

# Microsoft

## Exam Questions MD-102

Endpoint Administrator



NEW QUESTION 1

- (Exam Topic 1)

You need to ensure that computer objects can be created as part of the Windows Autopilot deployment. The solution must meet the technical requirements. To what should you grant the right to create the computer objects?

- A. Server2
- B. Server1
- C. GroupA
- D. DC1

Answer: B

Explanation:

Reference:  
<https://blog.matrixpost.net/set-up-windows-autopilot-production-environment-part-2/>

NEW QUESTION 2

- (Exam Topic 1)

You implement the planned changes for Connection1 and Connection2  
How many VPN connections will there be for User1 when the user signs in to Device 1 and Devke2? To answer select the appropriate options in the answer area.  
NOTE; Each correct selection is worth one point.

Answer Area

Device1:

1

2345

Device2:

1

2345

- A. Mastered
- B. Not Mastered

Answer: A

Explanation:

Graphical user interface, table Description automatically generated

NEW QUESTION 3

- (Exam Topic 1)

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
If User1 adds a shortcut to the desktop of Device1, when User1 signs in to Device3, the same shortcut will appear on the desktop.	<input type="radio"/>	<input type="radio"/>
If User1 sets the desktop background to blue on Device2, when User1 signs in to Device4, the desktop background will be blue.	<input type="radio"/>	<input type="radio"/>
If User2 increases the size of the font in the command prompt of Device2, when User2 signs in to Device3, the command prompt will show the increased font size.	<input type="radio"/>	<input type="radio"/>

- A. Mastered
- B. Not Mastered

Answer: A

Explanation:

Text, letter Description automatically generated

NEW QUESTION 4

- (Exam Topic 1)

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

Statements	Yes	No
Device1 is marked as compliant.	<input type="radio"/>	<input type="radio"/>
Device4 is marked as compliant.	<input type="radio"/>	<input type="radio"/>
Device5 is marked as compliant.	<input type="radio"/>	<input type="radio"/>

- A. Mastered
- B. Not Mastered

Answer: A

Explanation:  
Text Description automatically generated

NEW QUESTION 5  
- (Exam Topic 2)  
What should you configure to meet the technical requirements for the Azure AD-joined computers?

- A. Windows Hello for Business from the Microsoft Intune blade in the Azure portal.
- B. The Accounts options in an endpoint protection profile.
- C. The Password Policy settings in a Group Policy object (GPO).
- D. A password policy from the Microsoft Office 365 portal.

Answer: A

Explanation:  
References:  
<https://docs.microsoft.com/en-us/windows/security/identity-protection/hello-for-business/hello-manage-inorgani>

NEW QUESTION 6  
- (Exam Topic 2)  
You need to capture the required information for the sales department computers to meet the technical requirements.  
Which Windows PowerShell command should you run first?

- A. Install-Module WindowsAutoPilotIntune
- B. Install-Script Get-WindowsAutoPilotInfo
- C. Import-AutoPilotCSV
- D. Get-WindowsAutoPilotInfo

Answer: B

Explanation:  
References:  
<https://docs.microsoft.com/en-us/windows/deployment/windows-autopilot/existing-devices>  
"This topic describes how to convert Windows 7 or Windows 8.1 domain-joined computers to Windows 10 devices joined to either Azure Active Directory or Active Directory (Hybrid Azure AD Join) by using Windows Autopilot"

NEW QUESTION 7  
- (Exam Topic 2)  
What should you upgrade before you can configure the environment to support co-management?

- A. the domain functional level
- B. Configuration Manager
- C. the domain controllers
- D. Windows Server Update Services (WSUS)

Answer: B

Explanation:  
References:  
<https://docs.microsoft.com/en-us/sccm/comanage/tutorial-co-manage-clients>

NEW QUESTION 8  
- (Exam Topic 3)  
Your company has an Azure AD tenant named contoso.com that contains several Windows 10 devices.  
When you join new Windows 10 devices to contoso.com, users are prompted to set up a four-digit pin.  
You need to ensure that the users are prompted to set up a six-digit pin when they join the Windows 10 devices to contoso.com.  
Solution: From the Microsoft Entra admin center, you configure automatic mobile device management (MDM) enrollment. From the Microsoft Intune admin center, you create and assign a device restrictions profile.  
Does this meet the goal?

- A. Yes

B. No

Answer: B

NEW QUESTION 9

- (Exam Topic 3)

You have the on-premises servers shown in the following table.

