MS-102$^{\text{Q\&As}}$

Microsoft 365 Certified: Enterprise Administrator Expert

QUESTION 1

HOTSPOT

You have a Microsoft 365 E5 tenant that uses Microsoft Intune.

You need to configure Intune to meet the following requirements:

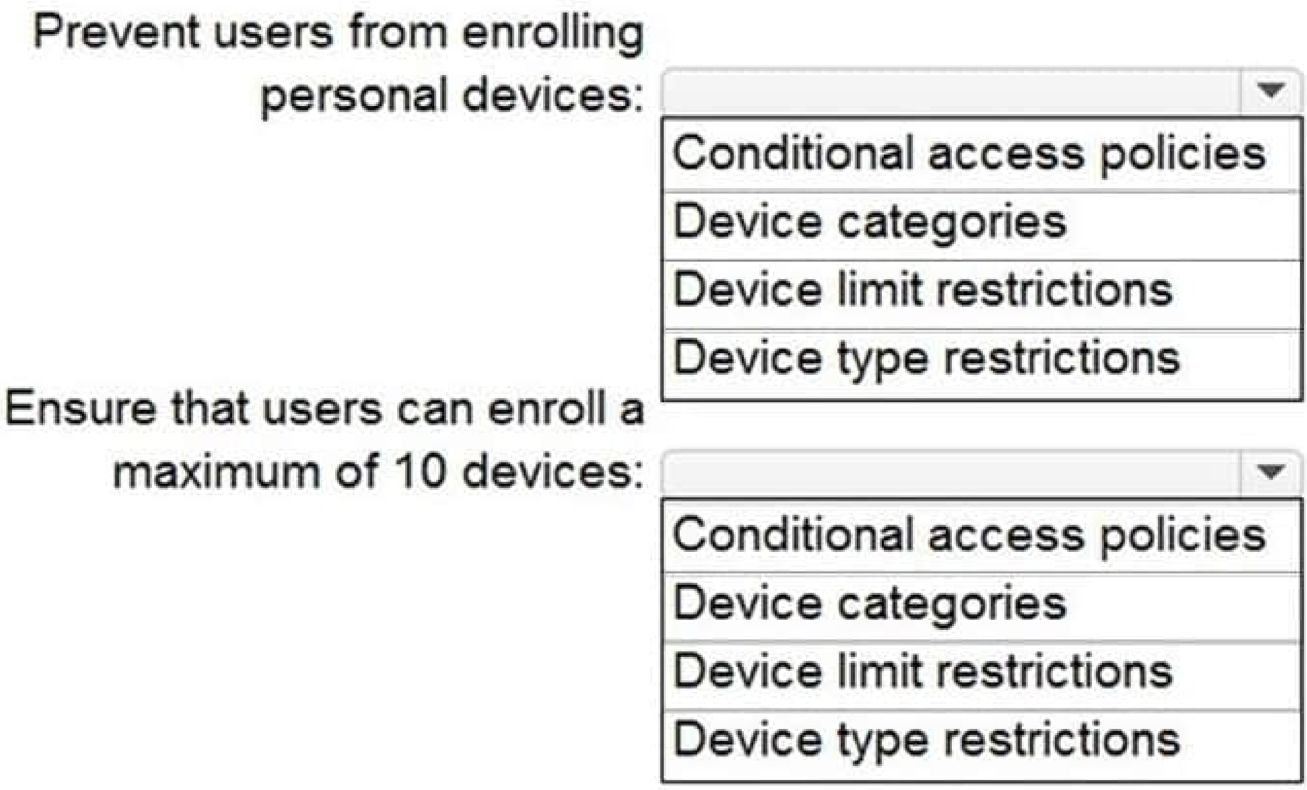
Prevent users from enrolling personal devices.

Ensure that users can enroll a maximum of 10 devices.

What should you use for each requirement? To answer, select the appropriate options in the answer area.

NOTE: Each correct selection is worth one point.

Hot Area:



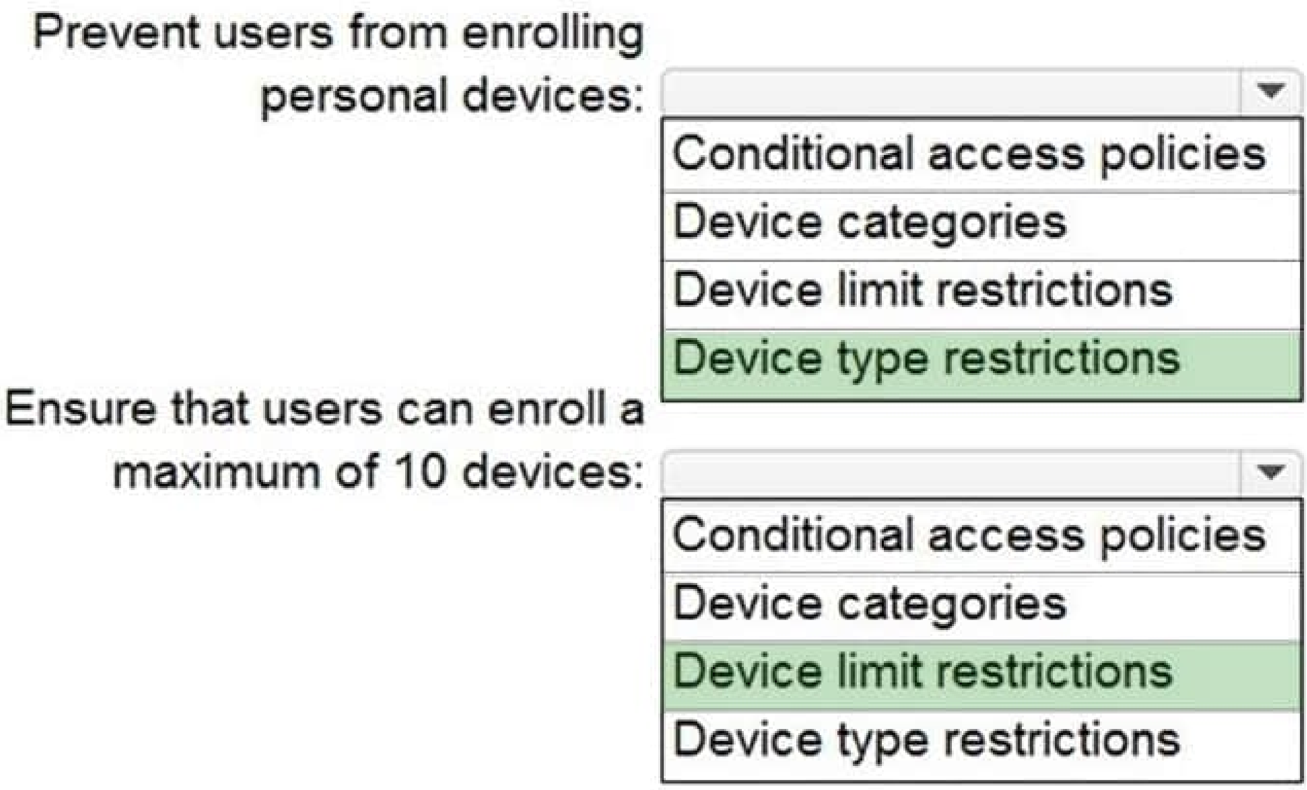
Prevent users from enrolling personal devices:

- Conditional access policies
- Device categories
- Device limit restrictions
- Device type restrictions

Ensure that users can enroll a maximum of 10 devices:

- Conditional access policies
- Device categories
- Device limit restrictions
- Device type restrictions

Correct Answer:



Prevent users from enrolling personal devices:

- Conditional access policies
- Device categories
- Device limit restrictions
- [✓ Device type restrictions]

Ensure that users can enroll a maximum of 10 devices:

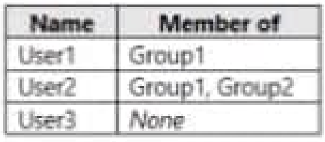
- Conditional access policies
- Device categories
- [✓ Device limit restrictions]
- Device type restrictions

QUESTION 2

HOTSPOT

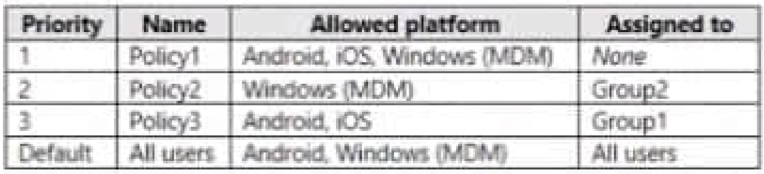
You have several devices enrolled in Microsoft Endpoint Manager.

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



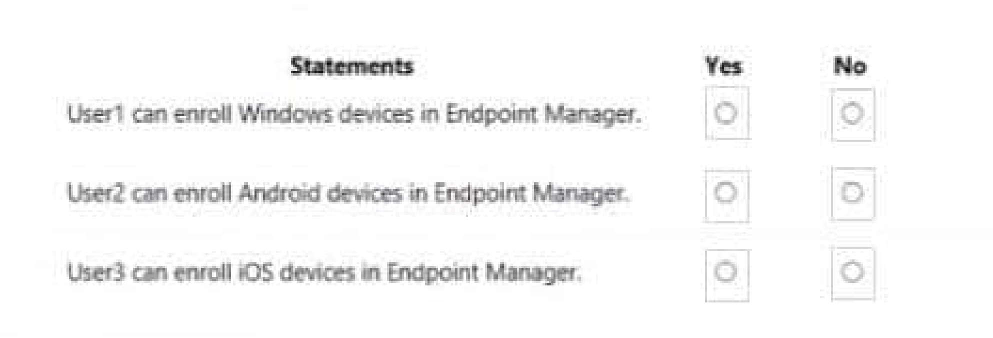
Name	Member of
User1	Group1
User2	Group1, Group2
User3	*None*

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



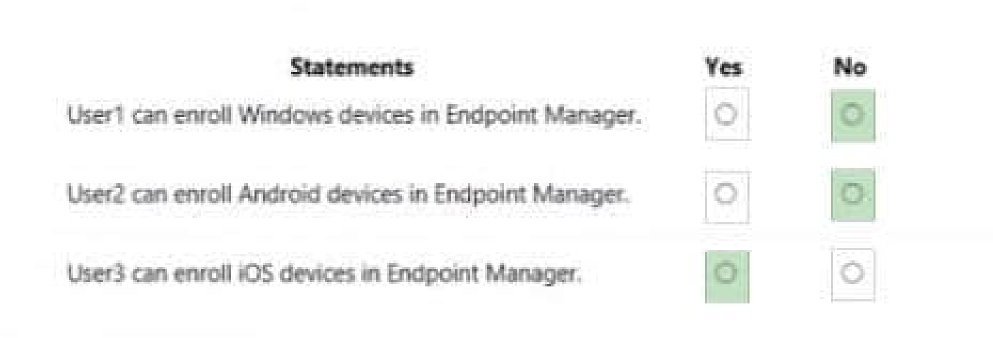
Priority	Name	Allowed platform	Assigned to
1	Policy1	Android, iOS, Windows (MDM)	*None*
2	Policy2	Windows (MDM)	Group2
3	Policy3	Android, iOS	Group1
Default	All users	Android, Windows (MDM)	All users

Hot Area:



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.	○	○

Correct Answer:

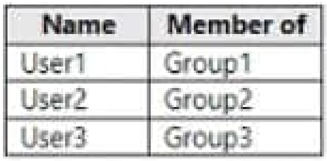


Statements	Yes	No
User1 can enroll Windows devices in Endpoint Manager.	○	●
User2 can enroll Android devices in Endpoint Manager.	○	●
User3 can enroll iOS devices in Endpoint Manager.	●	○

QUESTION 3

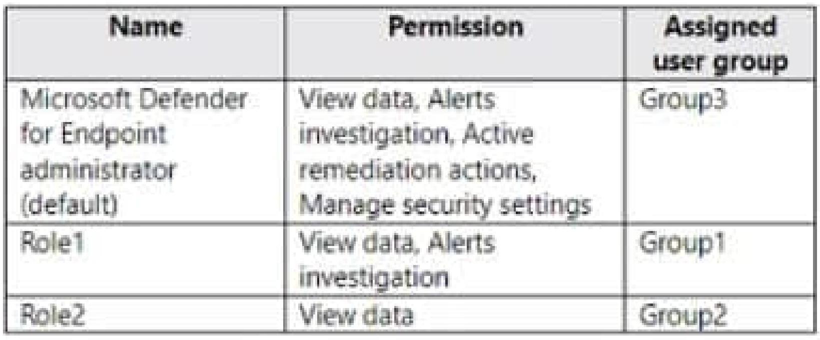
HOTSPOT

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



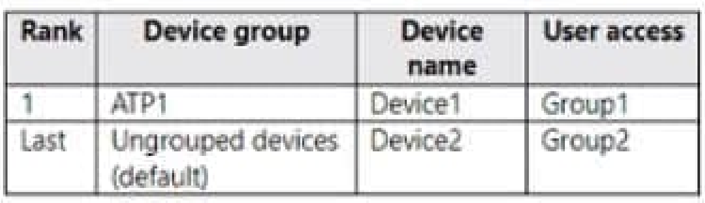
Name	Member of
User1	Group1
User2	Group2
User3	Group3

Your company uses Microsoft Defender for Endpoint. Microsoft Defender for Endpoint contains the roles shown in the following table.



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

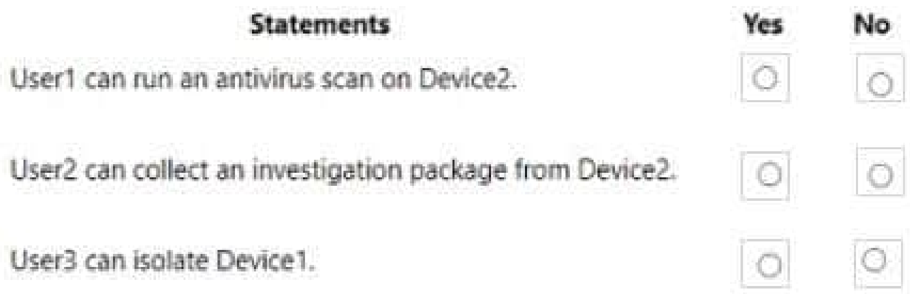
Microsoft Defender for Endpoint contains the device groups shown in the following table.



Rank	Device group	Device name	User access
1	ATP1	Device1	Group1
Last	Ungrouped devices (default)	Device2	Group2

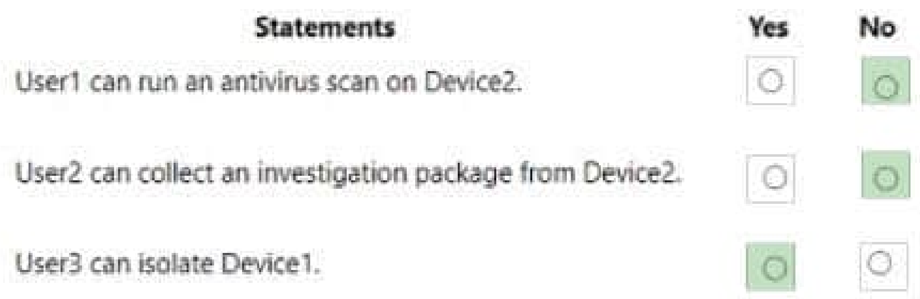
For each of the following statements, select Yes if the statement is true. Otherwise, select No. NOTE: Each correct selection is worth one point.

Hot Area:



Statements	Yes	No
User1 can run an antivirus scan on Device2.	○	○
User2 can collect an investigation package from Device2.	○	○
User3 can isolate Device1.	○	○

Correct Answer:



Statements	Yes	No
User1 can run an antivirus scan on Device2.	○	[✓ ○]
User2 can collect an investigation package from Device2.	○	[✓ ○]
User3 can isolate Device1.	[✓ ○]	○

QUESTION 4

HOTSPOT

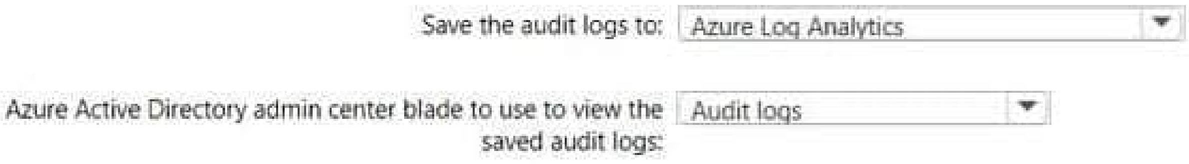
You have a Microsoft 365 tenant.

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.

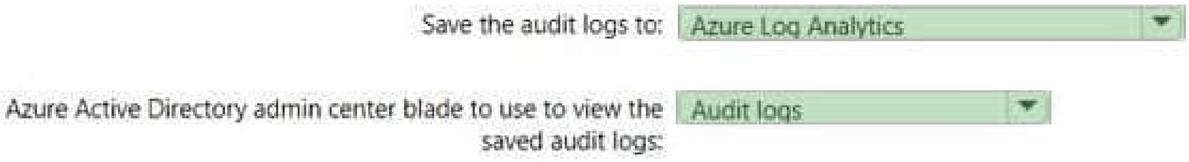
Hot Area:



Save the audit logs to: Azure Log Analytics

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

Correct Answer:



Save the audit logs to: [✓ Azure Log Analytics]

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

QUESTION 5

You have a Microsoft 365 E5 tenant.

You need to ensure that when a document containing a credit card number is added to the tenant, the document is encrypted.

Which policy should you use?

A. a retention policy

B. a retention label policy

C. an auto-labeling policy

D. an insider risk policy

Correct Answer: C

Reference:

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