Microsoft.Premium.MS-102.44q - DEMO

Number: MS-10
Passing Score: 800
Time Limit: 120 min
File Version:

Exam Code: MS-102

Exam Name: Microsoft 365 Administrator

Case 02

QUESTION 1

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

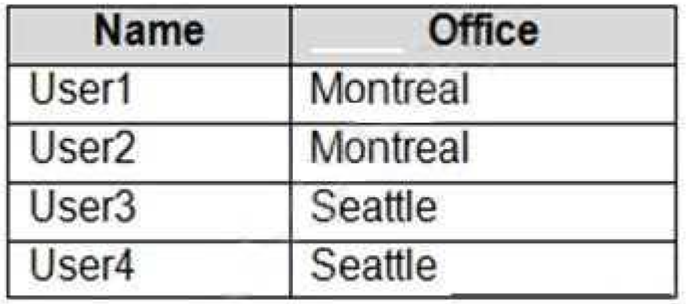
General Overviews

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.

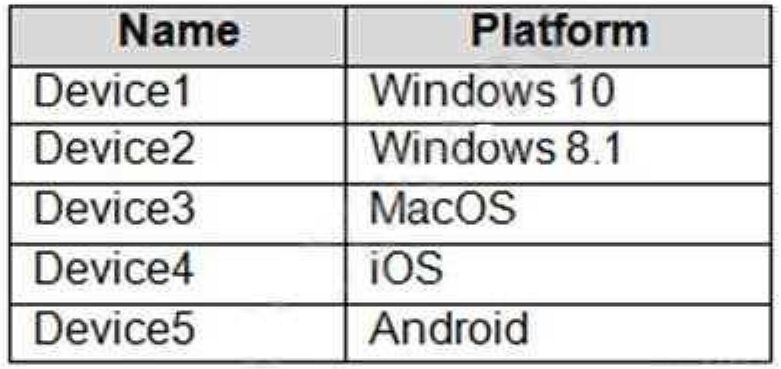


Name	Office
User1	Montreal
User2	Montreal
User3	Seattle
User4	Seattle

Microsoft Cloud Environment

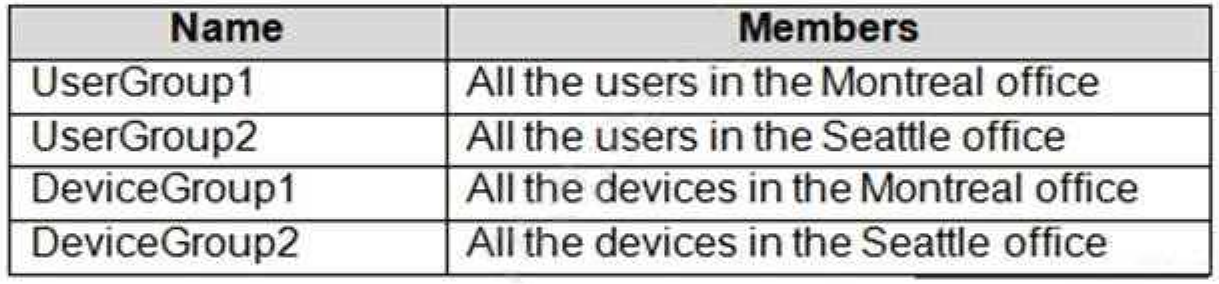
Litware has a Microsoft 365 subscription that contains a verified domain named litware.com. The subscription syncs to the on-premises domain.

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.



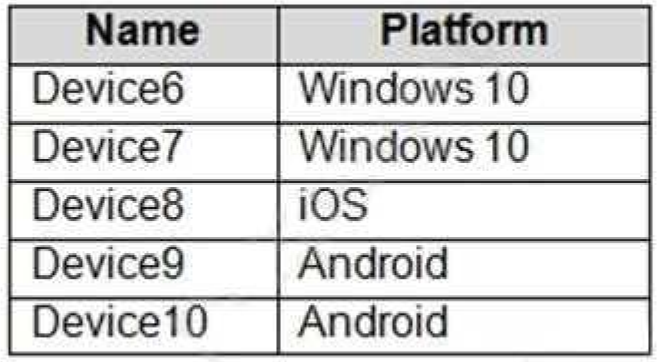
Name	Members
UserGroup1	All the users in the Montreal office
UserGroup2	All the users in the Seattle office
DeviceGroup1	All the devices in the Montreal office
DeviceGroup2	All the devices in the Seattle office

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.
A.
B.
C.
D.

Correct Answer:
Section:
Explanation:

QUESTION 2

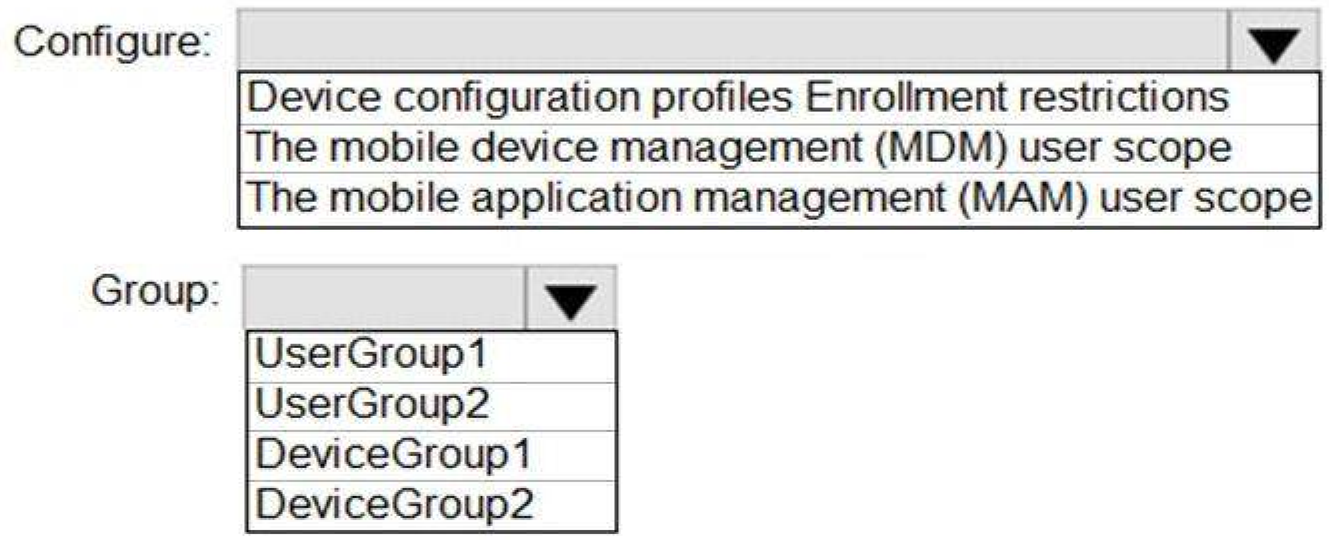
HOTSPOT

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:

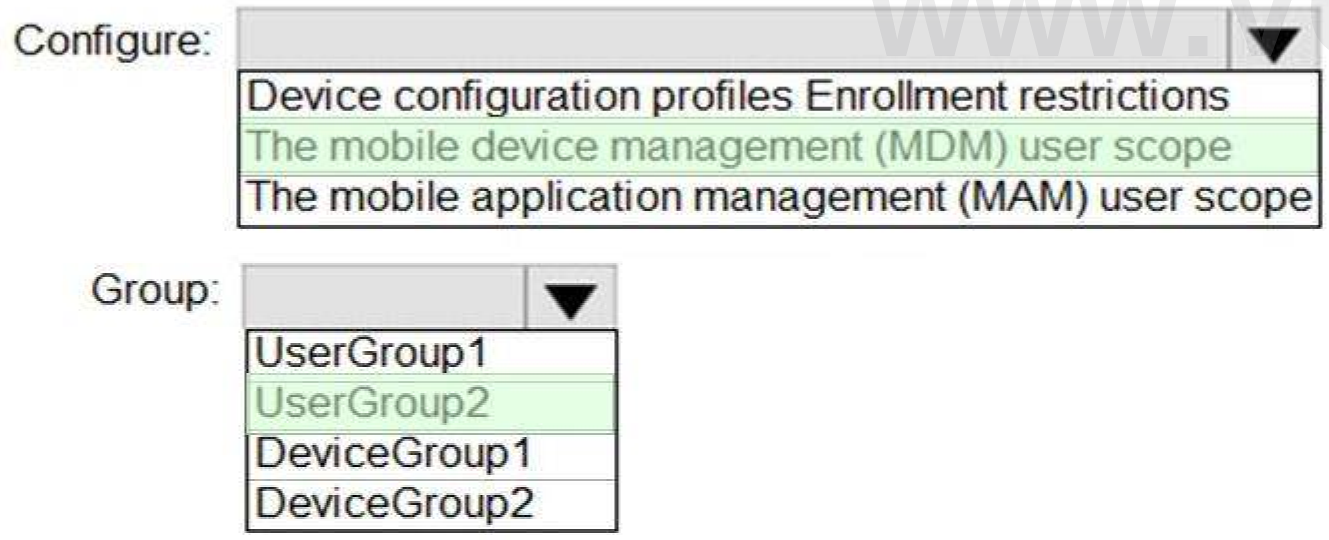
UserGroup1

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 3

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

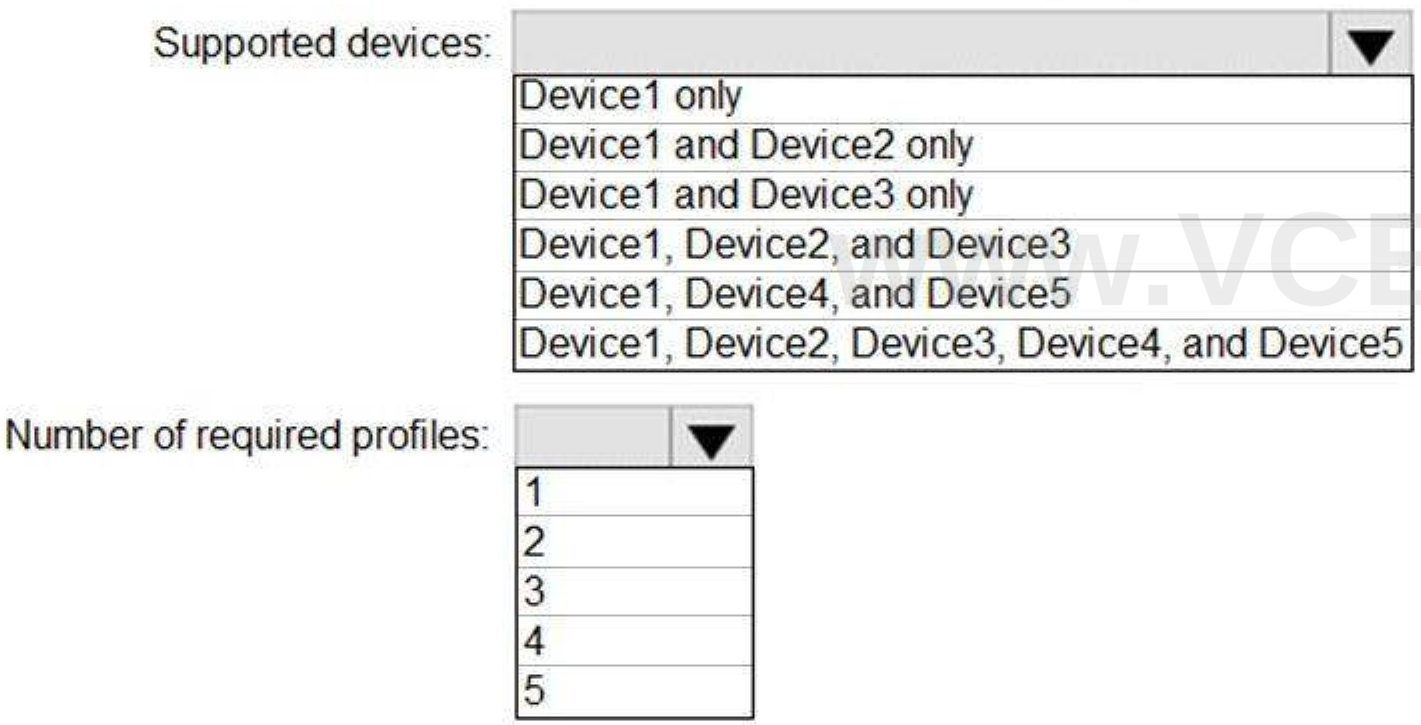
D. Dynamic Delivery

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

QUESTION 4

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:



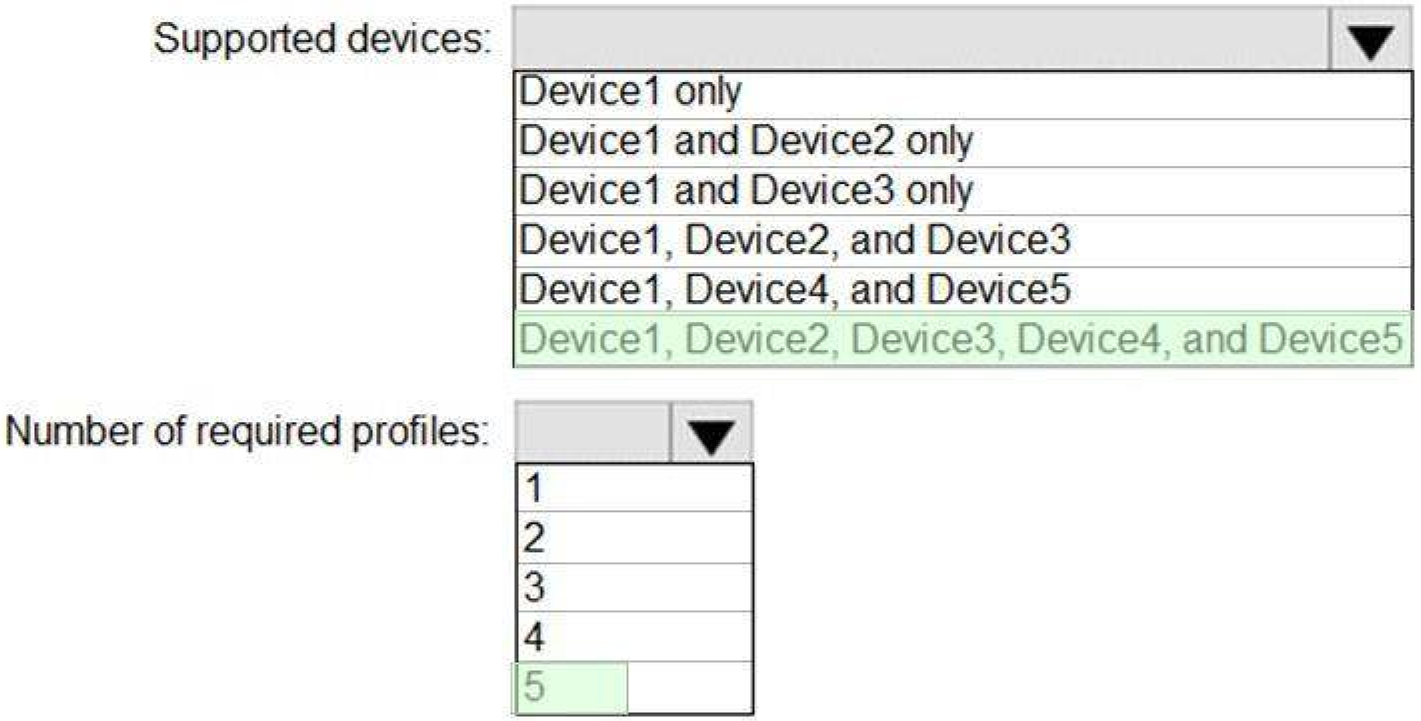
Supported devices:

