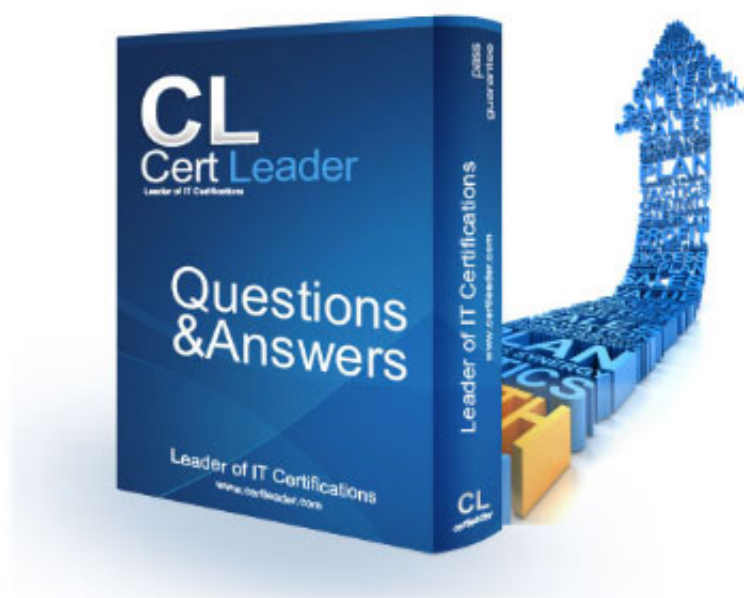


# MD-102 Dumps

## Endpoint Administrator

<https://www.certleader.com/MD-102-dumps.html>



**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 uses Microsoft Intune Suite. You use Microsoft Intune to manage Windows 11 devices.

You need to implement passwordless authentication that requires users to use number matching Which authentication method should you use?

- A. Microsoft Authenticator
- B. voice calls
- C. FIDO2 security keys
- D. text messages

**Answer:** A

**NEW QUESTION 3**

- (Exam Topic 4)

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 4**

- (Exam Topic 4)

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:

Windows Server Update Services (WSUS)
Microsoft Endpoint Configuration Manager
Windows Update for Business

Manage the configuration by using:

A Group Policy object (GPO)
Microsoft Endpoint Configuration Manager
Microsoft Intune

Manage the traffic by using:

Delivery Optimization
BranchCache
Peer cache

- 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 5**

- (Exam Topic 4)

Your network contains an Active Directory domain named contoso.com. The domain contains two computers named Computer1 and Computer2 that run Windows 10. On Computer1, you need to run the

Invoke-Command cmdlet to execute several PowerShell commands on Computer2. What should you do first?

- A. On Computer2, run the Enable-PSRemoting cmdlet.
- B. On Computer2, add Computer1 to the Remote Management Users group.
- C. From Active Directory, configure the Trusted for Delegation setting for the computer account of Computer2.
- D. On Computer1, run the HcK-PSSession cmdlet.

**Answer:** C

**NEW QUESTION 6**

- (Exam Topic 4)

You have an Azure AD tenant named contoso.com.

You need to ensure that users are not added automatically to the local Administrators group when they join their Windows 11 device to contoso.com.

What should you configure?

- A. Windows Autopilot
- B. provisioning packages for Windows
- C. Security defaults in Azure AD
- D. Device settings in Azure AD

**Answer:** D

**Explanation:**

To ensure that users are not added automatically to the local Administrators group when they join their Windows 11 device to contoso.com, you should configure the Device settings in Azure AD. The Device settings allow you to manage which users can join devices to Azure AD and whether they are added as local administrators or standard users. By default, users who join devices to Azure AD are added to the local Administrators group, but you can change this setting to None or Selected.

The other options are not relevant for this scenario because:

- Windows Autopilot is a service that allows you to pre-configure new devices and enroll them automatically to Azure AD and Microsoft Intune. It does not control the local administrator role of the users who join the devices.
- Provisioning packages for Windows are files that contain custom settings and policies that can be applied to Windows devices during the setup process. They do not affect the Azure AD join process or the local administrator role of the users.
- Security defaults in Azure AD are a set of basic identity security mechanisms that are enabled by default to protect your organization from common attacks. They do not include any settings related to device management or local administrator role.

References: Manage device identities using the Microsoft Entra admin center, Windows Autopilot, Provisioning packages for Windows 10, What are security

defaults?

### NEW QUESTION 7

- (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	

- A. Mastered
- B. Not Mastered

**Answer: A**

#### Explanation:

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>

### NEW QUESTION 8

- (Exam Topic 4)

You have a Microsoft Azure subscription that contains an Azure Log Analytics workspace.

You deploy a new computer named Computer1 that runs Windows 10. Computer1 is in a workgroup. You need to ensure that you can use Log Analytics to query events from Computer1.

What should you do on Computer1?

- A. Join Azure AD.
- B. Configure Windows Defender Firewall
- C. Create an event subscription.
- D. Install the Azure Monitor Agent.

**Answer: D**

### NEW QUESTION 9

- (Exam Topic 4)

You need to implement mobile device management (MDM) for personal devices that run Windows 11. The solution must meet the following requirements:

- Ensure that you can manage the personal devices by using Microsoft Intune.
  - Ensure that users can access company data seamlessly from their personal devices.
  - Ensure that users can only sign in to their personal devices by using their personal account
- What should you use to add the devices to Azure AD?

