

Microsoft

Exam Questions MD-102

Endpoint Administrator



NEW QUESTION 1

- (Exam Topic 4)

You have an Azure subscription.

You have an on-premises Windows 11 device named Device 1. You plan to monitor Device1 by using Azure Monitor.

You create a data collection rule (DCR) named DCR1 in the subscription. To what should you associate DCR1 ?

- A. Azure Network Watcher
- B. Device1
- C. a Log Analytics workspace
- D. a Monitored Object

Answer: B

Explanation:

To monitor Device1 by using Azure Monitor, you should associate DCR1 with Device1. A data collection rule (DCR) defines the data collection process in Azure Monitor, such as what data to collect, how to transform it, and where to send it. A DCR can be associated with multiple virtual machines and specify different data sources, such as Azure Monitor Agent, custom logs, or Azure Event Hubs1. To associate a DCR with a virtual machine, you need to install the Azure Monitor Agent on the machine and then select the DCR from the list of available rules2. You can also use Azure Policy to automatically install the agent and associate a DCR with any virtual machines or virtual machine scale sets as they are created in your subscription3.

The other options are not correct for this scenario because:

> Azure Network Watcher is a service that provides network performance monitoring and diagnostics for Azure resources. It is not related to data collection rules or Azure Monitor4.

> A Log Analytics workspace is a destination where you can send the data collected by a data collection rule. It is not an entity that you can associate a DCR with5.

> A Monitored Object is not a valid term in the context of Azure Monitor or data collection rules. References: Data collection rules in Azure Monitor, Configure data collection for Azure Monitor Agent, U

Azure Policy to install Azure Monitor Agent and associate with a DCR, What is Azure Network Watcher?, Log Analytics workspaces in Azure Monitor

NEW QUESTION 2

- (Exam Topic 4)

You have a Microsoft 365 subscription that includes Microsoft Intune.

You need to implement a Microsoft Defender for Endpoint solution that meets the following requirements:

- Enforces compliance for Defender for Endpoint by using Conditional Access
- Prevents suspicious scripts from running on devices

What should you configure? To answer, drag the appropriate features to the correct requirements. Each feature 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.

Features	Answer Area
A device restriction policy	Enforces compliance: <input type="text"/>
A security baseline	Prevents suspicious scripts: <input type="text"/>
An attack surface reduction (ASR) rule	
An Intune connection	

Solution:

To enforce compliance for Defender for Endpoint by using Conditional Access, you need to configure an Intune connection in the Defender for Endpoint portal. This allows you to use Intune device compliance policies to evaluate the health and compliance status of devices that are enrolled in Defender for Endpoint. You can then use Conditional Access policies to block or allow access to cloud apps based on the device compliance status. References:

<https://docs.microsoft.com/en-us/windows/security/threat-protection/microsoft-defender-atp/conditional-access>

To prevent suspicious scripts from running on devices, you need to configure an attack surface reduction (ASR) rule in Intune. ASR rules are part of the endpoint protection settings that you can apply to devices by using device configuration profiles. You can use the ASR rule "Block Office applications from creating child processes" to prevent Office applications from launching child processes such as scripts or executables. References:

<https://docs.microsoft.com/en-us/mem/intune/protect/endpoint-protection-windows-10#attack-surface-reduction>

Does this meet the goal?

- A. Yes
- B. No

Answer: A

NEW QUESTION 3

- (Exam Topic 4)

You have a Microsoft 365 subscription that uses Microsoft Intune.

You plan to use Windows Autopilot to provision 25 Windows 11 devices. You need to meet the following requirements during device provisioning:

- Display the progress of app and profile deployments.
- Join the devices to Azure AD.

What should you configure to meet each requirement? To answer drag the appropriate settings to the correct requirements. Each setting 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.

Settings

- CNAME Validation
- Co-management Settings
- Deployment Profiles
- Enrollment notifications
- Enrollment Status Page

Answer Area

Display the progress of app and profile deployments:

Join the devices to Azure AD:

Solution:

Settings

- CNAME Validation
- Co-management Settings
- Deployment Profiles
- Enrollment notifications
- Enrollment Status Page

Answer Area

Display the progress of app and profile deployments:

Join the devices to Azure AD:

Does this meet the goal?

- A. Yes
- B. No

Answer: A

NEW QUESTION 4

- (Exam Topic 4)

You have a Microsoft 365 subscription. All devices run Windows 10.

You need to prevent users from enrolling the devices in the Windows Insider Program.