Name	Description
DC1	Domain controller that runs Windows Server 2022
Server1	Standalone server that runs Windows Server 2022
Server2	Member server that runs Windows Server 2022 and has the Remote Access role installed
Server3	Member server that runs Windows Server 2019
Server4	Red Hat Enterprise Linux (RHEL) 8.4 server

You have a Microsoft 365 E5 subscription that contains Android and iOS devices. All the devices are managed by using Microsoft Intune.

You need to implement Microsoft Tunnel for Intune. The solution must minimize the number of open firewall ports.

To which server can you deploy a Tunnel Gateway server, and which inbound ports should be allowed on the server to support Microsoft Tunnel connections? To answer, select the appropriate options in the answer area.

NOTE: Each correct selection is worth one point.

Server: 

Server1

Server2

Server3

Server4

Ports: 

TCP 443 only

UDP 443 only

TCP 1723 only

TCP 443 and UDP 443 only

TCP 443, TCP 1723, and UDP 443

A. Mastered

B. Not Mastered

Answer: A

Explanation:

Box 1: Server4

Microsoft Tunnel is a VPN gateway solution for Microsoft Intune that runs in a container on Linux and allows access to on-premises resources from iOS/iPadOS and Android Enterprise devices using modern authentication and Conditional Access.

Box 2: TCP 443 and UDP 443 only

Some traffic goes to your public facing IP address for the Tunnel. The VPN channel will use TCP, TLS, UDP, and DTLS over port 443.

By default, port 443 is used for both TCP and UDP, but this can be customized via the Intune Saerver Configuration – Server port setting. If changing the default port (443) ensure your inbound firewall rules are adjusted to the custom port.

Incorrect:

TCP 1723 is not used.

Reference: <https://docs.microsoft.com/en-us/mem/intune/protect/microsoft-tunnel-overview>

NEW QUESTION 10

- (Exam Topic 3)

You have an Azure AD tenant named contoso.com that contains the devices shown in the following table.

Name	Operating system
Device1	Windows 10
Device2	Android 8.0
Device3	Android 9
Device4	iOS 11.0
Device5	iOS 11.4.1

AH devices contain an app named App1 and are enrolled in Microsoft Intune.

You need to prevent users from copying data from App1 and pasting the data into other apps.

Which type of policy and how many policies should you create in Intune? To answer, select the appropriate options in the answer area.

NOTE: Each correct selection is worth one point.

Answer Area

Policy type: 

App protection policy

App configuration policy

App protection policy

Conditional access policy

Device compliance policy

Minimum number of policies: 

1

2

3

4

5

- A. Mastered
- B. Not Mastered

Answer: A

Explanation:

of Corre Answer Only: The correct answer is app protection policy because it allows you to customize the settings of apps for iOS/iPadOS or Android devices1. One of the settings you can configure is Restrict cut, copy, and paste between other apps, which lets you prevent users from copying data from App1 and pasting the data into other apps2. You only need one policy to apply this setting to all devices that have App1 installed. References: 1: App configuration policies for Microsoft Intune | Microsoft Learn <https://learn.microsoft.com/en-us/mem/intune/apps/app-configuration-policies-overview> 2: Troubleshoot restricting cut, copy, and paste between applications - Intune | Microsoft Learn <https://learn.microsoft.com/en-us/troubleshoot/mem/intune/app-protection-policies/troubleshoot-cut-copy-paste>

NEW QUESTION 10

- (Exam Topic 3)  
You have an Azure AD tenant named contoso.com that contains the users shown in the following table.

Name	Role
Admin1@contoso.com	Security Administrator
Admin2@contoso.com	Cloud Device Administrator
User1@contoso.com	None

You have a computer named Computer1 that runs Windows 10. Computer1 is in a workgroup and has the local users shown in the following table.

Name	Member of
Administrator1	Network Configuration Operators
Administrator2	Power Users
UserA	Administrators

UserA joins Computer1 to Azure AD by using user1@contoso.com.  
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
User1@contoso.com is a member of the local Administrators group on Computer1.	<input type="radio"/>	<input type="radio"/>
Admin1@contoso.com can configure the firewall and Microsoft Defender on Computer1.	<input type="radio"/>	<input type="radio"/>
Admin2@contoso.com can install software on Computer1.	<input type="radio"/>	<input type="radio"/>

- A. Mastered
- B. Not Mastered

Answer: A

Explanation:

Answer Area

Statements	Yes	No
User1@contoso.com is a member of the local Administrators group on Computer1.	<input type="radio"/>	<input checked="" type="radio"/>
Admin1@contoso.com can configure the firewall and Microsoft Defender on Computer1.	<input type="radio"/>	<input checked="" type="radio"/>
Admin2@contoso.com can install software on Computer1.	<input type="radio"/>	<input checked="" type="radio"/>

NEW QUESTION 12

- (Exam Topic 3)  
You have a Microsoft 365 subscription that contains 100 devices enrolled in Microsoft Intune. You need to review the startup processes and how often each device restarts.