- A. Azure AD registered
- B. hybrid Azure AD join
- C. AD joined

**Answer: A**

#### Explanation:

To implement MDM for personal devices that run Windows 11, you should use Azure AD registered. Azure AD registered devices are devices that are connected to your organization’s resources using a personal device and a personal account. You can manage these devices by using Microsoft Intune and enable seamless access to company data. Users can only sign in to their personal devices by using their personal account, not their organizational account. Azure AD registered devices support Windows 10 or newer, iOS, Android, macOS, and Ubuntu 20.04/22.04 LTS1.

The other options are not suitable for this scenario because:

➤ Hybrid Azure AD join is for corporate-owned and managed devices that are joined to both on-premises Active Directory and Azure AD. Users can sign in to these devices by using their organizational account that exists in both directories2.

➤ AD joined is for devices that are joined only to on-premises Active Directory. These devices are not managed by Microsoft Intune and do not have access to cloud resources3.

References: What are Azure AD registered devices?, What are hybrid Azure AD joined devices?, What is Active Directory domain join?



## NEW QUESTION 10

- (Exam Topic 4)

You create a Windows Autopilot deployment profile.

You need to configure the profile settings to meet the following requirements:

- Include the hardware serial number in the computer name.

Which two settings should you configure? To answer, select the appropriate settings in the answer area.

NOTE: Each correct selection is worth one point.

### Answer Area

## Create profile ...

Windows PC

✓ Basics **2 Out-of-box experience (OOBE)** 3 Assignments 4 Review + create

### Configure the out-of-box experience for your Autopilot devices

Deployment mode *	ⓘ	User-Driven	▼
Join to Azure AD as *	ⓘ	Azure AD joined	▼
Microsoft Software License Terms ⓘ	Show	Hide	
<p>ⓘ important information about hiding license terms</p>			
Privacy settings ⓘ	Show	Hide	
<p>ⓘ The default value for diagnostic data collection has changed for devices running Windows 10, version 1903 and later. <a href="#">Learn more</a></p>			
Hide change account options ⓘ	Show	Hide	
User account type ⓘ	Administrator	Standard	
Allow White Glove OOBE ⓘ	No	Yes	
Language (Region) ⓘ	Operating system default		▼
Automatically configure keyboard ⓘ	No	Yes	
Apply device name template ⓘ	No	Yes	

- A. Mastered
- B. Not Mastered

**Answer:** A

#### Explanation:

Reference:

<https://docs.microsoft.com/en-us/mem/autopilot/profiles>

## NEW QUESTION 10

- (Exam Topic 4)

You have a Microsoft Intune subscription that is configured to use a PFX certificate connector to an on-premises Enterprise certification authority (CA).

You need to use Intune to configure autoenrollment for Android devices by using public key pair (PKCS) certificates.

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

Obtain the root certificate.

From the Microsoft Endpoint Manager admin center, create a trusted certificate configuration profile.

From the Enterprise CA, configure certificate managers.

From the Microsoft Endpoint Manager admin center, configure enrollment restrictions.

From the Microsoft Endpoint Manager admin center, create a PKCS certificate configuration profile.

Answer Area

⏪

⏩

⏴

⏵

- A. Mastered
- B. Not Mastered

Answer: A

Explanation:

Graphical user interface, text, application, email Description automatically generated

Reference:

<https://docs.microsoft.com/en-us/mem/intune/protect/certificates-pfx-configure>

NEW QUESTION 11

- (Exam Topic 4)

You have a Windows 10 device named Device1 that is joined to Active Directory and enrolled in Microsoft Intune.

Device1 is managed by using Group Policy and Intune.

You need to ensure that the Intune settings override the Group Policy settings. What should you configure?

- A. a device configuration profile
- B. a device compliance policy
- C. an MDM Security Baseline profile
- D. a Group Policy Object (GPO)

Answer: A

Explanation:

A device configuration profile is a collection of settings that can be applied to devices enrolled in Microsoft Intune. You can use device configuration profiles to manage Windows 10 devices that are joined to Active Directory and enrolled in Intune. To ensure that the Intune settings override the Group Policy settings, you need to enable the policy CSP setting called MDMWinsOverGP in the device configuration profile. This setting will give precedence to the MDM policy over any conflicting Group Policy settings. References: [Us policy CSP settings to create custom device configuration profiles]

NEW QUESTION 12

- (Exam Topic 4)

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

You use Microsoft Intune and Configuration Manager to manage devices.

You need to recommend a deployment plan for new Windows 11 devices. The solution must meet the following requirements:

- Devices for the marketing department must be joined to the AD DS domain only. The IT department will install complex applications on the devices at build time, before giving the devices to the marketing department users.
- Devices for The sales department must be Azure AD joined. The devices will be shipped directly from the manufacturer to The homes of the sales department users.
- Administrative effort must be minimized.

Which deployment method should you recommend for each department? To answer, select the appropriate options in the answer area. NOTE: Each correct selection is worth one point.

Answer Area

Sales:

Windows Autopilot with automatic registration

Configuration Manager

Windows Autopilot with automatic registration

Windows Autopilot with manual registration

Windows Autopilot with OEM registration

Marketing:

Configuration Manager

Configuration Manager

Windows Autopilot with automatic registration

Windows Autopilot with manual registration

Windows Autopilot with OEM registration

- A. Mastered
- B. Not Mastered

**Answer:** A

**Explanation:**

**Answer Area**



**NEW QUESTION 13**

- (Exam Topic 4)

You have a Microsoft 365 E5 subscription that uses Microsoft Intune. You have the Windows 11 devices shown in the following table.

Name	Member of	BitLocker Drive Encryption (BitLocker)
Device1	Group1	Enabled
Device2	Group1, Group3	Disabled
Device3	Group1, Group2	Enabled

You deploy the device compliance policy shown in the exhibit. (Click the Exhibit tab.)

