant
- [✓ marked as noncompliant]
- removed from the database

Rooted devices will be ▼

- allowed to access company resources
- marked as compliant
- [✓ prevented from accessing company resources]
- reported with a low device threat

Section:
Explanation:
https://docs.microsoft.com/en-us/mem/intune/protect/compliance-policy-create-android

QUESTION 87
You have a Microsoft 365 E5 tenant.
You create a retention label named Retention1 as shown in the following exhibit.



Review your settings

Name
Retention1

Description for admins

Description for users

File plan descriptors
Reference Id:1
Business function/department Legal
Category: Compliance
Authority type: Legal

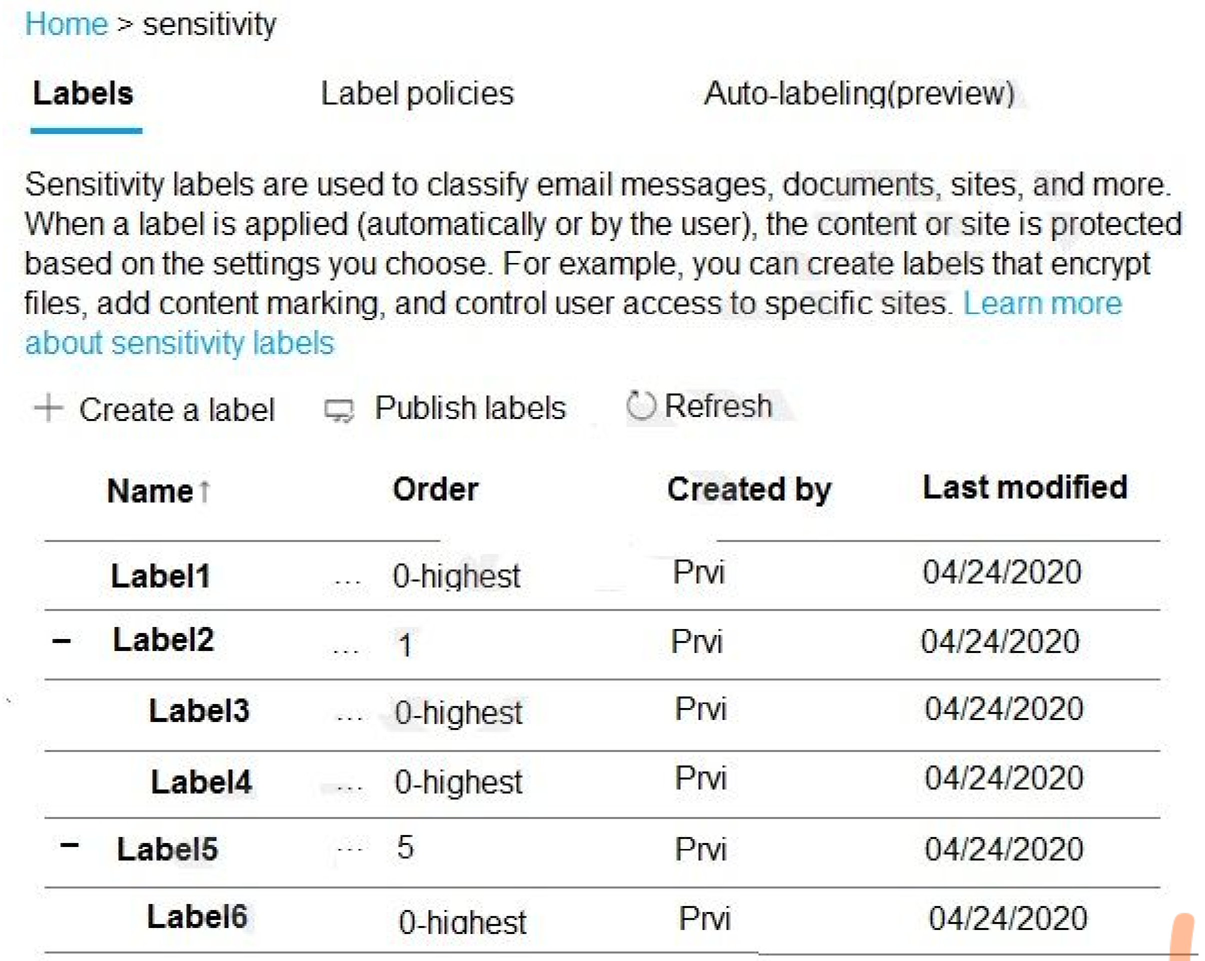
Retention
7 years
Retain only
Based on when it was created

When users attempt to apply Retention1, the label is unavailable.
You need to ensure that Retention1 is available to all the users.
What should you do?

A. Create a new label policy
B. Modify the Authority type setting for Retention!
C. Modify the Business function/department setting for Retention 1.
D. Use a file plan CSV template to import Retention1.

Correct Answer: A
Section:
Explanation:
https://docs.microsoft.com/en-us/microsoft-365/compliance/create-apply-retention-labels?view=o365-worldwide

QUESTION 88
You have the sensitivity labels shown in the following exhibit.



Home > sensitivity

Sensitivity labels are used to classify email messages, documents, sites, and more. When a label is applied (automatically or by the user), the content or site is protected based on the settings you choose. For example, you can create labels that encrypt files, add content marking, and control user access to specific sites. Learn more about sensitivity labels

Name↑	Order	Created by	Last modified
Label1	0-highest	Prvi	04/24/2020
− Label2	1	Prvi	04/24/2020
Label3	0-highest	Prvi	04/24/2020
Label4	0-highest	Prvi	04/24/2020
− Label5	5	Prvi	04/24/2020
Label6	0-highest	Prvi	04/24/2020

Which labels can users apply to content?

A. Label3, Label4, and Label6 only

B. Label1, Label2. Label3. Label4. Label5. and Label6

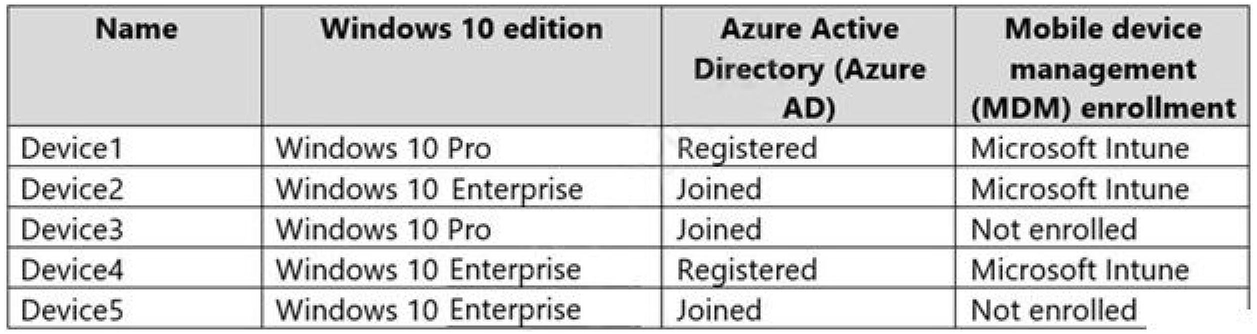
C. Label1, Label2, and Label5 only

D. Label1, Label3, Label4, and Label6 only

Correct Answer: D
Section:
Explanation:
https://docs.microsoft.com/en-us/microsoft-365/compliance/sensitivity-labels?view=o365-worldwide

QUESTION 89

You have a Microsoft 365 E5 tenant that contains the devices shown in the following table.



Name	Windows 10 edition	Azure Active Directory (Azure AD)	Mobile device management (MDM) enrollment
Device1	Windows 10 Pro	Registered	Microsoft Intune
Device2	Windows 10 Enterprise	Joined	Microsoft Intune
Device3	Windows 10 Pro	Joined	Not enrolled
Device4	Windows 10 Enterprise	Registered	Microsoft Intune
Device5	Windows 10 Enterprise	Joined	Not enrolled

You add custom apps to the private store in Microsoft Store Business.
You plan to create a policy to show only the private store in Microsoft Store for Business.

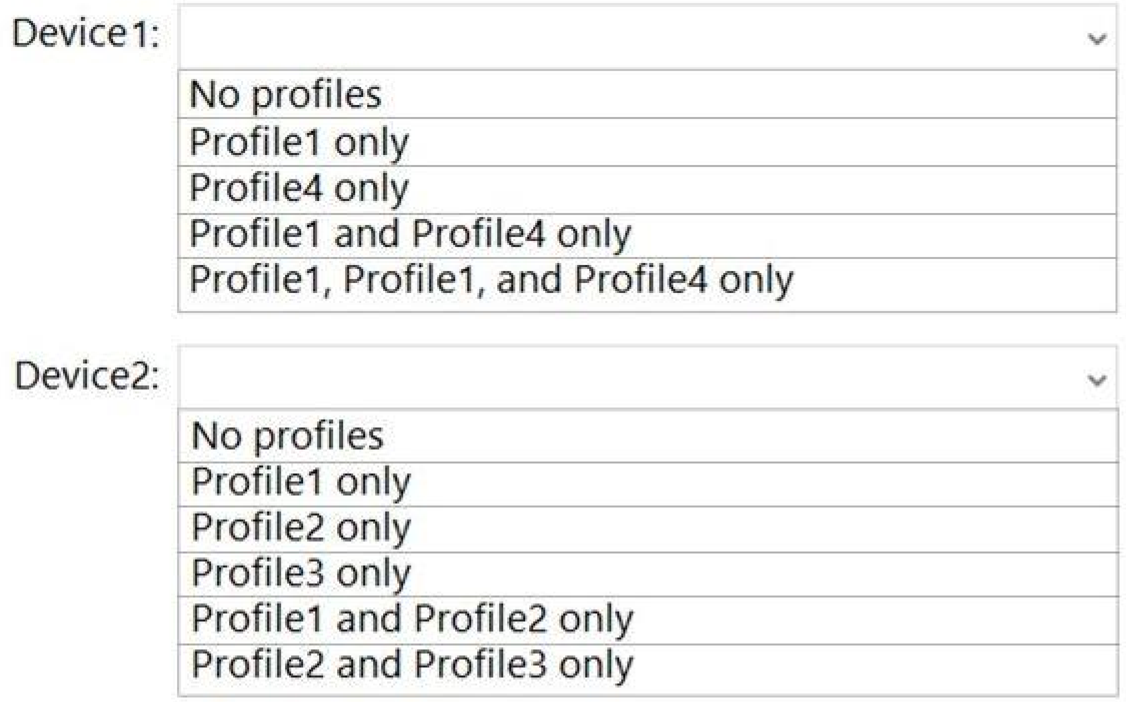
To which devices can the policy be applied?

A. Device2 only
B. Device1 and Device3 only
C. Device2 and Device4 only
D. Device2, Device3, and Device5 only
E. Device1, Device2, Device3, Device4, and Device5

Correct Answer: C
Section:

QUESTION 90
HOTSPOT
You have a Microsoft 365 E5 subscription that uses Microsoft Intune.
You have devices enrolled in Intune as shown in the following table.
You create the device configuration profiles shown in the following table.
Which profiles will be applied to each device? To answer, select the appropriate options in the answer area.
NOTE: Each correct selection is worth one point.

Hot Area:



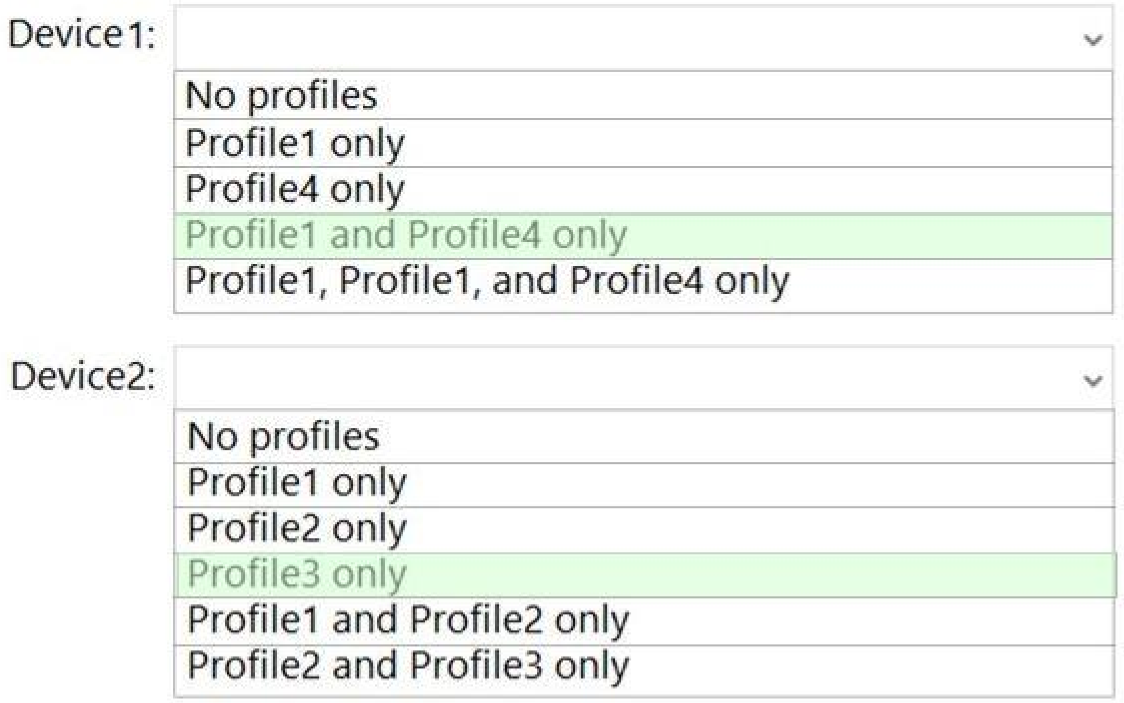
Device1:

- No profiles
- Profile1 only
- Profile4 only
- Profile1 and Profile4 only
- Profile1, Profile1, and Profile4 only

Device2:

- No profiles
- Profile1 only
- Profile2 only
- Profile3 only
- Profile1 and Profile2 only
- Profile2 and Profile3 only

Answer Area:



Device1:

- No profiles
- Profile1 only
- Profile4 only
- Profile1 and Profile4 only
- Profile1, Profile1, and Profile4 only

Device2:

- No profiles
- Profile1 only
- Profile2 only
- Profile3 only
- Profile1 and Profile2 only
- Profile2 and Profile3 only

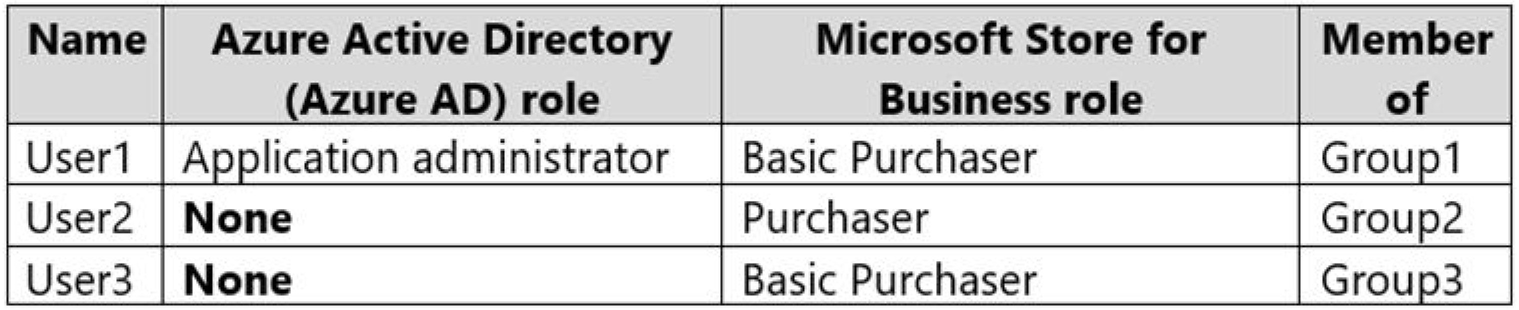
Section:
Explanation:

QUESTION 91
You have a Microsoft 365 E5 tenant that uses Microsoft Intune.
You need to ensure that users can select a department when they enroll their device in Intune.
What should you create?

A. scope tags
B. device configuration profiles
C. device categories
D. device compliance policies

Correct Answer: C
Section:
Explanation:
https://docs.microsoft.com/en-us/mem/intune/enrollment/device-group-mapping

QUESTION 92
HOTSPOT
You have a Microsoft 365 E5 tenant that contains the users shown in the following table.

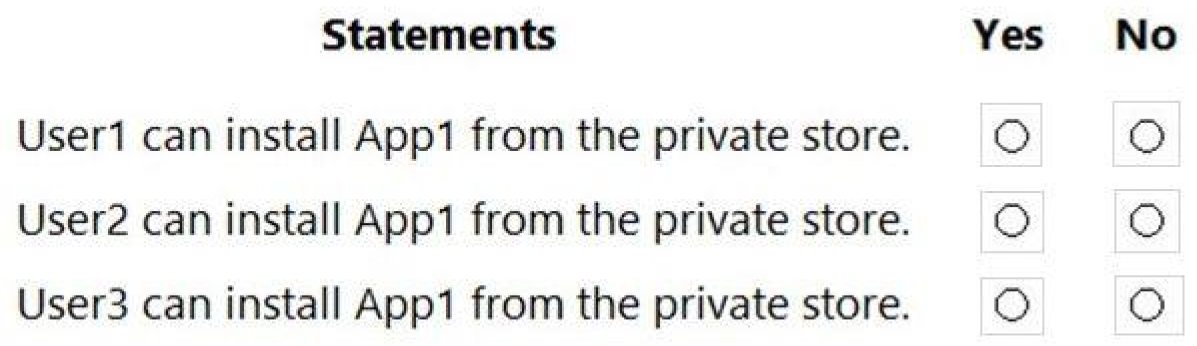


Name	Azure Active Directory (Azure AD) role	Microsoft Store for Business role	Member of
User1	Application administrator	Basic Purchaser	Group1
User2	**None**	Purchaser	Group2
User3	**None**	Basic Purchaser	Group3

You perform the following actions:

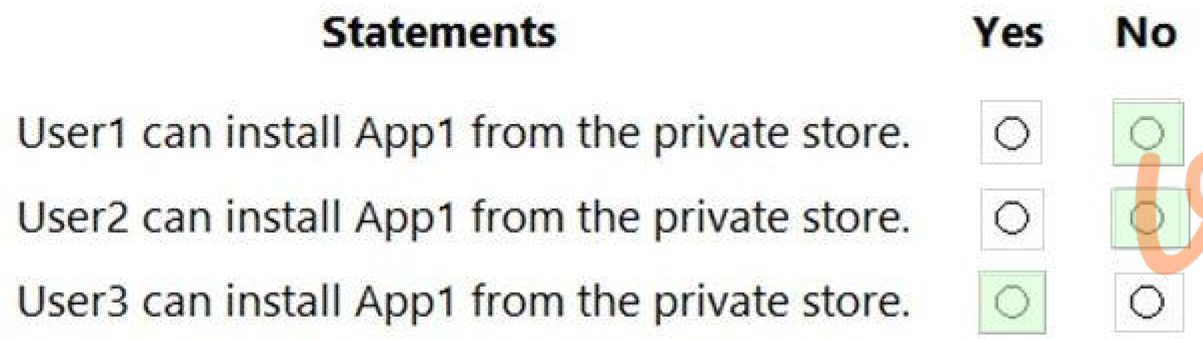
Provision the private store in Microsoft Store for Business.
Add an app named App1 to the private store.
Set Private store availability for App1 to Specific groups, and then select Group3.
For each of the following statements, select Yes if the statement is true. Otherwise, select No.
NOTE: Each correct selection is worth one point.

Hot Area:



Statements	Yes	No
User1 can install App1 from the private store.	○	○
User2 can install App1 from the private store.	○	○
User3 can install App1 from the private store.	○	○

Answer Area:



Statements	Yes	No
User1 can install App1 from the private store.	○	[✓ ○]
User2 can install App1 from the private store.	○	[✓ ○]
User3 can install App1 from the private store.	[✓ ○]	○

Section:
Explanation:
https://docs.microsoft.com/en-us/microsoft-store/app-inventory-management-microsoft-store-for-business#private-store-availability

QUESTION 93
Your company has multiple offices.
You have a Microsoft 365 E5 tenant that uses Microsoft Intune for device management. Each office has a local administrator.
You need to ensure that the local administrators can manage only the devices in their respective office.
What should you use?