What should you use?

- A. Endpoint analytics
- B. Intune Data Warehouse
- C. Azure Monitor
- D. Device Management

**Answer:** B

#### NEW QUESTION 13

- (Exam Topic 3)

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

Name	Description
Group1	Azure AD group that contains a user named User1
Group2	Azure AD group that contains iOS devices

You create a Conditional Access policy named CAPolicy1 that will block access to Microsoft Exchange Online from iOS devices. You assign CAPolicy1 to Group1. You discover that User1 can still connect to Exchange Online from an iOS device. You need to ensure that CAPolicy1 is enforced. What should you do?

- A. Configure a new terms of use (TOU).
- B. Assign CAPolicy1 to Group2.
- C. Enable CAPolicy1
- D. Add a condition in CAPolicy1 to filter for devices.

**Answer:** B

#### Explanation:

Common signals that Conditional Access can take in to account when making a policy decision include the following signals:

\* User or group membership

Policies can be targeted to specific users and groups giving administrators fine-grained control over access.

\* Device

Users with devices of specific platforms or marked with a specific state can be used when enforcing Conditional Access policies.

Use filters for devices to target policies to specific devices like privileged access workstations.

\* Etc.

Reference: <https://learn.microsoft.com/en-us/azure/active-directory/conditional-access/overview>

#### NEW QUESTION 14

- (Exam Topic 3)

Your company has an Azure AD tenant named contoso.com that contains several Windows 10 devices. When you join new Windows 10 devices to contoso.com, users are prompted to set up a four-digit pin. You need to ensure that the users are prompted to set up a six-digit pin when they join the Windows 10 devices to contoso.com.

Solution: From the Microsoft Entra admin center, you configure automatic mobile device management (MDM) enrollment. From the Microsoft Intune admin center, you configure the Windows Hello for Business enrollment options.

Does this meet the goal?

- A. Yes
- B. No

**Answer:** B

#### NEW QUESTION 17

- (Exam Topic 3)

You have a Microsoft 365 subscription that uses Microsoft Intune Suite. You use Microsoft Intune to manage devices.

You use Windows Autopilot to deploy Windows 11 to devices.

A support engineer reports that when a deployment fails, they cannot collect deployment logs from failed device.

You need to ensure that when a deployment fails, the deployment logs can be collected. What should you configure?

- A. the automatic enrollment settings
- B. the Windows Autopilot deployment profile
- C. the enrollment status page (ESP) profile
- D. the device configuration profile

**Answer:** B

#### NEW QUESTION 18

- (Exam Topic 3)

Your network contains an Active Directory domain. The domain contains a computer named Computer1 that runs Windows 8.1.

Computer1 has apps that are compatible with Windows 10.

You need to perform a Windows 10 in-place upgrade on Computer1.

Solution: You copy the Windows 10 installation media to a network share. You start Computer1 from Windows PE (WinPE), and then you run setup.exe from the network share.

Does this meet the goal?

- A. Yes
- B. No

**Answer:** B

#### NEW QUESTION 22

- (Exam Topic 3)

You have a Microsoft Intune subscription.

You have devices enrolled in Intune as shown in the following table.

Name	Operating system
Device1	Android 8.1.0
Device2	Android 9
Device3	iOS 11.4.1
Device4	iOS 12.3.1
Device5	iOS 12.3.2

An app named App1 is installed on each device.

What is the minimum number of app configuration policies required to manage App1 ?