Basics [Edit](#)

Name	Policy1
Description	--
Platform	Windows 10 and later
Profile type	Windows 10/11 compliance policy

Compliance settings [Edit](#)

Device Health

Require BitLocker	Require
-------------------	---------

Actions for noncompliance [Edit](#)

Action	Schedule	Message template	Additional recipients (via email)
Mark device noncompliant	Immediately		

Scope tags [Edit](#)

Default

Assignments [Edit](#)

Included groups

Group
Group1
Group3

Excluded groups

Group
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
Device1 will have Policy1 assigned and will be marked as compliant.	<input type="radio"/>	<input type="radio"/>
Device2 will have Policy1 assigned and will be marked as compliant.	<input type="radio"/>	<input type="radio"/>
Device3 will have Policy1 assigned and will be marked as compliant.	<input type="radio"/>	<input type="radio"/>

- A. Mastered
- B. Not Mastered

Answer: A

Explanation:



Answer Area

Statements

Device1 will have Policy1 assigned and will be marked as compliant.

Yes

☒

No

☐

Device2 will have Policy1 assigned and will be marked as compliant.

☐
☒

Device3 will have Policy1 assigned and will be marked as compliant.

☐
☒

**NEW QUESTION 18**

- (Exam Topic 4)

You have the devices shown in the following table.

Name	Operating system	Description
Device1	32-bit version of Windows 10	Retired device
Device2	64-bit version of Windows 11	New device
Server1	Windows Server 2019	File server

You need to migrate app data from Device1 to Device2. The data must be encrypted and stored on Seryer1 during the migration.

Which command should you run on each device? To answer, select the appropriate options in the answer area. NOTE: Each correct selection is worth one point.

Answer Area

Device1:

- LoadState.exe \\server1\share1 /i:MigApp.xml /v:13 /decrypt /key:"mysecretKey"
- LoadState.exe \\server1\share1 /i:MigApp.xml /v:8 /decrypt
- LoadState.exe \\server1\share1 /i:MigDocs.xml /v:13 /decrypt/key:"mysecretKey"
- ScanState.exe \\server1\share1 /i:MigApp.xml /config:Config.xml /v:13 /encrypt /key:"mysecretKey"
- ScanState.exe \\server1\share1 /i:MigApp.xml /config:Config.xml /v:8 /encrypt
- ScanState.exe \\server1\share1 /i:MigDocs.xml /v:13 /encrypt /key:"mysecretkey"

Device2:

- LoadState.exe \\server1\share1 /i:MigApp.xml /v:13 /decrypt /key:"mysecretKey"
- LoadState.exe \\server1\share1 /i:MigApp.xml /v:8 /decrypt
- LoadState.exe \\server1\share1 /i:MigDocs.xml /v:13 /decrypt/key:"mysecretKey"
- ScanState.exe \\server1\share1 /i:MigApp.xml /config:Config.xml /v:13 /encrypt /key:"mysecretKey"
- ScanState.exe \\server1\share1 /i:MigApp.xml /config:Config.xml /v:8 /encrypt
- ScanState.exe \\server1\share1 /i:MigDocs.xml /v:13 /encrypt /key:"mysecretkey"

- A. Mastered
- B. Not Mastered

Answer: A

Explanation:

Answer Area

Device1:

- LoadState.exe \\server1\share1 /i:MigApp.xml /v:13 /decrypt /key:"mysecretKey"
- LoadState.exe \\server1\share1 /i:MigApp.xml /v:8 /decrypt
- LoadState.exe \\server1\share1 /i:MigDocs.xml /v:13 /decrypt/key:"mysecretKey"
- ScanState.exe \\server1\share1 /i:MigApp.xml /config:Config.xml /v:13 /encrypt /key:"mysecretKey"
- ScanState.exe \\server1\share1 /i:MigApp.xml /config:Config.xml /v:8 /encrypt
- ScanState.exe \\server1\share1 /i:MigDocs.xml /v:13 /encrypt /key:"mysecretkey"

Device2:

- LoadState.exe \\server1\share1 /i:MigApp.xml /v:13 /decrypt /key:"mysecretKey"
- LoadState.exe \\server1\share1 /i:MigApp.xml /v:8 /decrypt
- LoadState.exe \\server1\share1 /i:MigDocs.xml /v:13 /decrypt/key:"mysecretKey"
- ScanState.exe \\server1\share1 /i:MigApp.xml /config:Config.xml /v:13 /encrypt /key:"mysecretKey"
- ScanState.exe \\server1\share1 /i:MigApp.xml /config:Config.xml /v:8 /encrypt
- ScanState.exe \\server1\share1 /i:MigDocs.xml /v:13 /encrypt /key:"mysecretkey"

**NEW QUESTION 23**

- (Exam Topic 4)

You have an Azure AD group named Group1. Group1 contains two Windows 10 Enterprise devices named Device1 and Device2. You create a device configuration profile named Profile1. You assign Profile1 to Group1. You need to ensure that Profile1 applies to Device1 only. What should you modify in Profile1?

- A. Assignments
- B. Settings

- C. Scope (Tags)  
D. Applicability Rules

**Answer:** D

**Explanation:**

To ensure that Profile1 applies to Device1 only, you need to modify the Applicability Rules in Profile1. You can use applicability rules to filter which devices receive a profile based on criteria such as device model, manufacturer, or operating system version. You can create an applicability rule that matches Device1's properties and excludes Device2's properties. References:

<https://docs.microsoft.com/en-us/mem/intune/configuration/device-profile-assign#applicability-rules>

**NEW QUESTION 27**

- (Exam Topic 4)

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 32**

- (Exam Topic 4)

You have a computer that runs Windows 10 and contains two local users named User1 and User2. You need to ensure that the users can perform the following actions:

- User 1 must be able to adjust the date and time.
- User2 must be able to clear Windows logs.