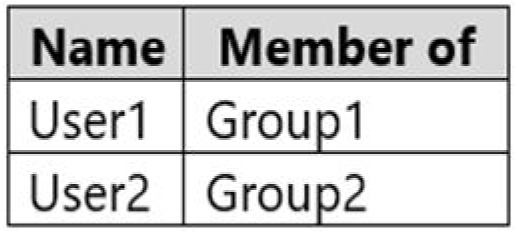
A. scope tags
B. configuration profiles
C. device categories
D. conditional access policies

Correct Answer: A
Section:
Explanation:
https://docs.microsoft.com/en-us/mem/intune/fundamentals/scope-tags

QUESTION 94

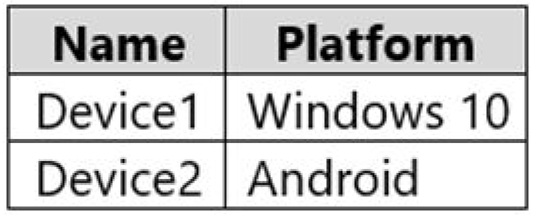
HOTSPOT

You have a Microsoft 365 E5 tenant that contains the users shown in the following table.



Name	Member of
User1	Group1
User2	Group2

You purchase the devices shown in the following table.



Name	Platform
Device1	Windows 10
Device2	Android

In Microsoft Endpoint Manager, you create an enrollment status page profile that has the following settings:

Show app and profile configuration progress: Yes

Allow users to collect logs about installation errors: Yes

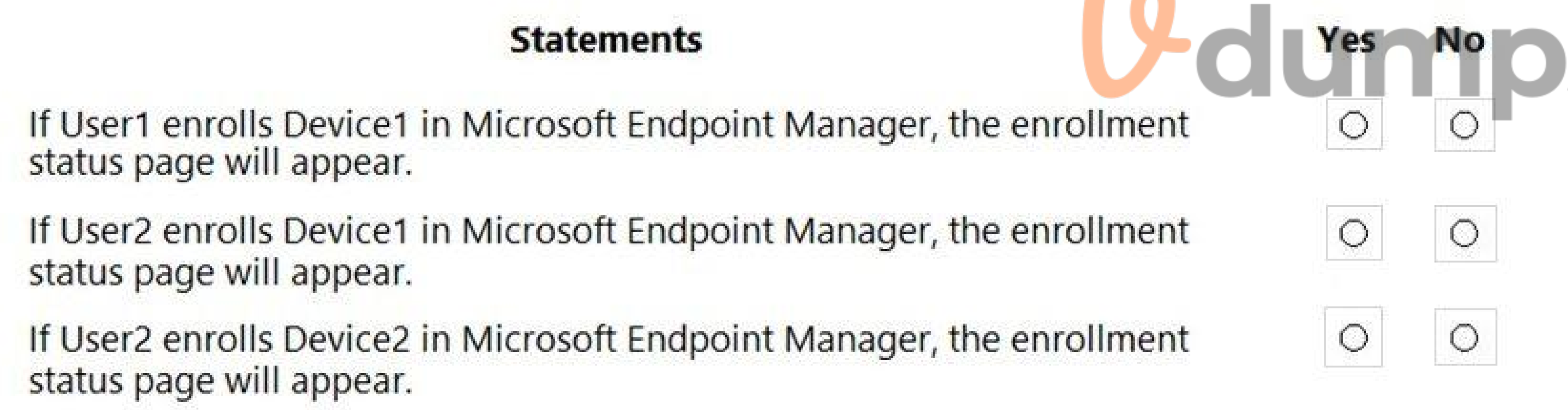
Only show page to devices provisioned by out-of-box experience (OOBE): No

Assignments: Group2

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

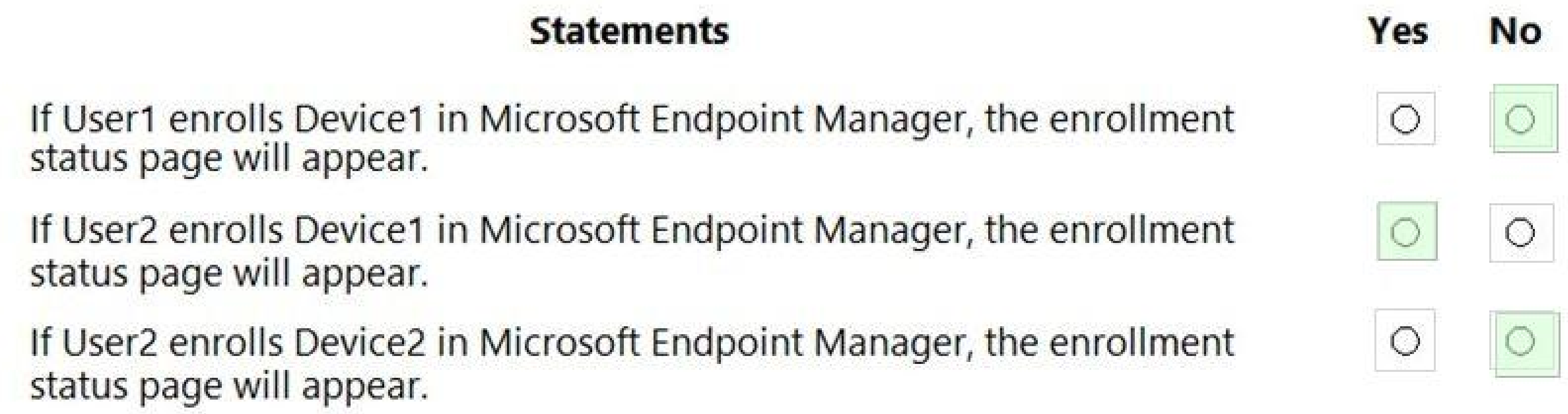
NOTE: Each correct selection is worth one point.

Hot Area:



Statements	Yes	No
If User1 enrolls Device1 in Microsoft Endpoint Manager, the enrollment status page will appear.	○	○
If User2 enrolls Device1 in Microsoft Endpoint Manager, the enrollment status page will appear.	○	○
If User2 enrolls Device2 in Microsoft Endpoint Manager, the enrollment status page will appear.	○	○

Answer Area:

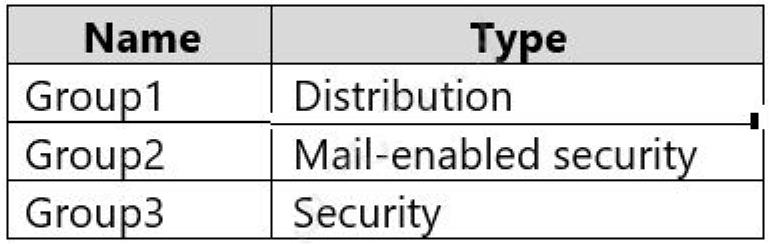


Statements	Yes	No
If User1 enrolls Device1 in Microsoft Endpoint Manager, the enrollment status page will appear.	○	[✓ ○]
If User2 enrolls Device1 in Microsoft Endpoint Manager, the enrollment status page will appear.	[✓ ○]	○
If User2 enrolls Device2 in Microsoft Endpoint Manager, the enrollment status page will appear.	○	[✓ ○]

Section:

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

QUESTION 95
You have a Microsoft 365 tenant that contains the groups shown in the following table.



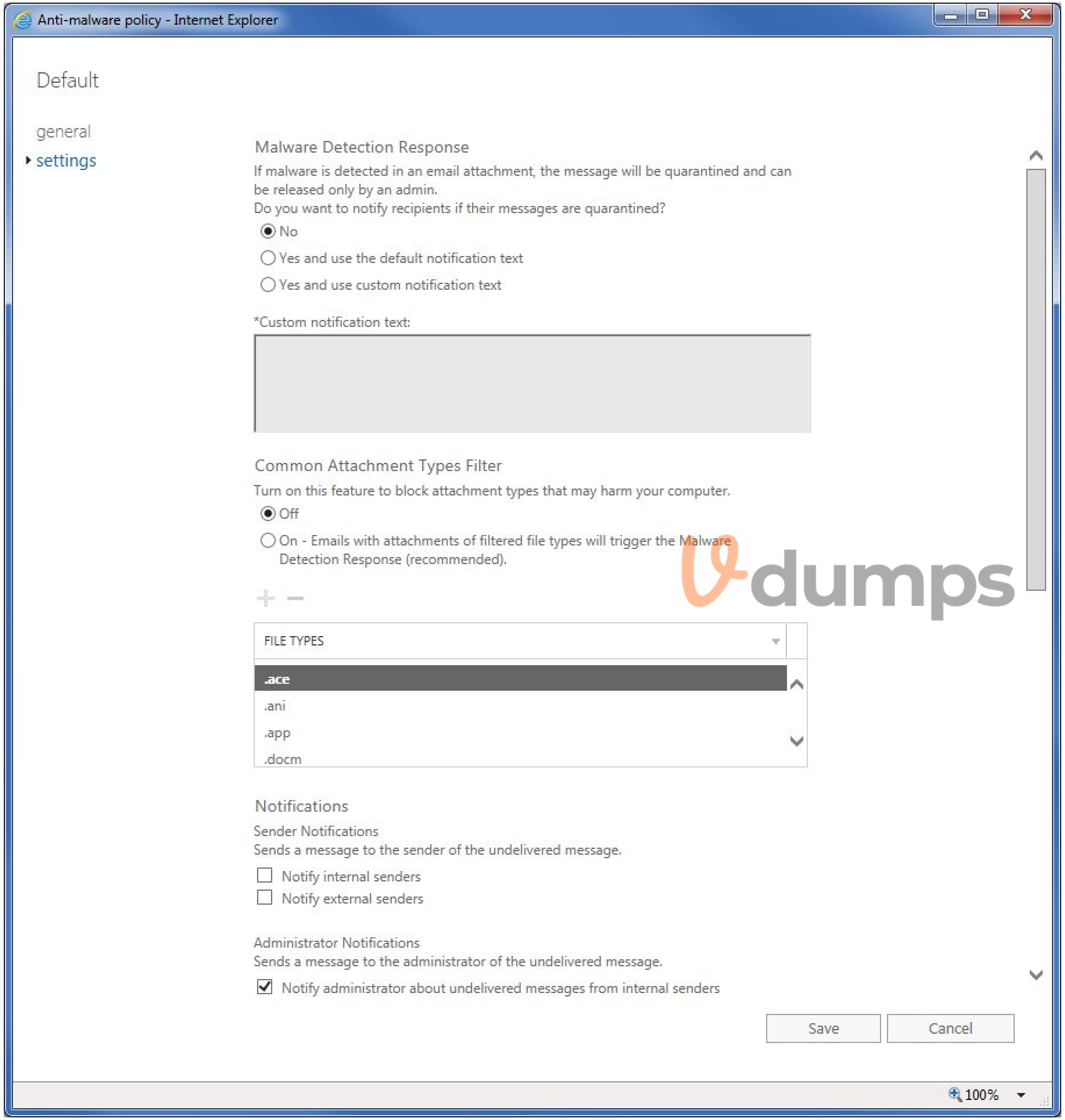
Name	Type
Group1	Distribution
Group2	Mail-enabled security
Group3	Security

You plan to create a new Windows 10 Security Baseline profile.
To which groups can you assign to the profile?

A. Group3 only
B. Group1 and Group3 only
C. Group2 and Group3 only
D. Group1. Group2. and Group3

Correct Answer: A
Section:
Explanation:
https://docs.microsoft.com/en-us/mem/intune/protect/security-baselines-configure#create-the-profile
https://docs.microsoft.com/en-us/microsoft-365/admin/create-groups/compare-groups?view=o365-worldwide

QUESTION 96
You have a Microsoft 365 E5 subscription that contains a user named User1.
The subscription has a single anti-malware policy as shown in the following exhibit.



Anti-malware policy - Internet Explorer

Default

general

settings

Malware Detection Response

If malware is detected in an email attachment, the message will be quarantined and can be released only by an admin.

Do you want to notify recipients if their messages are quarantined?

● No

○ Yes and use the default notification text

○ Yes and use custom notification text

*Custom notification text:

Common Attachment Types Filter

Turn on this feature to block attachment types that may harm your computer.

● Off

○ On - Emails with attachments of filtered file types will trigger the Malware Detection Response (recommended).

FILE TYPES
.ace
.ani
.app
.docm

Notifications

Sender Notifications

Sends a message to the sender of the undelivered message.

□ Notify internal senders

□ Notify external senders

Administrator Notifications

Sends a message to the administrator of the undelivered message.

☑ Notify administrator about undelivered messages from internal senders

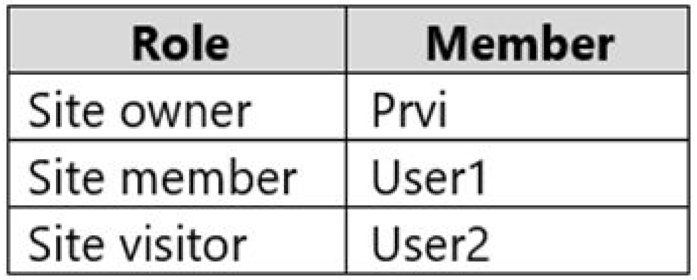
An email message that contains text and two attachments is sent to User1. One attachment is infected with malware.

How will the email message and the attachments be processed?

A. Both attachments will be removed. The email message will be quarantined, and Used will receive an email message without any attachments and an email message that includes the following text: 'Malware was removed.'
B. The email message will be quarantined, and the message will remain undelivered.
C. Both attachments will be removed. The email message will be quarantined, and User1 will receive a copy of the message containing the original text and a new attachment that includes the following text: 'Malware was removed.'
D. The malware-infected attachment will be removed. The email message will be quarantined, and User1 will receive a copy of the message containing only the uninfected attachment.

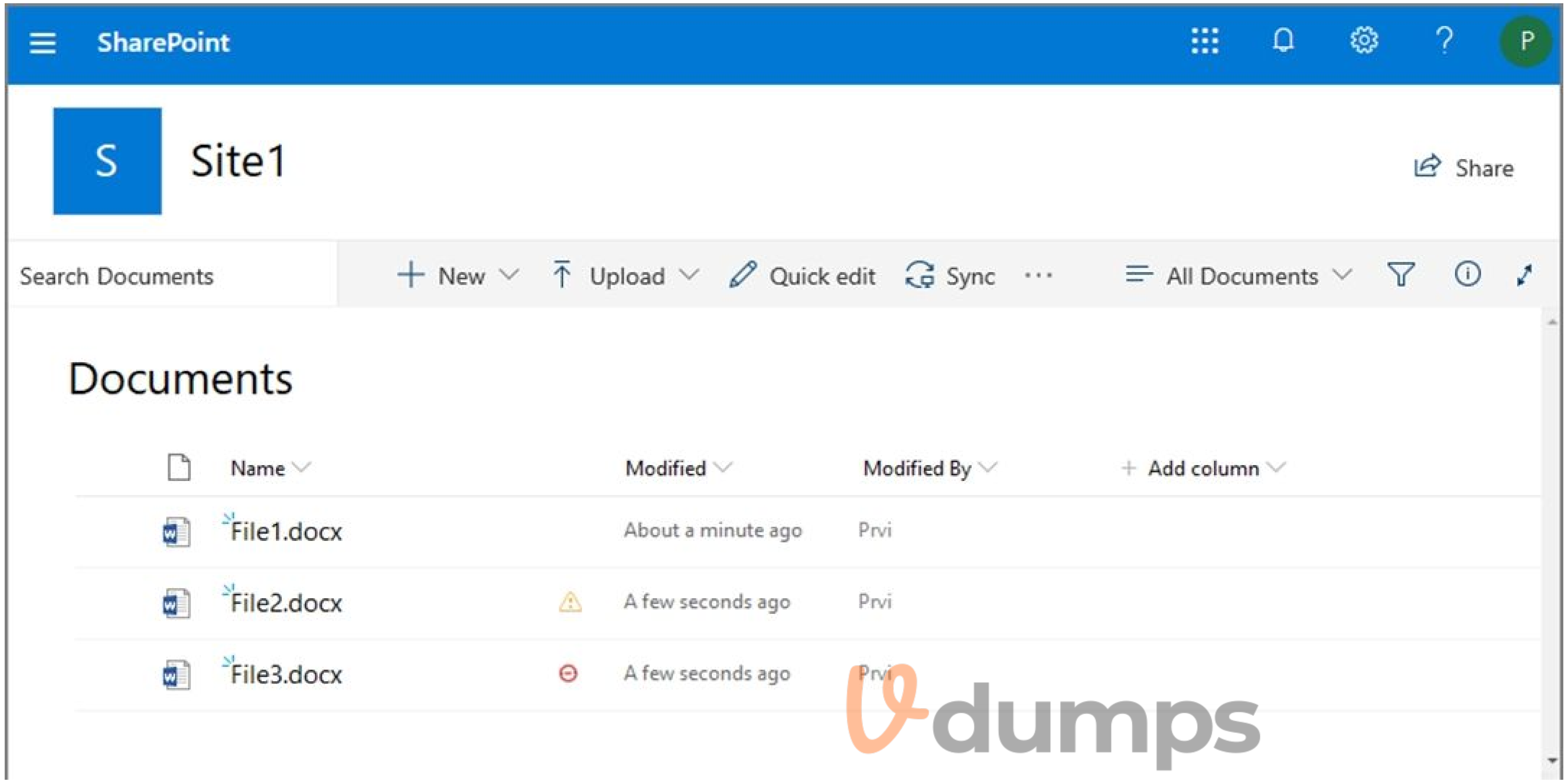
Correct Answer: C
Section:
Explanation:
https://docs.microsoft.com/en-us/microsoft-365/security/office-365-security/anti-malware-protection?view=o365-worldwide#anti-malware-policies

QUESTION 97
HOTSPOT
From the Microsoft 365 compliance center, you configure a data loss prevention (DLP) policy for a Microsoft SharePoint Online site named Site1. Site1 contains the roles shown in the following table.



Role	Member
Site owner	Prvi
Site member	User1
Site visitor	User2

Prvi creates the files shown in the exhibit. (Click the Exhibit tab.)

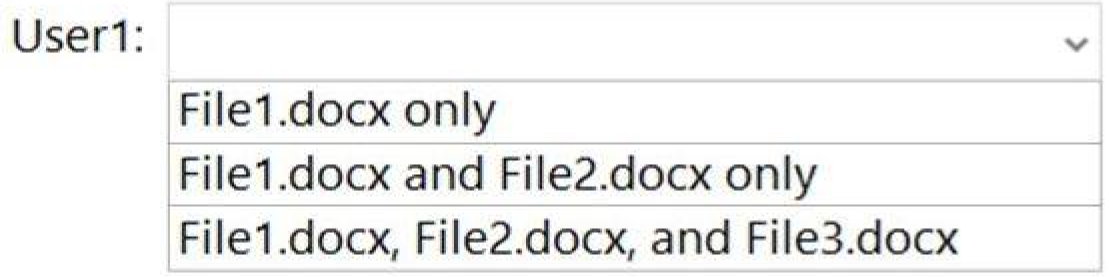


Documents

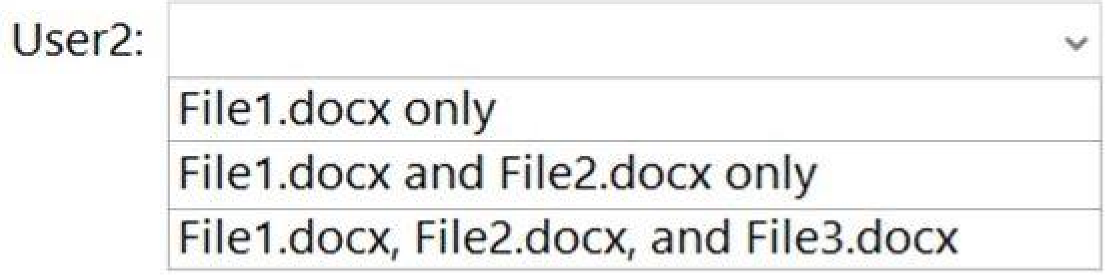
Name		Modified	Modified By	Add column
File1.docx		About a minute ago	Prvi	
File2.docx	⚠	A few seconds ago	Prvi	
File3.docx	⊖	A few seconds ago	Prvi	

Which files can User1 and User2 open? To answer, select the appropriate options in the answer area.
NOTE: Each correct selection is worth one point.