- A. 1
- B. 2
- C. 3
- D. 4
- E. 5

**Answer:** B

#### Explanation:

The correct answer is B because you need to create two app configuration policies for managed devices, one for iOS/iPadOS devices and one for Android devices<sup>1</sup>. App configuration policies let you customize the settings of apps for iOS/iPadOS or Android devices<sup>1</sup>. The settings are assigned to user groups and applied when the app runs<sup>1</sup>. The app developer or supplier provides the configuration settings (keys and values) that are exposed to Intune<sup>1</sup>. You can't use a single app configuration policy for both iOS/iPadOS and Android devices because they have different configuration settings<sup>2</sup>. References: 1: App configuration policies for Microsoft Intune | Microsoft Learn

<https://learn.microsoft.com/en-us/mem/intune/apps/app-configuration-policies-overview> 2: Add app configuration policies for managed iOS/iPadOS devices | Microsoft Learn <https://learn.microsoft.com/en-us/mem/intune/apps/app-configuration-policies-use-ios>

#### NEW QUESTION 23

- (Exam Topic 3)

You have a Microsoft 365 E5 subscription that contains 150 hybrid Azure AD joined Windows devices. All the devices are enrolled in Microsoft Intune. You need to configure Delivery Optimization on the devices to meet the following requirements:

- Allow downloads from the internet and from other computers on the local network.
- Limit the percentage of used bandwidth to 50. What should you use?

- A. a configuration profile
- B. a Windows Update for Business Group Policy setting
- C. a Microsoft Peer-to-Peer Networking Services Group Policy setting
- D. an Update ring for Windows 10 and later profile

**Answer:** A

#### Explanation:

A configuration profile is the correct answer because it allows you to configure Delivery Optimization settings for Windows devices in Intune. You can specify the download mode, bandwidth limit, caching options, and more. A configuration profile is a template that contains one or more settings that you can apply to groups of devices. References:

- Windows 10 Delivery Optimization settings for Intune - Microsoft Intune | Microsoft Learn
- Delivery Optimization settings in Microsoft Intune

#### NEW QUESTION 24

- (Exam Topic 3)

You have a Microsoft 365 E5 subscription that contains 100 iOS devices enrolled in Microsoft Intune. You need to ensure that notifications of iOS updates are deferred for 30 days after the updates are released. What should you create?

- A. a device configuration profile based on the Device features template
- B. a device configuration profile based on the Device restrictions template
- C. an update policy for iOS/iPadOS
- D. an iOS app provisioning profile

**Answer:** C

#### Explanation:

Manage iOS/iPadOS software update policies in Intune, delay visibility of software updates.

When you use update policies for iOS, you might have need to delay visibility of an iOS software update. Reasons to delay visibility include:

Prevent users from updating the OS manually

To deploy an older update while preventing users from installing a more recent one

To delay visibility, deploy a device restriction template that configures the following settings: Defer software updates = Yes

This doesn't affect any scheduled updates. It represents days before software updates are visible to end users after release.

Delay default visibility of software updates = 1 to 90 90 days is the maximum delay that Apple supports.

Reference: <https://docs.microsoft.com/en-us/mem/intune/protect/software-updates-ios>

#### NEW QUESTION 26

- (Exam Topic 3)  
 You have computer that run Windows 10 and connect to an Azure Log Analytics workspace. The workspace is configured to collect all available events from 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 on
- E. 1, 2, 3, and 4

**Answer:** E

**Explanation:**  
 All events from Windows event logs are collected in the Log Analytics workspace, regardless of the event level or source. Therefore, events 1, 2, 3, and 4 are all collected in the workspace. References: <https://docs.microsoft.com/en-us/azure/azure-monitor/agents/data-sources-windows-events>

**NEW QUESTION 30**

- (Exam Topic 3)  
 You have an Azure Active Directory (Azure AD) tenant that contains the users shown in the following table.

Name	Member of
User1	Group1
User2	Group2

You have devices enrolled in Microsoft Intune as shown in the following table.

Name	Platform	Member of
Device1	Windows 10	Group1
Device2	Android	Group1
Device3	iOS	Group2

From Intune, you create and send a custom notification named Notification1 to Group1.  
 For each of the following statements, select Yes if the statement is true. Otherwise, select No.  
 NOTE: Each correct selection is worth one point.

Statements	Yes	No
User1 receives Notification1 on Device1.	<input type="radio"/>	<input type="radio"/>
User2 receives Notification1 on Device2.	<input type="radio"/>	<input type="radio"/>
User1 receives Notification1 on Device3.	<input type="radio"/>	<input type="radio"/>

- A. Mastered
- B. Not Mastered

**Answer:** A

**Explanation:**  
 A screenshot of a computer Description automatically generated with medium confidence  
 Reference:  
<https://docs.microsoft.com/en-us/mem/intune/remote-actions/custom-notifications>

**NEW QUESTION 32**

- (Exam Topic 3)  
 You have a Microsoft 365 E5 subscription that contains 500 macOS devices enrolled in Microsoft Intune. You need to ensure that you can apply Microsoft Defender for Endpoint antivirus policies to the macOS devices. The solution must minimize administrative effort.  
 What should you do?