What two configurations should you perform from the Microsoft Intune admin center? Each correct answer is a complete solution.

NOTE: Each correct selection is worth one point.

- A. a device restrictions device configuration profile
- B. an app configuration policy
- C. a Windows 10 and later security baseline
- D. a custom device configuration profile
- E. a Windows 10 and later update ring

Answer: AE

NEW QUESTION 5

- (Exam Topic 4)

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.


computer1

Actions ▾

Domain: adatum.com
 OS: Windows10 64-bit (Build 17134)

[Machine IP addresses >](#)

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

Solution:

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

Does this meet the goal?

- A. Yes
- B. No

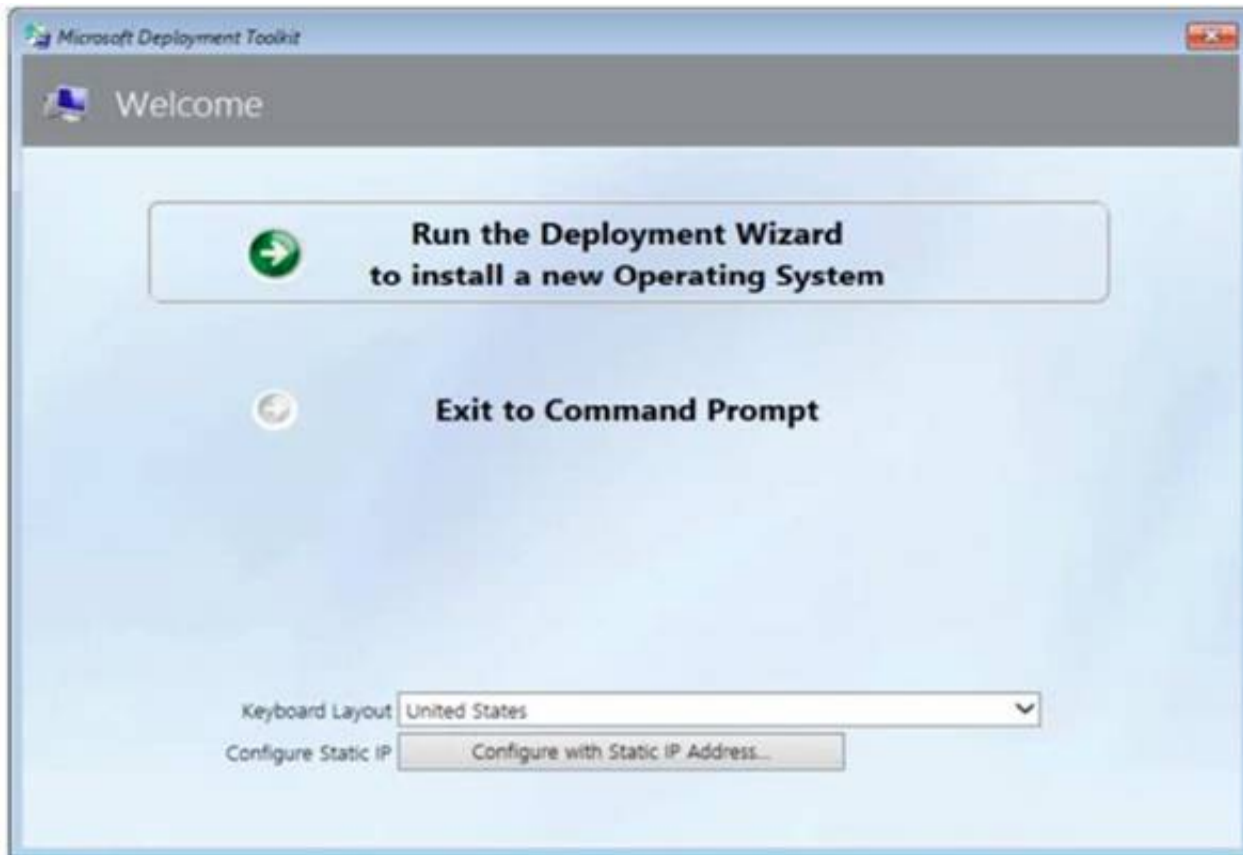
Answer: A

NEW QUESTION 6

- (Exam Topic 4)

You have a Microsoft Deployment Toolkit (MDT) server named MDT1.

When computers start from the LiteTouchPE_x64.iso image and connect to MDT1. the welcome screen appears as shown In the following exhibit.