Hot Area:

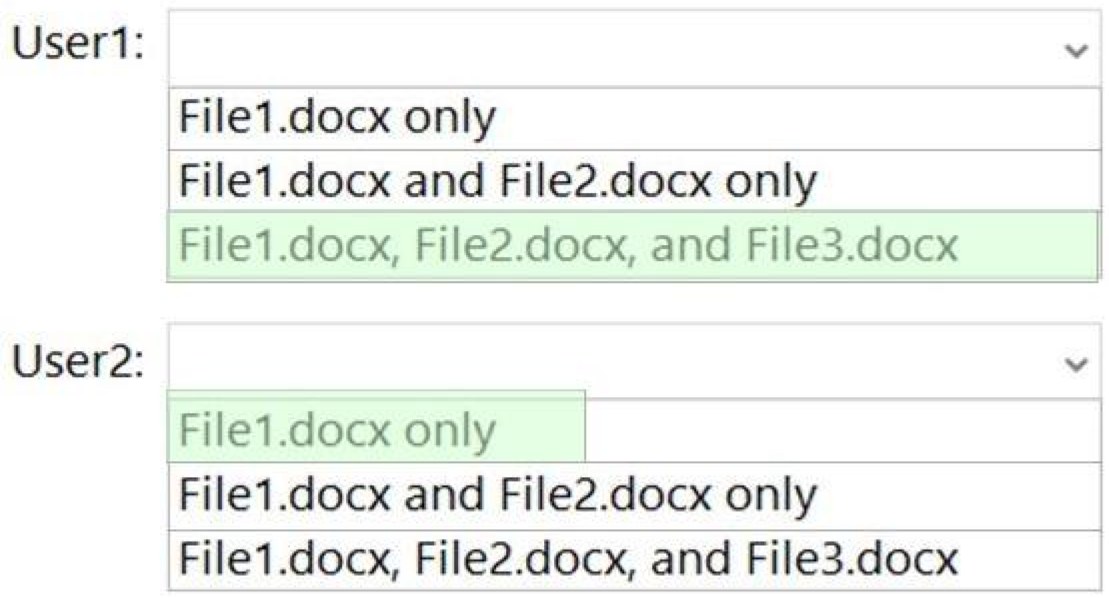

User1:

- File1.docx only
- File1.docx and File2.docx only
- File1.docx, File2.docx, and File3.docx


User2:

- File1.docx only
- File1.docx and File2.docx only
- File1.docx, File2.docx, and File3.docx

Answer Area:



User1:

File1.docx only

File1.docx and File2.docx only

[✓ File1.docx, File2.docx, and File3.docx]

User2:

[✓ File1.docx only]

File1.docx and File2.docx only

File1.docx, File2.docx, and File3.docx

Section:

Explanation:

https://sharepointmaven.com/4-security-roles-of-a-sharepoint-site/

https://gcc.microsoftcrmportals.com/blogs/office365-news/190220SPIcons/

QUESTION 98

Your on-premises network contains an Active Directory domain named Contoso.com and 500 devices that run either macOS, Windows 8.1. Windows 10, or Windows 11. All the devices are managed by using Microsoft Endpoint Configuration Manager. The domain syncs with Azure Active Directory (Azure AD).

You plan to implement a Microsoft 365 E5 subscription and enable co-management. Which devices can be co-managed after the implementation?

A. Windows 11 and Windows 10 only

B. Windows 11, Windows 10-Windows8.1.andmacOS

C. Windows 11 and macOS only

D. Windows 11 only

E. Windows 11. Windows 10, and Windows8.1 only

Correct Answer: C

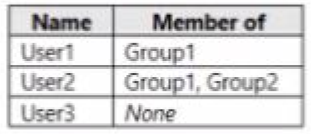
Section:

QUESTION 99

HOTSPOT

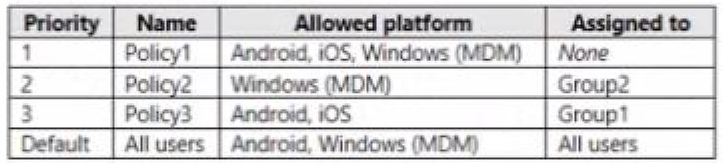
You have several devices enrolled in Microsoft Endpoint Manager.

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



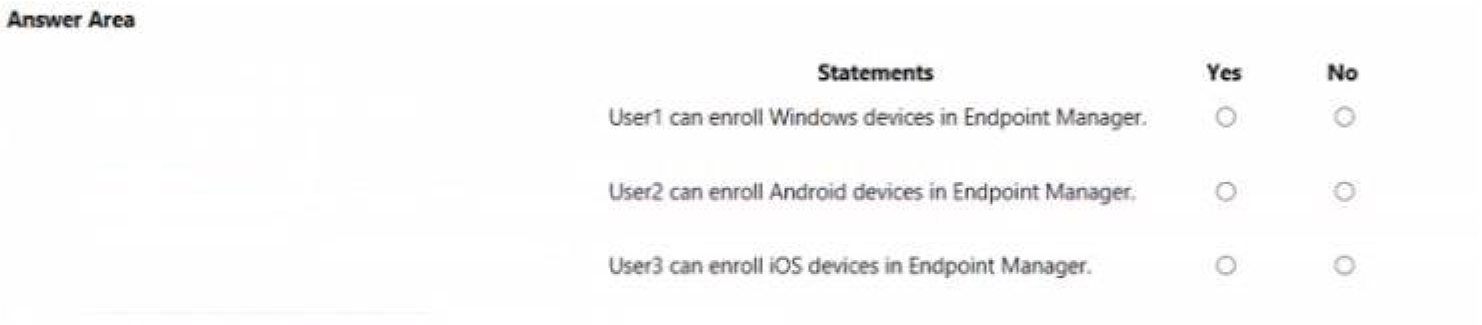
Name	Member of
User1	Group1
User2	Group1, Group2
User3	*None*

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

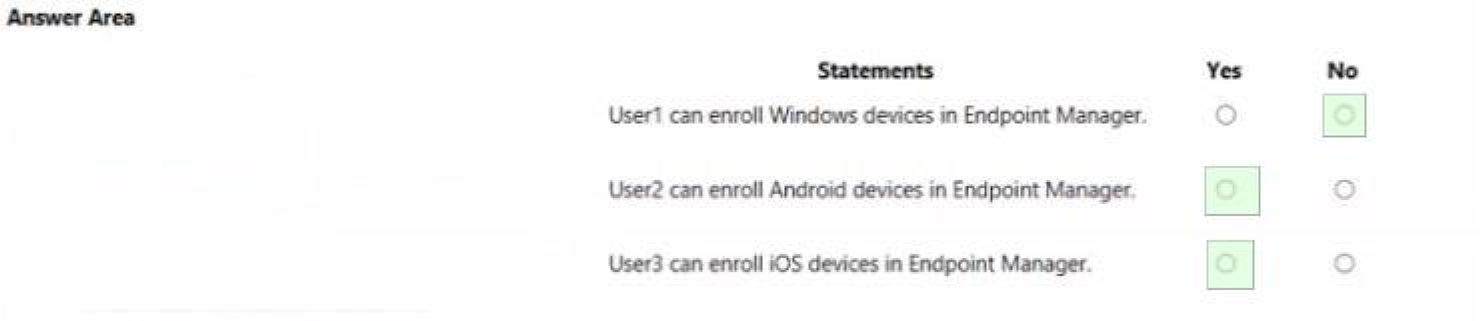
Hot Area:



Answer Area

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

Answer Area:



Answer Area

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

Section:

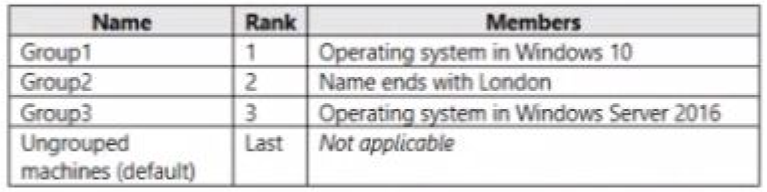
Explanation:

QUESTION 100

HOTSPOT

You use Microsoft Defender for Endpoint.

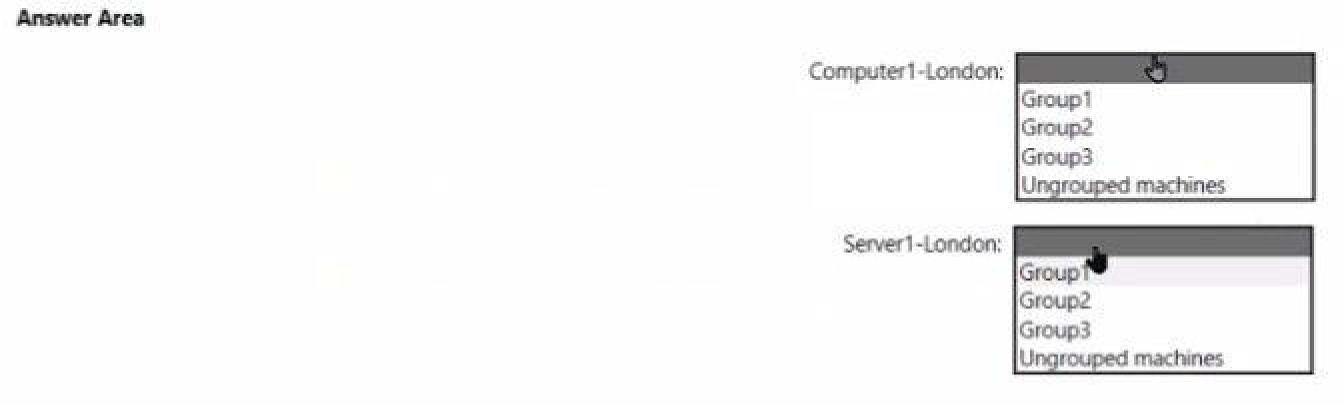
You have the Microsoft Defender for Endpoint device groups shown in the following table



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 for Endpoint as shown in the following table.

Hot Area:

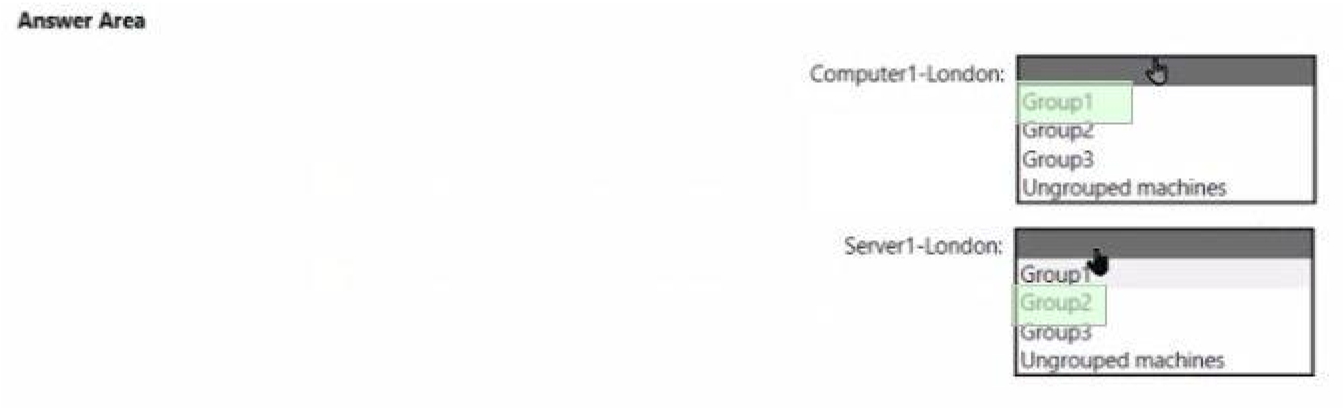


Answer Area

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

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

Answer Area:



Answer Area

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

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

Section:
Explanation:

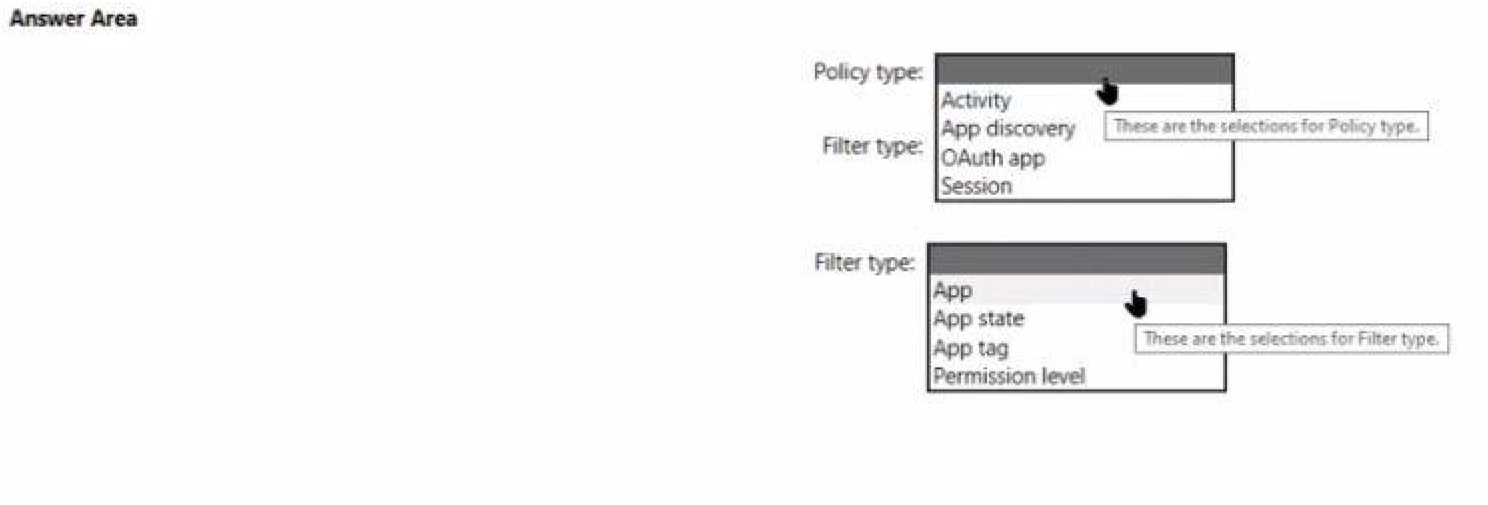
QUESTION 101
You have a Microsoft 365 E5 subscription.
You create an account tor a new security administrator named SecAdmin1.
You need to ensure that SecAdmin1 can manage Microsoft Defender for Office 365 settings and policies for Microsoft Teams, SharePoint and OneDrive.
Solution: From the Azure Active Directory admin center, you assign SecAdmin1 the Teams Administrator role.
Does this meet the goal?

A. Yes
B. no

Correct Answer: B
Section:

QUESTION 102
HOTSPOT
You have a Microsoft 365 E5 subscription that uses Microsoft Defender for Cloud Apps.
You need to create a policy that will generate an email alert when a banned app is detected requesting permission to access user information or data in the subscription.
What should you configure? To answer, select the appropriate options in the answer area.
NOTE: Each correct selection is worth one point.

Hot Area:



Answer Area

Policy type:
- Activity
- App discovery
- OAuth app
- Session

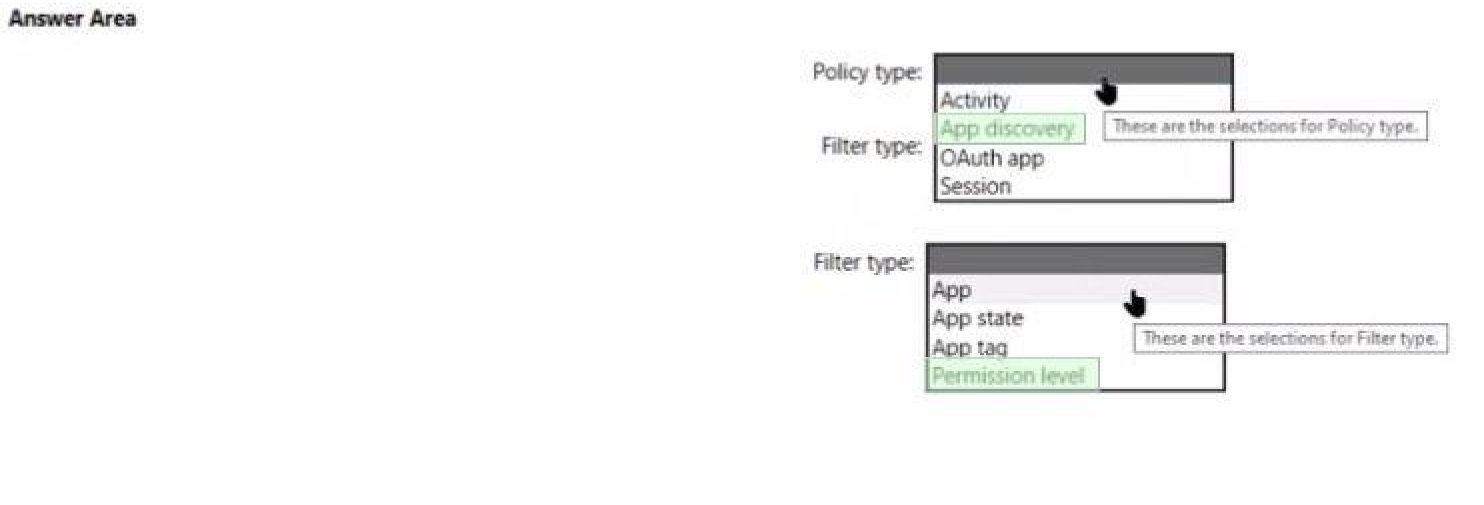
These are the selections for Policy type.

Filter type:

Filter type:
- App
- App state
- App tag
- Permission level

These are the selections for Filter type.

Answer Area:



Answer Area

Policy type:

- Activity
- App discovery
- OAuth app
- Session

These are the selections for Policy type.

Filter type:

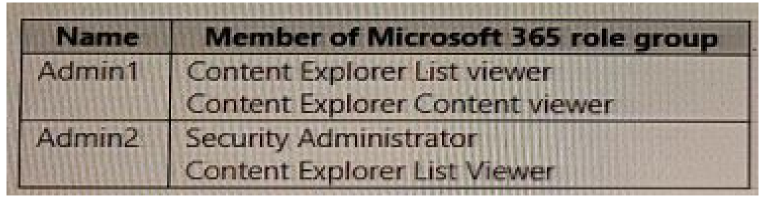
Filter type:

- App
- App state
- App tag
- Permission level

These are the selections for Filter type.

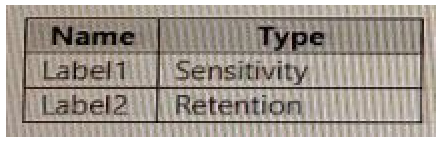
Section:
Explanation:

QUESTION 103
HOTSPOT
You have a Microsoft 365 E5 subscription that contains the users shown in the following table.



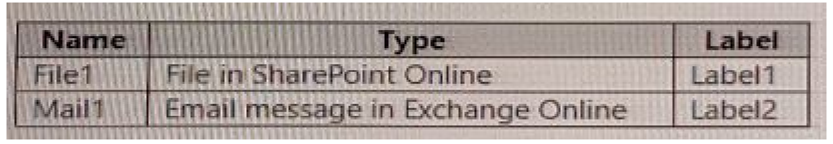
Name	Member of Microsoft 365 role group
Admin1	Content Explorer List viewer Content Explorer Content viewer
Admin2	Security Administrator Content Explorer List Viewer

You have labels in Microsoft 365 as shown in the following table.



Name	Type
Label1	Sensitivity
Label2	Retention

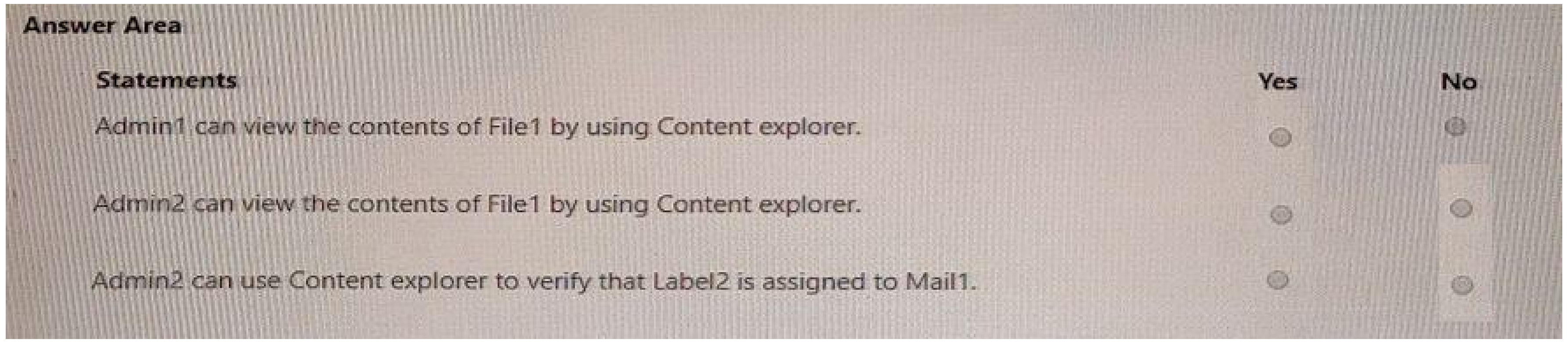
The content in Microsoft 365 is assigned labels as shown in the following table.