- 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 5

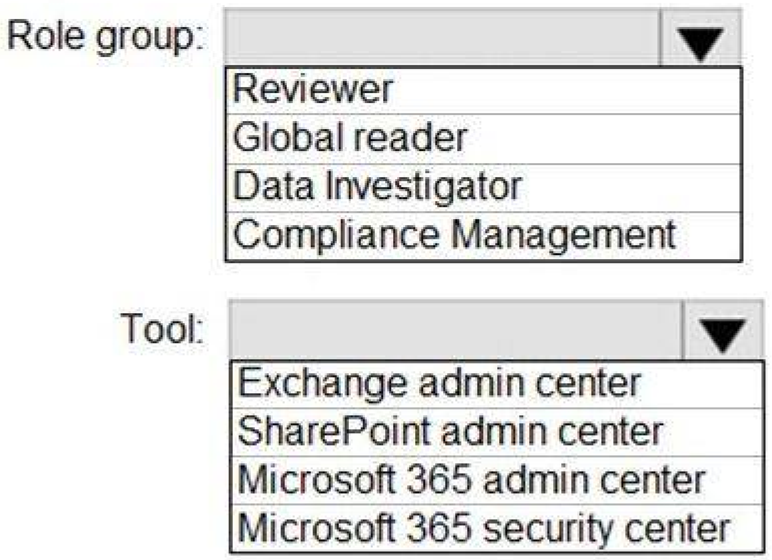
HOTSPOT

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:



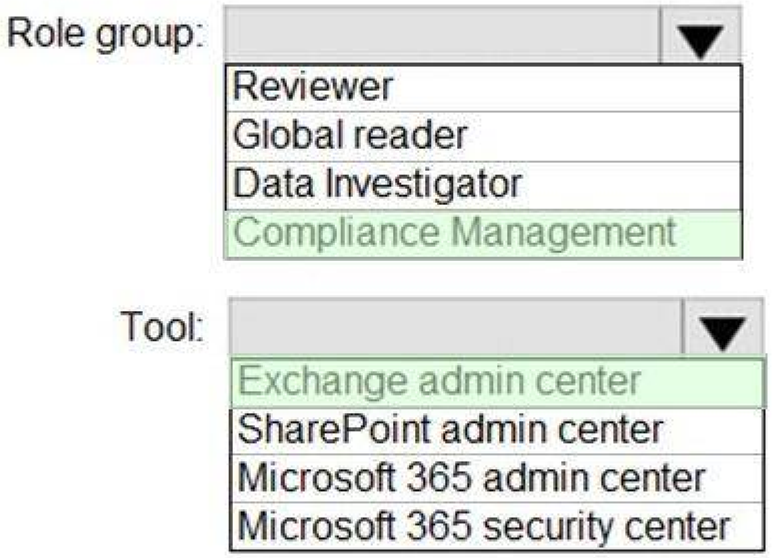
Role group:

- 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 6

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 7

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 8

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 9

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 10

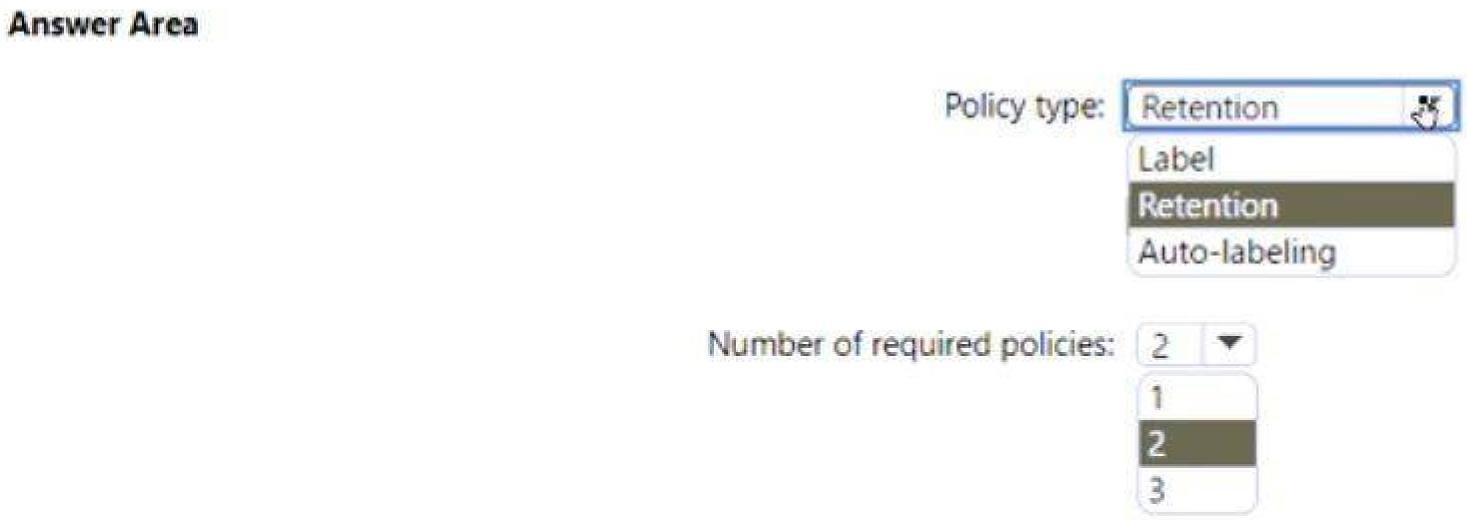
HOTSPOT

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

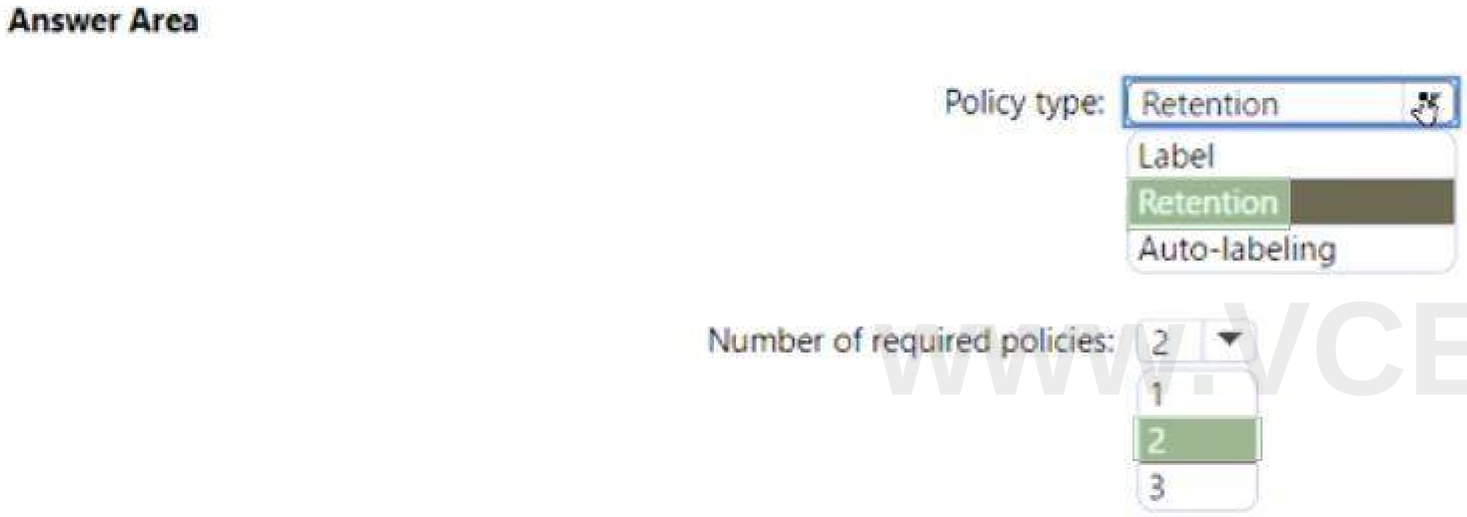
Policy type: Retention

- Label
- Retention
- Auto-labeling

Number of required policies: 2

- 1
- 2
- 3

Answer Area:



Answer Area

Policy type: Retention

- Label
- [✓ Retention]
- Auto-labeling

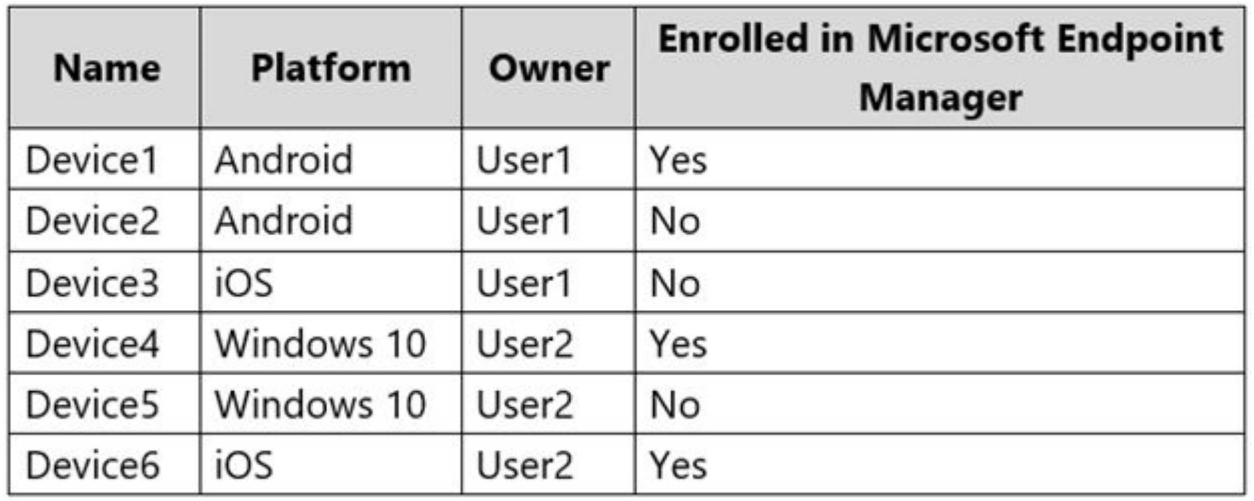
Number of required policies: 2

- 1
- [✓ 2]
- 3

Section:
Explanation:

Exam C

QUESTION 1
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

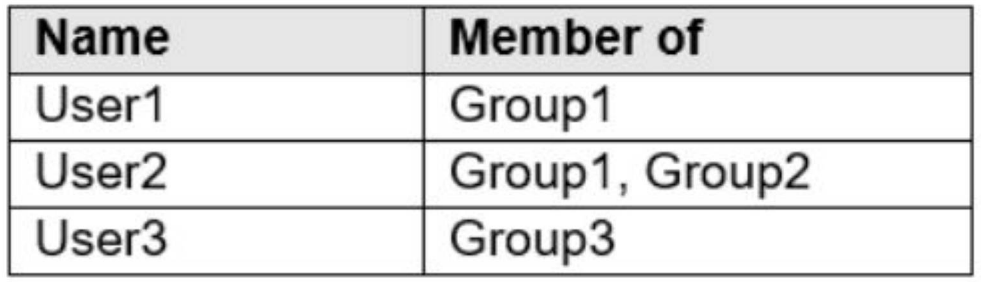
Correct Answer: C
Section:
Explanation:

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 2

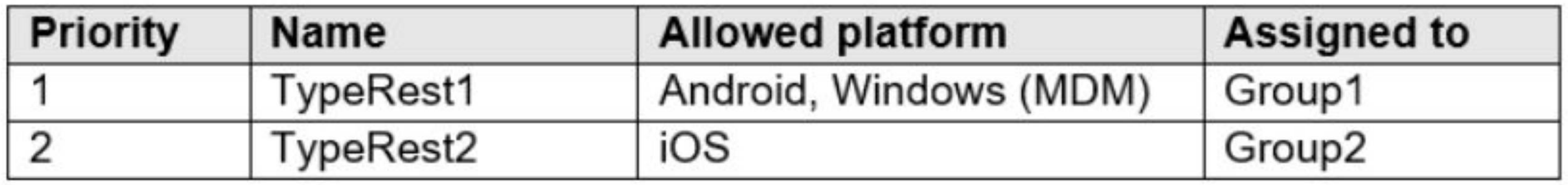
HOTSPOT

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



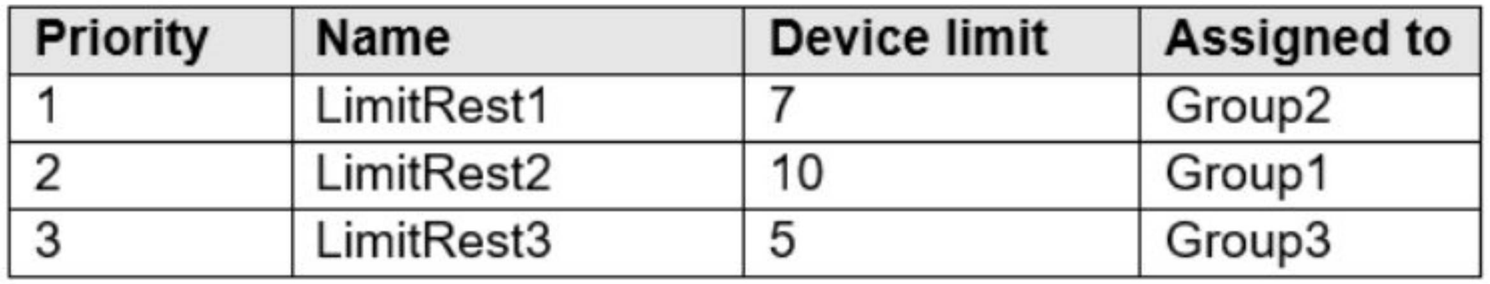
Name	Member of
User1	Group1
User2	Group1, Group2
User3	Group3