The solution must use the principle of least privilege.

To which group should you add each user? To answer, drag the appropriate groups to the correct users. Each group 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.

- A. Mastered  
B. Not Mastered

**Answer:** A

**Explanation:**

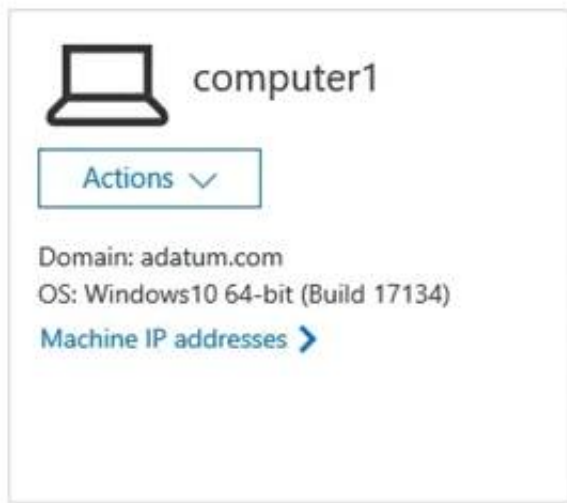
**NEW QUESTION 35**

- (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.



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 36

- (Exam Topic 4)

You have a Microsoft 365 ES subscription that uses Microsoft Intune. Devices are enrolled in Intune as shown in the following table.

Name	Platform	Enrolled by using
Device1	iOS	Apple Automated Device Enrollment (ADE)
Device2	iPadOS	Apple Automated Device Enrollment (ADE)
Device3	iPadOS	The Company Portal app

The devices are the members of groups as shown in the following table.

Name	Members
Group1	Device1, Device2, Device3
Group2	Device2

You create an JOS/iPadOS update profile as shown in the following exhibit.



Create profile

iOS/iPadOS

✓ Basics

✓ Update policy settings

✓ Assignments

Review + create

Summary

Basics

Name

Profile1

Description

--

Update policy settings

Update to install

Install iOS/iPadOS Latest update

Schedule type

Update outside of scheduled time

Time zone

UTC±00

Time window

Start day	Start time	End day	End time
Monday	1 AM	Wednesday	1 PM
Friday	1 AM	Saturday	11 PM

Assignments

Included groups

Group

Group Members

Group1

3 devices, 0 users

Excluded groups

Group

Group Members

Group2

1 devices, 0 users

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 an iOS update becomes available on Tuesday at 5 AM, the update is installed on Device1 automatically on Wednesday.	<input type="radio"/>	<input checked="" type="radio"/>
If an iPadOS update becomes available on Thursday at 2 AM, the update is installed on Device2 automatically on Thursday.	<input checked="" type="radio"/>	<input type="radio"/>
If an iPadOS update becomes available on Friday at 10 PM, the update is installed on Device3 automatically on Sunday.	<input checked="" type="radio"/>	<input type="radio"/>

- A. Mastered
- B. Not Mastered

Answer: A

Explanation:

Answer Area

Statements	Yes	No
If an iOS update becomes available on Tuesday at 5 AM, the update is installed on Device1 automatically on Wednesday.	<input type="radio"/>	<input checked="" type="radio"/>
If an iPadOS update becomes available on Thursday at 2 AM, the update is installed on Device2 automatically on Thursday.	<input checked="" type="radio"/>	<input type="radio"/>
If an iPadOS update becomes available on Friday at 10 PM, the update is installed on Device3 automatically on Sunday.	<input checked="" type="radio"/>	<input type="radio"/>



You have a Microsoft 365 E5 subscription that contains the devices shown in the following table. All devices have Microsoft Edge installed. From the Microsoft Intune admin center, you create a Microsoft You need to apply Edge1 to all the supported devices. To which devices should you apply Edge1?

- A. Device1 only
- B. Device1 and Device2 only
- C. Device1, Device2, and Device3 only
- D. Device1, Device2, and Device4 only
- E. Device1, Device2, Device3, and Device4

**Answer:** E

#### NEW QUESTION 41

- (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.



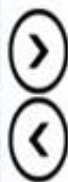
You need to prevent the welcome screen from appearing when the computers connect to MDT1.

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

- Modify the CustomSettings.ini file.
- Update the deployment share.
- Modify the Bootstrap.ini file.
- Replace the ISO image.
- Modify the task sequence.

##### Answer Area



- A. Mastered
- B. Not Mastered

**Answer:** A

##### Explanation:

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>

#### NEW QUESTION 42

- (Exam Topic 4)

You use Microsoft Intune and Intune Data Warehouse.

You need to create a device inventory report that includes the data stored in the data warehouse. What should you use to create the report?

- A. the Azure portal app
- B. Endpoint analytics
- C. the Company Portal app

D. Microsoft Power BI

**Answer:** D

**Explanation:**

You can use the Power BI Compliance app to load interactive, dynamically generated reports for your Intune tenant. Additionally, you can load your tenant data in Power BI using the OData link. Intune provides connection settings to your tenant so that you can view the following sample reports and charts related to: Devices  
Enrollment

App protection policy Compliance policy

Device configuration profiles Software updates

Device inventory logs

Note: Load the data in Power BI using the OData link

With a client authenticated to Azure AD, the OData URL connects to the RESTful endpoint in the Data Warehouse API that exposes the data model to your reporting client. Follow these instructions to use Power BI Desktop to connect and create your own reports.