Name	Type	Label
File1	File in SharePoint Online	Label1
Mail1	Email message in Exchange Online	Label2

You have labels In Microsoft 365 as shown in the following table.
For each of the following statements, select Yes if the statement is true. Otherwise, select No.

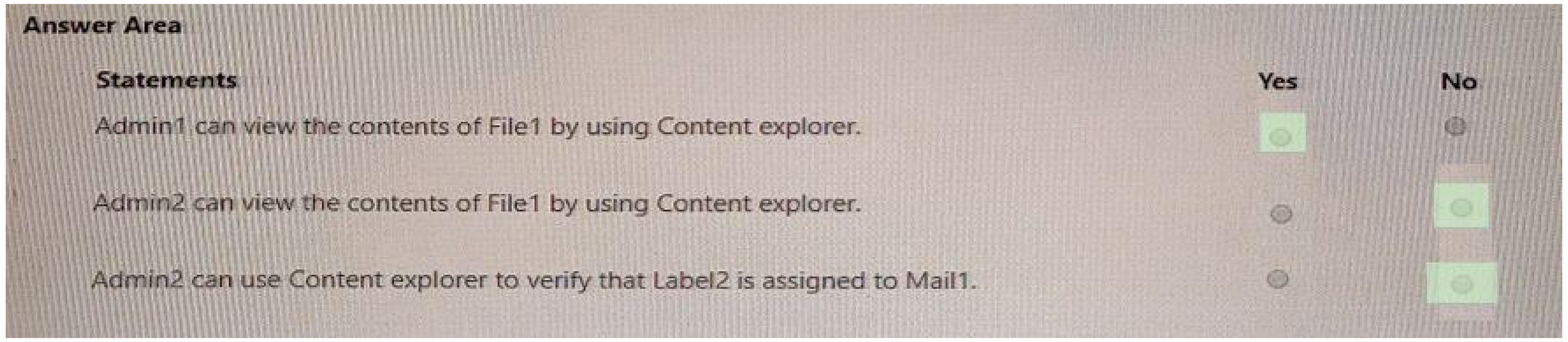
Hot Area:



Answer Area

Statements	Yes	No
Admin1 can view the contents of File1 by using Content explorer.	○	○
Admin2 can view the contents of File1 by using Content explorer.	○	○
Admin2 can use Content explorer to verify that Label2 is assigned to Mail1.	○	○

Answer Area:

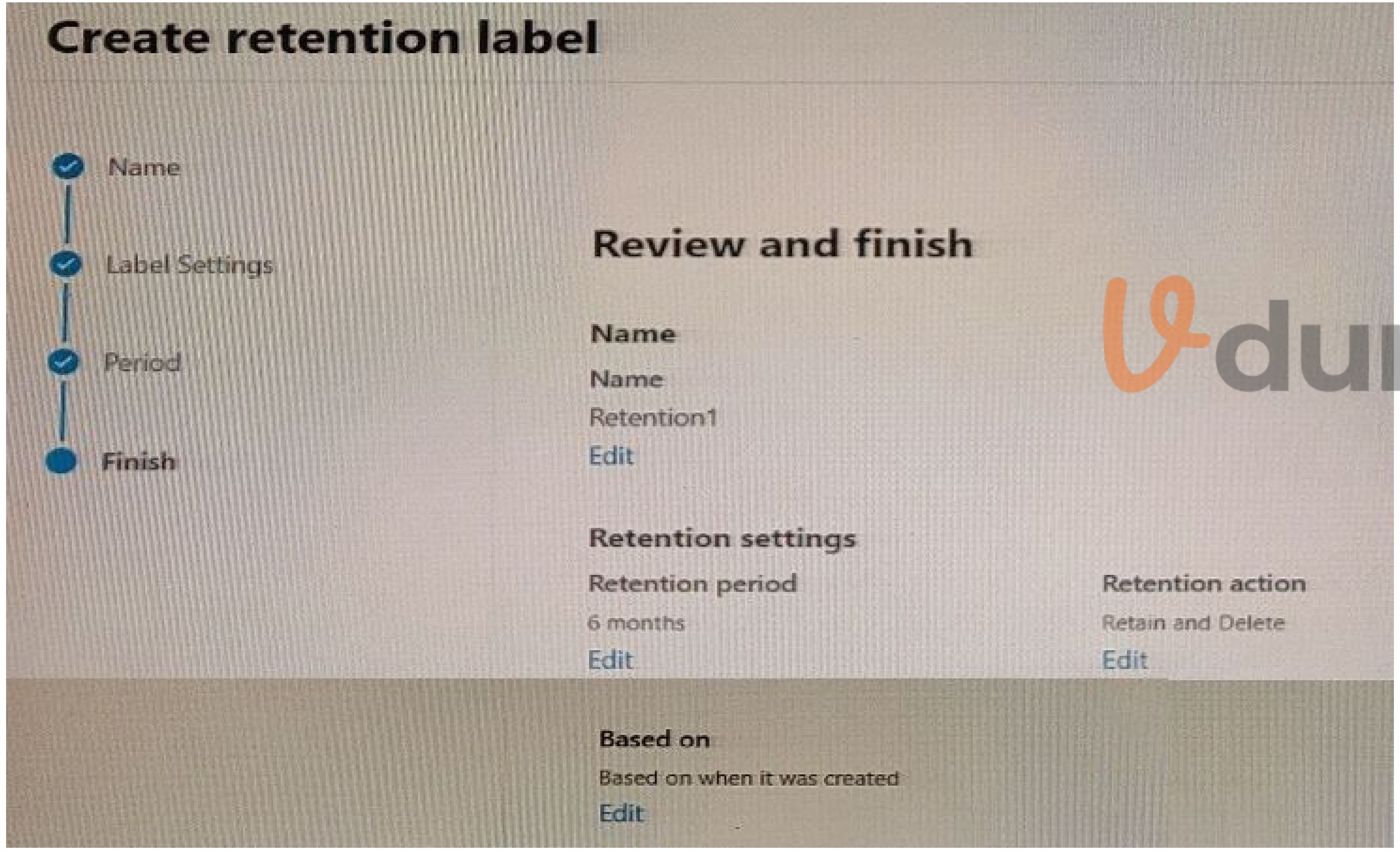


Answer Area

Statements	Yes	No
Admin1 can view the contents of File1 by using Content explorer.	[✓ ○]	○
Admin2 can view the contents of File1 by using Content explorer.	○	[✓ ○]
Admin2 can use Content explorer to verify that Label2 is assigned to Mail1.	○	[✓ ○]

Section:
Explanation:

QUESTION 104
You have a Microsoft 365 subscription.
You create a retention label named Retention1 as shown in the following exhibit.



Create retention label

Review and finish

Name

Name
Retention1
Edit

Retention settings

Retention period
6 months
Edit

Retention action
Retain and Delete
Edit

Based on
Based on when it was created
Edit

You apply Retention! to all the Microsoft OneDrive content.
On January 1, 2020, a user stores a file named File1 in OneDrive.
On January 10, 2020, the user modifies File1.
On February 1, 2020, the user deletes File1.
When will File1 be removed permanently and unrecoverable from OneDrive?

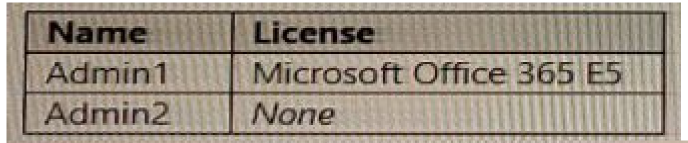
A. February 1, 2020
B. July 1.2020
C. July 10, 2020
D. August 1, 2020

Correct Answer: B
Section:

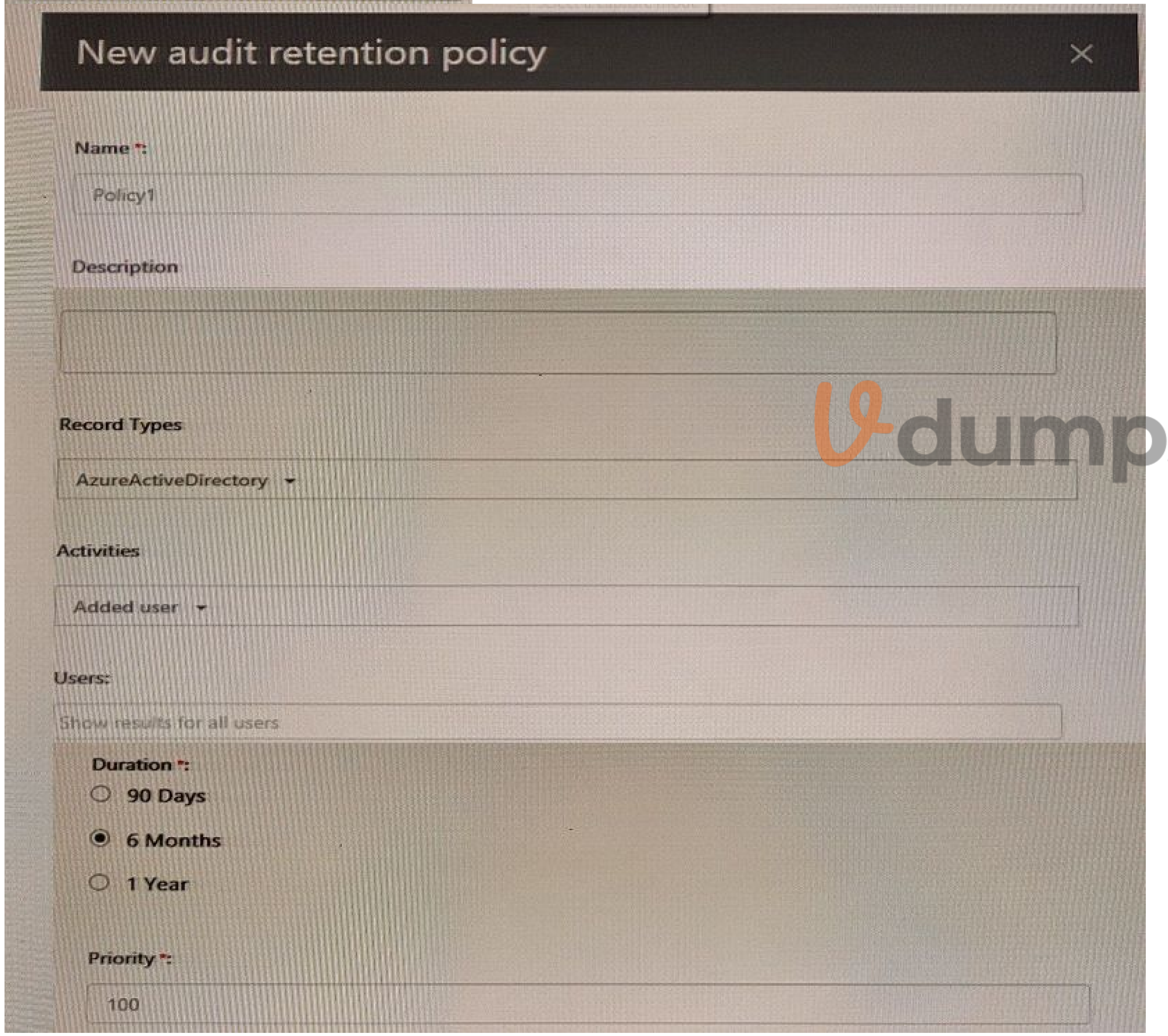
QUESTION 105

HOTSPOT

You have a Microsoft 365 E5 subscription that has auditing turned on. The subscription contains the users shown in the following table.



Name	License
Admin1	Microsoft Office 365 E5
Admin2	*None*



New audit retention policy

Name *: Policy1

Description

Record Types: AzureActiveDirectory

Activities: Added user

Users: Show results for all users

Duration *:
○ 90 Days
● 6 Months
○ 1 Year

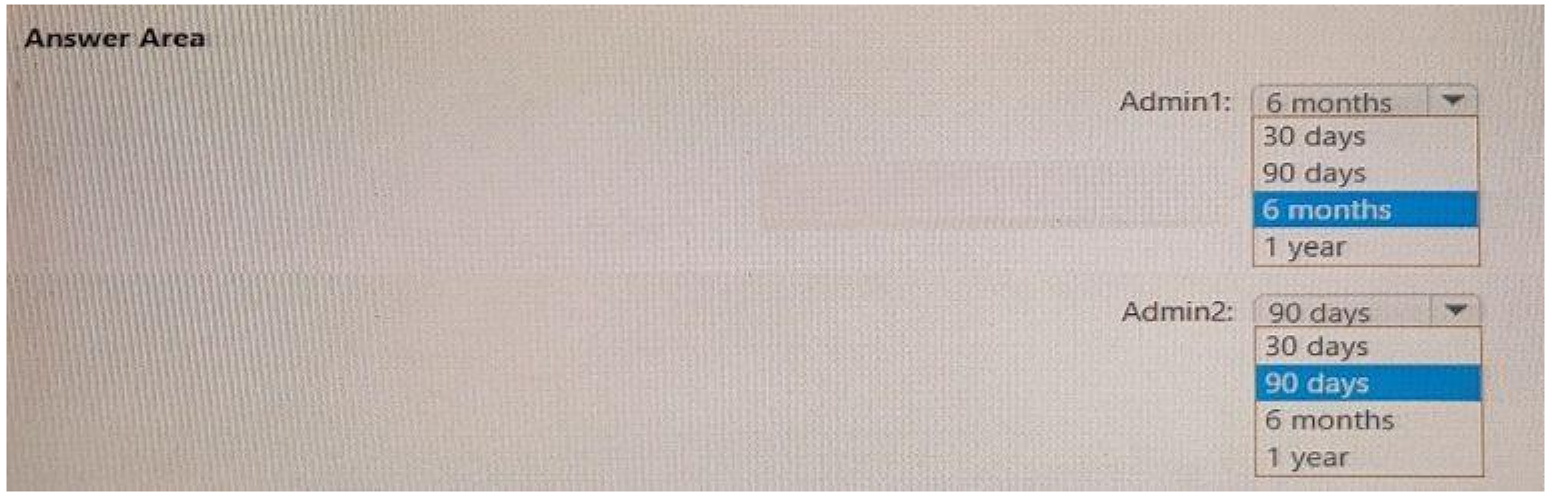
Priority *: 100

You plan to create a new user named User1.

How long will the user creation audit event be available if Admin1 or Admin2 creates User1? To answer, select the appropriate options in the answer area.

Each correct selection is worth one point.

Hot Area:



Answer Area

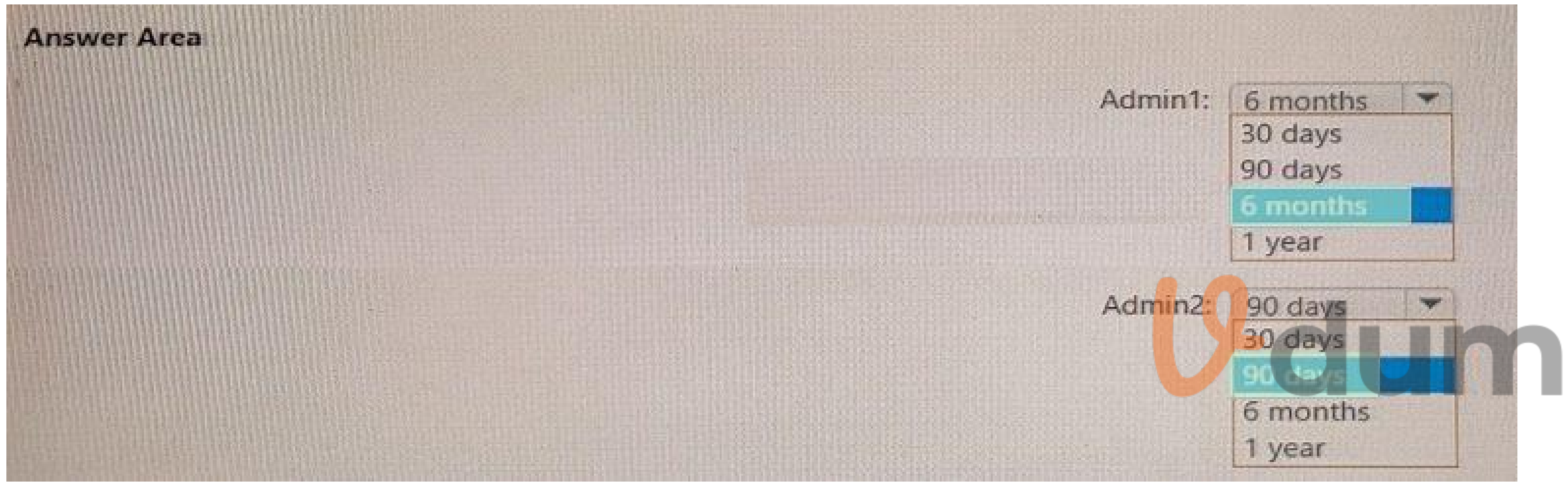
Admin1: 6 months

- 30 days
- 90 days
- 6 months
- 1 year

Admin2: 90 days

- 30 days
- 90 days
- 6 months
- 1 year

Answer Area:



Answer Area

Admin1: 6 months

- 30 days
- 90 days
- 6 months
- 1 year

Admin2: 90 days

- 30 days
- 90 days
- 6 months
- 1 year

Section:
Explanation:

QUESTION 106

You have a Microsoft 365 subscription.
From Microsoft 365 Defender, 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:

QUESTION 107

You have a Microsoft 365 subscription that uses Microsoft Defender for Office 365.
A Built-in protection preset security policy is applied to the subscription.
Which two policy types will be applied by the Built-in protection policy? Each correct answer presents a complete solution.
NOTE: Each correct selection is worth one point.

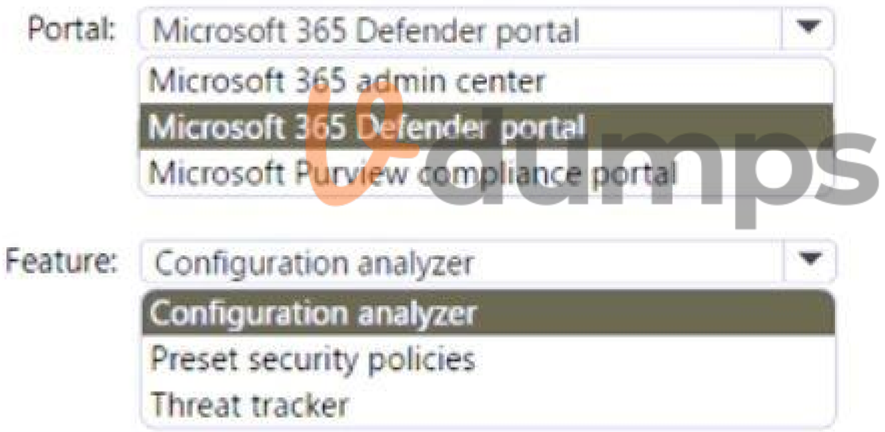
A. Anti-malware
B. Anti-phishing
C. Safe Attachments
D. Anti-spam
E. Safe Links

Correct Answer: C, E
Section:

QUESTION 108
HOTSPOT
You have a Microsoft 365 subscription that uses Microsoft Defender for Office 365.
You need to identify the settings that are below the Standard protection profile settings in the preset security policies.
What should you use? To answer, select the appropriate options in the answer area.
NOTE: Each correct selection is worth one point.

Hot Area:

Answer Area



Portal: Microsoft 365 Defender portal

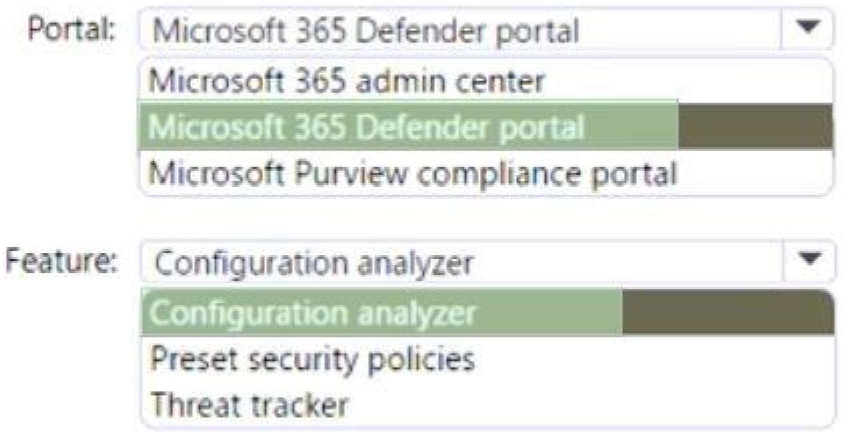
Microsoft 365 admin center
Microsoft 365 Defender portal
Microsoft Purview compliance portal

Feature: Configuration analyzer

Configuration analyzer
Preset security policies
Threat tracker

Answer Area:

Answer Area



Portal: Microsoft 365 Defender portal

Microsoft 365 admin center
Microsoft 365 Defender portal
Microsoft Purview compliance portal

Feature: Configuration analyzer

Configuration analyzer
Preset security policies
Threat tracker

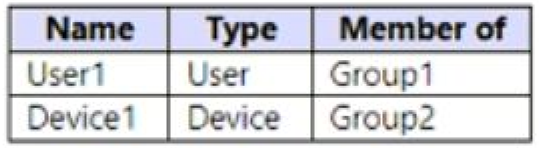
Section:

Explanation:

QUESTION 109

HOTSPOT

You have a Microsoft 365 E5 subscription that uses Microsoft intune. The subscription contains the resources shown in the following table.