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

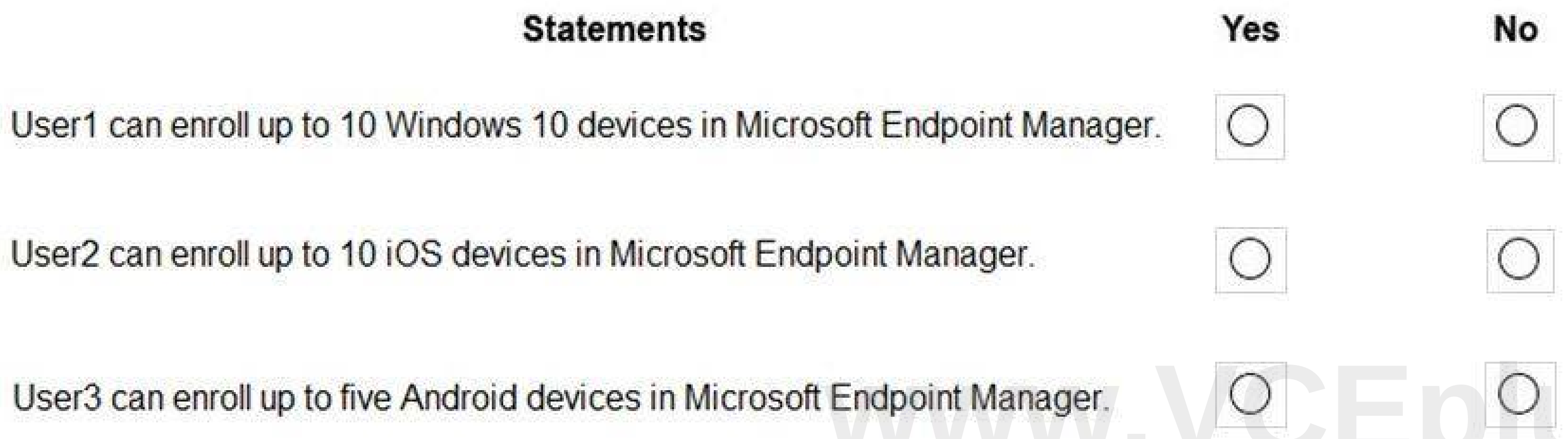
In Microsoft Endpoint Manager, you create three device limit restrictions that have the settings shown in the following table.



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

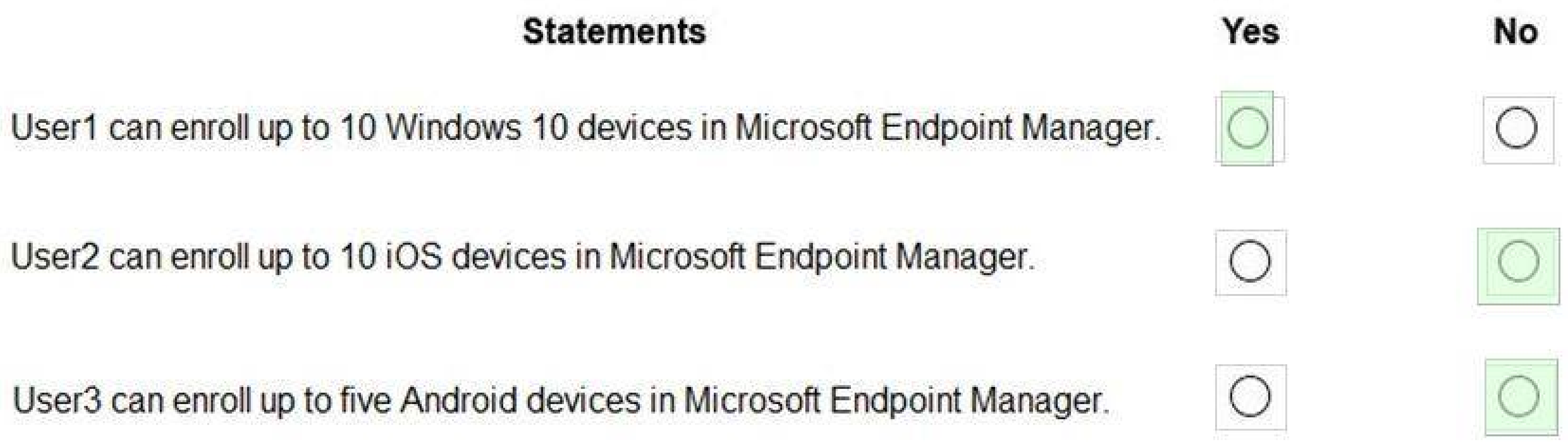
For each of the following statements, select Yes if the statement is true. Otherwise, select No.
NOTE: Each correct selection is worth one point.

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.	○	[✓ ○]

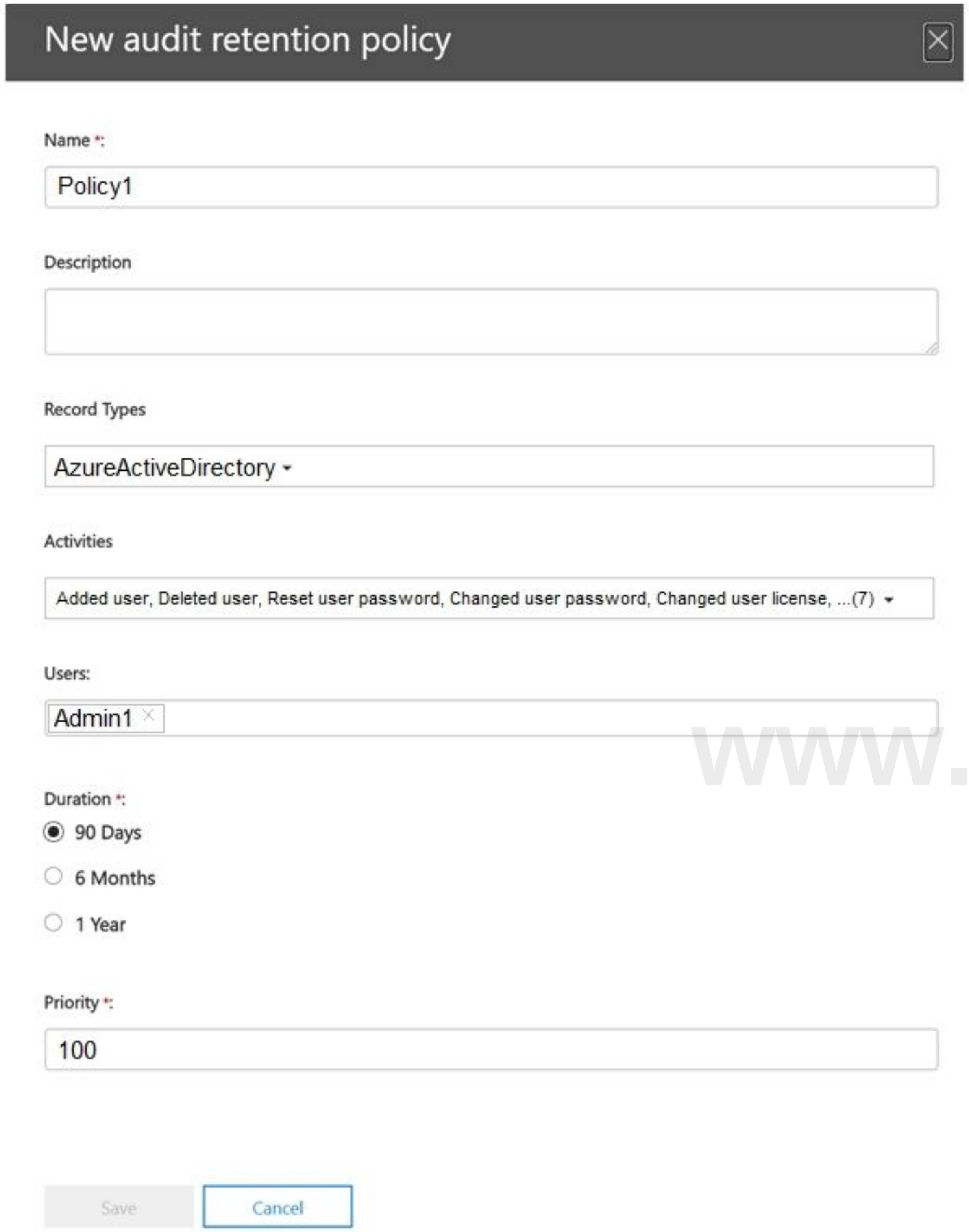
Section:
Explanation:

QUESTION 3
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 4
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

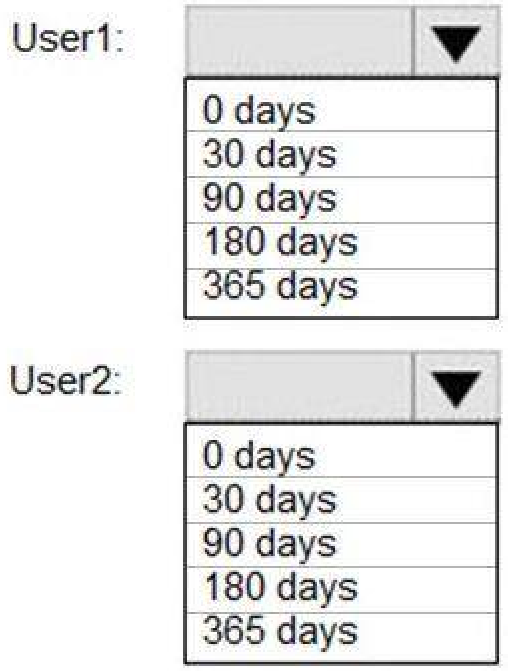
○ 6 Months

○ 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:



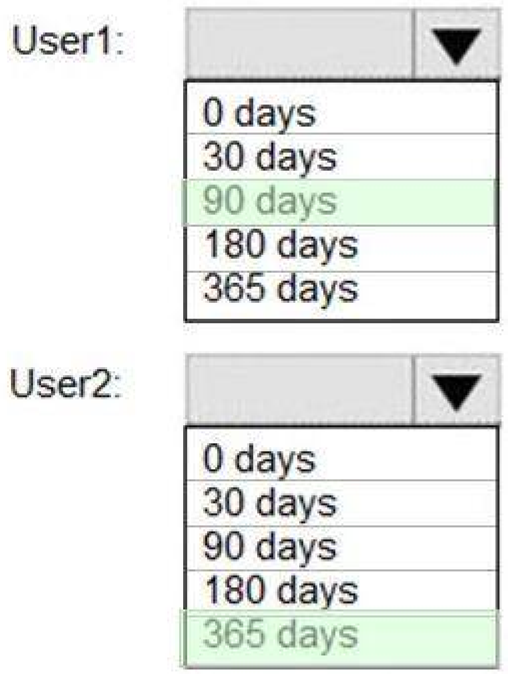
User1:

0 days
30 days
90 days
180 days
365 days

User2:

0 days
30 days
90 days
180 days
365 days

Answer Area:



User1:

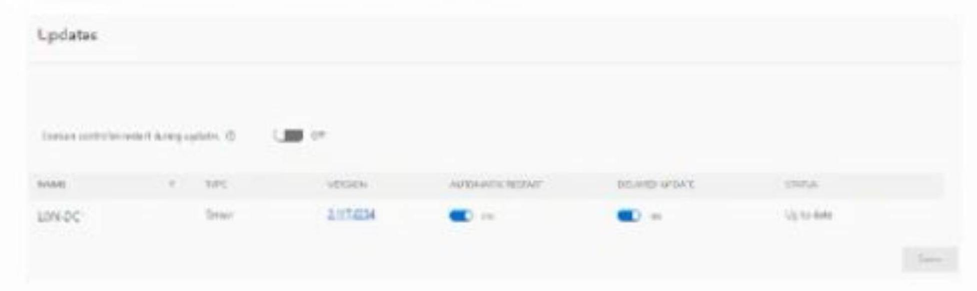
0 days
30 days
[✓ 90 days]
180 days
365 days

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 5
You implement Microsoft Azure Advanced Threat Protection (Azure ATP).
You have an Azure ATP sensor configured as shown in the following exhibit.



Updates

[illegible] [illegible]

NAME	TYPE	VERSION	AUTOMATIC RESTART	DELAYED UPDATE	STATUS
LON-DC	[illegible]	[illegible]	[illegible]	[illegible]	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:
Explanation:

QUESTION 6

HOTSPOT

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

Name	Microsoft 365 role
User1	Cloud application administrator
User2	Application administrator
User3	Application developer
User4	None

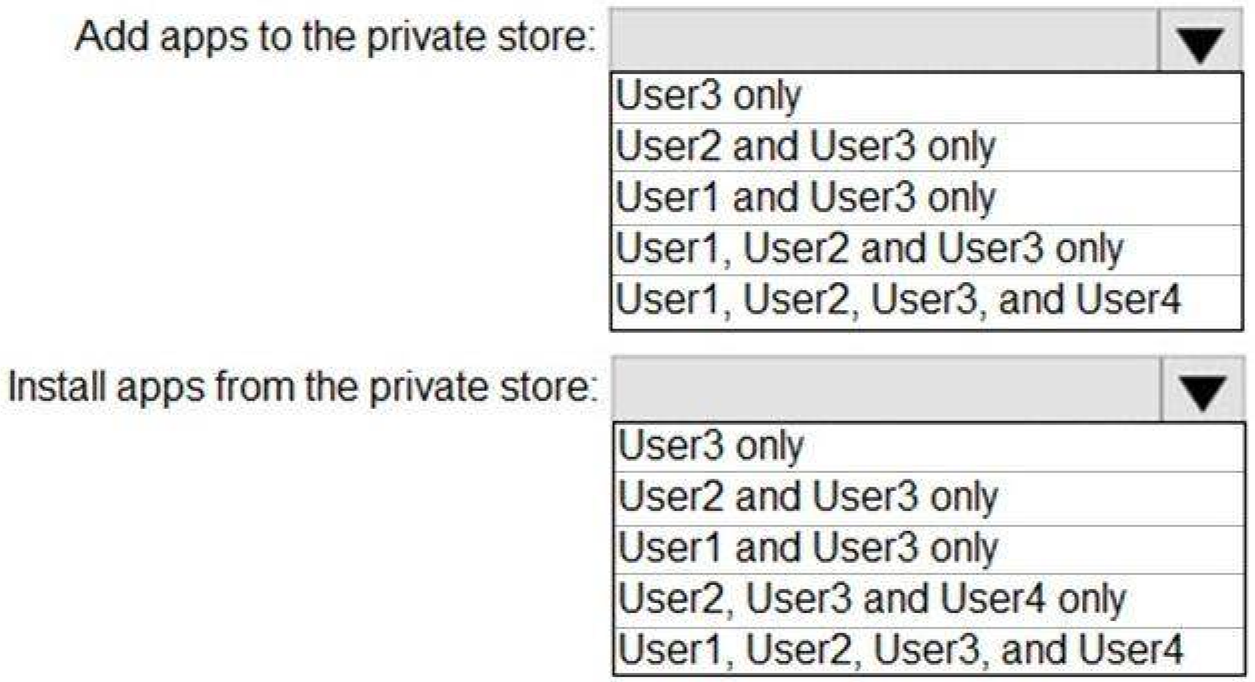
Users are assigned Microsoft Store for Business roles as shown in the following table.