You need to prevent the welcome screen from appearing when the computers connect to MDT1.

Which three 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
Modify the CustomSettings.ini file.	
Update the deployment share.	
Modify the Bootstrap.ini file.	➤
Replace the ISO image.	⬅
Modify the task sequence.	

Solution:

Box 1: Modify the Bootstrap.ini file.

Add this to your bootstrap.ini file and then update the deployment share and use the new boot media created in that process:

SkipBDDWelcome=YES

Box 2: Modify the CustomSettings.ini file. SkipBDDWelcome

Indicates whether the Welcome to Windows Deployment wizard page is skipped.

For this property to function properly it must be configured in both CustomSettings.ini and BootStrap.ini. BootStrap.ini is processed before a deployment share (which contains CustomSettings.ini) has been selected.

Box 3: Update the deployment share. Reference:

<https://docs.microsoft.com/en-us/mem/configmgr/mdt/toolkit-reference#table-6-deployment-wizard-pages>

Does this meet the goal?

- A. Yes
- B. No

Answer: A

NEW QUESTION 7

- (Exam Topic 4)

You have a Microsoft 365 subscription that contains 1,000 Windows 11 devices enrolled in Microsoft Intune. You plan to create and monitor the results of a compliance policy used to validate the BIOS version of the 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
Review the compliance dashboard for results.	1
Create and assign a compliance policy that has System Security settings configured.	2
Review the Conditional Access Insights and Reporting workbook for results.	3
Create a PowerShell discovery script and a JSON file.	4
Upload the PowerShell script to Intune.	
Upload the JSON file to Azure AD.	
Create and assign a custom compliance policy.	

Solution:

Actions	Answer Area
Review the compliance dashboard for results.	Create a PowerShell discovery script and a JSON file.
Create and assign a compliance policy that has System Security settings configured.	Upload the PowerShell script to Intune.
Review the Conditional Access Insights and Reporting workbook for results.	Upload the JSON file to Azure AD.
Create a PowerShell discovery script and a JSON file.	Create and assign a custom compliance policy.
Upload the PowerShell script to Intune.	
Upload the JSON file to Azure AD.	
Create and assign a custom compliance policy.	

Does this meet the goal?

- A. Yes
- B. No

Answer: A

NEW QUESTION 8

- (Exam Topic 4)

Your network contains an on-premises Active Directory Domain Services (AD DS) domain that syncs with an Azure AD tenant.

You have a Microsoft 365 subscription

You plan to use Windows Autopilot to deploy new Windows devices. You plan to create a deployment profile.

You need to ensure that The deployment meets the following requirements:

- Devices must be joined to AD DS regardless of their current working location.
- Users in the marketing department must have a line-of-business (LOB) app installed during the deployment. The solution must minimize administrative effort.

What should you do for each requirement? To answer, select the appropriate options in the answer area. NOTE: Each correct selection is worth one point.

Answer Area

Devices must be joined to AD DS regardless of their current working location:

- Install the Intune connector for Active Directory.
- Deploy Always On VPN.
- Install the Intune connector for Active Directory.**
- Modify the Autopilot deployment profile.
- Edit the Co-management settings in Intune.

The marketing department users must have an LOB app installed during the deployment:

- Modify the Autopilot deployment profile.
- Modify the Autopilot deployment profile.**
- Create a Microsoft Intune app deployment.
- Create a device configuration profile in Intune.

Solution:

Answer Area

Devices must be joined to AD DS regardless of their current working location:

- Install the Intune connector for Active Directory.
- Deploy Always On VPN.
- Install the Intune connector for Active Directory.**
- Modify the Autopilot deployment profile.
- Edit the Co-management settings in Intune.

The marketing department users must have an LOB app installed during the deployment:

- Modify the Autopilot deployment profile.
- Modify the Autopilot deployment profile.**
- Create a Microsoft Intune app deployment.
- Create a device configuration profile in Intune.

Does this meet the goal?

- A. Yes
- B. No

Answer: A

NEW QUESTION 9

- (Exam Topic 4)

Your network contains an on-premises Active Directory domain. The domain contains two computers named Computer1 and Computer2 that run Windows 10.

You install Windows Admin Center on Computer1.

You need to manage Computer2 from Computer1 by using Windows Admin Center. What should you do on Computer2?

- A. Update the TrustedHosts list
- B. Run the Enable-PSRemoting cmdlet
- C. Allow Windows Remote Management (WinRM) through the Microsoft Defender firewall.
- D. Add an inbound Microsoft Defender Firewall rule.