- Sign in to the Microsoft Endpoint Manager admin center.
- Select Reports > Intune Data warehouse > Data warehouse.
- Retrieve the custom feed URL from the reporting blade, for example:
- Open Power BI Desktop.
- Choose File > Get Data. Select OData feed.
- Choose Basic.
- Type or paste the OData URL into the URL box.
- Select OK.
- If you have not authenticated to Azure AD for your tenant from the Power BI desktop client, type your credentials. To gain access to your data, you must authorize with Azure Active Directory (Azure AD) using OAuth 2.0.
- Select Organizational account.
- Type your username and password.
- Select Sign In.
- Select Connect.
- Select Load.

Reference: <https://docs.microsoft.com/en-us/mem/intune/developer/reports-proc-get-a-link-powerbi>

**NEW QUESTION 43**

- (Exam Topic 4)

You have a computer named Computer5 that has Windows 10 installed. You create a Windows PowerShell script named config.ps1.

You need to ensure that config.ps1 runs after feature updates are installed on Computer5. Which file should you modify on Computer5?

- A. LiteTouch.wsf
- B. SetupConfig.ini
- C. Unattendb\*
- D. Unattend.xml

**Answer:** B

**Explanation:**

SetupConfig.ini is a file that can be used to customize the behavior of Windows Setup during feature updates. You can use this file to specify commands or scripts that run before or after the installation process. To run a PowerShell script after a feature update, you can use the PostOOBE parameter in SetupConfig.ini and specify the path to the script file. References: [SetupConfig.ini reference]

**NEW QUESTION 47**

- (Exam Topic 4)

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:

Ports:

- 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 48**

- (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.

Statements	Yes	No
User1 can enroll Device1 in Intune by using automatic enrollment.	<input type="radio"/>	<input type="radio"/>
User1 can enroll Device2 in Intune by using automatic enrollment.	<input type="radio"/>	<input type="radio"/>
User2 can enroll Device1 in Intune by using automatic enrollment.	<input type="radio"/>	<input type="radio"/>

- A. Mastered  
B. Not Mastered

**Answer:** A



Explanation:

**Statements**

User1 can enroll Device1 in Intune by using automatic enrollment.

**Yes**

☒

**No**

☐

User1 can enroll Device2 in Intune by using automatic enrollment.

**Yes**

☐

**No**

☒

User2 can enroll Device1 in Intune by using automatic enrollment.

**Yes**

☐

**No**

☒

**NEW QUESTION 51**

- (Exam Topic 4)

You have a Microsoft Intune subscription.

You are creating a Windows Autopilot deployment profile named Profile1 as shown in the following exhibit.

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**

Users who deploy a device by using Profile1  
**[answer choice]**.

	▼
are prevented from modifying any desktop settings	
can create additional local users on the device	
can modify the desktop settings for all device users	
can modify the desktop settings only for themselves	

Users can configure the **[answer choice]** during  
the deployment.

	▼
computer name	
Cortana settings	
keyboard layout	

- A. Mastered
- B. Not Mastered

**Answer: A**

Explanation:



## Answer Area

Users who deploy a device by using Profile1  
[answer choice].

are prevented from modifying any desktop settings
can create additional local users on the device
can modify the desktop settings for all device users
can modify the desktop settings only for themselves

Users can configure the [answer choice] during  
the deployment.

computer name
Cortana settings
keyboard layout

### NEW QUESTION 54

- (Exam Topic 4)

You have a Hyper-V host. The host contains virtual machines that run Windows 10 as shown in following table.

Name	Generation	Virtual TPM	Virtual processors	Memory
VM1	1	No	4	16 GB
VM2	2	Yes	2	4 GB
VM3	2	Yes	1	8 GB

Which virtual machines can be upgraded to Windows 11?

- A. VM1 only
- B. VM2 only
- C. VM2 and VM3 only
- D. VM1, VM2, and VM3

**Answer: C**

#### Explanation:

Windows 11 has certain hardware requirements that must be met in order to upgrade from Windows 10. Some of these requirements are as follows:

- > A processor with at least 1 GHz clock speed and 2 cores.
- > A system firmware that supports UEFI and Secure Boot.
- > A Trusted Platform Module (TPM) version 2.0 or higher.
- > At least 4 GB
- > At least 64 GB of system memory (RAM).
- > At least 64 GB of storage space.

In this scenario, the virtual machines that run Windows 10 have the following specifications:

- > VM3 is a generation 2 virtual machine with a virtual TPM, 1 virtual processor, and 8 GB of memory.
- VM1 cannot be upgraded to Windows 11 because it does not have a virtual TPM and it is not a generation 2 virtual machine. Generation 1 virtual machines do not support UEFI and Secure Boot, which are required for Windows 11. VM2 and VM3 can be upgraded to Windows 11 because they have a virtual TPM and they are generation 2 virtual machines. They also meet the minimum requirements for processor speed, cores, memory, and storage space.

### NEW QUESTION 58

- (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 59

- (Exam Topic 4)

You have 200 computers that run Windows 10. The computers are joined to Microsoft Azure Active Directory (Azure AD) and enrolled in Microsoft Intune. You need to configure an Intune device configuration profile to meet the following requirements:

- Prevent Microsoft Office applications from launching child processes.
- Block users from transferring files over FTP.

Which two settings should you configure in Endpoint protection? To answer, select the appropriate settings in the answer area.

NOTE: Each correct selection is worth one point.