User	Role
User1	None
User2	Basic Purchaser
User3	Purchaser
User4	Device Guard signer

Which users can add apps to the private store in Microsoft Store for Business, and which users can install apps from the private store? To answer, select the appropriate options in the answer area.

NOTE: Each correct selection is worth one point.

Hot Area:



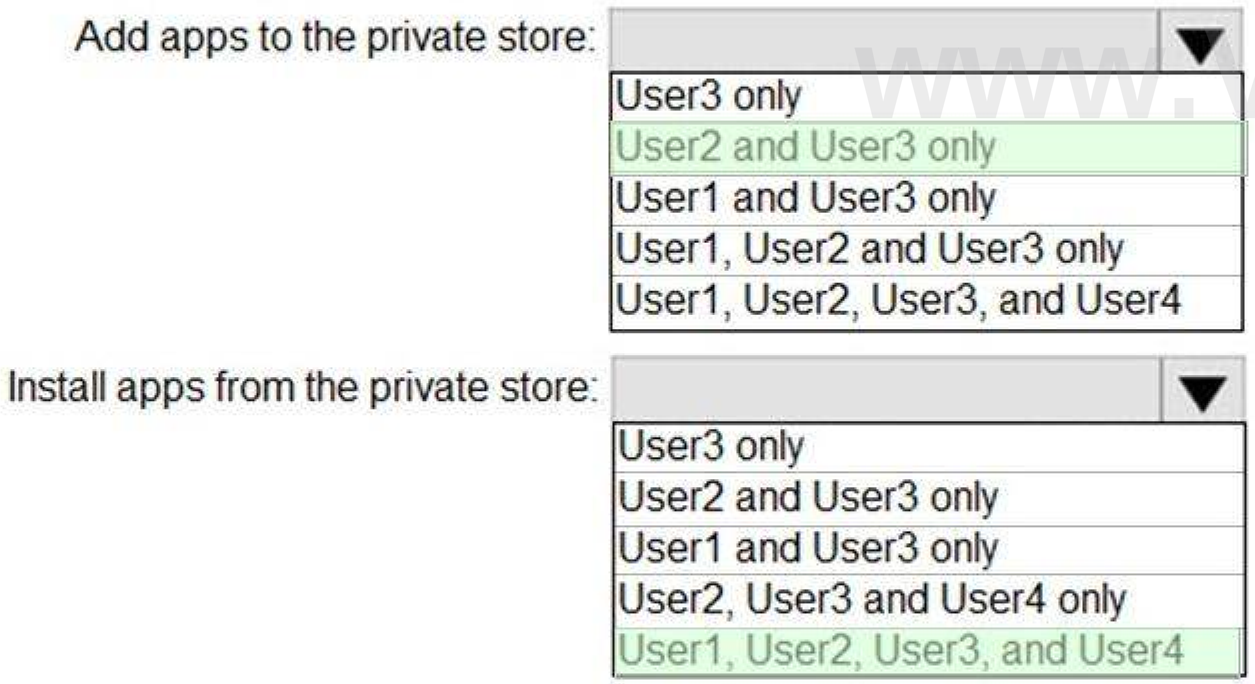
Add apps to the private store: ▼

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

Install apps from the private store: ▼

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

Answer Area:



Add apps to the private store: ▼

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

Install apps from the private store: ▼

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

Section:
Explanation:
https://docs.microsoft.com/en-us/microsoft-store/acquire-apps-microsoft-store-for-business
https://docs.microsoft.com/en-us/microsoft-store/distribute-apps-from-your-private-store

QUESTION 7
Your company has offices in five cities.

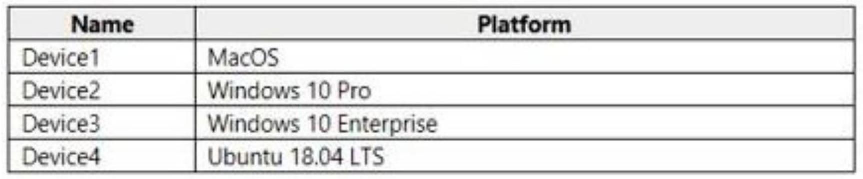
The company has a Microsoft 365 tenant.
Each office is managed by a local administrator.
You plan to deploy Microsoft Intune.
You need to recommend a solution to manage resources in intune that meets the following requirements:
Local administrators must be able to manage only the resources in their respective office.
Local administrators must be prevented from managing resources in other offices.
Administrative effort must be minimized.
What should you include in the recommendation?

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

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

QUESTION 8

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



Name	Platform
Device1	MacOS
Device2	Windows 10 Pro
Device3	Windows 10 Enterprise
Device4	Ubuntu 18.04 LTS

You plan to implement attack surface reduction (ASR) rules. Which devices will support the ASR rules?

A. Device 1, Device2, and Device3 only
B. Device3 only
C. Device2 and Device3 only
D. Device1, Device2, Devices and Device4

Correct Answer: C
Section:
Explanation:
https://docs.microsoft.com/en-us/microsoft-365/security/defender-endpoint/enable-attack-surface-reduction?view=o365-worldwide#requirements

QUESTION 9

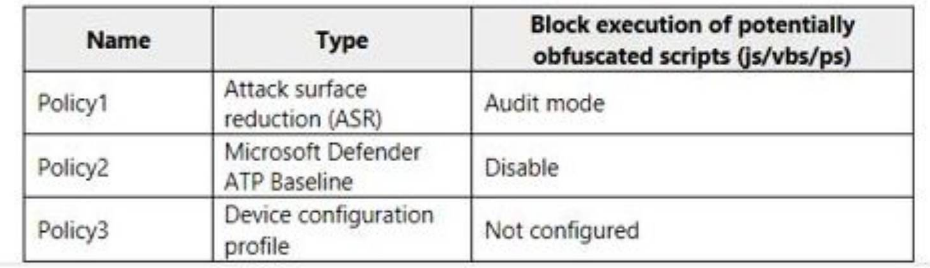
You have a Microsoft 365 tenant that contains 1,000 iOS devices enrolled in Microsoft Intune. You plan to purchase volume-purchased apps and deploy the apps to the devices. You need to track used licenses and manage the apps by using Intune. What should you use to purchase the apps?

A. Microsoft Store for Business
B. Apple Business Manager
C. Apple iTunes Store
D. Apple Configurator

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

QUESTION 10

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

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

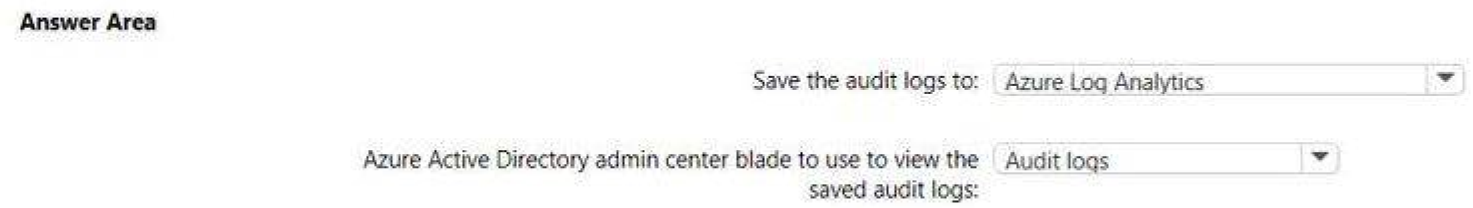
Correct Answer: C
Section:
Explanation:

QUESTION 11
You have a Microsoft 365 tenant that uses Microsoft Endpoint Manager for device management. You need to add the phone number of the help desk to the Company Portal app. What should you do?
A. From Customization in the Microsoft Endpoint Manager admin center, modify the support information for the tenant.
B. From the Microsoft Endpoint Manager admin center, create an app configuration policy.
C. From the Microsoft 365 admin center, modify Organization information.
D. From the Microsoft 365 admin center, modify Help desk information.

Correct Answer: A
Section:
Explanation:
https://systemcenterdudes.com/intune-company-portal-customization/

QUESTION 12
HOTSPOT
You have a Microsoft 365 tenant.
You need to retain Azure Active Directory (Azure AD) audit logs for two years. Administrators must be able to query the audit log information by using the Azure Active Directory admin center.
What should you do? To answer, select the appropriate options in the answer area.
NOTE: Each correct selection is worth one point.

Hot Area:

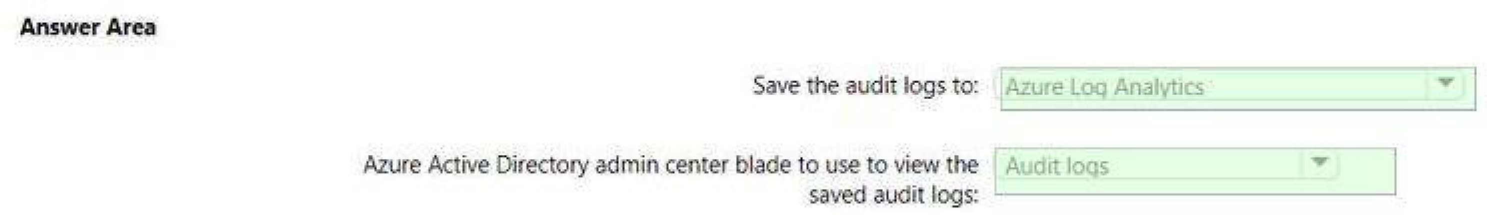


Answer Area

Save the audit logs to: Azure Log Analytics

Azure Active Directory admin center blade to use to view the saved audit logs: Audit logs

Answer Area:



Answer Area

Save the audit logs to: Azure Log Analytics

Azure Active Directory admin center blade to use to view the saved audit logs: Audit logs

Section:
Explanation:

QUESTION 13

You have a Microsoft 365 E5 subscription.

All users have Mac computers. All the computers are enrolled in Microsoft Endpoint Manager and onboarded to Microsoft Defender Advanced Threat Protection (Microsoft Defender ATP).

You need to configure Microsoft Defender ATP on the computers.

What should you create from the Endpoint Management admin center?

A. a device configuration profile

B. an update policy for iOS

C. a Microsoft Defender ATP baseline profile

D. a mobile device management (MDM) security baseline profile

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

QUESTION 14

HOTSPOT

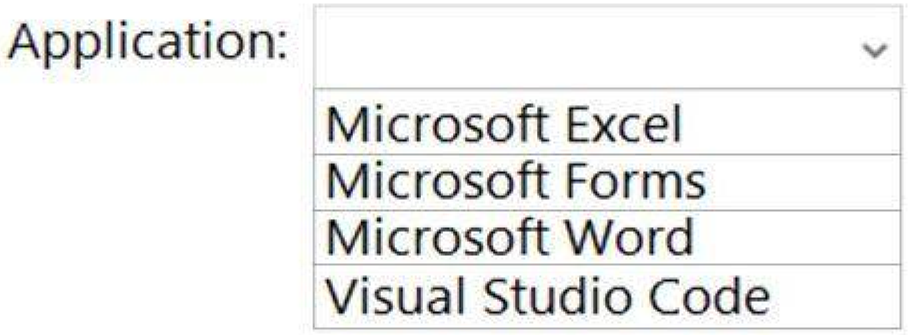
You have a Microsoft 365 tenant.

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.

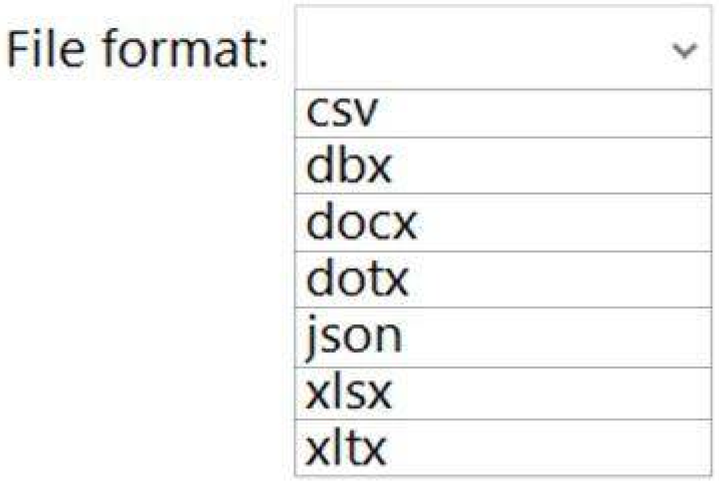
NOTE: Each correct selection is worth one point.