Answer: B

Explanation:

To manage a remote computer from Windows Admin Center, you need to enable PowerShell remoting on the remote computer. You can do this by running the Enable-PSRemoting cmdlet, which configures the WinRM service, creates a listener, and allows inbound firewall rules for PowerShell remoting. The other options are not sufficient or necessary for this task. References: Installation and configuration for Windows Remote Management

NEW QUESTION 10

- (Exam Topic 4)

You have a Microsoft 365 subscription that uses Microsoft Intune.

You need to ensure that you can deploy apps to Android Enterprise devices. What should you do first?

- A. Create a configuration profile.
- B. Add a certificate connector.
- C. Configure the Partner device management settings.
- D. Link your managed Google Play account to Intune.

Answer: D

NEW QUESTION 11

- (Exam Topic 4)

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

Name	Type
Device1	Windows 10
Device2	iOS
Device3	Android Enterprise

You need to ensure that only devices running trusted firmware or operating system builds can access network resources.

Which compliance policy setting should you configure for each device? To answer, drag the appropriate settings to the correct devices. Each setting 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.

Settings

- Require BitLocker.
- Prevent jailbroken devices from having corporate access.
- Prevent rooted devices from having corporate access.
- Require Secure Boot to be enabled on the device.

Answer Area

Device1:

Device2:

Device3:

Solution:

Box 1:

Device Compliance settings for Windows 10/11 in Intune

There are the different compliance settings you can configure on Windows devices in Intune. As part of your mobile device management (MDM) solution, use these settings to require BitLocker, set a minimum and maximum operating system, set a risk level using Microsoft Defender for Endpoint, and more.

Note: Windows Health Attestation Service evaluation rules Require BitLocker:

Windows BitLocker Drive Encryption encrypts all data stored on the Windows operating system volume. BitLocker uses the Trusted Platform Module (TPM) to help protect the Windows operating system and user

data. It also helps confirm that a computer isn't tampered with, even if its left unattended, lost, or stolen. If the computer is equipped with a compatible TPM, BitLocker uses the TPM to lock the encryption keys that protect the data. As a result, the keys can't be accessed until the TPM verifies the state of the computer.

Not configured (default) - This setting isn't evaluated for compliance or non-compliance.

Require - The device can protect data that's stored on the drive from unauthorized access when the system is off, or hibernates.

Box 2: Prevent jailbroken devices from having corporate access Device Compliance settings for iOS/iPadOS in Intune

There are different compliance settings you can configure on iOS/iPadOS devices in Intune. As part of your mobile device management (MDM) solution, use these settings to require an email, mark rooted (jailbroken) devices as not compliant, set an allowed threat level, set passwords to expire, and more.

Device Health Jailbroken devices

Supported for iOS 8.0 and later

Not configured (default) - This setting isn't evaluated for compliance or non-compliance. Block - Mark rooted (jailbroken) devices as not compliant.

Box 3: Prevent rooted devices from having corporate access. Device compliance settings for Android Enterprise in Intune

There are different compliance settings you can configure on Android Enterprise devices in Intune. As part of your mobile device management (MDM) solution, use these settings to mark rooted devices as not compliant, set an allowed threat level, enable Google Play Protect, and more.

Device Health - for Personally-Owned Work Profile Rooted devices

Not configured (default) - This setting isn't evaluated for compliance or non-compliance. Block - Mark rooted devices as not compliant.

Reference: <https://docs.microsoft.com/en-us/mem/intune/protect/compliance-policy-create-windows> <https://docs.microsoft.com/en-us/mem/intune/protect/compliance-policy-create-android-for-work> <https://docs.microsoft.com/en-us/mem/intune/protect/compliance-policy-create-ios>

Does this meet the goal?

- A. Yes
- B. No

Answer: A

NEW QUESTION 12

- (Exam Topic 4)

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

Name	Type
Device1	Windows 10
Device2	iOS
Device3	Android Enterprise

You need to ensure that only devices running trusted firmware or operating system build can access network resources.

Which compliance policy setting should you configure for each device? To answer, drag the appropriate settings to the correct devices. Each setting 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.

Settings

- Require BitLocker.
- Prevent jailbroken devices from having corporate access.
- Prevent rooted devices from having corporate access.
- Require Secure Boot to be enabled on the device.