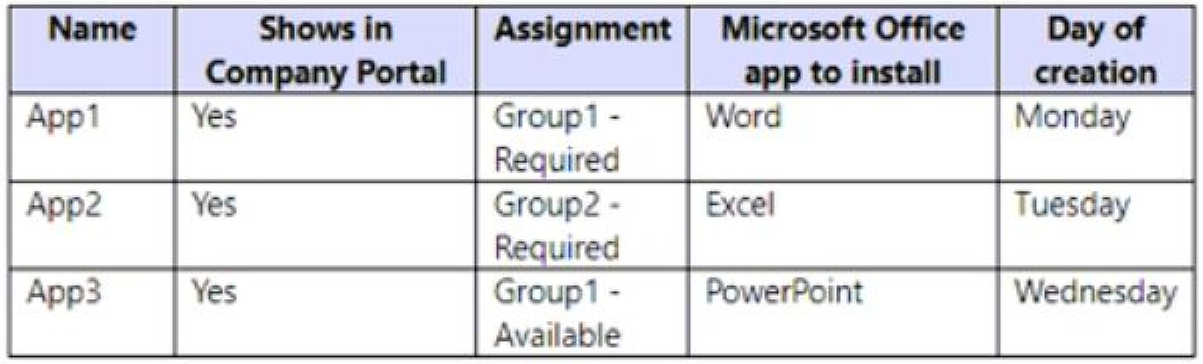


Name	Type	Member of
User1	User	Group1
Device1	Device	Group2

User1 is the owner of Device1.

You add Microsoft 365 Apps Windows 10 and later app types to Intune as shown in the following table.

On Thursday, you review the results of the app deployments.

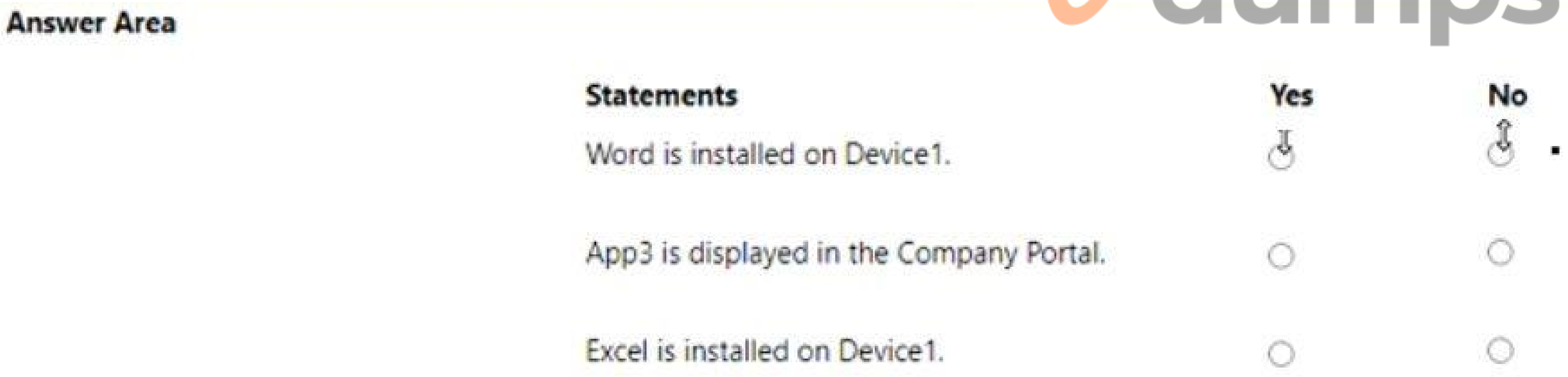


Name	Shows in Company Portal	Assignment	Microsoft Office app to install	Day of creation
App1	Yes	Group1 - Required	Word	Monday
App2	Yes	Group2 - Required	Excel	Tuesday
App3	Yes	Group1 - Available	PowerPoint	Wednesday

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

NOTE: Each correct selection is worth one point.

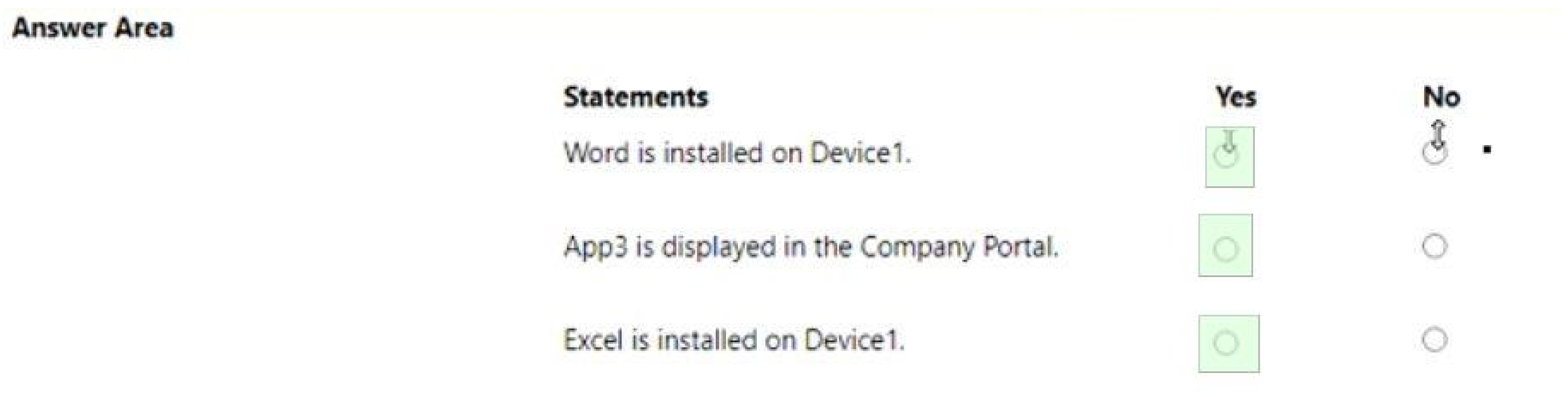
Hot Area:



Answer Area

Statements	Yes	No
Word is installed on Device1.	○	○
App3 is displayed in the Company Portal.	○	○
Excel is installed on Device1.	○	○

Answer Area:



Answer Area

Statements	Yes	No
Word is installed on Device1.	[✓ ○]	○
App3 is displayed in the Company Portal.	[✓ ○]	○
Excel is installed on Device1.	[✓ ○]	○

Section:
Explanation:

QUESTION 110
You have a Microsoft 365 tenant.
You plan to implement device configuration profiles in Microsoft Intune.
Which platform can you manage by using the profiles?

A. Ubuntu Linux
B. macOS
C. Android Enterprise
D. Windows 8.1

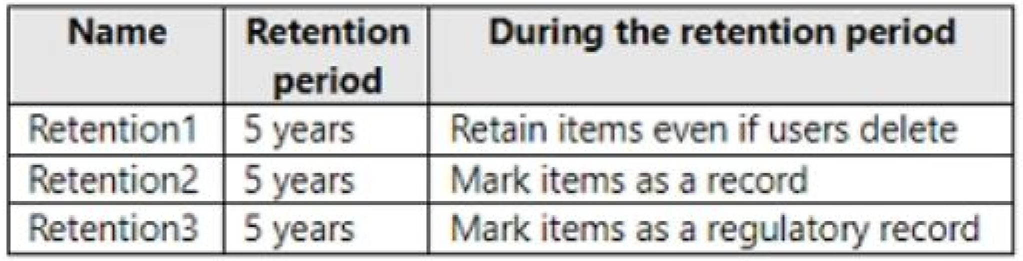
Correct Answer: D
Section:

QUESTION 111
You have a Microsoft 365 subscription that uses Microsoft Defender for Cloud Apps.
You configure a session control policy to block downloads from SharePoint Online sites.
Users report that they can still download files from SharePoint Online sites.
You need to ensure that file download is blocked while still allowing users to browse SharePoint Online sites.
What should you configure?

A. an access policy
B. a data loss prevention (DLP) policy
C. an activity policy
D. a Conditional Access policy

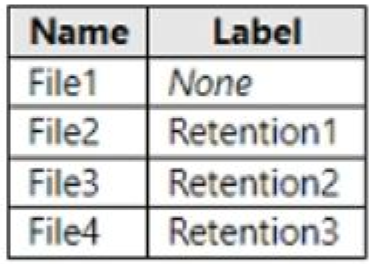
Correct Answer: A
Section:

QUESTION 112
HOTSPOT
You have a Microsoft 365 subscription that contains a user named User1 and a Microsoft SharePoint Online site named Site1. User1 is assigned the Owner role for Site1. To Site1, you publish the file plan retention labels shown in the following table.



Name	Retention period	During the retention period
Retention1	5 years	Retain items even if users delete
Retention2	5 years	Mark items as a record
Retention3	5 years	Mark items as a regulatory record

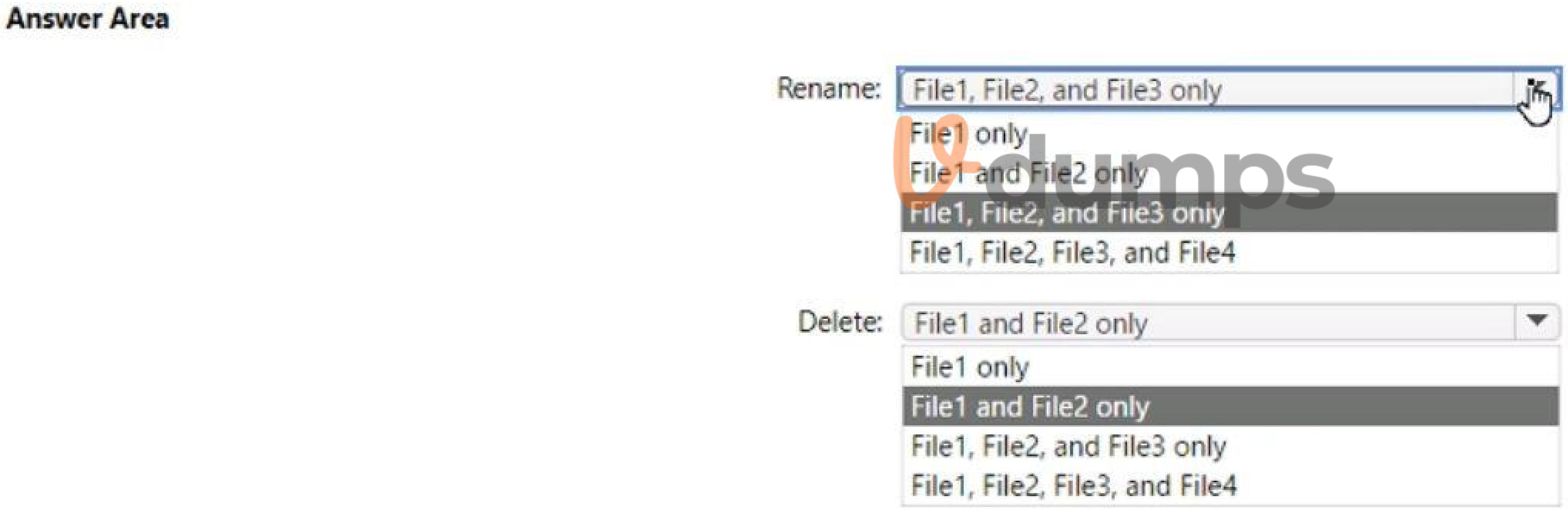
Site1 contains the files shown in the following table.



Name	Label
File1	*None*
File2	Retention1
File3	Retention2
File4	Retention3

Which files can User1 rename, and which files can User1 delete? To answer, select the appropriate options in the answer area.
NOTE: Each correct selection is worth one point.

Hot Area:



Answer Area

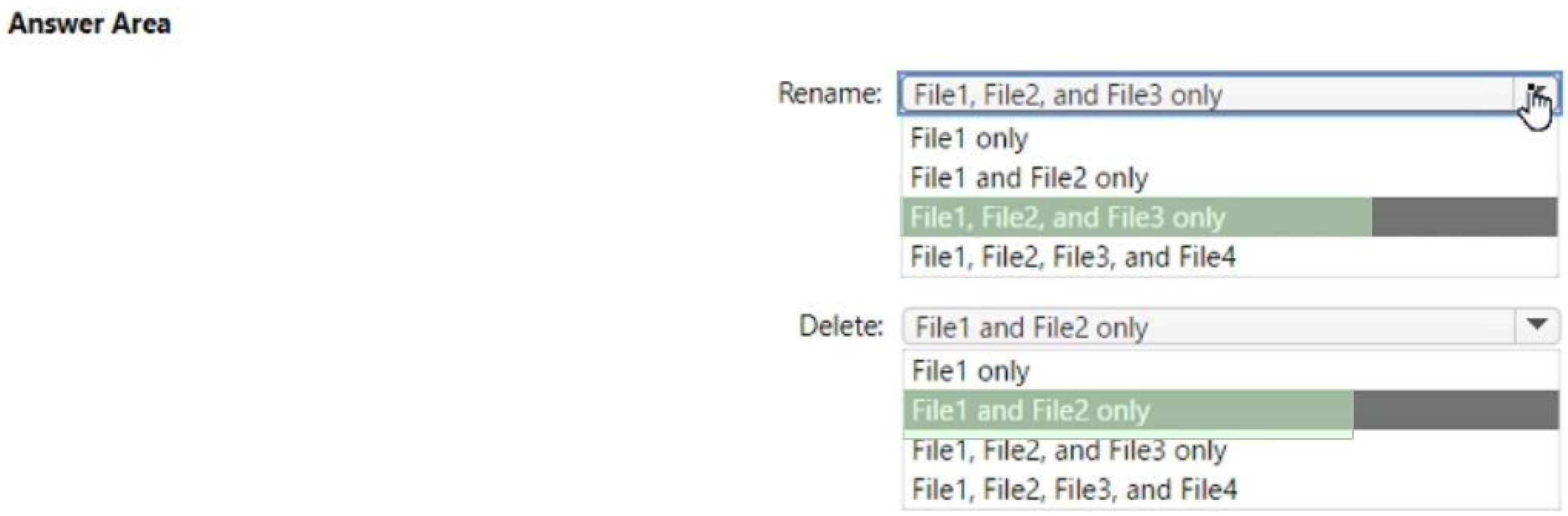
Rename: File1, File2, and File3 only

- File1 only
- File1 and File2 only
- File1, File2, and File3 only
- File1, File2, File3, and File4

Delete: File1 and File2 only

- File1 only
- File1 and File2 only
- File1, File2, and File3 only
- File1, File2, File3, and File4

Answer Area:



Answer Area

Rename: File1, File2, and File3 only

- File1 only
- File1 and File2 only
- [✓ File1, File2, and File3 only]
- File1, File2, File3, and File4

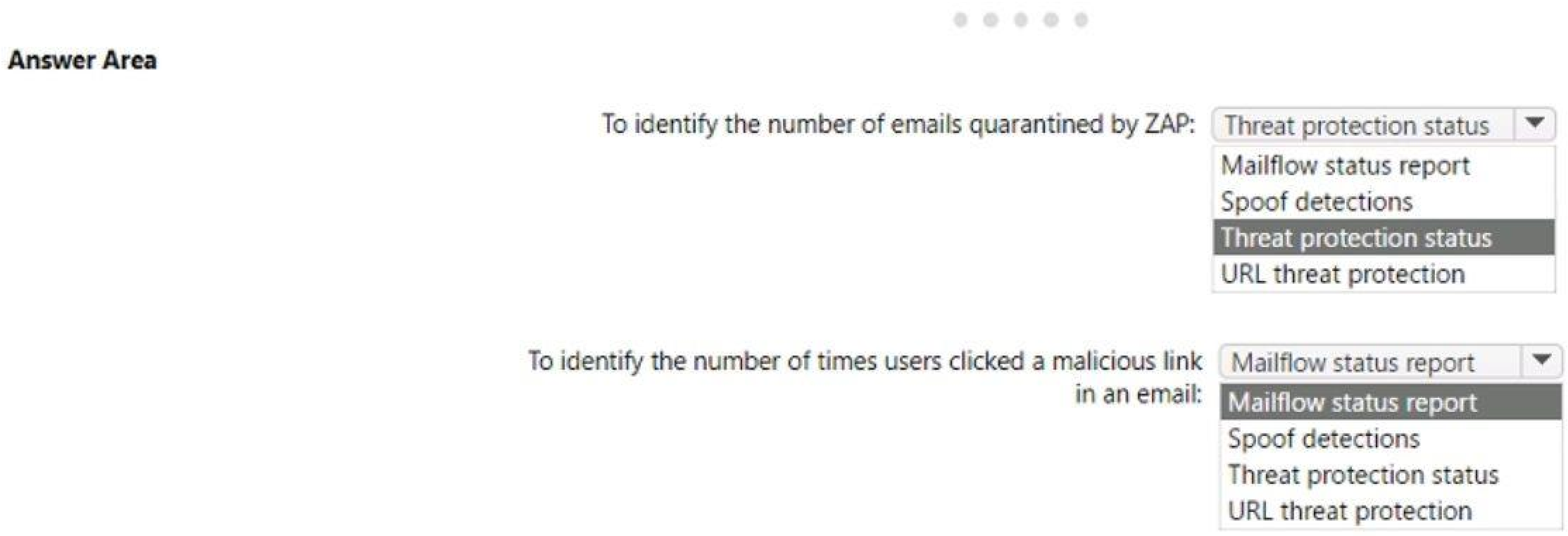
Delete: File1 and File2 only

- File1 only
- [✓ File1 and File2 only]
- File1, File2, and File3 only
- File1, File2, File3, and File4

Section:
Explanation:

QUESTION 113
HOTSPOT
You have a Microsoft 365 E5 subscription that uses Microsoft Defender for Office 365.
The subscription has the default inbound anti-spam policy and a custom Safe Attachments policy.
You need to identify the following information:
* The number of email messages quarantined by zero-hour auto purge (ZAP)
* The number of times users clicked a malicious link in an email message
Which Email & collaboration report should you use? To answer, select the appropriate options in the answer are
a. NOTE: Each correct selection is worth one point.