- A. Onboard the macOS devices to the Microsoft Purview compliance portal.
- B. From the Microsoft Intune admin center, create a security baseline.
- C. Install Defender for Endpoint on the macOS devices.



D. From the Microsoft Intune admin center, create a configuration profile.

**Answer:** C

**Explanation:**

To apply Microsoft Defender for Endpoint antivirus policies to the macOS devices, you need to install Defender for Endpoint on the devices. You can use Intune to deploy a script that installs Defender for Endpoint on macOS devices. After installation, you can use Intune to create and assign antivirus policies to the devices.

References:

<https://docs.microsoft.com/en-us/windows/security/threat-protection/microsoft-defender-atp/mac-install-with-int>

**NEW QUESTION 35**

- (Exam Topic 3)

You have a Microsoft 365 subscription that uses Microsoft Intune Suite. You use Microsoft Intune to manage devices.

You plan to deploy two apps named App1 and App2 to all Windows devices. App1 must be installed before App2.

From the Intune admin center, you create and deploy two Windows app (Win32) apps. You need to ensure that App1 is installed before App2 on every device.

What should you configure?

A. the App1 deployment configurations

B. a dynamic device group

C. a detection rule

D. the App2 deployment configurations

**Answer:** D

**Explanation:**

The correct answer is D because you can configure the dependencies for a Win32 app in the deployment configurations1. Dependencies are other Win32 apps that must be installed before your Win32 app can be installed1. You can add Win32 app dependencies only after your Win32 app has been added and uploaded to Intune2. In this case, you need to configure the App2 deployment configurations to add App1 as a dependency2. References: 1: Microsoft Intune Win32 App Dependencies - MSEndpointMgr <https://msendpointmgr.com/2019/06/03/new-intune-feature-win32-app-dependencies/> 2: Add and assign Win32 apps to Microsoft Intune | Microsoft Learn

<https://learn.microsoft.com/en-us/mem/intune/apps/apps-win32-add>

**NEW QUESTION 37**

- (Exam Topic 3)

You have 100 computers that run Windows 10. You have no servers. All the computers are joined to Microsoft Azure Active Directory (Azure AD).

The computers have different update settings, and some computers are configured for manual updates. You need to configure Windows Update. The solution must meet the following requirements:

> The configuration must be managed from a central location.

> Internet traffic must be minimized.

> Costs must be minimized.

How should you configure Windows Update? To answer, select the appropriate options in the answer area.

NOTE: Each correct selection is worth one point.

Windows Update technology to use:	<div>Windows Server Update Services (WSUS)</div> <div>Microsoft Endpoint Configuration Manager</div> <div>Windows Update for Business</div>
Manage the configuration by using:	<div>A Group Policy object (GPO)</div> <div>Microsoft Endpoint Configuration Manager</div> <div>Microsoft Intune</div>
Manage the traffic by using:	<div>Delivery Optimization</div> <div>BranchCache</div> <div>Peer cache</div>

A. Mastered

B. Not Mastered

**Answer:** A

**Explanation:**

Box 1: Windows Server Update Services (WSUS)

Windows Server Update Services (WSUS) enables information technology administrators to deploy the latest Microsoft product updates. You can use WSUS to fully manage the distribution of updates that are released through Microsoft Update to computers on your network.

Windows Server Update Services is a built-in server role that includes the following enhancements: Can be added and removed by using the Server Manager

Includes Windows PowerShell cmdlets to manage the most important administrative tasks in WSUS Etc.

Box 2: A Group Policy object

In an Active Directory environment, you can use Group Policy to define how computers and users can interact with Windows Update to obtain automatic updates from Windows Server Update Services (WSUS).

Box 3: BranchCache

BranchCache is a bandwidth-optimization feature that has been available since the Windows Server 2008 R2 and Windows 7 operating systems. Each client has a cache and acts as an alternate source for content that devices on its own network request. Windows Server Update Services (WSUS) and Microsoft Endpoint Manager can use BranchCache to optimize network bandwidth during update deployment, and it's easy to configure for either of them. BranchCache has two operating modes: Distributed Cache mode and Hosted Cache mode.

Reference: <https://docs.microsoft.com/en-us/windows/deployment/update/waas-branchcache> <https://docs.microsoft.com/en-us/windows-server/administration/windows-server-update-services/deploy/4-conf>

NEW QUESTION 41

- (Exam Topic 3)  
You use Windows Admin Center to remotely administer computers that run Windows 10.  
When connecting to Windows Admin Center, you receive the message shown in the following exhibit.