Answer Area

### Create Profile

**\*Name**

MD101

**Description**

Enter a description

**\*Platform**

Windows 10 and later

**\*Profile type**

Endpoint protection

Settings >

Configure >

Scope (Tags)  
0 scope(s) selected >

### Endpoint protection

Windows 10 and later

Select a category to configure settings

Windows Defender Application Gu...  
11 settings available >

Windows Defender Firewall  
40 settings available >

Windows Defender SmartScreen  
2 settings available >

Windows Encryption  
37 settings available >

Windows Defender Exploit Guard  
20 settings available >

Windows Defender Application Co...  
2 settings available >

Windows Defender Application Gua...  
1 setting available >

Windows Defender Security Center  
14 settings available >

Local device security options  
46 settings available >

Xbox services  
5 settings available >

OK

- A. Mastered  
B. Not Mastered

**Answer:** A

**Explanation:**

A screenshot of a computer Description automatically generated

References:

<https://docs.microsoft.com/en-us/intune/endpoint-protection-windows-10>

#### NEW QUESTION 60

- (Exam Topic 4)

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. From the Microsoft Endpoint Manager admin center, create a configuration profile.  
B. From the Microsoft Endpoint Manager admin center, create a security baseline.  
C. Onboard the macOS devices to the Microsoft 365 compliance center.  
D. Install Defender for Endpoint on the macOS devices.

**Answer:** D

**Explanation:**

Just install, and use Defender for Endpoint on Mac. Reference:

<https://docs.microsoft.com/en-us/microsoft-365/security/defender-endpoint/microsoft-defender-endpoint-mac>

#### NEW QUESTION 63

- (Exam Topic 4)

You have a Microsoft 365 subscription.

You plan to enroll devices in Microsoft Endpoint Manager that have the platforms and versions shown in the following table.

Platform	Version
Android	8, 9
iOS	11, 12

You need to configure device enrollment to meet the following requirements:

- Ensure that only devices that have approved platforms and versions can enroll in Endpoint Manager.
- Ensure that devices are added to Microsoft Azure Active Directory (Azure AD) groups based on a selection made by users during the enrollment.

Which device enrollment setting should you configure for each requirement? To answer, select the appropriate options in the answer area.

NOTE: Each correct selection is worth one point.

### Answer Area

Ensure that only devices that have approved platforms and versions can enroll in Endpoint Manager:

	▼
Android enrollment	
Apple enrollment	
Corporate device identifiers	
Device categories	
Enrollment restrictions	
Windows enrollment	

Ensure that devices are added to Azure AD groups based on a selection made by users during enrollment:

	▼
Android enrollment	
Apple enrollment	
Corporate device identifiers	
Device categories	
Enrollment restrictions	
Windows enrollment	

- A. Mastered
- B. Not Mastered

**Answer:** A

#### Explanation:

A screenshot of a computer Description automatically generated

Reference:

<https://docs.microsoft.com/en-us/mem/intune/enrollment/enrollment-restrictions-set> <https://docs.microsoft.com/en-us/mem/intune/enrollment/device-group-mapping>

#### NEW QUESTION 64

- (Exam Topic 4)

You have the MDM Security Baseline profile shown in the MDM exhibit. (Click the MDM tab.) You have the ASR Endpoint Security profile shown in the ASR exhibit. (Click the ASR tab.)

[Home](#) > [Endpoint security](#) > [MDM Security Baseline](#) >

## Create profile

Block Office applications from injecting code into other processes ⓘ

Disable



Block Office applications from creating executable content ⓘ

Audit mode



Block all Office applications from creating child processes ⓘ

Audit mode



Block Win32 API calls from Office macro ⓘ

Disable



Block execution of potentially obfuscated scripts (js/vbs/ps) ⓘ

Disable





[Home](#) > [Endpoint security](#) > [ASR Endpoint security](#) >

## Edit profile

### Attack Surface Reduction Rules

Block credential stealing from the Windows local security authority subsystem (lsass.exe) ⓘ	Audit mode ▼
Block Adobe Reader from creating child processes ⓘ	Audit mode ▼
Block Office applications from injecting code into other processes ⓘ	Audit mode ▼
Block Office applications from creating executable content ⓘ	Audit mode ▼
Block all Office applications from creating child processes ⓘ	Audit mode ▼
Block Win32 API calls from Office macro ⓘ	Audit mode ▼

You plan to deploy both profiles to devices enrolled in Microsoft Intune. You need to identify how the following settings will be configured on the devices:

- Block Office applications from creating executable content
- Block Win32 API calls from Office macro

Currently, the settings are disabled locally on each device.

What are the effective settings on the devices? To answer, select the appropriate options in the answer area. NOTE: Each correct selection is worth one point.

### Answer Area

Block Office applications from creating executable content:	<div><div></div><div>Audit mode</div><div>Block</div><div>Disable</div><div>Warn</div></div>
Block Win32 API calls from Office macro:	<div><div></div><div>Audit mode</div><div>Block</div><div>Disable</div><div>Warn</div></div>

- A. Mastered  
B. Not Mastered

**Answer:** A

**Explanation:**

### Answer Area

Block Office applications from creating executable content:	<div><div></div><div>Audit mode</div><div>Block</div><div>Disable</div><div>Warn</div></div>
Block Win32 API calls from Office macro:	<div><div></div><div>Audit mode</div><div>Block</div><div>Disable</div><div>Warn</div></div>

**NEW QUESTION 67**

- (Exam Topic 4)



You have a Microsoft 365 tenant that uses Microsoft Intune and contains the devices shown in the following table.