Hot Area:



Application:

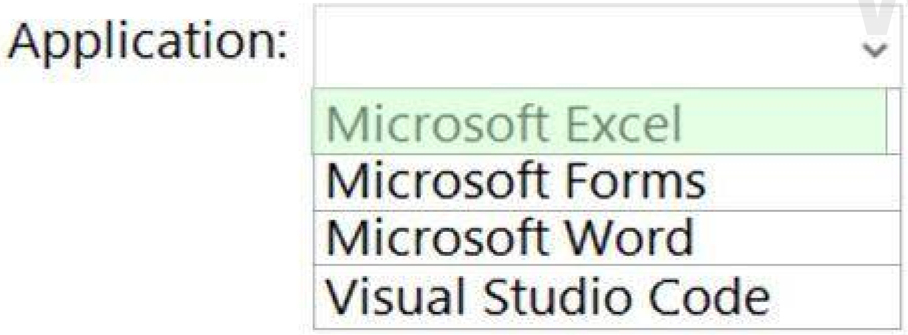
- Microsoft Excel
- Microsoft Forms
- Microsoft Word
- Visual Studio Code



File format:

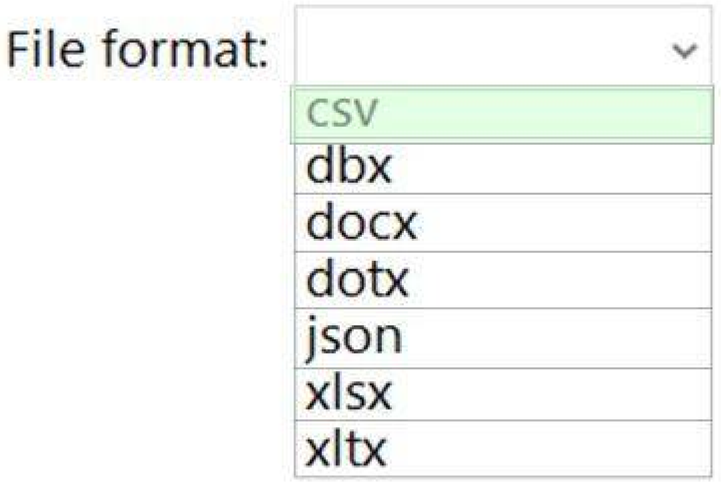
- csv
- dbx
- docx
- dotx
- json
- xlsx
- xltx

Answer Area:



Application:

- [✓ Microsoft Excel]
- Microsoft Forms
- Microsoft Word
- Visual Studio Code



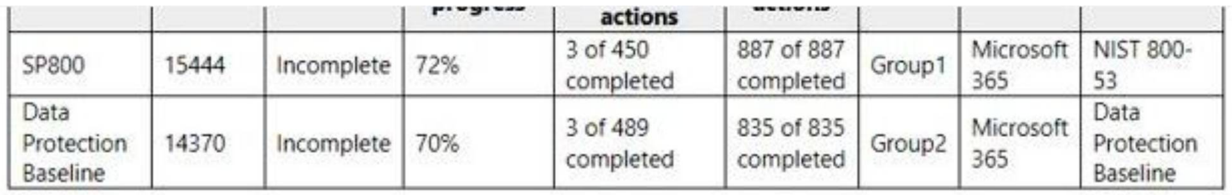
File format:

- [✓ 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

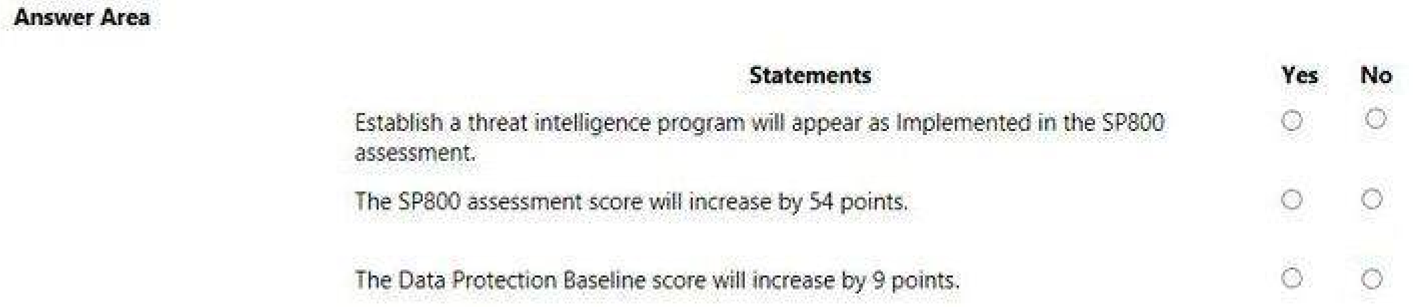
QUESTION 15
HOTSPOT



			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.

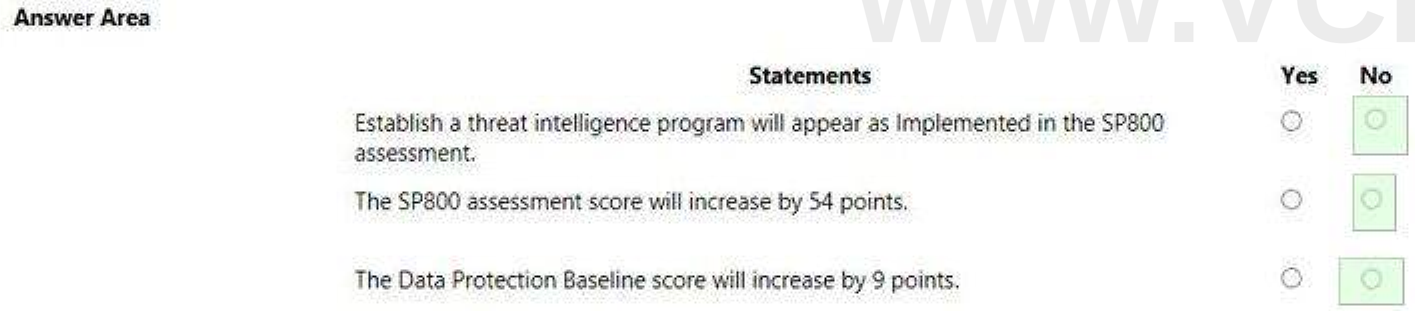
Hot Area:



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:



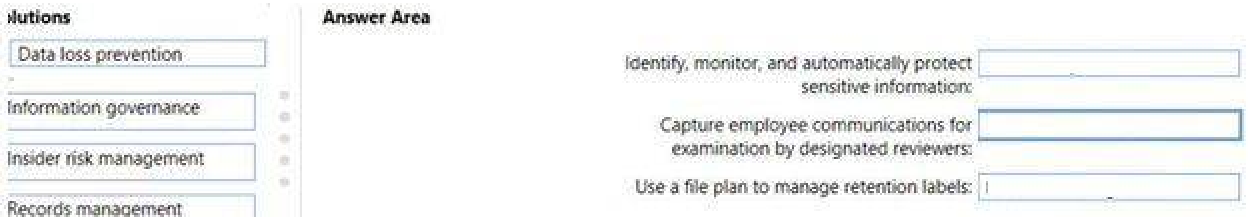
Answer Area

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 16
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

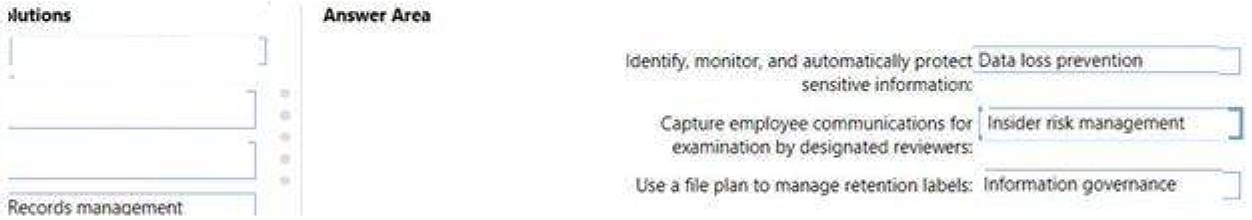
Answer Area

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 17

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.

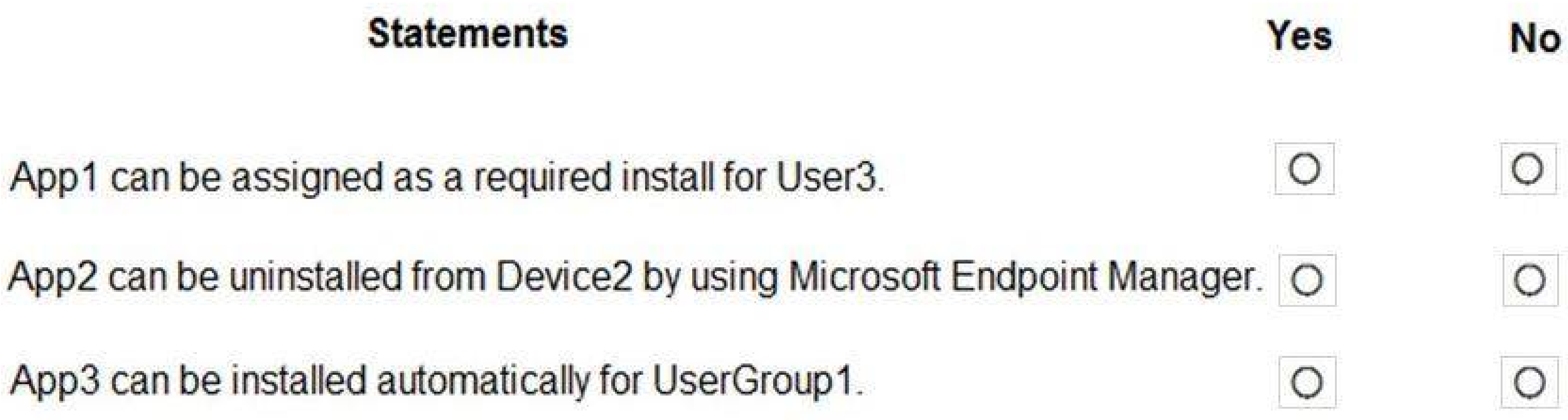
Name	Type
App1	iOS store app
App2	Android store app
App3	Microsoft store app

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.

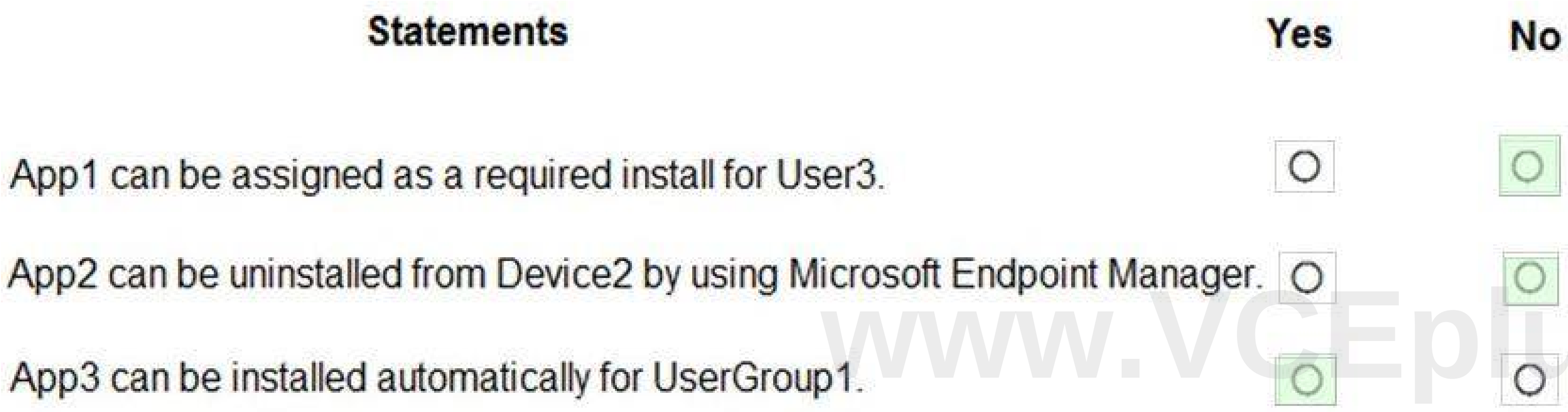
NOTE: Each correct selection is worth one point.

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.	[✓ ○]	○

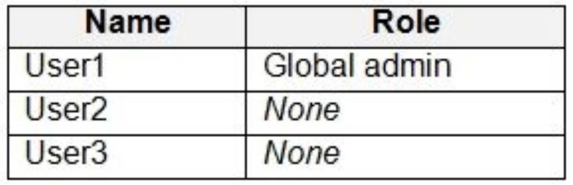
Section:
Explanation:
https://docs.microsoft.com/en-us/mem/intune/apps/apps-deploy
https://docs.microsoft.com/en-us/mem/intune/apps/apps-windows-10-app-deploy

QUESTION 18
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

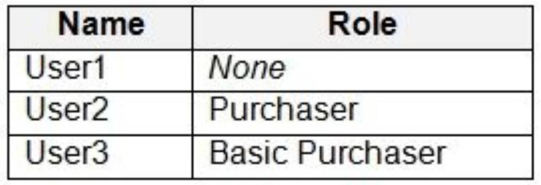
Correct Answer: C
Section:
Explanation:
https://docs.microsoft.com/en-us/deployedge/configure-edge-with-intune

QUESTION 19
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*

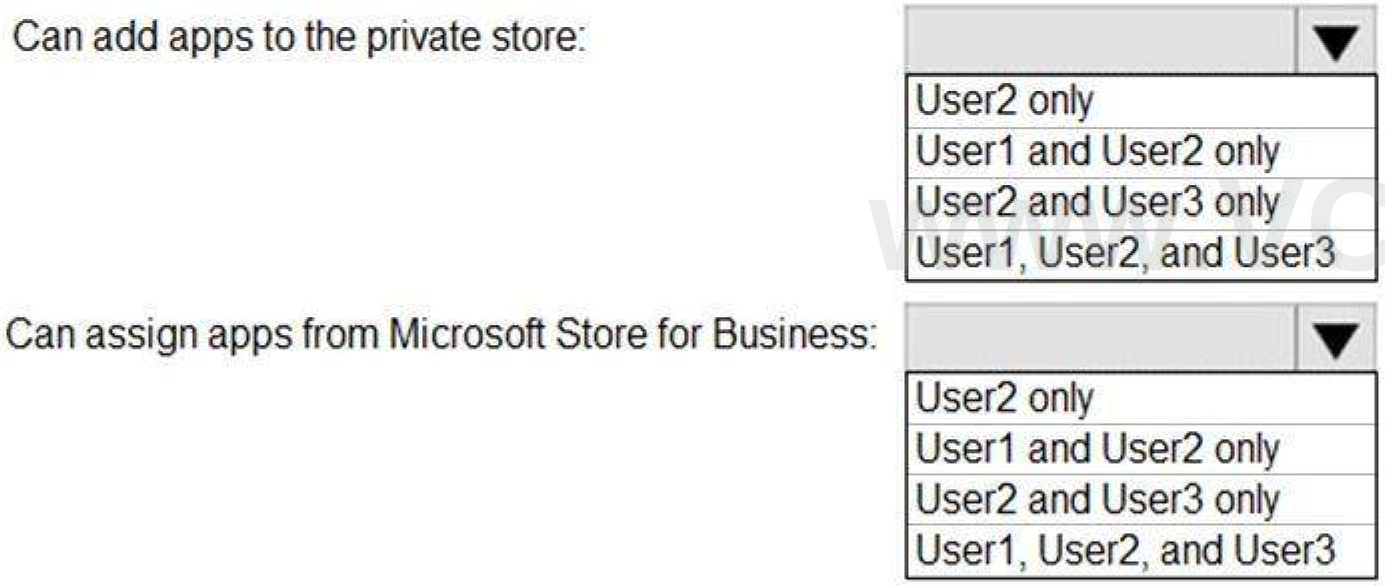
You provision the private store in Microsoft Store for Business.
You assign Microsoft Store for Business roles to the users as shown in the following table.