Answer Area

Device1:

Device2:

Device3:

Solution:

Settings

- Require BitLocker.
- Prevent jailbroken devices from having corporate access.
- Prevent rooted devices from having corporate access.
- Require Secure Boot to be enabled on the device.

Answer Area

Device1:

Device2:

Device3:

Does this meet the goal?

- A. Yes
- B. No

Answer: A

NEW QUESTION 13

- (Exam Topic 3)

You need to prepare for the deployment of the Phoenix office computers. What should you do first?

- A. Generalize the computers and configure the Mobility (MDM and MAM) settings from the Azure Active Directory admin center.
- B. Extract the hardware ID information of each computer to a CSV file and upload the file from the Microsoft Intune blade in the Azure portal.
- C. Extract the hardware ID information of each computer to an XML file and upload the file from the Devices settings in Microsoft Store for Business.
- D. Extract the serial number information of each computer to a CSV file and upload the file from the Microsoft Intune blade in the Azure portal.

Answer: A

Explanation:

Reference:

<https://docs.microsoft.com/en-us/windows/deployment/windows-autopilot/existing-devices>

NEW QUESTION 14

- (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 15

- (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"/>

Solution:

Text Description automatically generated

Does this meet the goal?

- A. Yes
- B. No

Answer: A

NEW QUESTION 16

- (Exam Topic 4)

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 17

- (Exam Topic 4)

You have a Microsoft 365 tenant that uses Microsoft Intune.

You use the Company Portal app to access and install published apps to enrolled devices. From the Microsoft Intune admin center, you add a Microsoft Store app. Which two App information types are visible in the Company Portal? NOTE: Each correct selection is worth one point.

- A. Privacy URL
- B. Information URL
- C. Developer
- D. Owner

Answer: AC

NEW QUESTION 18

- (Exam Topic 4)

You have groups that use the Dynamic Device membership type as shown in the following table.

Name	Syntax
Group1	(device.deviceOwnership -eq "Company")
Group2	(device.deviceOwnership -eq "Personal")

You are deploying Microsoft 365 apps.

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

Name	Ownership	Platform
LT1	Company	Windows 10 Enterprise x64
LT2	Personal	Windows 10 Enterprise x64
LT3	Company	MacOS Big Sur

In the Microsoft Endpoint Manager admin center, you create a Microsoft 365 Apps app as shown in the exhibit. (Click the Exhibit tab.)

App Information [Edit](#)

Name	Microsoft 365 Apps for Windows 10
Description	Microsoft 365 Apps for Windows 10
Publisher	Microsoft
Category	Productivity
Show this as a featured app in the Company Portal	No
Information URL	https://products.office.com/en-us/explore-office-for-home
Privacy URL	https://privacy.microsoft.com/en-US/privacystatement
Developer	Microsoft
Owner	Microsoft
Notes	---
Logo	
Architecture	Teams, Word
Update channel	64-bit
Remove other versions	Current Channel
Version to install	Yes
Use shared computer activation	Latest
Accept the Microsoft Software License	No
Teams on behalf of users	No
Install background service for Microsoft Search in Bing	No
Apps to be installed as part of the suite	1 language(s) selected

Assignments [Edit](#)

Group mode	Group
<input type="checkbox"/> Required	
<input checked="" type="checkbox"/> Included	Group1
Available for enrolled devices	

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
LT1 will have Microsoft Office 365 installed	<input type="radio"/>	<input type="radio"/>
LT2 will have Microsoft Office 365 installed	<input type="radio"/>	<input type="radio"/>
LT3 will have Microsoft Office 365 installed	<input type="radio"/>	<input type="radio"/>

Solution:

Graphical user interface, text, application Description automatically generated

Reference:

<https://docs.microsoft.com/en-us/mem/intune/apps/apps-add-office365>

<https://docs.microsoft.com/en-us/mem/intune/apps/apps-deploy> <https://docs.microsoft.com/en-us/mem/intune/apps/apps-add>

Does this meet the goal?

- A. Yes
- B. No

Answer: A

NEW QUESTION 19

- (Exam Topic 4)

You have a Microsoft 365 subscription. The subscription contains computers that run Windows 11 and are enrolled in Microsoft Intune. You need to create a

compliance policy that meets the following requirements:

- Requires BitLocker Drive Encryption (BitLocker) on each device
- Requires a minimum operating system version

Which setting of the compliance policy should you configure for each requirement? To answer, drag the appropriate settings to the correct requirements. Each setting 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.