Name	Platform
Device1	Windows 10
Device2	macOS

In Microsoft Intune Endpoint security, you need to configure a disk encryption policy for each device. Which encryption type should you use for each device, and which role-based access control (RBAC) role in Intune should you use to manage the encryption keys? To answer, select the appropriate options in the answer area.  
NOTE: Each correct selection is worth one point.

Answer Area

Device1:

FileVault

Cryptsetup

Encrypting File System (EFS)

BitLocker Drive Encryption (BitLocker)

Device2:

FileVault

Cryptsetup

Encrypting File System (EFS)

BitLocker Drive Encryption (BitLocker)

RBAC role:

Help Desk Operator

Application Manager

Intune Role Administrator

Policy and Profile Manager

- A. Mastered
- B. Not Mastered

Answer: A

Explanation:

Graphical user interface, text, application Description automatically generated

#### NEW QUESTION 68

- (Exam Topic 4)

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 70

- (Exam Topic 4)

Your company uses Microsoft Intune to manage devices. You need to ensure that only Android devices that use Android work profiles can enroll in Intune. Which two configurations should you perform in the device enrollment restrictions? Each correct answer presents part of the solution.  
NOTE Each correct selection is worth one point.

- A. From Platform Settings, set Android device administrator Personally Owned to Block.
- B. From Platform Settings, set Android Enterprise (work profile) to Allow.
- C. From Platform Settings, set Android device administrator Personally Owned to Allow
- D. From Platform Settings, set Android device administrator to Block.

Answer: AB

Explanation:

To ensure that only Android devices that use Android work profiles can enroll in Intune, you need to perform two configurations in the device enrollment restrictions. First, you need to set Android device administrator Personally Owned to Block. This prevents users from enrolling personal Android devices that use device administrator mode. Second, you need to set Android Enterprise (work profile) to Allow. This allows users to enroll corporate-owned or personal Android devices that use work profiles. References: <https://docs.microsoft.com/en-us/mem/intune/enrollment/enrollment-restrictions-set>

#### NEW QUESTION 73

- (Exam Topic 4)

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: C**

**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 dependency 2. 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 78**

- (Exam Topic 4)

You have a Microsoft 365 subscription.

You plan to use Windows Autopilot to provision 25 Windows 11 devices. You need to configure the Out-of-box experience (OOBE) settings.

What should you create in the Microsoft Intune admin center?

- A. an enrollment status page (ESP)
- B. a deployment profile
- C. a compliance policy
- D. a PowerShell script
- E. a configuration profile

**Answer: B**

**NEW QUESTION 81**

- (Exam Topic 4)

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 devices1. App configuration policies let you customize the settings of apps for iOS/iPadOS or Android devices1. The settings are assigned to user groups and applied when the app runs1. The app developer or supplier provides the configuration settings (keys and values) that are exposed to Intune1. You can't use a single app configuration policy for both iOS/iPadOS and Android devices because they have different configuration settings2. 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 85**

- (Exam Topic 4)

You have the Microsoft Deployment Toolkit (MDT) installed in three sites as shown in the following table.

MDT instance name	Site	Default gateway
MDT1	New York	10.1.1.0/24
MDT2	London	10.5.5.0/24
MDT3	Dallas	10.4.4.0/24

You use Distributed File System (DFS) Replication to replicate images in a share named Production. You configure the following settings in the Bootstrap.ini file.

[Settings]

Priority=DefaultGateway, Default

[DefaultGateway]

10.1.1.1=NewYork

10.5.5.1=London

[NewYork]

DeployRoot=\\MDT1\Production\$

[London]

DeployRoot=\\MDT2\Production\$

KeyboardLocale=en-gb -

[Default]

DeployRoot=\\MDT3\Production\$

KeyboardLocale=en-us -

You plan to deploy Windows 10 to the computers shown in the following table.

Name	IP address
LT1	10.1.1.240
DT1	10.5.5.115
TB1	10.2.2.193

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

TB1 will download the image from MDT3.

☐
☐

DT1 will have a KeyboardLocale of en-gb.

☐
☐

LT1 will download the image from MDT1.

☐
☐

- A. Mastered
- B. Not Mastered

Answer: A

Explanation:

### Statements

Yes

No

TB1 will download the image from MDT3.

☐
☒

DT1 will have a KeyboardLocale of en-gb.

☒
☐

LT1 will download the image from MDT1.

☒
☐

### NEW QUESTION 90

- (Exam Topic 3)

You need to meet the technical requirements for the LEG department computers.

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
Configure the commercial ID on the LEG department computers.	
Create an Azure Machine Learning service workspace.	
Create an Azure Log Analytics workspace.	
Install the Microsoft Monitoring Agent on the LEG department computers.	
Add a solution to a workspace.	

- A. Mastered  
B. Not Mastered

**Answer:** A

**Explanation:**

A screenshot of a white box Description automatically generated

Reference:

<https://docs.microsoft.com/en-us/windows/deployment/update/windows-analytics-azure-portal>

**NEW QUESTION 91**

- (Exam Topic 3)

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

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

**Answer:** A

**Explanation:**

References:

<https://docs.microsoft.com/en-us/microsoft-store/add-profile-to-devices#manage-autopilot-deployment-profiles>

**NEW QUESTION 93**

- (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 95**

- (Exam Topic 3)

To which devices do Policy1 and Policy2 apply? To answer, select the appropriate options in the answer area. NOTE: Each correct selection is worth one point.