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:



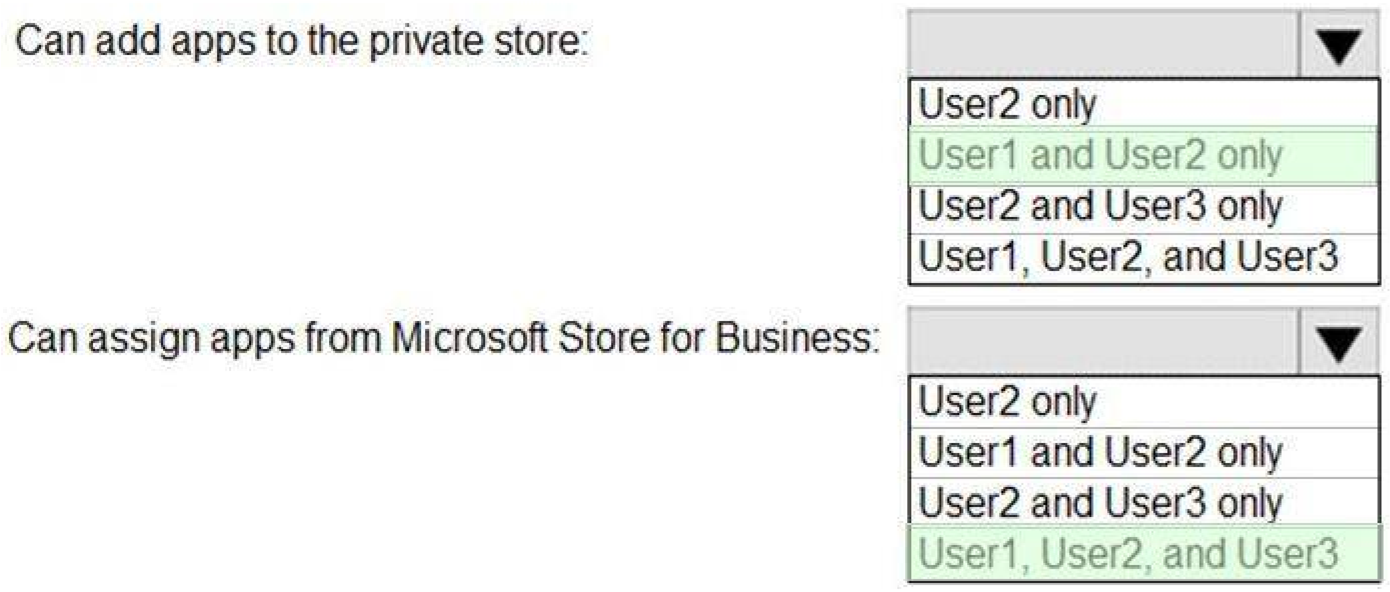
Can add apps to the private store:

- 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

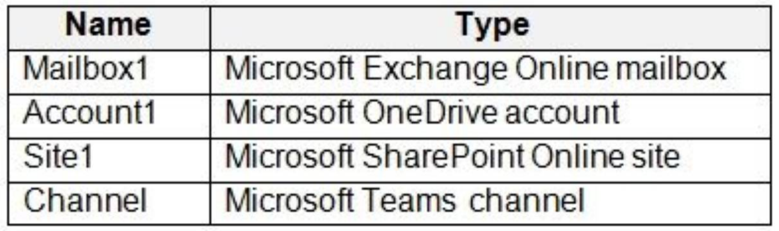
Can assign apps from Microsoft Store for Business:

- 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 20

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?

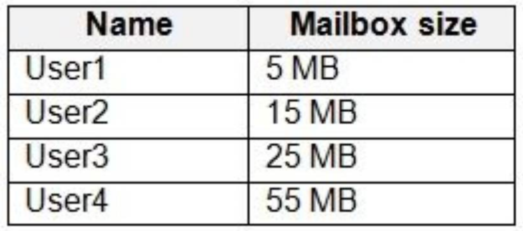
A. Mailbox1 and Site1 only
B. Mailbox1, Account1, and Site1 only
C. Account1 and Site1 only
D. Mailbox1, Account1, Site1, and Channel1
E. Account1, Site1, and Channel1 only

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

QUESTION 21

HOTSPOT

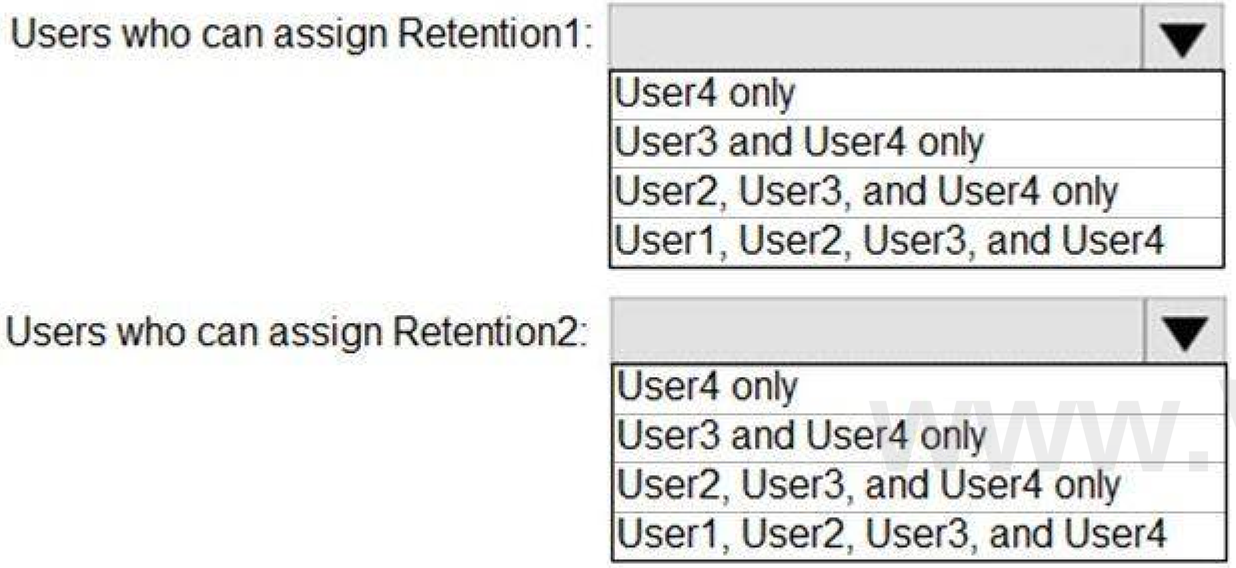
You have a Microsoft 365 E5 subscription that contains the users shown in the following table.



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:



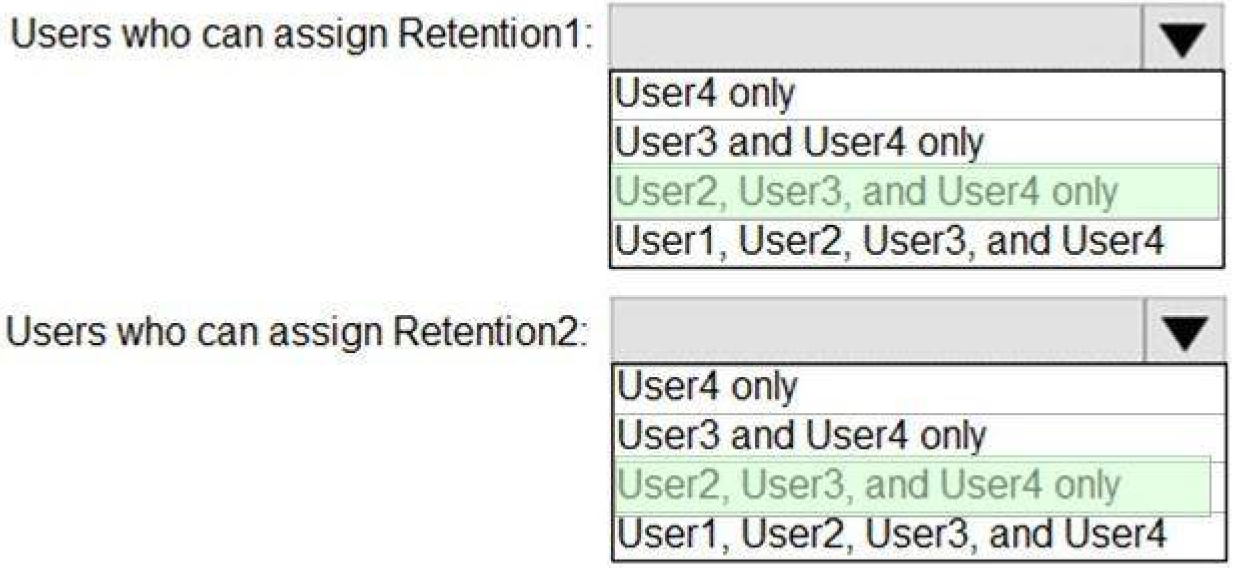
Users who can assign Retention1:

- 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 22

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

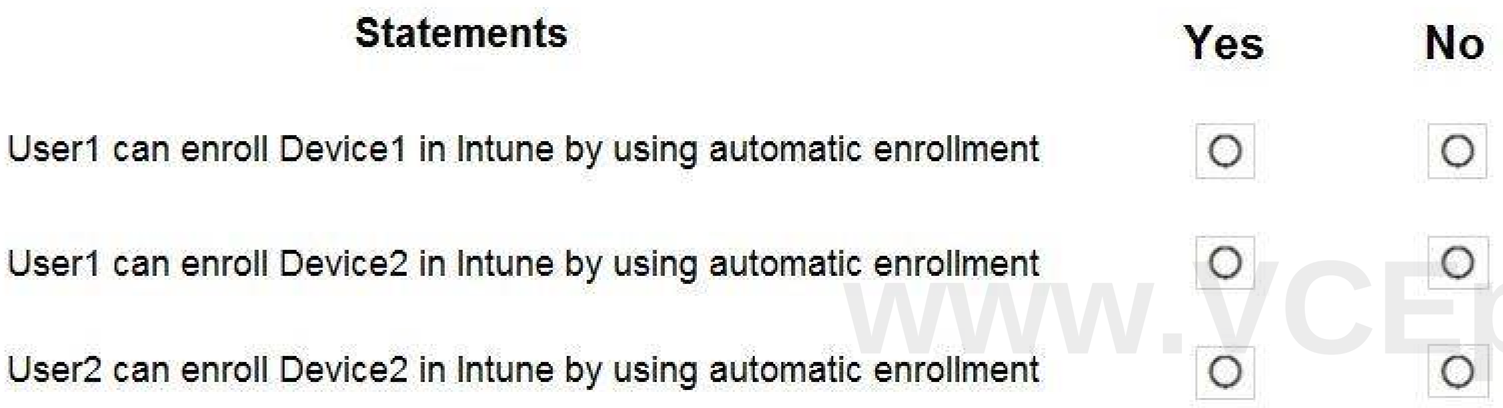
Groups: Group2

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.

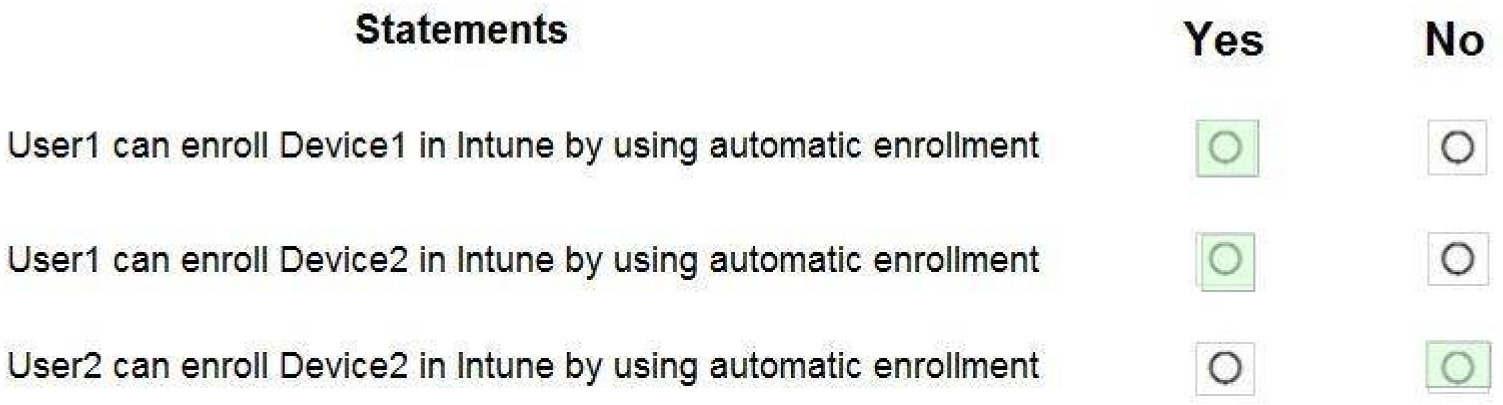
NOTE: Each correct selection is worth one point.

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

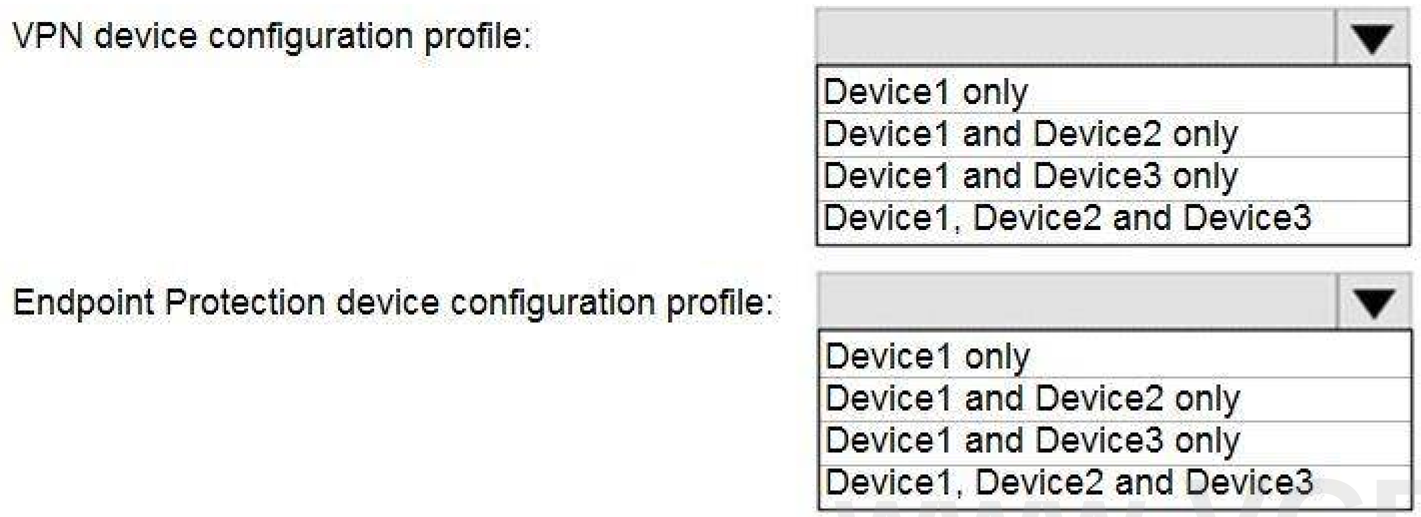
https://docs.microsoft.com/en-us/mem/intune/enrollment/android-enroll-device-administrator

