Question: 335

CertyIQ

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 Intune admin center, you assign the Endpoint Security Manager role to User1.
Does this meet the goal?

A.Yes

B.No

Question: 336 CertyIQ

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 Entra tenant named contoso.com.
You purchase an Android device named Device1.
You need to register Device1 in contoso.com.
Solution: You use the Google Chrome app.
Does this meet the goal?

A.Yes

B.No

Name	Action
Action1	Locate device
Action2	Remote lock

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
You can use Action1 on Device1.	○	○
You can use Action2 on Device2.	○	○
You can use Action2 on Device3.	○	○

The tenant contains the devices shown in the following table.

Name	Operating system
Device1	Windows 11
Device2	Windows 10
Device3	Windows 11

The devices have the enrollment restrictions shown in the following table.

Name	MDM	Personally owned devices	Minimum version	Included groups	Priority
Restriction1	Allow	Block	*None*	Group1	1
Restriction2	Allow	Allow	10.0.22000	Group1 Group2	2

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
User2 can enroll Device1 by using the Company Portal app.	○	○
User1 can enroll Device2 by using automatic enrollment.	○	○
User1 can enroll Device3 by using the Company Portal app.	○	○

Question: 343

CertyIQ

HOTSPOT

-

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

Name	Platform
Device1	Windows 11
Device2	Android
Device3	iOS
Device4	iPadOS

Which devices can be Microsoft Entra joined, and which devices can be Microsoft Entra registered? To answer, select the appropriate options in the answer area.

NOTE: Each correct selection is worth one point.

Answer Area

Microsoft Entra joined:

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

Microsoft Entra registered:

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

Question: 347

CertyIQ

DRAG DROP

-

You have a Microsoft 365 E5 subscription and use Microsoft Intune.
You need to use Microsoft Cloud PKI to deploy personal user certificates to all Windows 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.

Actions	Answer Area
Create device configuration SCEP certificate profiles.	
Create an issuing certification authority (CA).	
Create device configuration PKCS certificate profiles.	
Create device configuration trusted certificate profiles.	
Create a root certification authority (CA).	
Create an account protection profile.	
Create a Windows platform script.	

Answer Area

For the connection, use:

- Remote Desktop
- Remote Help
- Windows Remote Management (WinRM)

For elevated access, use:

- Endpoint Privilege Manager
- Help Desk Operator
- Policy and Profile manager

Answer Area

Device1:

- Collect diagnostics only
- Locate device only
- Remote lock only
- Collect diagnostics and Locate device only
- Locate device and Remote lock only
- Collect diagnostics, Locate device, and Remote lock

Device2:

- Collect diagnostics only
- Locate device only
- Remote lock only
- Collect diagnostics and Locate device only
- Locate device and Remote lock only
- Collect diagnostics, Locate device, and Remote lock

Device3:

- Collect diagnostics only
- Locate device only
- Remote lock only
- Collect diagnostics and Locate device only
- Locate device and Remote lock only
- Collect diagnostics, Locate device, and Remote lock

Answer Area

Device1:

- Enroll the device in Intune.
- Install the Intune app.
- Install the Microsoft Defender for Endpoint app.

Device2:

- Change the Device Ownership property.
- Install Edge.
- Install the Microsoft Defender for Endpoint app.

Answer Area

Statements	Yes	No
Admin1 can join Device1 to contoso.com.	○	○
User1 can join Device2 to contoso.com.	○	○
User1 can join Device3 to contoso.com.	○	○

Device1 was onboarded to Microsoft Defender for Endpoint by using a local script.
You use Microsoft Intune to manage Device1.
You plan to use the machine risk score in a compliance policy.
You need to ensure that the machine risk score is evaluated based on data from Defender for Endpoint.
What should you do? To answer, select the appropriate options in the answer area.
NOTE: Each correct selection is worth one point.

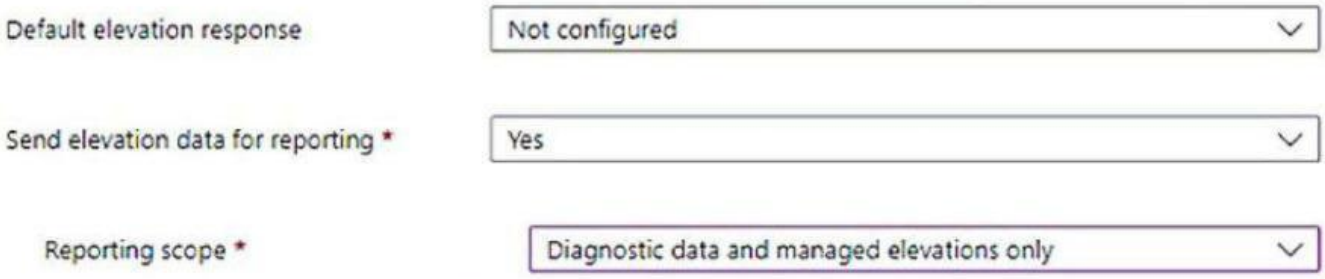
Answer Area

From the Endpoints settings of the Microsoft Defender portal:

- Configure the Advanced features settings.
- Configure the Intune Permissions settings.
- Select Onboarding, and then configure the Deployment method setting.

From the Microsoft Intune admin center:

- Create a Configuration profile.
- Configure the Compliance settings.
- Configure the Microsoft Defender for Endpoint settings.



No EPM elevation rules policies are configured.
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.

Answer Area

Software installations will **[answer choice]**.

- be denied.
- require support approval.
- require user confirmation.

[Answer choice] will be reported.

- All diagnostic data and elevations
- No diagnostic data or elevations
- Only diagnostic data

Answer Area

Sync:

- 25
- 50
- 100
- 500
- 1000

Collect diagnostics:

- 25
- 50
- 100
- 500
- 1000

Answer Area

EnterpriseEnrollment-s

- .cloud.microsoft
- .manage.microsoft.com
- .onmicrosoft.com
- .windows.net

EnterpriseRegistration

- .cloud.microsoft
- .manage.microsoft.com
- .onmicrosoft.com
- .windows.net