Hot Area:



Answer Area

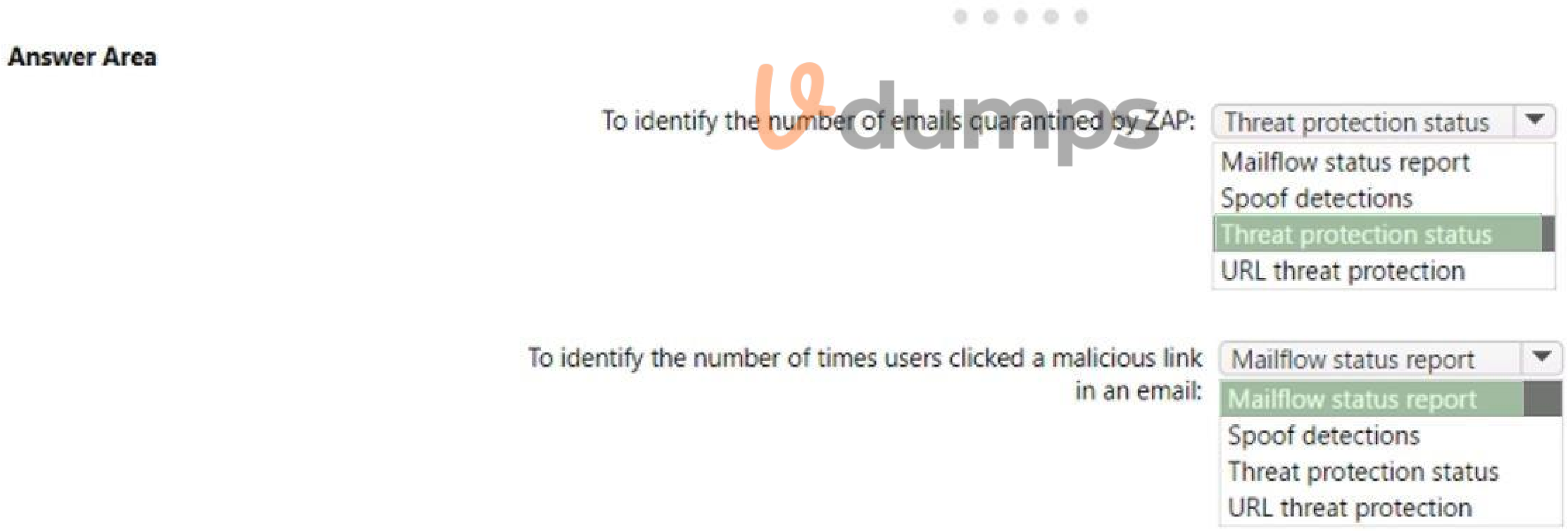
To identify the number of emails quarantined by ZAP: Threat protection status

- Mailflow status report
- Spoof detections
- Threat protection status
- URL threat protection

To identify the number of times users clicked a malicious link in an email: Mailflow status report

- Mailflow status report
- Spoof detections
- Threat protection status
- URL threat protection

Answer Area:



Answer Area

To identify the number of emails quarantined by ZAP: Threat protection status

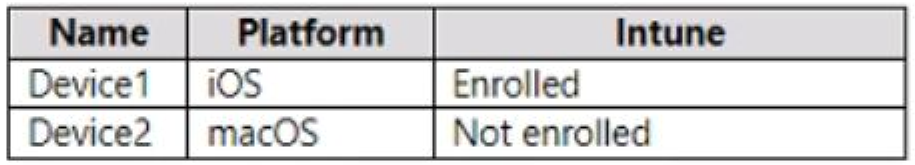
- Mailflow status report
- Spoof detections
- Threat protection status
- URL threat protection

To identify the number of times users clicked a malicious link in an email: Mailflow status report

- Mailflow status report
- Spoof detections
- Threat protection status
- URL threat protection

Section:
Explanation:

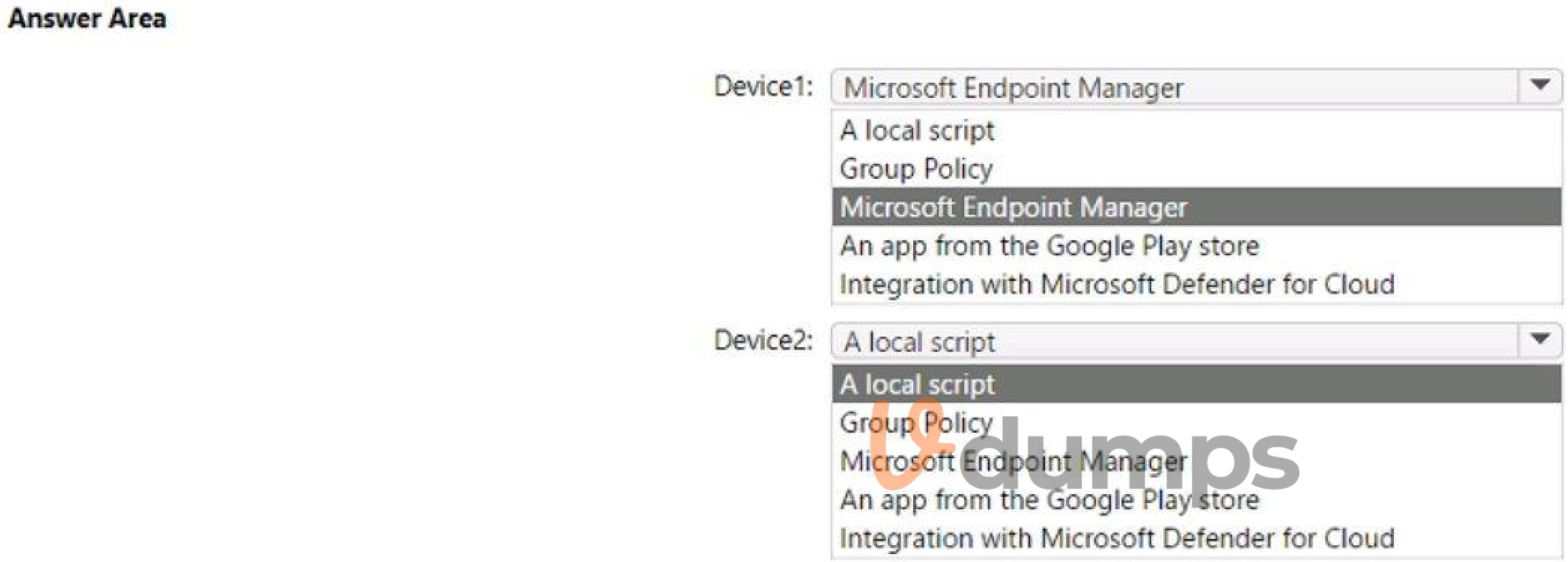
QUESTION 114
HOTSPOT
You have a Microsoft 365 E5 subscription that uses Microsoft Intune and contains the devices shown in the following table.



Name	Platform	Intune
Device1	iOS	Enrolled
Device2	macOS	Not enrolled

You need to onboard Device1 and Device2 to Microsoft Defender for Endpoint.
What should you use to onboard each device? To answer, select the appropriate options in the answer area.
NOTE: Each correct selection is worth one point.

Hot Area:



Answer Area

Device1: Microsoft Endpoint Manager

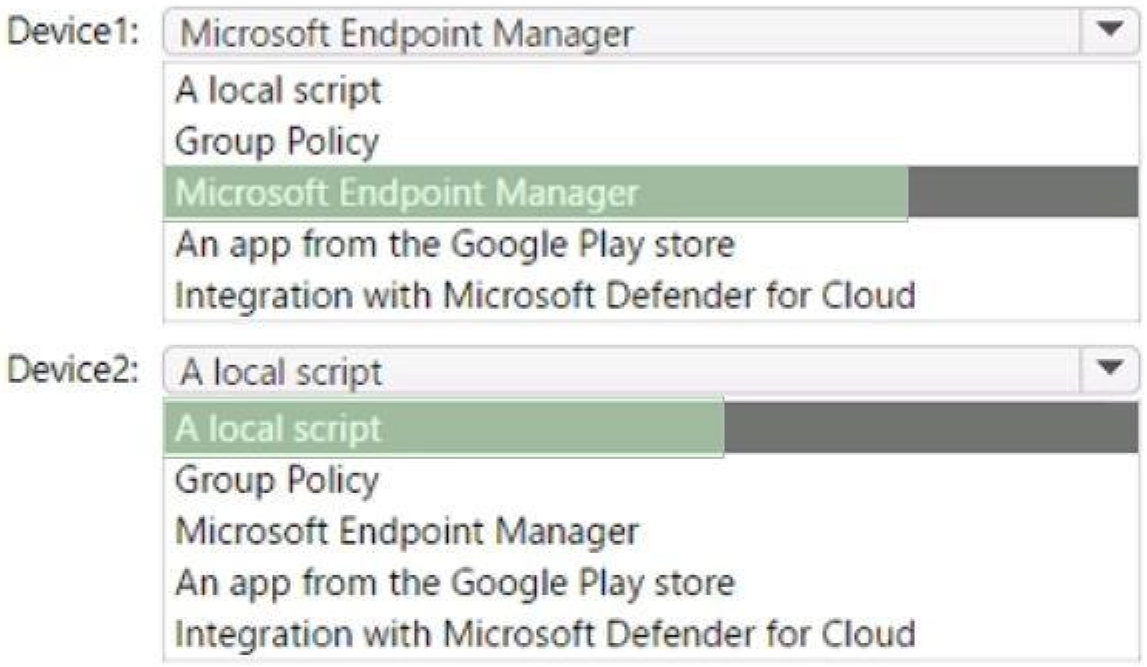
- A local script
- Group Policy
- Microsoft Endpoint Manager
- An app from the Google Play store
- Integration with Microsoft Defender for Cloud

Device2: A local script

- A local script
- Group Policy
- Microsoft Endpoint Manager
- An app from the Google Play store
- Integration with Microsoft Defender for Cloud

Answer Area:

Answer Area



Device1: Microsoft Endpoint Manager

- A local script
- Group Policy
- Microsoft Endpoint Manager
- An app from the Google Play store
- Integration with Microsoft Defender for Cloud

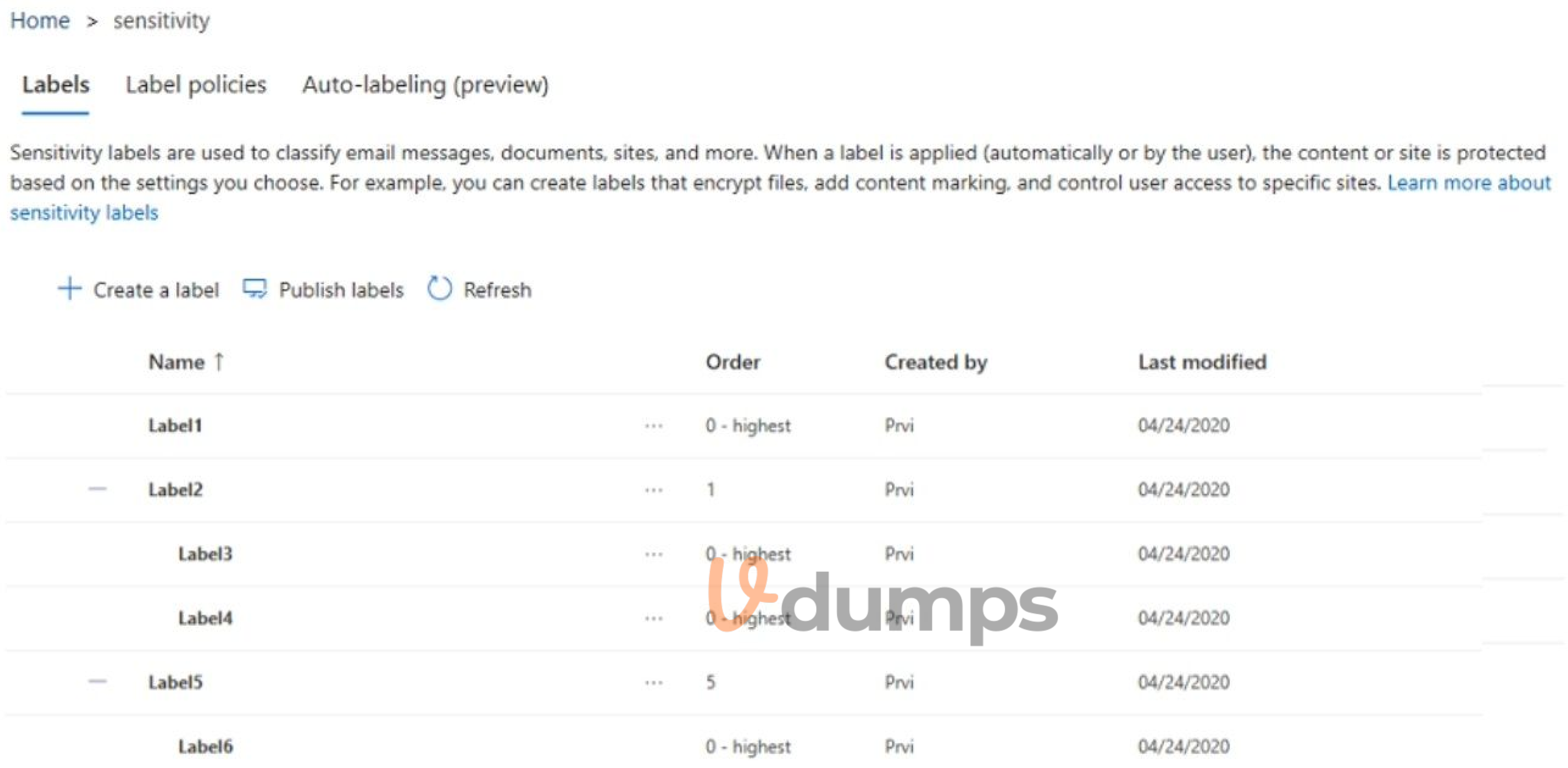
Device2: A local script

- A local script
- Group Policy
- Microsoft Endpoint Manager
- An app from the Google Play store
- Integration with Microsoft Defender for Cloud

Section:
Explanation:

QUESTION 115

You have a Microsoft 365 E5 subscription that has published sensitivity labels shown in the following exhibit.



Home > sensitivity

Labels Label policies Auto-labeling (preview)

Sensitivity labels are used to classify email messages, documents, sites, and more. When a label is applied (automatically or by the user), the content or site is protected based on the settings you choose. For example, you can create labels that encrypt files, add content marking, and control user access to specific sites. Learn more about sensitivity labels

Name ↑	Order	Created by	Last modified
Label1	0 - highest	Prvi	04/24/2020
Label2	1	Prvi	04/24/2020
Label3	0 - highest	Prvi	04/24/2020
Label4	0 - highest	Prvi	04/24/2020
Label5	5	Prvi	04/24/2020
Label6	0 - highest	Prvi	04/24/2020

Which labels can users apply to content?

A. Label1, Label2, and Label5 only
B. Label3. Label4, and Label6 only
C. Label1, Label3, Labe2, and Label6 only
D. Label1, Label2, Label3, Label4, Label5. and Label6

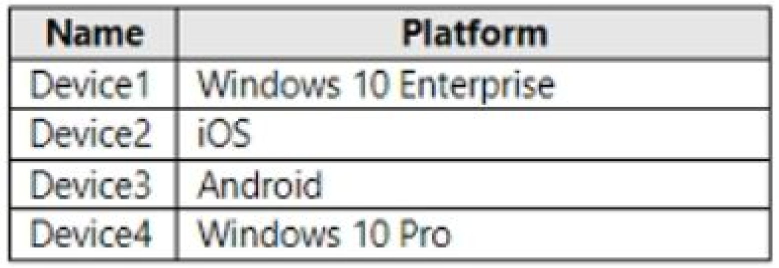
Correct Answer: C
Section:

QUESTION 116
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 the Exchange admin center create a mail flow rule.
B. From Microsoft 365 Defender, start a message trace.
C. From Microsoft Defender for Cloud Apps, create an activity policy.
D. From the Microsoft Purview compliance portal, create a label and a label policy.

Correct Answer: D
Section:

QUESTION 117
You have a Microsoft 365 E5 tenant that contains the devices shown in the following table.



Name	Platform
Device1	Windows 10 Enterprise
Device2	iOS
Device3	Android
Device4	Windows 10 Pro

The devices are managed by using Microsoft Intune.
You plan to use a configuration profile to assign the Delivery Optimization settings.
Which devices will support the settings?

A. Device1 only
B. Device1 and Device4
C. Device1, Device3, and Device4
D. Device1, Device2, Device3, and Device4

Correct Answer: A
Section:

QUESTION 118
Your on-premises network contains an Active Directory domain.
You have a Microsoft 365 E5 subscription.
You plan to implement a hybrid configuration that has the following requirements:
* Minimizes the number of times users are prompted for credentials when they access Microsoft 365 resources
* Supports the use of Azure AD Identity Protection
You need to configure Azure AD Connect to support the planned implementation. Which two options should you select? Each correct answer presents part of the solution.
NOTE: Each correct selection is worth one point.

A. Password Hash Synchronization
B. Password writeback
C. Directory extension attribute sync
D. Enable single sign-on
E. Pass-through authentication

Correct Answer: A, B
Section:

QUESTION 119

Your company has three main offices and one branch office. The branch office is used for research.
The company plans to implement a Microsoft 365 tenant and to deploy multi-factor authentication.
You need to recommend a Microsoft 365 solution to ensure that multi-factor authentication is enforced only for users in the branch office.
What should you include in the recommendation?

A. Azure AD password protection

B. a Microsoft Intune device configuration profile

C. a Microsoft Intune device compliance policy

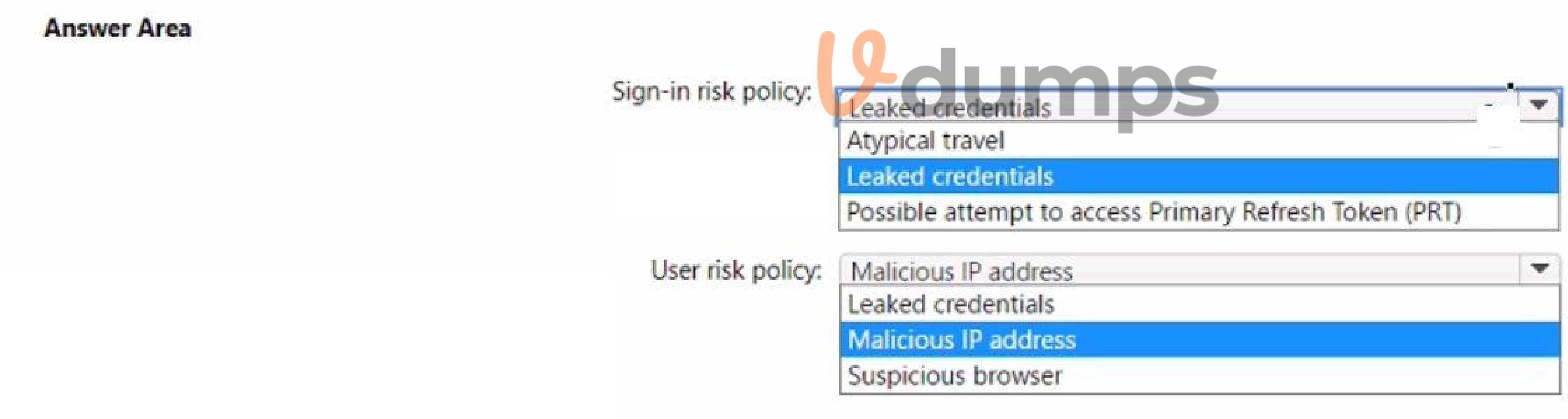
D. Azure AD conditional access

Correct Answer: D
Section:

QUESTION 120

HOTSPOT
You have a Microsoft 365 E5 subscription.
You plan to implement identity protection by configuring a sign-in risk policy and a user risk policy. Which type of risk is detected by each policy? To answer, select the appropriate options in the answer area.
NOTE: Each correct selection is worth one point.

Hot Area:



Answer Area

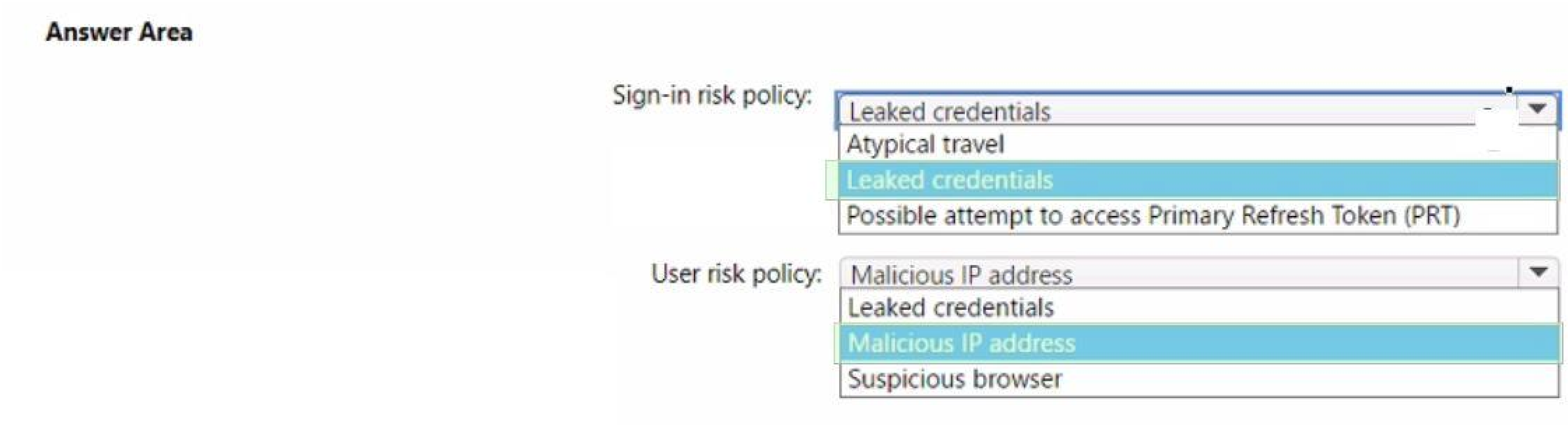
Sign-in risk policy: Leaked credentials

- Atypical travel
- Leaked credentials
- Possible attempt to access Primary Refresh Token (PRT)

User risk policy: Malicious IP address

- Leaked credentials
- Malicious IP address
- Suspicious browser

Answer Area:



Answer Area

Sign-in risk policy: Leaked credentials

- Atypical travel
- Leaked credentials
- Possible attempt to access Primary Refresh Token (PRT)

User risk policy: Malicious IP address

- Leaked credentials
- Malicious IP address
- Suspicious browser

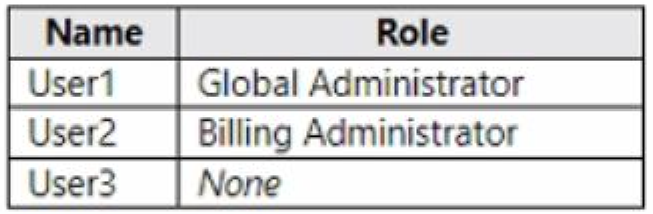
Section:
Explanation:

QUESTION 121
You have a Microsoft 365 E5 subscription.
You create a Conditional Access policy that blocks access to an app named App1 when users trigger a high-risk sign-in event.
You need to reduce false positives for impossible travel when the users sign in from the corporate network.
What should you configure?