QUESTION 23

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:



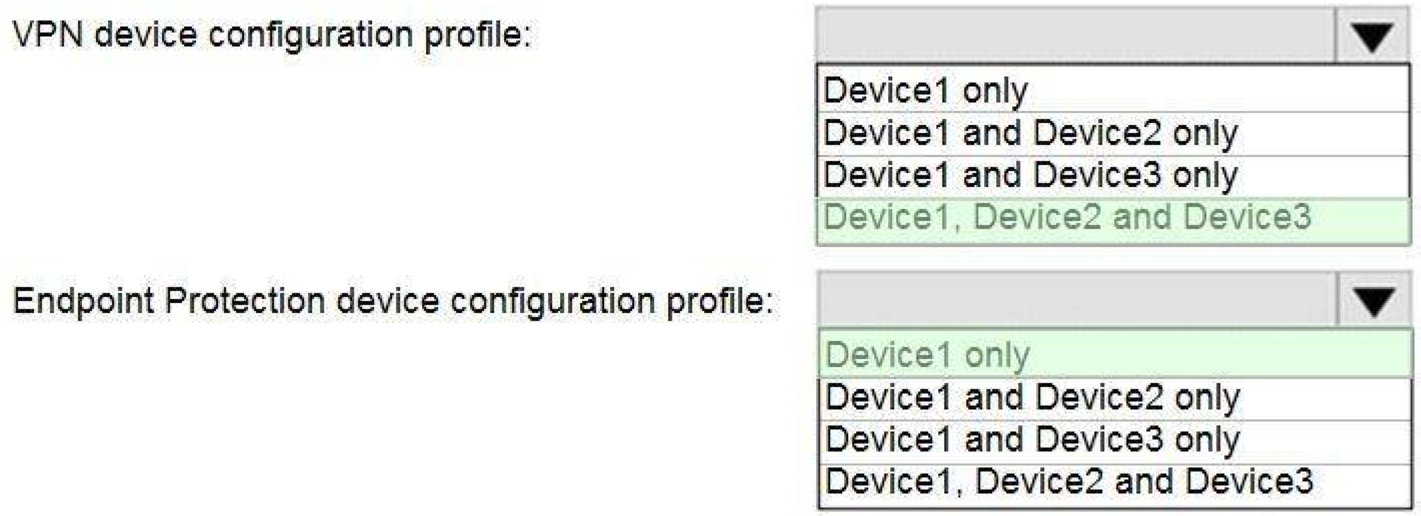
VPN device configuration profile:

- 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

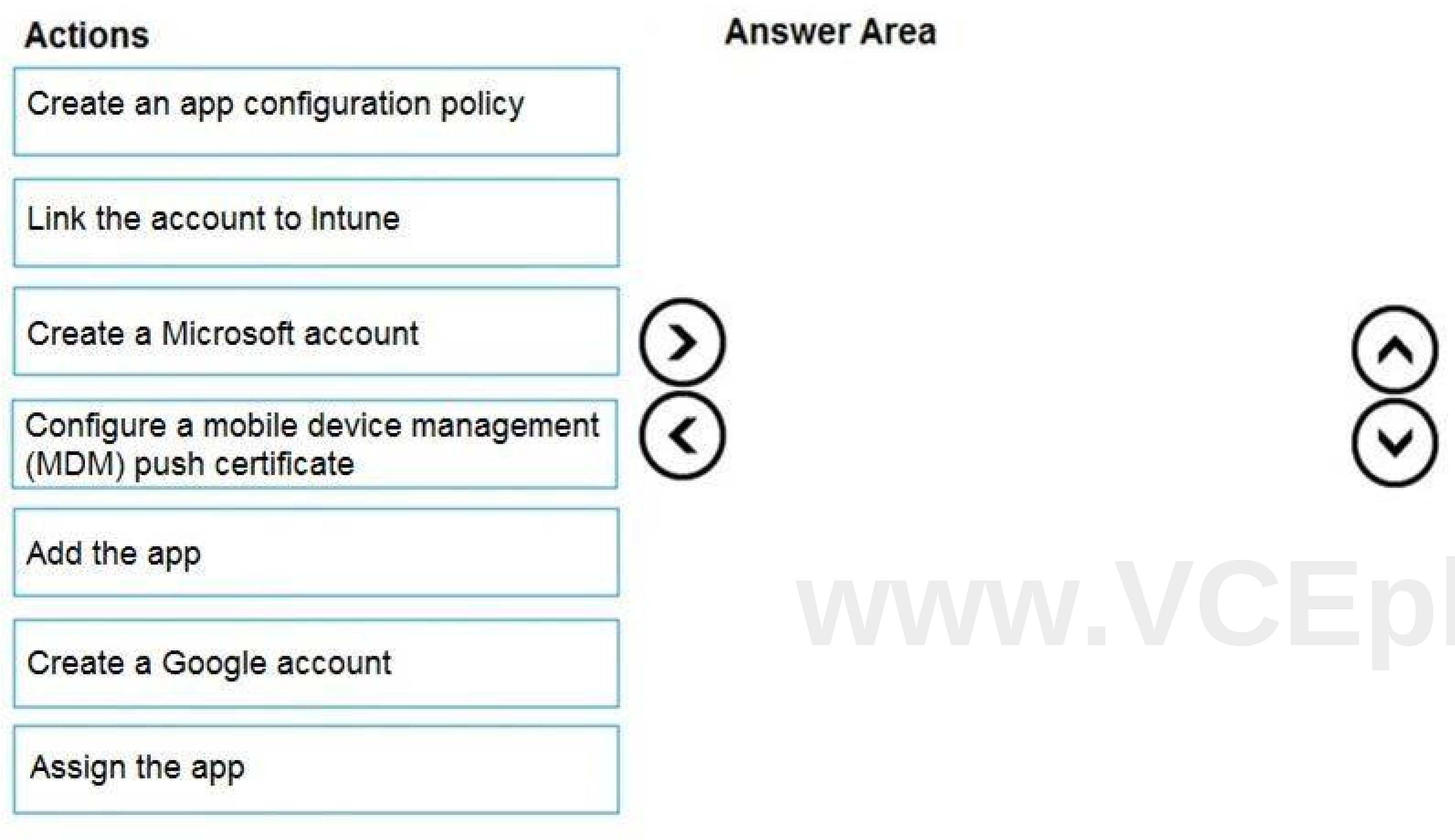
Section:
Explanation:
https://docs.microsoft.com/en-us/mem/intune/configuration/vpn-settings-configure
https://docs.microsoft.com/en-us/mem/intune/protect/endpoint-protection-macos

QUESTION 24
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:

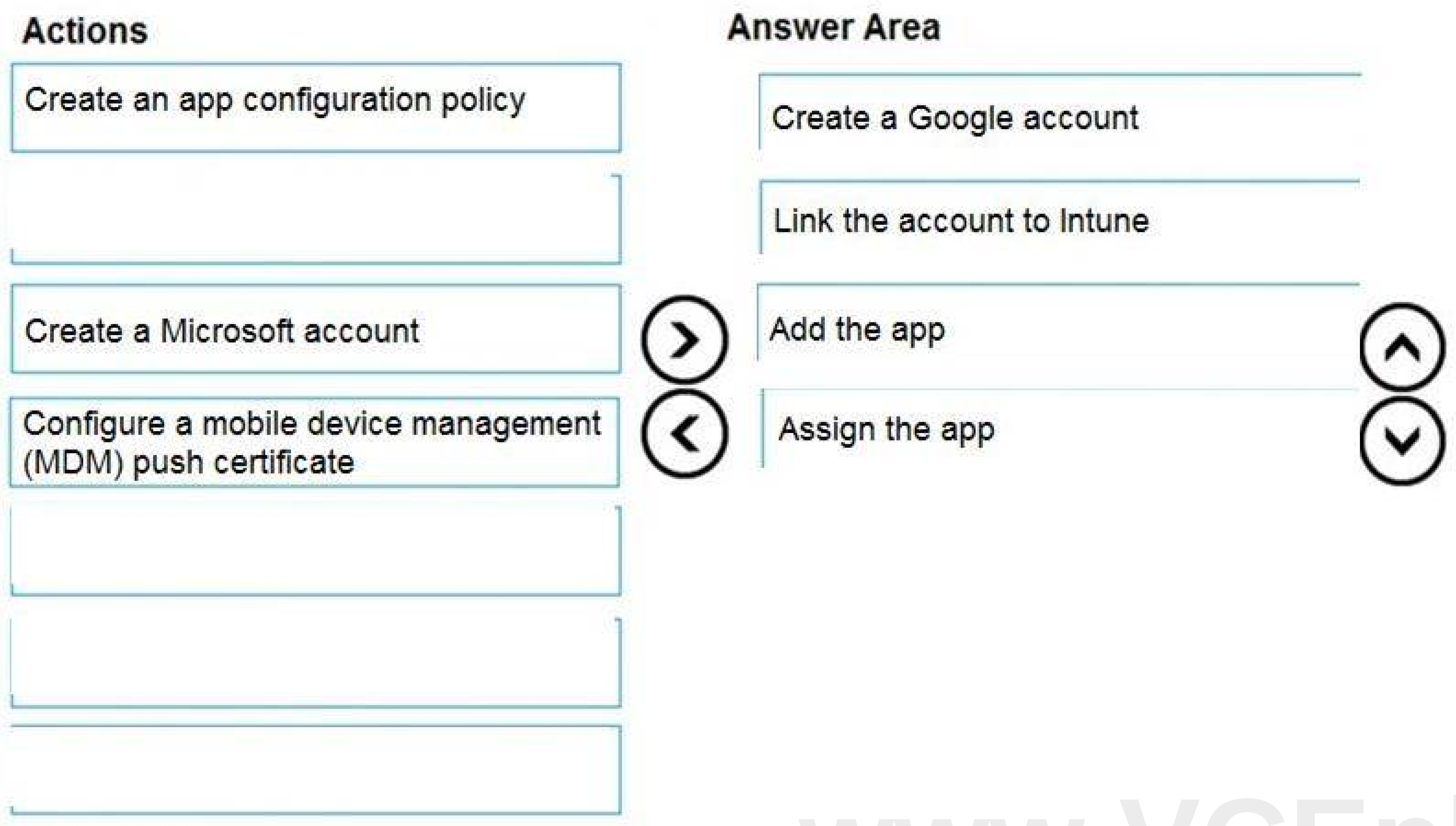


Actions

- 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

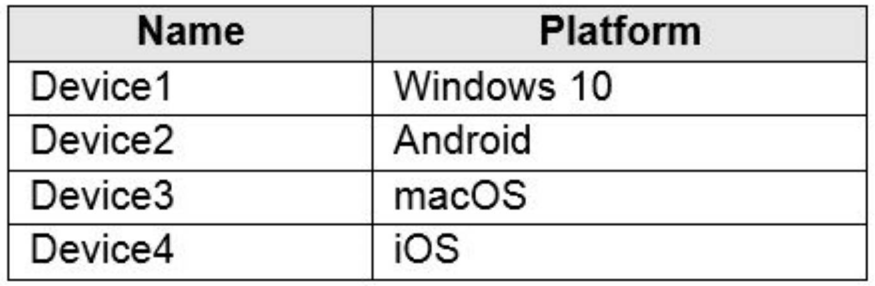
- Create an app configuration policy
- Create a Microsoft account
- Configure a mobile device management (MDM) push certificate

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 25
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

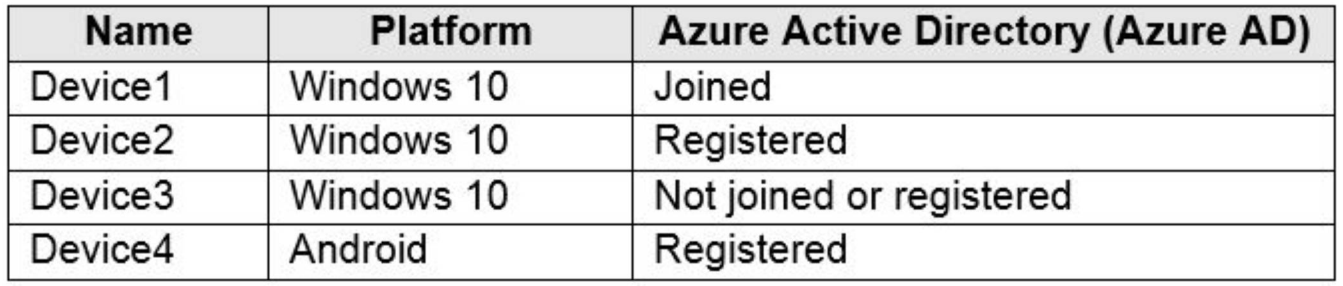
You plan to deploy Microsoft 365 Apps for enterprise by using Microsoft Endpoint Manager.
To which devices can you deploy Microsoft 365 Apps for enterprise?