Settings

Device Health

Device Properties

Microsoft Defender for Endpoint

System Security

Answer Area

Requires BitLocker:

Requires a minimum operating system version:

Solution:

Settings

Device Health

Device Properties

Microsoft Defender for Endpoint

System Security

Answer Area

Requires BitLocker:

Requires a minimum operating system version:

Does this meet the goal?

- A. Yes
- B. No

Answer: A

NEW QUESTION 20

- (Exam Topic 4)

You have an Azure Active Directory Premium Plan 2 subscription that contains the users shown in the following table.

Name	Member of	Assigned license
User1	Group1	Enterprise Mobility + Security E5
User2	Group2	Enterprise Mobility + Security E5

You purchase the devices shown in the following table.

Name	Type
Device1	Windows 10
Device2	Android

You configure automatic mobile device management (MDM) and mobile application management (MAM) enrollment by using the following settings:

- > MDM user scope: Group1
- > MAM user scope: 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
If User1 registers Device1 in contoso.com, Device1 is enrolled automatically in Microsoft Intune.	<input type="radio"/>	<input type="radio"/>
If User1 joins Device1 to contoso.com, Device2 is enrolled automatically in Microsoft Intune.	<input type="radio"/>	<input type="radio"/>
If User2 registers Device3 in contoso.com, Device3 is enrolled automatically in Microsoft Intune.	<input type="radio"/>	<input type="radio"/>

Solution:

Reference: <https://docs.microsoft.com/en-us/mem/intune/enrollment/android-enroll> <https://powerautomate.microsoft.com/fr-fr/blog/mam-flow-mobile/>

Does this meet the goal?

- A. Yes

B. No

Answer: A

NEW QUESTION 21

- (Exam Topic 4)

You use the Microsoft Deployment Toolkit (MDT) to manage Windows 11 deployments. From Deployment Workbench, you modify the WinPE settings and add PowerShell support. You need to generate a new set of WinPE boot image files that contain the updated settings. What should you do?

- A. From the Deployment Shares node, update the deployment share.
- B. From the Advanced Configuration node, create new media.
- C. From the Packages node, import a new operating system package
- D. From the Operating Systems node, import a new operating system.

Answer: A

NEW QUESTION 22

- (Exam Topic 4)

You use Microsoft Defender for Endpoint to protect computers that run Windows 10.

You need to assess the differences between the configuration of Microsoft Defender for Endpoint and the Microsoft-recommended configuration baseline. Which tool should you use?

- A. Microsoft Defender for Endpoint Power 81 app
- B. Microsoft Secure Score
- C. Endpoint Analytics
- D. Microsoft 365 Defender portal

Answer: B

NEW QUESTION 23

- (Exam Topic 4)

You install a feature update on a computer that runs Windows 10. How many days do you have to roll back the update?

- A. 5
- B. 10
- C. 14
- D. 30

Answer: B

NEW QUESTION 24

- (Exam Topic 4)

You have SOO Windows 10 devices enrolled in Microsoft Intune.

You plan to use Exploit protection in Microsoft Intune to enable the following system settings on the devices:

- Data Execution Prevention (DEP)
- Force randomization for images (Mandatory ASLR)

You need to configure a Windows 10 device that will be used to create a template file.

Which protection areas on the device should you configure in the Windows Security app before you create the template file? To answer, drag the appropriate protection areas to the correct settings. Each protection area 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.

Protection areas	Answer Area
Account protection	DEP: <input type="text"/>
App & browser control	Mandatory ASLR: <input type="text"/>
Device security	
Virus & threat protection	

Solution:

Exploit protection is a feature that helps protect against malware that uses exploits to infect devices and spread. Exploit protection consists of many mitigations that can be applied to either the operating system or individual apps1.

To configure a Windows 10 device that will be used to create a template file for Exploit protection, you need to configure the following protection areas on the device in the Windows Security app:

- DEP: Device security. Data Execution Prevention (DEP) is a mitigation that prevents code from running in memory regions marked as non-executable. You can enable DEP system-wide or for specific apps in the Device security section of the Windows Security app1.
- Mandatory ASLR: App & browser control. Force randomization for images (Mandatory ASLR) is a mitigation that randomizes the location of executable images in memory, making it harder for attackers to predict where to inject code. You can enable Mandatory ASLR system-wide or for specific apps in the App & browser control section of the Windows Security app1.

Does this meet the goal?

- A. Yes
- B. No

Answer: A

NEW QUESTION 25

.....

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](#)