A. exclusion groups
B. multi-factor authentication (MFA)
C. named locations
D. user risk policies

Correct Answer: C
Section:

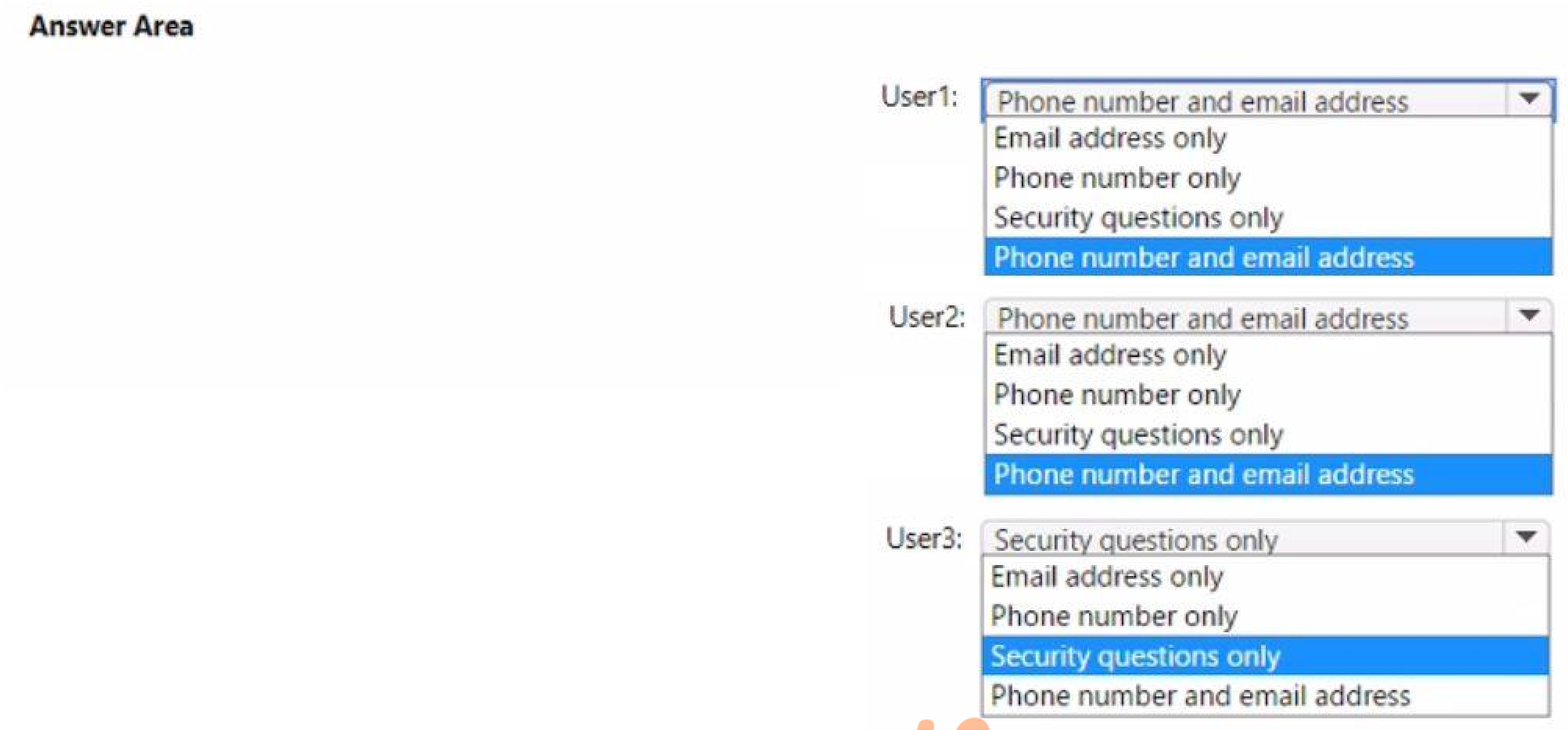
QUESTION 122
HOTSPOT
You have an Azure AD tenant that contains the users shown in the following table.



Name	Role
User1	Global Administrator
User2	Billing Administrator
User3	*None*

You enable self-service password reset for all users. You set Number of methods required to reset to 1, and you set Methods available to users to Security questions only.
What information must be configured for each user before the user can perform a self-service password reset? To answer, select the appropriate options in the answer area.
NOTE: Each correct selection is worth one point.

Hot Area:



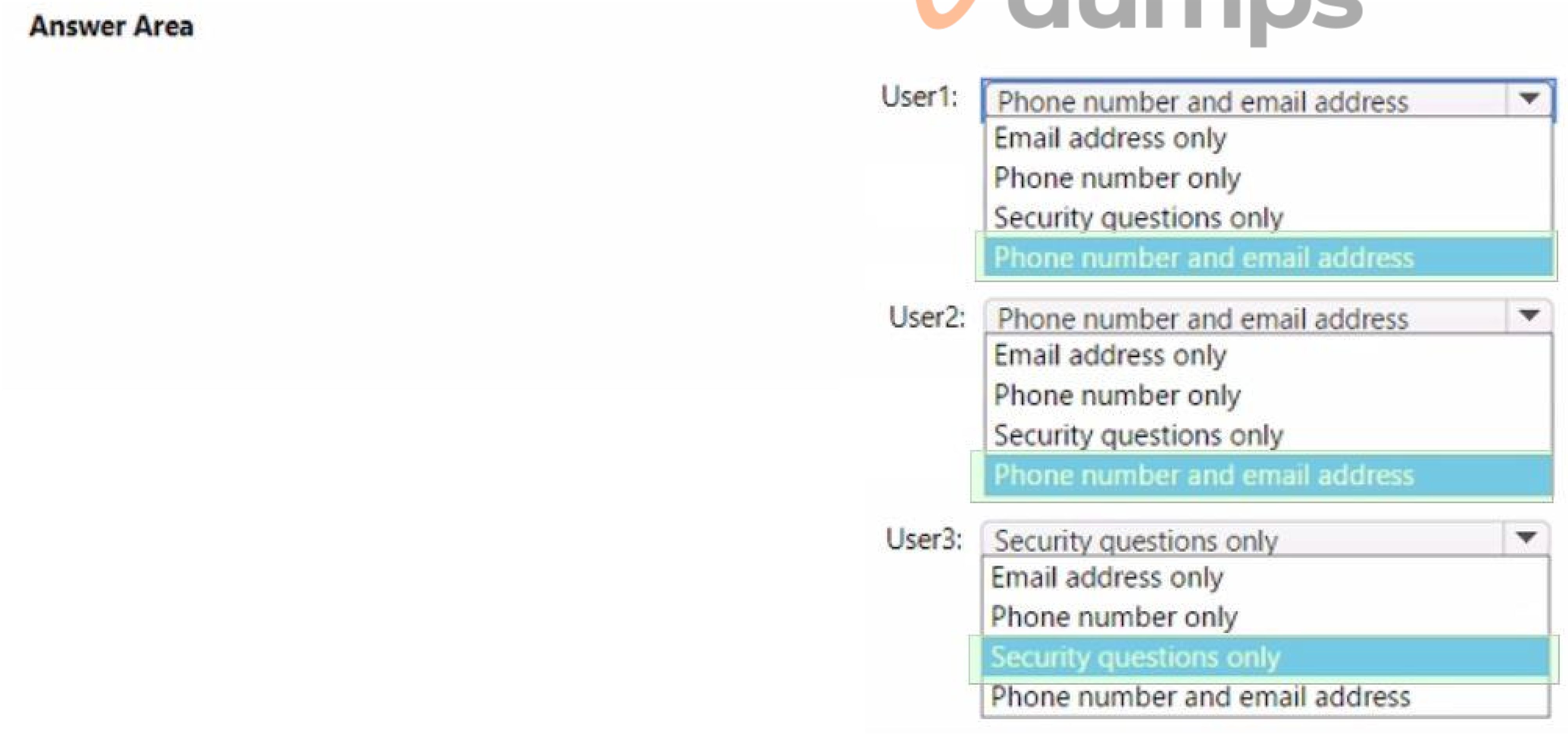
Answer Area

User1: Phone number and email address
- Email address only
- Phone number only
- Security questions only
- [✓ Phone number and email address]

User2: Phone number and email address
- Email address only
- Phone number only
- Security questions only
- [✓ Phone number and email address]

User3: Security questions only
- Email address only
- Phone number only
- [✓ Security questions only]
- Phone number and email address

Answer Area:



Answer Area

User1: Phone number and email address
- Email address only
- Phone number only
- Security questions only
- [✓ Phone number and email address]

User2: Phone number and email address
- Email address only
- Phone number only
- Security questions only
- [✓ Phone number and email address]

User3: Security questions only
- Email address only
- Phone number only
- [✓ Security questions only]
- Phone number and email address

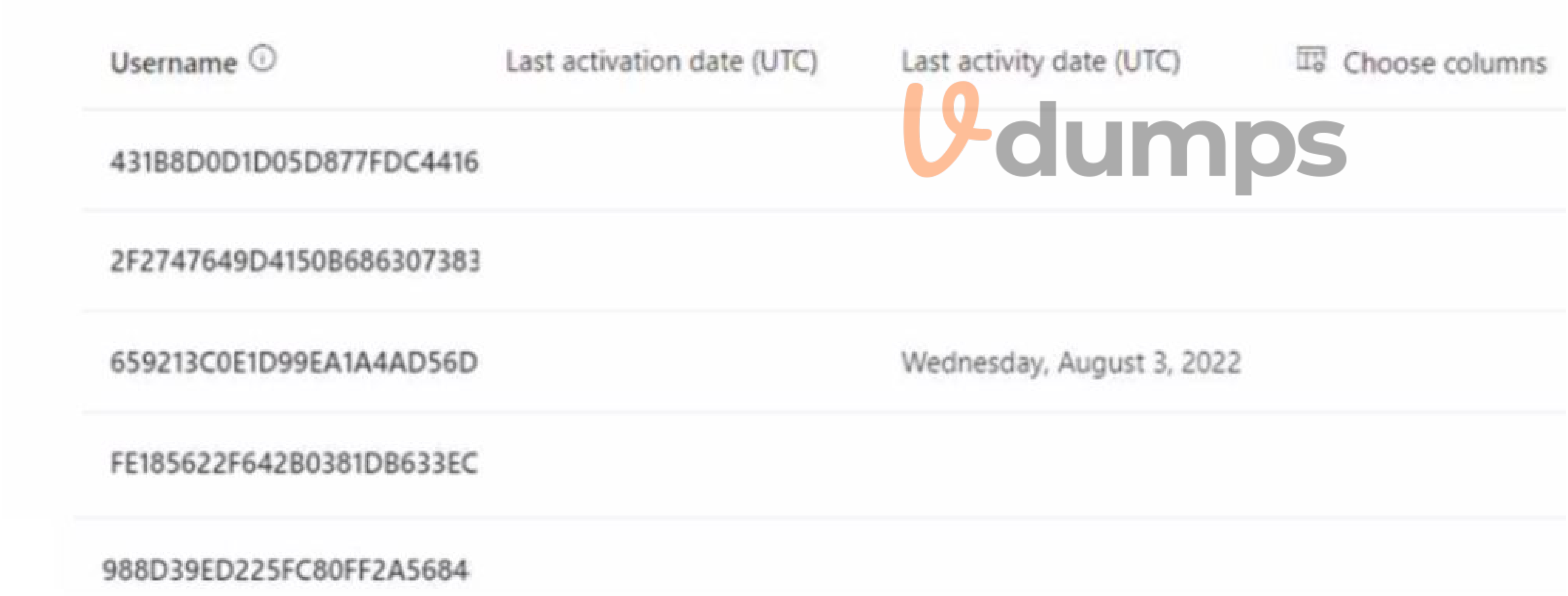
Section:
Explanation:

QUESTION 123
You have a Microsoft 365 E5 subscription.
Users have Android or iOS devices and access Microsoft 365 resources from computers that run Windows 11 or MacOS.
You need to implement passwordless authentication. The solution must support all the devices.
Which authentication method should you use?

A. Windows Hello
B. FID02 compliant security keys
C. Microsoft Authenticator app

Correct Answer: C
Section:

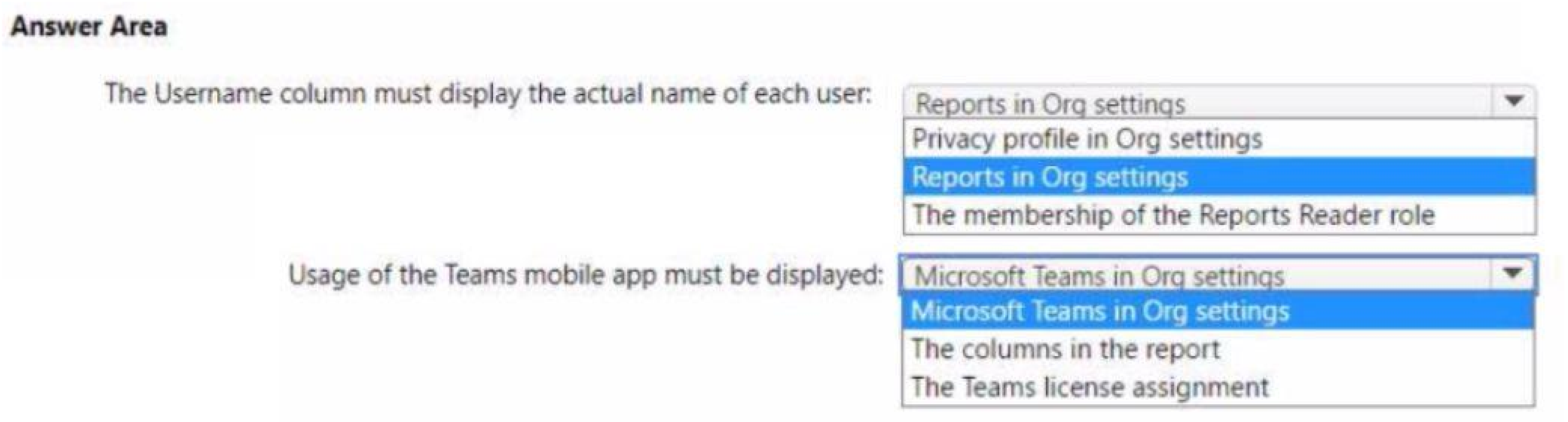
QUESTION 124
HOTSPOT
You have a Microsoft 365 subscription.
From the Microsoft 365 admin center, you open the Microsoft 365 Apps usage report as shown in the following exhibit.



Username	Last activation date (UTC)	Last activity date (UTC)
431B8D0D1D05D877FDC4416		
2F2747649D4150B686307383		
659213C0E1D99EA1A4AD56D		Wednesday, August 3, 2022
FE185622F642B0381DB633EC		
988D39ED225FC80FF2A5684		

You need ensure that the report meets the following requirements:
* The Username column must display the actual name of each user.
* Usage of the Microsoft Teams mobile app must be displayed.
What should you modify for each requirement? To answer, select the appropriate options in the answer area. NOTE: Each correct selection is worth one point.

Hot Area:



Answer Area

The Username column must display the actual name of each user:

Reports in Org settings

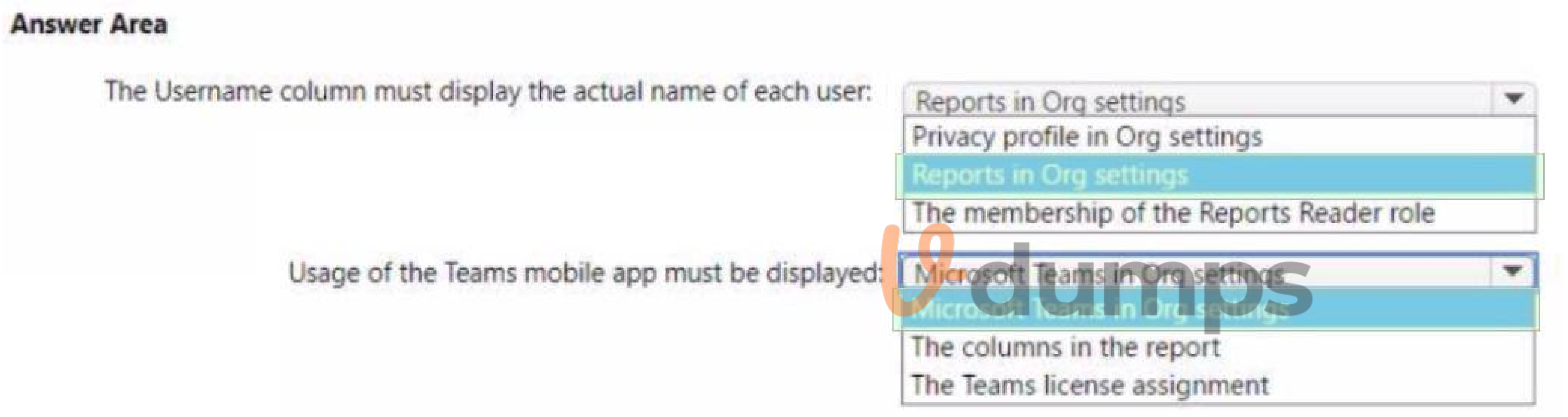
- Privacy profile in Org settings
- Reports in Org settings
- The membership of the Reports Reader role

Usage of the Teams mobile app must be displayed:

Microsoft Teams in Org settings

- Microsoft Teams in Org settings
- The columns in the report
- The Teams license assignment

Answer Area:



Answer Area

The Username column must display the actual name of each user:

Reports in Org settings

- Privacy profile in Org settings
- [✓ Reports in Org settings]
- The membership of the Reports Reader role

Usage of the Teams mobile app must be displayed:

Microsoft Teams in Org settings

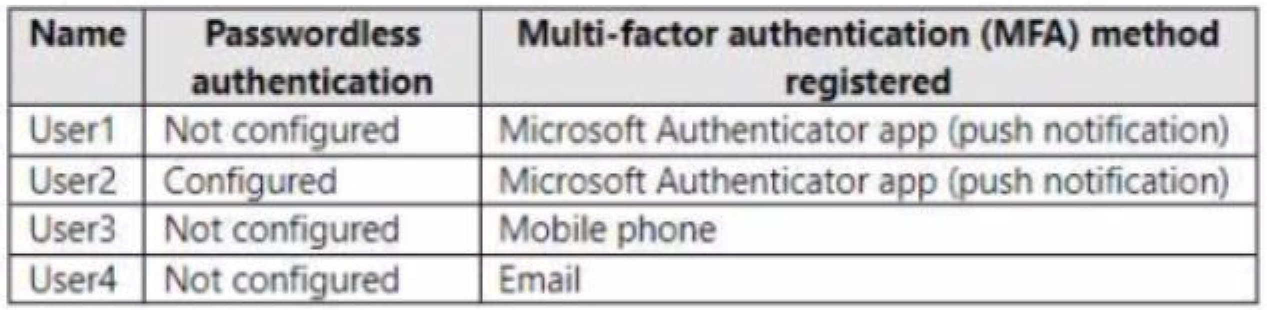
- [✓ Microsoft Teams in Org settings]
- The columns in the report
- The Teams license assignment

Section:

Explanation:

QUESTION 125

You have a Microsoft 365 E5 subscription that contains the users shown in the following table.



Name	Passwordless authentication	Multi-factor authentication (MFA) method registered
User1	Not configured	Microsoft Authenticator app (push notification)
User2	Configured	Microsoft Authenticator app (push notification)
User3	Not configured	Mobile phone
User4	Not configured	Email

You plan to create a Conditional Access policy that will use GPS-based named locations.

Which users can the policy protect?

A. User2 and User4 only

B. User1 and User3 only

C. Userl1 only

D. User1, User2. User3. and User4

Correct Answer: C
Section:

QUESTION 126

HOTSPOT

You have a Microsoft 365 E5 subscription that contains the users shown in the following table.

Each user has an Android device with the Microsoft Authenticator app installed and has set up phone sign-in.