Policy1:

	<input type="checkbox"/>
Device1 only	<input type="checkbox"/>
Device2 only	<input type="checkbox"/>
Device3 only	<input type="checkbox"/>
Device4 only	<input type="checkbox"/>
Device2 and Device3 only	<input type="checkbox"/>
Device1 and Device3 only	<input type="checkbox"/>
Device1, Device2, and Device 3	<input type="checkbox"/>

Policy2:

	<input type="checkbox"/>
Device1 only	<input type="checkbox"/>
Device2 only	<input type="checkbox"/>
Device3 only	<input type="checkbox"/>
Device4 only	<input type="checkbox"/>
Device2 and Device3 only	<input type="checkbox"/>
Device1 and Device3 only	<input type="checkbox"/>
Device1, Device2, and Device 3	<input type="checkbox"/>

- A. Mastered  
B. Not Mastered

Answer: A

Explanation:

Reference:

<https://docs.microsoft.com/en-us/intune/device-profile-assign>

#### NEW QUESTION 97

- (Exam Topic 3)

What is the maximum number of devices that User1 and User2 can enroll in Intune? To answer, select the appropriate options in the answer area.

NOTE: Each correct selection is worth one point.

User1 can enroll a maximum of:

	<input type="checkbox"/>
5 devices	<input type="checkbox"/>
10 devices	<input type="checkbox"/>
15 devices	<input type="checkbox"/>
1,000 devices	<input type="checkbox"/>
An unlimited number of devices	<input type="checkbox"/>

User2 can enroll a maximum of:

	<input type="checkbox"/>
5 devices	<input type="checkbox"/>
10 devices	<input type="checkbox"/>
15 devices	<input type="checkbox"/>
1,000 devices	<input type="checkbox"/>
An unlimited number of devices	<input type="checkbox"/>

- A. Mastered  
B. Not Mastered

Answer: A

Explanation:

User1 can enroll a maximum of:

	<input type="checkbox"/>
5 devices	<input checked="" type="checkbox"/>
10 devices	<input checked="" type="checkbox"/>
15 devices	<input type="checkbox"/>
1,000 devices	<input type="checkbox"/>
An unlimited number of devices	<input type="checkbox"/>

User2 can enroll a maximum of:

	<input type="checkbox"/>
5 devices	<input type="checkbox"/>
10 devices	<input checked="" type="checkbox"/>
15 devices	<input checked="" type="checkbox"/>
1,000 devices	<input type="checkbox"/>
An unlimited number of devices	<input type="checkbox"/>

**NEW QUESTION 99**

- (Exam Topic 3)

You need to meet the technical requirements for the IT department. What should you do first?

- A. From the Azure Active Directory blade in the Azure portal, enable Seamless single sign-on.
- B. From the Configuration Manager console, add an Intune subscription.
- C. From the Azure Active Directory blade in the Azure portal, configure the Mobility (MDM and MAM) settings.
- D. From the Microsoft Intune blade in the Azure portal, configure the Windows enrollment settings.

**Answer:** C

**Explanation:**

Reference:

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

**NEW QUESTION 102**

- (Exam Topic 3)

You need to meet the technical requirements for the iOS devices. Which object should you create in Intune?

- A. A compliance policy
- B. An app protection policy
- C. A Deployment profile
- D. A device configuration profile

**Answer:** D

**Explanation:**

References:

<https://docs.microsoft.com/en-us/intune/device-restrictions-configure> <https://docs.microsoft.com/en-us/intune/device-restrictions-ios>

**NEW QUESTION 104**

- (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 106**

- (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 110**

- (Exam Topic 2)

You need to recommend a solution to meet the device management requirements.

What should you include in the recommendation? To answer, select the appropriate options in the answer area. NOTE: Each correct selection is worth one point.

For the Research department employees:

<input type="checkbox"/>
An app configuration policy
An app protection policy
Azure information Protection
iOS app provisioning profiles

For the Sales department employees:

<input type="checkbox"/>
An app configuration policy
An app protection policy
Azure information Protection
iOS app provisioning profiles

- A. Mastered
- B. Not Mastered

**Answer:** A

**Explanation:**

Reference:

<https://github.com/MicrosoftDocs/IntuneDocs/blob/master/intune/app-protection-policy.md>

<https://docs.microsoft.com/en-us/azure/information-protection/configure-usage-rights#do-not-forward-option-fo>

#### NEW QUESTION 112

- (Exam Topic 2)

What should you use to meet the technical requirements for Azure DevOps?

- A. An app protection policy
- B. Windows Information Protection (WIP)
- C. Conditional access
- D. A device configuration profile

**Answer:** C

**Explanation:**

References:

<https://docs.microsoft.com/en-us/azure/devops/organizations/accounts/manage-conditional-access?view=azure-devops>

#### NEW QUESTION 113

- (Exam Topic 2)

You need to resolve the performance issues in the Los Angeles office.

How should you configure the update settings? To answer, select the appropriate options in the answer area. NOTE: Each correct selection is worth one point.

**Answer Area**

Change Delivery Optimization  
download mode to:

<input type="checkbox"/>
Bypass mode
HTTP blended with internet peering
HTTP blended with peering behind same NAT
Simple download mode with no peering

Update Active Hours Start to:

<input type="checkbox"/>
10 AM
11 AM
10 PM
11 PM

Update Active Hours End to:

<input type="checkbox"/>
10 AM
11 AM
10 PM
11 PM

- A. Mastered
- B. Not Mastered

**Answer:** A

**Explanation:**

A screenshot of a computer Description automatically generated with low confidence

Reference:

<https://docs.microsoft.com/en-us/windows/deployment/update/waas-delivery-optimization> <https://2pintsoftware.com/delivery-optimization-dl-mode/>

**NEW QUESTION 118**

- (Exam Topic 2)

You need to meet the device management requirements for the developers. What should you implement?

- A. folder redirection
- B. