



MD-102^{Q&As}

Endpoint Administrator

Pass Microsoft MD-102 Exam with 100% Guarantee

Free Download Real Questions & Answers **PDF** and **VCE** file from:

<https://www.geekcert.com/md-102.html>

100% Passing Guarantee
100% Money Back Assurance

Following Questions and Answers are all new published by Microsoft
Official Exam Center

- ⚙️ **Instant Download** After Purchase
- ⚙️ **100% Money Back** Guarantee
- ⚙️ **365 Days** Free Update
- ⚙️ **800,000+** Satisfied Customers





QUESTION 1

HOTSPOT

Your network contains an Active Directory domain. Active Directory is synced with Azure AD.

There are 500 Active Directory domain-joined computers that run Windows 10 and are enrolled in Microsoft Intune.

You plan to implement Microsoft Defender Exploit Guard.

You need to create a custom Microsoft Defender Exploit Guard policy, and then distribute the policy to all 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:

Answer Area

Tool to use to configure the settings:

	▼
Microsoft Purview compliance portal	
Windows Security app	
Microsoft Intune admin center	

Distribution method:

	▼
An Azure policy	
An Endpoint Protection configuration profile	
An Intune device compliance policy	
A device restrictions configuration profile	

Correct Answer:



Answer Area

Tool to use to configure the settings:

	▼
Microsoft Purview compliance portal	
Windows Security app	
Microsoft Intune admin center	

Distribution method:

	▼
An Azure policy	
An Endpoint Protection configuration profile	
An Intune device compliance policy	
A device restrictions configuration profile	

Reference: <https://docs.microsoft.com/en-us/windows/security/threat-protection/microsoft-defender-atp/import-export-exploit-protection-emet-xml#manage-or-deploy-a-configuration> <https://docs.microsoft.com/en-us/intune/endpoint-protection-windows-10> <https://docs.microsoft.com/en-us/windows/security/threat-protection/microsoft-defender-atp/enable-exploit-protection>

QUESTION 2

You have the Microsoft Deployment Toolkit (MDT) installed. You install and customize Windows 11 on a reference computer.

You need to capture an image of the reference computer and ensure that the image can be deployed to multiple computers.

Which command should you run before you capture the image?

- A. dism
- B. wpeinit
- C. sysprep
- D. bcdedit

Correct Answer: C

Sysprep (System Preparation) prepares a Windows client or Windows Server installation for imaging. Sysprep can remove PC-specific information from a Windows installation (generalizing) so it can be installed on different PCs.

Reference: <https://docs.microsoft.com/en-us/windows-hardware/manufacture/desktop/sysprep--system-preparation--overview>

QUESTION 3



HOTSPOT

You have an Azure AD tenant named contoso.com.

You have the devices shown in the following table.

Name	Platform
Device1	Windows 11
Device2	Windows 10
Device3	iOS
Device4	Ubuntu Linux

Which devices can be Azure AD joined, and which devices can be registered in contoso.com? To answer, select the appropriate options in the answer area. NOTE: Each correct selection is worth one point.

Hot Area:

Answer Area

Azure AD joined:

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

Registered in contoso.com:

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

Correct Answer:



Answer Area

Azure AD joined:

▼

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

Registered in contoso.com:

▼

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

Azure AD join capable Devices: <https://learn.microsoft.com/en-us/azure/active-directory/devices/concept-directory-join>

Azure AD registered Devices: <https://learn.microsoft.com/en-us/azure/active-directory/devices/concept-device-registration>

QUESTION 4

You have computers that run Windows 10 and connect to an Azure Log Analytics workspace. The workspace is configured to collect all available events from the Windows event logs.

The computers have the logged events shown in the following table.

Event ID	Log	Type	Computer
1	Application	Success	Computer1
2	System	Information	Computer1
3	Security	Audit Success	Computer2
4	System	Error	Computer2

Which events are collected in the Log Analytics workspace?

- A. 1 only
- B. 2 and 3 only
- C. 1 and 3 only
- D. 1, 2, and 4 only
- E. 1, 2, 3, and 4

Correct Answer: D



Collect Windows event log data sources with Log Analytics agent

Windows event logs are one of the most common data sources for Log Analytics agents on Windows virtual machines because many applications write to the Windows event log. You can collect events from standard logs, such as System and Application, and any custom logs created by applications you need to monitor.

Incorrect:

Not 3: Not Security events.

Reference:

<https://learn.microsoft.com/en-us/azure/azure-monitor/agents/data-sources-windows-events>

QUESTION 5

DRAG DROP

You have a Microsoft 365 subscription that uses Microsoft Defender for Endpoint.

You plan to onboard the following types of devices to Defender for Endpoint:

1.

macOS

2.

Linux Server

What should you use to onboard each device? To answer, drag the appropriate tools to the correct device types. Each tool 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:

Tools

Ansible

Group Policy

Microsoft Intune

Virtual Desktop Infrastructure (VDI) scripts

Answer Area

macOS:

Linux Server:

Correct Answer:



Tools

Group Policy

Virtual Desktop Infrastructure (VDI) scripts

Answer Area

macOS: Microsoft Intune

Linux Server: Ansible

Box 1: Microsoft Intune

For macOS you can use the following methods:

Local script

Microsoft Intune

JAMF Pro

Mobile Device Management

Box 2: Ansible

You can deploy Microsoft Defender for Endpoint on Linux with Ansible.

Reference:

<https://learn.microsoft.com/en-us/microsoft-365/security/defender-endpoint/switch-to-mde-phase-3>

<https://learn.microsoft.com/en-us/microsoft-365/security/defender-endpoint/linux-install-with-ansible>

[MD-102 PDF Dumps](#)

[MD-102 Exam Questions](#)

[MD-102 Braindumps](#)