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 26
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 27
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:
Explanation:

QUESTION 28
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 29
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 30
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:
Explanation:

QUESTION 31
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 32

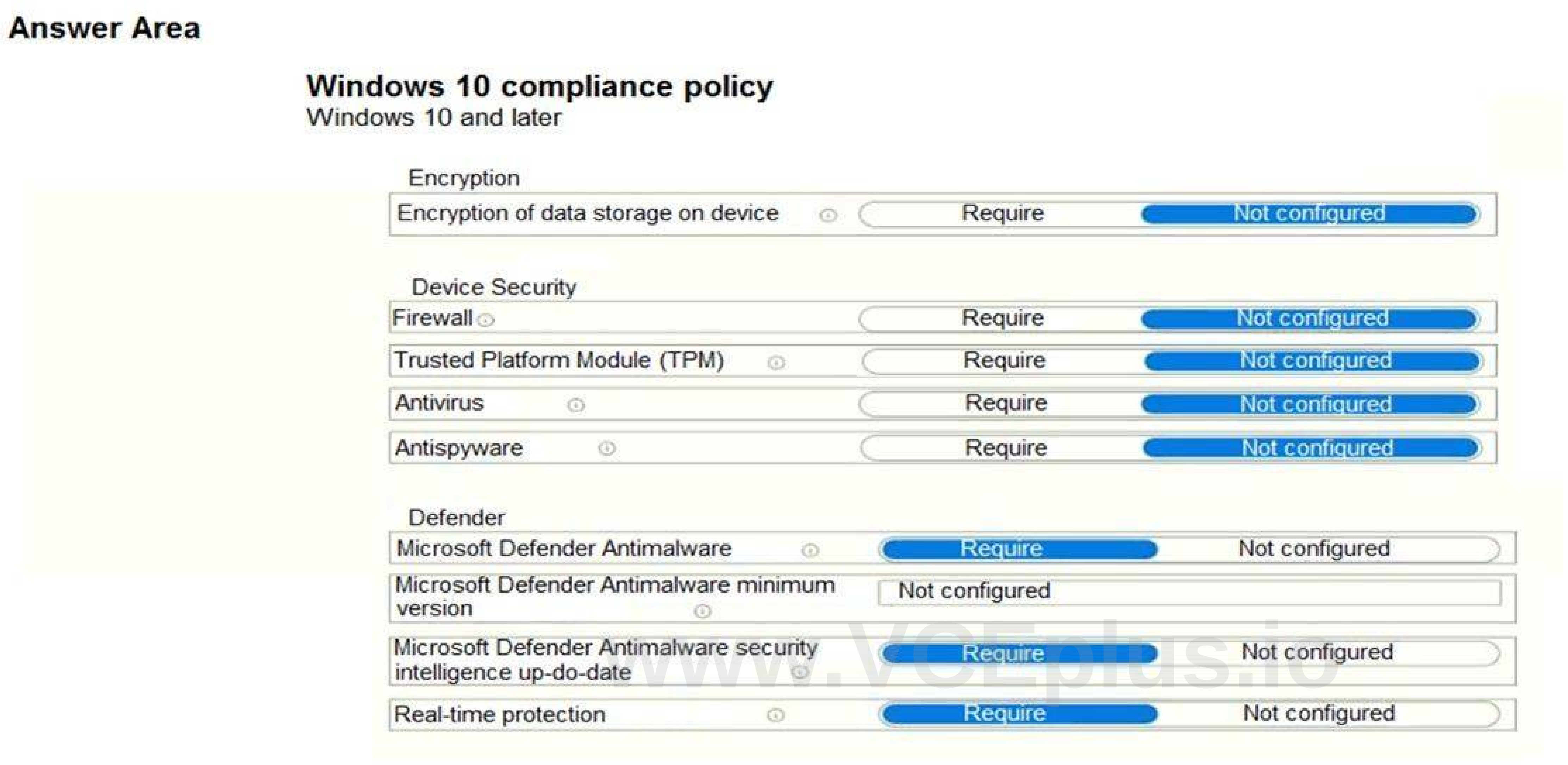
You have a Microsoft 365 tenant and a LinkedIn company page.
You plan to archive data from the LinkedIn page to Microsoft 365 by using the LinkedIn connector.
Where can you store data from the LinkedIn connector?

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 33
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

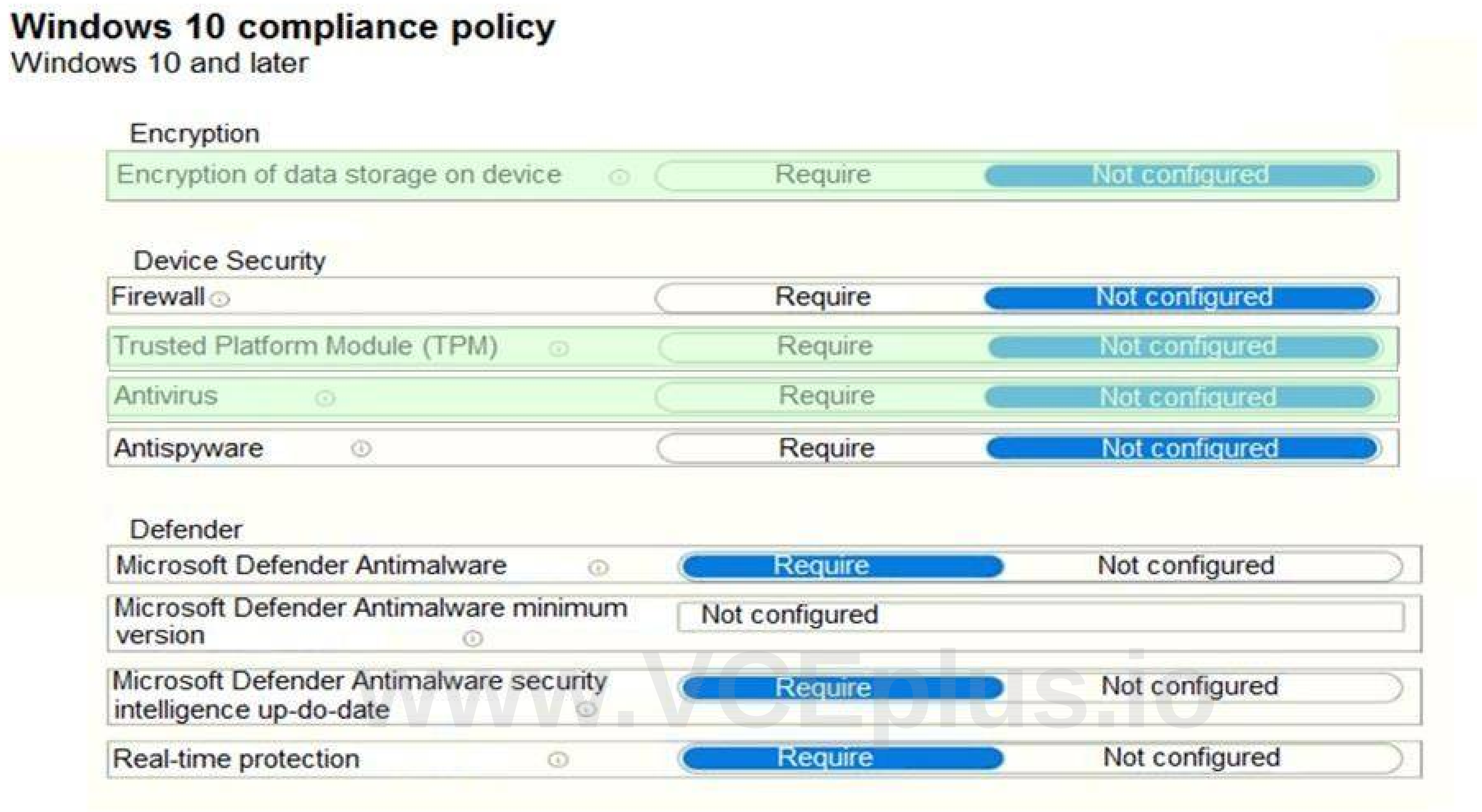
Firewall	Require	[✓ Not configured]
Trusted Platform Module (TPM)	Require	[✓ Not configured]
Antivirus	Require	[✓ Not configured]
Antispyware	Require	[✓ Not configured]

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

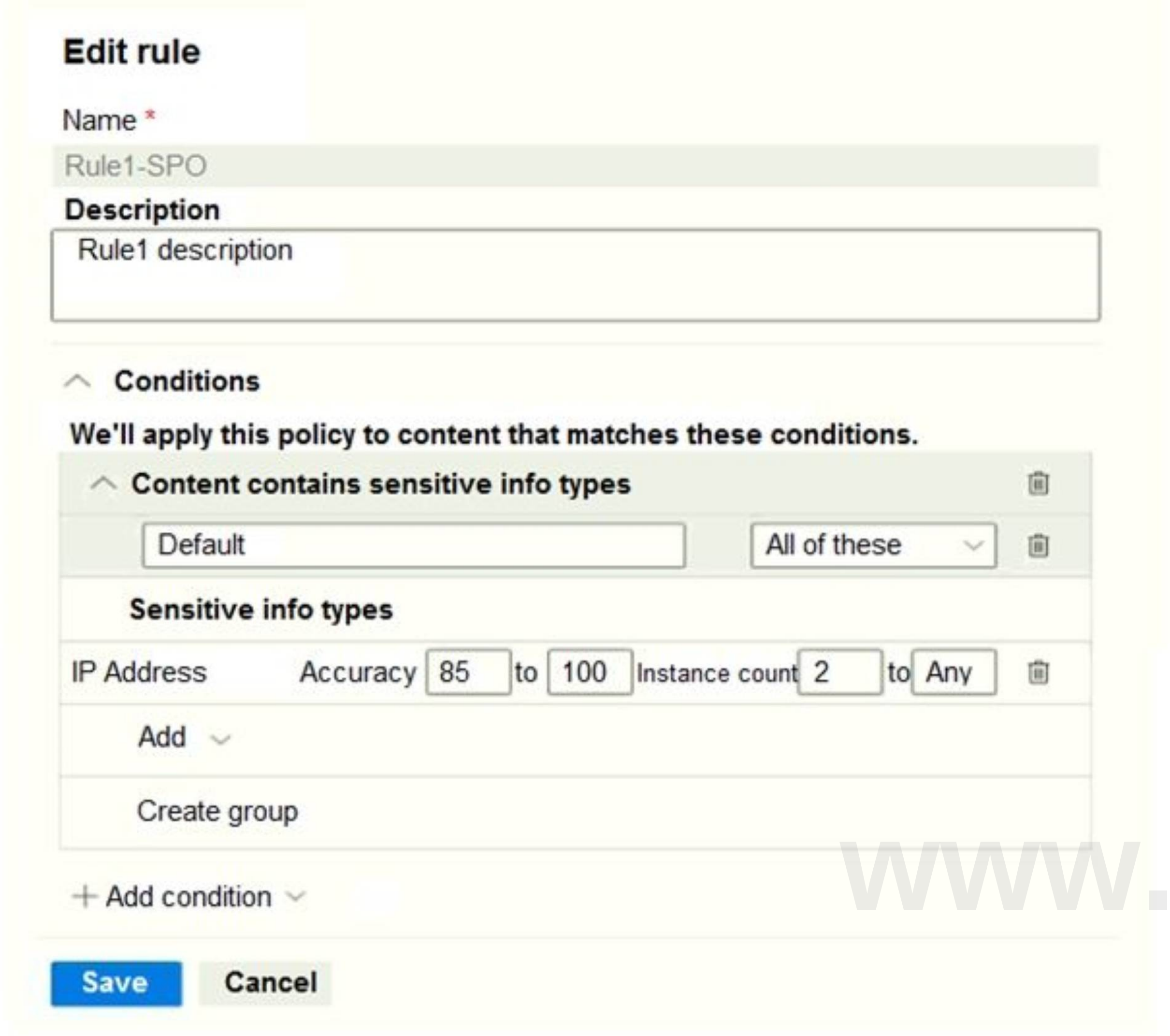
Section:
Explanation:
https://docs.microsoft.com/en-us/mem/intune/protect/compliance-policy-create-windows

QUESTION 34
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

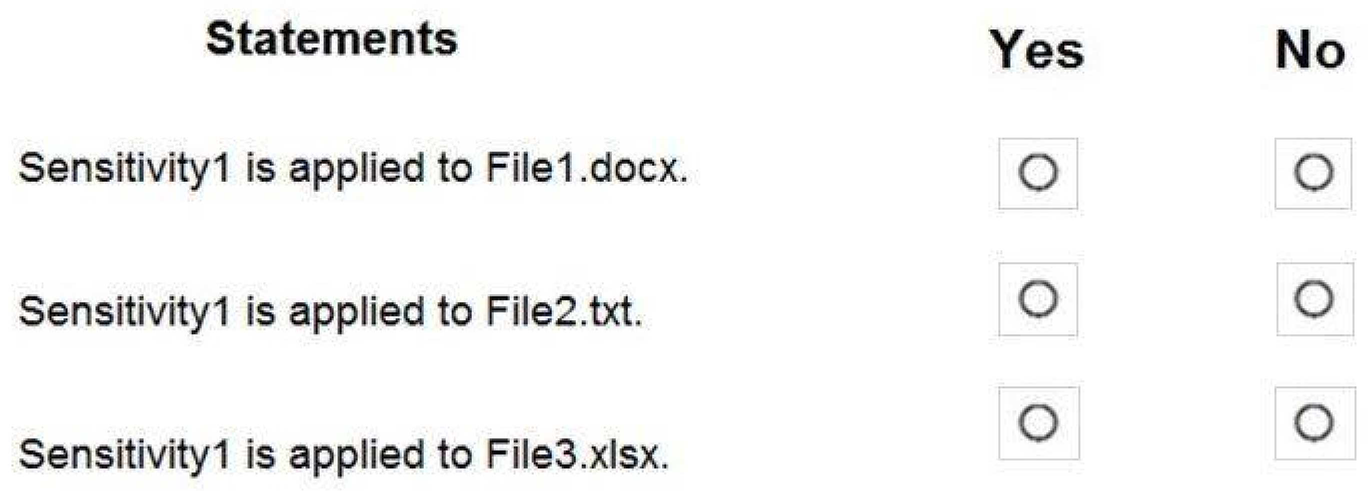
Default — All of these

Sensitive info types

IP Address Accuracy 85 to 100 Instance count 2 to Any

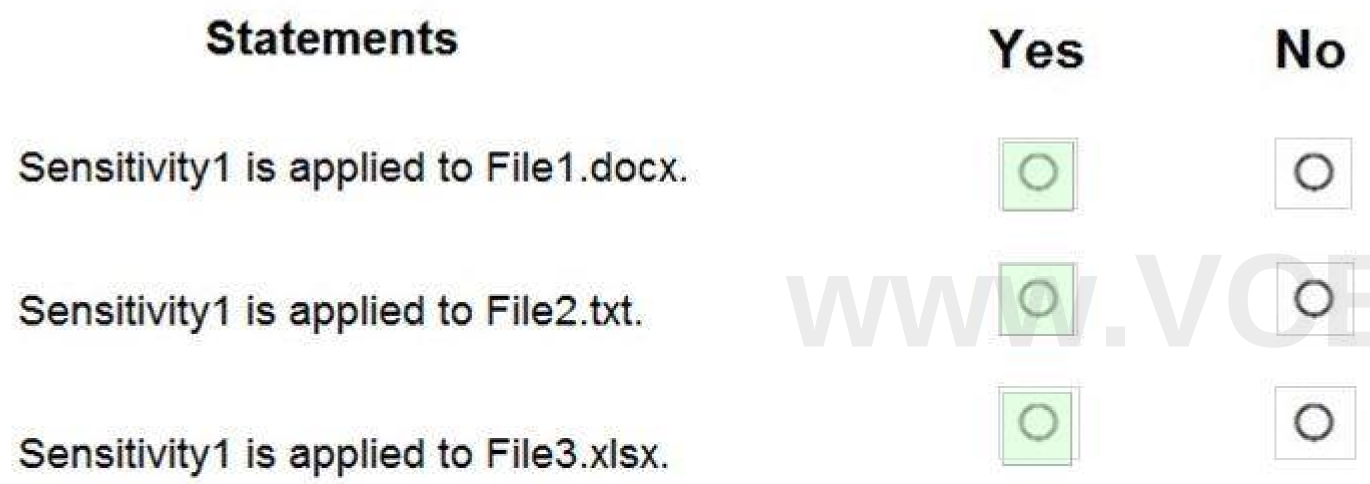
For each of the following statements, select Yes if the statement is true. Otherwise, select No.
NOTE: Each correct selection is worth one point.

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