The subscription has the following Conditional Access policy:

* Name: Policy1

* Assignments

o Users and groups: Group1, Group2

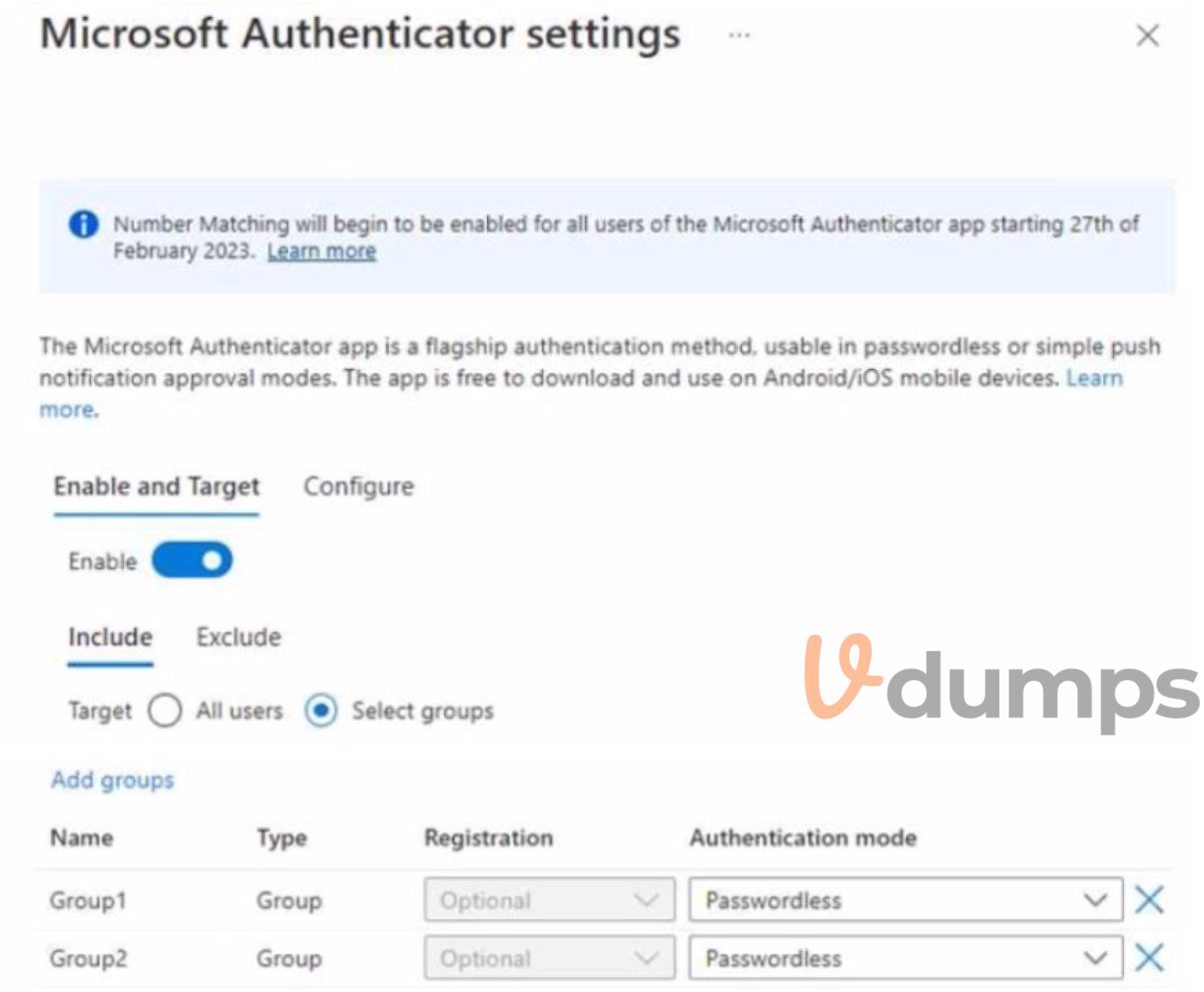
o Cloud apps or actions: All cloud apps

* Access controls

o Grant Require multi-factor authentication

* Enable policy: On

From Microsoft Authenticator settings for the subscription, the Enable and Target settings are configured as shown in the exhibit. (Click the Exhibit tab.)



Microsoft Authenticator settings ··· ✕

Number Matching will begin to be enabled for all users of the Microsoft Authenticator app starting 27th of February 2023. Learn more

The Microsoft Authenticator app is a flagship authentication method, usable in passwordless or simple push notification approval modes. The app is free to download and use on Android/iOS mobile devices. Learn more.

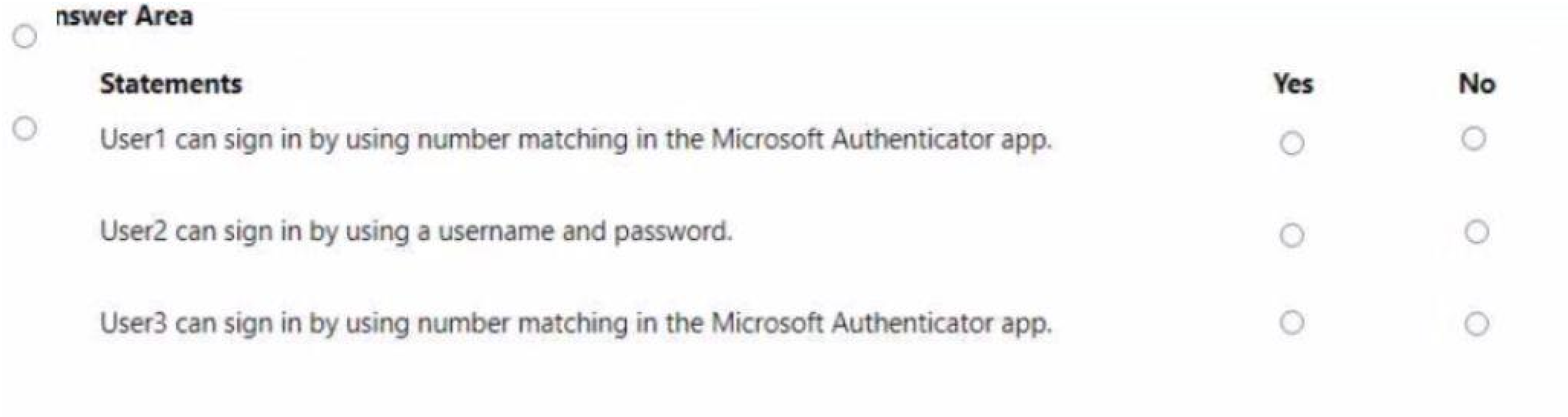
Enable ●

Target ○ All users ● Select groups

Name	Type	Registration	Authentication mode	
Group1	Group	Optional	Passwordless	✕
Group2	Group	Optional	Passwordless	✕

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:

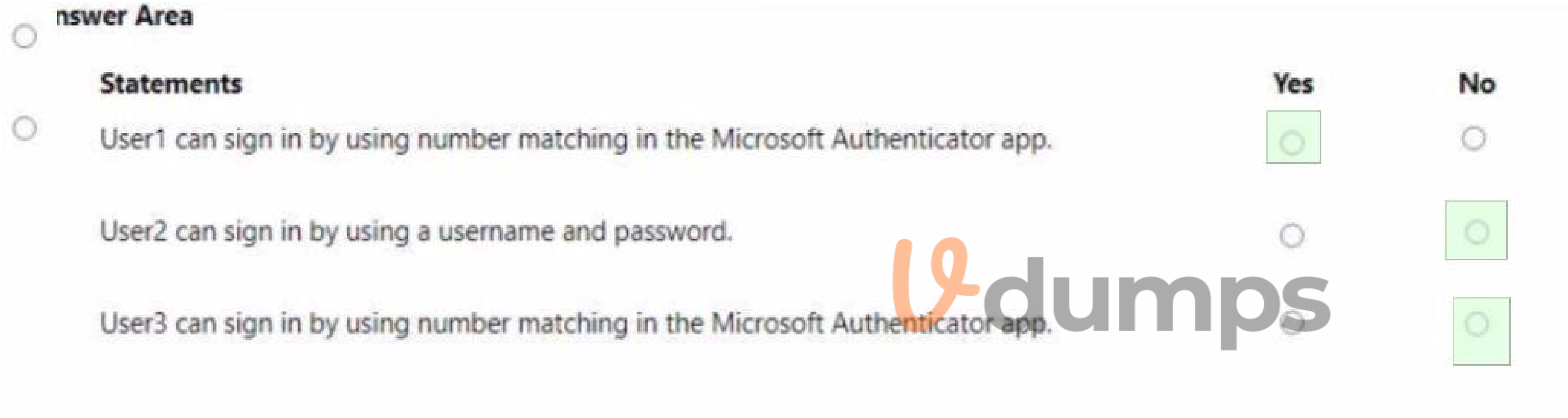


○ nswer Area

○

Statements	Yes	No
User1 can sign in by using number matching in the Microsoft Authenticator app.	○	○
User2 can sign in by using a username and password.	○	○
User3 can sign in by using number matching in the Microsoft Authenticator app.	○	○

Answer Area:



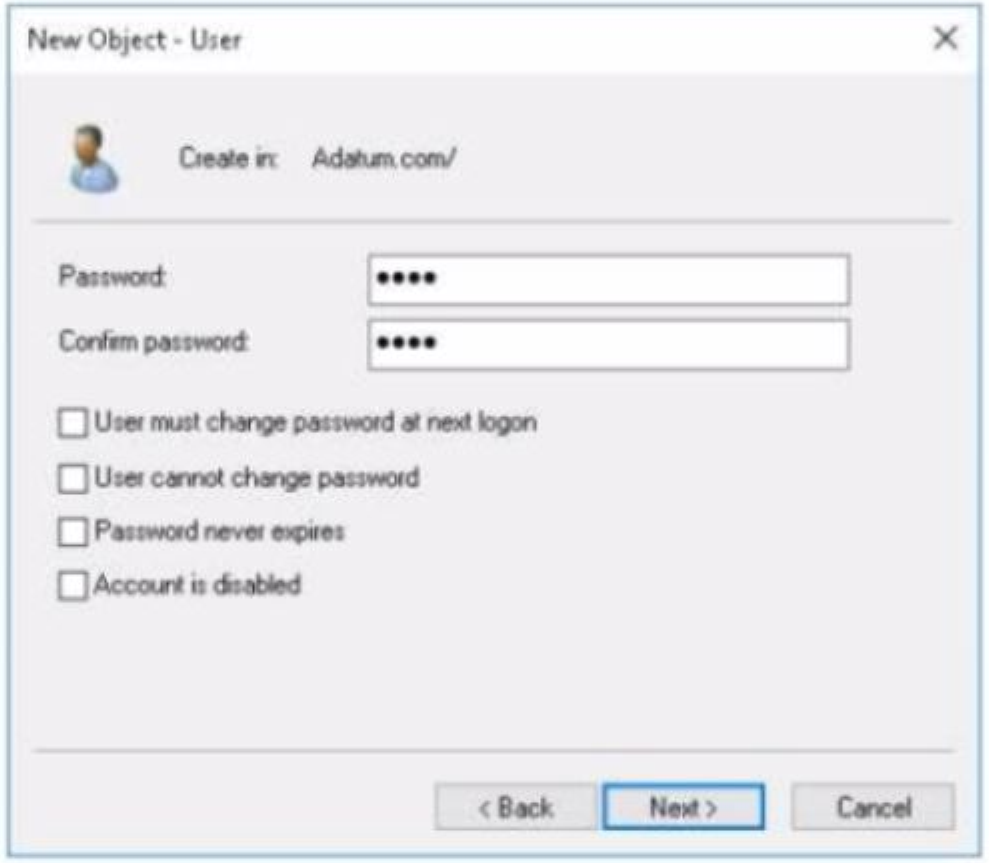
○ nswer Area

○

Statements	Yes	No
User1 can sign in by using number matching in the Microsoft Authenticator app.	[✓ ○]	○
User2 can sign in by using a username and password.	○	[✓ ○]
User3 can sign in by using number matching in the Microsoft Authenticator app.	○	[✓ ○]

Section:
Explanation:

QUESTION 127
HOTSPOT
Your network contains an on-premises Active Directory domain named adatum.com that syncs to Azure AD by using the Azure AD Connect Express Settings. Password write back is disabled.
You create a user named User1 and enter Pass in the Password field as shown in the following exhibit.



New Object - User

Create in: Adatum.com/

Password: ••••

Confirm password: ••••

□ User must change password at next logon

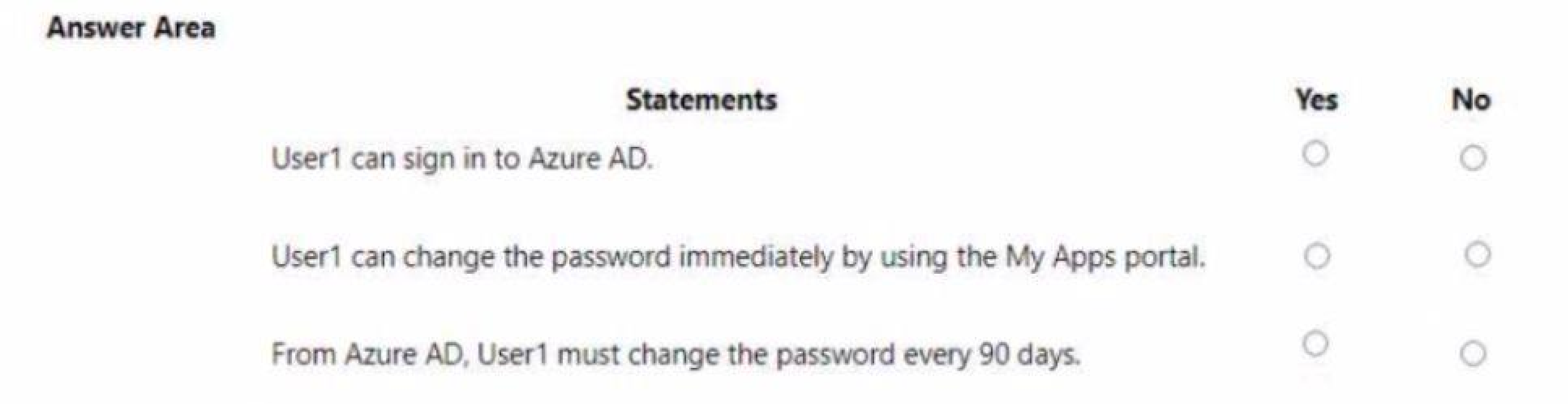
□ User cannot change password

□ Password never expires

□ Account is disabled

The Azure AD password policy is configured as shown in the following exhibit.
Password policy
Set the password policy for all users in your organization.
Days before passwords expire 90
Days before a user is notified about 14
expiration
You confirm that User1 is synced to Azure AD.
For each of the following statements, select Yes if the statement is true. Otherwise, select No.
NOTE: Each correct selection is worth one point.

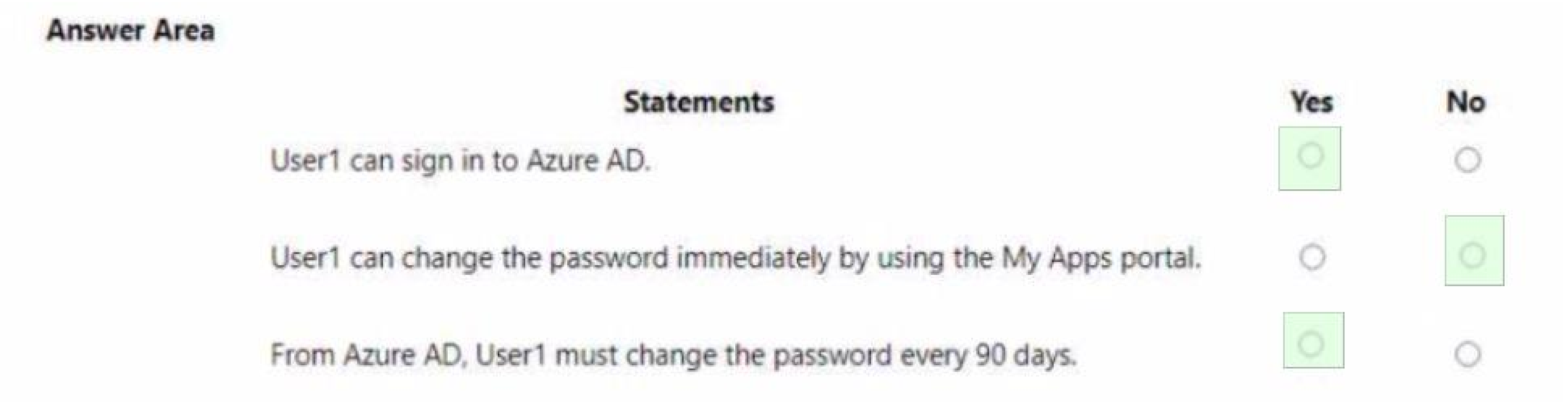
Hot Area:



Answer Area

Statements	Yes	No
User1 can sign in to Azure AD.	○	○
User1 can change the password immediately by using the My Apps portal.	○	○
From Azure AD, User1 must change the password every 90 days.	○	○

Answer Area:



Answer Area

Statements	Yes	No
User1 can sign in to Azure AD.	[✓ ○]	○
User1 can change the password immediately by using the My Apps portal.	○	[✓ ○]
From Azure AD, User1 must change the password every 90 days.	[✓ ○]	○

Section:
Explanation:

QUESTION 128
You have a Microsoft 365 E5 subscription.
On Monday, you create a new user named User1.
On Tuesday, User1 signs in for the first time and perform the following actions:
* Signs in to Microsoft Exchange Online from an anonymous IP address
* Signs in to Microsoft SharePoint Online from a device in New York City.
* Establishes Remote Desktop connections to hosts in Berlin and Hong Kong, and then signs in to SharePoint Online from the Remote Desktop connections
Which types of sign-in risks will Azure AD Identity Protection detect for User1?

A. anonymous IP address only
B. anonymous IP address and atypical travel
C. anonymous IP address, atypical travel, and unfamiliar sign-in properties
D. unfamiliar sign-in properties and atypical travel only
E. anonymous IP address and unfamiliar sign-in properties only

Correct Answer: A
Section:

QUESTION 129
Your on-premises network contains an Active Directory domain.
You have a Microsoft 365 subscription.
You need to sync the domain with the subscription. The solution must meet the following requirements:
* On-premises Active Directory password complexity policies must be enforced.
* Users must be able to use Microsoft Entra Self-Service Password Reset (SSPR).
What should you use?

A. Microsoft Entra ID Protection
B. Microsoft Entra Seamless Single Sign-On (Microsoft Entra Seamless SSO)
C. pass-through authentication
D. password hash synchronization

Correct Answer: C

Section:

QUESTION 130

Your company has three main offices and one branch office. The branch office is used for research.
The company plans to implement a Microsoft 365 tenant and to deploy multi-factor authentication.
You need to recommend a Microsoft 365 solution to ensure that multi-factor authentication is enforced only for users in the branch office.
What should you include in the recommendation?

A. Microsoft Entra conditional access

B. a Microsoft Intune device compliance policy

C. a Microsoft Intune device configuration profile

D. Microsoft Entra password protection

Correct Answer: A
Section:

QUESTION 131

Youi network contains an Active Directory domain.
You have a Microsoft Entra tenant that has Security defaults disabled.
Microsoft Entra Connect Sync is configured for directory synchronization. Password hash synchronization and pass-through authentication are disabled.
You need to enable Microsoft Entra ID Protection to detect leaked credentials.
What should you do first?

A. From Microsoft Entra Connect, enable password hash synchronization.

B. From the Microsoft Entra admin center, enable Security defaults.

C. From Microsoft Entra Connect, enable pass-through authentication.

D. From the Microsoft Entra admin center, configure verifiable credentials.

Correct Answer: A
Section:

QUESTION 132

You have a Microsoft 365 E5 subscription.
You plan to create an anti-malware policy named Policy1.
You need to ensure that Policy1 can detect malicious email messages that were already delivered to a user's mailbox.
What should you do in the Microsoft Defender portal?

A. Enable zero-hour auto purge (ZAP).

B. Modify the common attachments filter.

C. Configure a quarantine policy.

D. Enable enhanced filtering.

Correct Answer: A
Section:

QUESTION 133

You have a Microsoft 365 E5 subscription that contains devices onboarded to Microsoft Defender for Endpoint. You integrate Microsoft Defender for Cloud Apps with Defender for Endpoint. You need identify which cloud apps and services were used most during the last 30 days What should you do?

A. Generate a Cloud Discovery snapshot report.

B. Generate a monthly security summary report

C. Create a threat analytics alert notification.

D. Generate a Cloud Discovery executive report

Correct Answer: B
Section: