Question: 384

HOTSPOT

-

You have a Microsoft 365 E5 subscription that contains three Windows devices named Device1, Device2, and Device3. The devices are managed by using Microsoft Intune. Each device contains a file named Script1.ps1.
Users do NOT have local administrator permissions for the devices.
The subscription contains the groups shown in the following table.

Name	Member
Group1	Device1
Group2	Device2
Group3	Device3

You create two Endpoint Privilege Management (EPM) elevation settings policies that have the following settings:
•Name: Policy1
•Endpoint Privilege Management: Enabled
oDefault elevation response: Deny all requests
oAllow Elevation Detection: No
oSend elevation data for reporting: No
•Assignments:
oIncluded groups: Group1
•Name: Policy2
•Endpoint Privilege Management: Require support approval
oAllow Elevation Detection: No
oSend elevation data for reporting: No
•Assignments:
oIncluded groups: Group3

You create an EPM elevation rules policy named RulesPolicy1 that has the following settings:
•Rule name: Rule1
oElevation type: Automatic
oChild process behavior: Deny all
oFile name: Script1.ps1
oFile hash:
•Assignments: Group 1, 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.

Answer Area

Statements	Yes	No
A user on Device1 must get approval before the user can run Script1.ps1 with elevated privileges.	○	○
A user on Device2 must get approval before the user can run Script1.ps1 with elevated privileges.	○	○
A user on Device3 must get approval before the user can run Script1.ps1 with elevated privileges.	○	○

Note: This section contains one or more sets of questions with the same scenario and problem. Each question presents a unique solution to the problem. You must determine whether the solution meets the stated goals. More than one solution in the set might solve the problem. It is also possible that none of the solutions in the set solve the problem.
After you answer a question in this section, you will NOT be able to return. As a result, these questions do not appear on the Review Screen.
You have a Microsoft 365 E5 subscription. The subscription contains devices that are Microsoft Entra joined and enrolled in Microsoft Intune.
You create a user named User1.
You need to ensure that User1 can rotate BitLocker recovery keys by using Intune.
Solution: From the Microsoft Entra admin center, you assign the Cloud Device Administrator role to User1.
Does this meet the goal?

A.Yes

B.No

Question: 387

CertyIQ

HOTSPOT

-

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

Name	Member of
User1	Group1
User2	Group2
User3	*None*

You have the devices shown in the following table.

Name	Platform	Description
Device1	Windows 11	Workgroup
Device2	macOS	Microsoft Entra registered
Device3	Android	Microsoft Entra registered

The Windows Enrollment settings have the following configurations:

•MDM user scope: Group1

•Windows Information Protection (WIP) user scope: Group2

You configure Microsoft Intune enrollment restrictions as shown in the exhibit. (Click the Exhibit tab.)

All services > Devices | Enrollment > Enrollment restrictions > All Users | Properties >

Edit restriction

Device type restriction

Platform settings | Review + save

Specify the platform configuration restrictions that must be met for a device to enroll. Use compliance policies to restrict devices after enrollment. Define versions as major.minor.build. Version restrictions only apply to devices enrolled with the Company Portal. Intune classifies devices as personally-owned by default. Additional action is required to classify devices as corporate-owned. Learn more

Statements	Yes	No
User1 can enroll Device1 in Intune.	○	○
User2 can enroll Device2 in Intune.	○	○
User3 can enroll Device3 in Intune.	○	○

Question: 389 CertyIQ

HOTSPOT
-
You have a Microsoft 365 E5 subscription that contains 500 Windows devices and the resources shown in the following table.

Name	Description
User1	User
Group1	Security group
Device1	Windows device enrolled in Microsoft Intune
Device2	Microsoft Entra joined Windows device

Both devices have Microsoft 365 aps installed.
You need to create and assign a Polices for Office Apps policy that will block macros from running in Office files from the internet.
Which portal should you use, and what is the scope of the policy? To answer, select the appropriate options in the answer area.
NOTE: Each correct selection is worth one point.

Portal:

- The Microsoft Intune admin center only
- The Microsoft 365 Apps admin center only
- The Microsoft Intune admin center and Microsoft 365 admin center only
- The Microsoft Intune admin center and Microsoft 365 Apps admin center only
- The Microsoft 365 Apps admin center and Microsoft 365 admin center only
- The Microsoft Intune admin center, Microsoft 365 Apps admin center and Microsoft 368 admin center

Scope:

- Device1 only
- Group1 only
- Device1 and Device2 only
- Group1 and User1 only
- Device1, Group1, and User1 only
- Device1, Device2, Group1 and User1

Question: 391 CertyIQ

HOTSPOT

-

You have a hybrid environment that contains a Microsoft Entra tenant and an on-premises Active Directory Domain Services (AD DS) domain.

You purchase the devices shown in the following table.

Name	Platform
Device1	Windows 11
Device2	iOS

Which Microsoft Entra join type can each device use? To answer, select the appropriate options in the answer area

NOTE: Each correct selection is worth one point.

Device1:

- Microsoft Entra joined only
- Microsoft Entra registered only
- Microsoft Entra hybrid joined only
- Microsoft Entra joined or Microsoft Entra registered only
- Microsoft Entra registered, Microsoft Entra joined, or Microsoft Entra hybrid joined

Device2:

- Microsoft Entra joined only
- Microsoft Entra registered only
- Microsoft Entra hybrid joined only
- Microsoft Entra joined or Microsoft Entra registered only
- Microsoft Entra registered, Microsoft Entra joined, or Microsoft Entra hybrid joined