You need to prevent the message from appearing when you connect to Windows Admin Center. To which certificate store should you import the certificate?

- A. Personal
- B. Trusted Root Certification Authorities
- C. Client Authentication Issuers

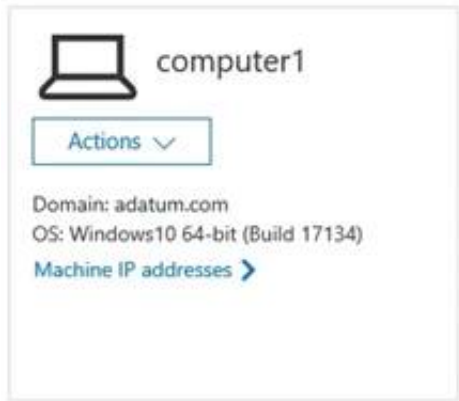
Answer: B

NEW QUESTION 44

- (Exam Topic 3)  
Your company uses Microsoft Defender for Endpoint Microsoft Defender for Endpoint includes the device groups shown in the following table.

Rank	Name	Members
1	Group1	Tag Equals demo And OS In Windows 10
2	Group2	Tag Equals demo
3	Group3	Domain Equals adatum.com
4	Group4	Domain Equals adatum.com And OS In Windows 10
5	Group5	Name starts with COMP
Last	Ungrouped machines (default)	Not applicable

You onboard a computer to Microsoft Defender for Endpoint as shown in the following exhibit.



What is the effect of the Microsoft Defender for Endpoint configuration? To answer, select the appropriate options in the answer area.  
NOTE: Each correct selection is worth one point.

Answer Area

Computer1 will be a member of:

Group3 only

Group4 only

Grou5 only

Group3, Group4, and Group5 only

If you add the tag demo to Computer1, Computer1 will be a member of:

Group1 only

Group2 only

Group1 and Group2 only

Group1, Group2, Group3, Group4, and Group5

- A. Mastered
- B. Not Mastered

Answer: A

Explanation:

Answer Area

Computer1 will be a member of:

Group3 only

Group4 only

Grou5 only

Group3, Group4, and Group5 only

If you add the tag demo to Computer1, Computer1 will be a member of:

Group1 only

Group2 only

Group1 and Group2 only

Group1, Group2, Group3, Group4, and Group5

NEW QUESTION 49

- (Exam Topic 3)

You have a Microsoft Deployment Toolkit (MDT) deployment share named DS1. in the Out-of-Box Drivers node, you create folders that contain drivers for different hardware models. You need to configure the Inject Drivers MDT task to use PnP detection to install the drivers for one of the hardware models. What should you do first?

A. Import an OS package.  
B. Create a selection profile.  
C. Add a Gather task to the task sequence.  
D. Add a Validate task to the task sequence.

Answer: B

NEW QUESTION 53

- (Exam Topic 3)

You have a Microsoft 365 E5 subscription that contains 1,000 Windows 11 devices. All the devices are enrolled in Microsoft Intune. You plan to integrate Intune with Microsoft Defender for Endpoint. You need to establish a service-to-service connection between Intune and Defender for Endpoint. Which settings should you configure in the Microsoft Endpoint Manager admin center?

A. Connectors and tokens  
B. Premium add-ons  
C. Microsoft Tunnel Gateway  
D. Tenant enrollment

Answer: A

**Explanation:**

Microsoft Defender for Endpoint – Important Service and Endpoint Settings You Should Configure Right Now.

As a prerequisite, however, head to tenant administration > connectors and tokens > Microsoft Defender for Endpoint and confirm the connection is enabled. You previously set this up in the advanced settings of Microsoft 365 Defender.

Reference: <https://petri.com/microsoft-defender-for-endpoint-which-settings-configure-right-now/>

NEW QUESTION 57

.....

## Thank You for Trying Our Product

### We offer two products:

1st - We have Practice Tests Software with Actual Exam Questions

2nd - Questions and Answers in PDF Format

### MD-102 Practice Exam Features:

- \* MD-102 Questions and Answers Updated Frequently
- \* MD-102 Practice Questions Verified by Expert Senior Certified Staff
- \* MD-102 Most Realistic Questions that Guarantee you a Pass on Your First Try
- \* MD-102 Practice Test Questions in Multiple Choice Formats and Updates for 1 Year

**100% Actual & Verified — Instant Download, Please Click**  
**[Order The MD-102 Practice Test Here](#)**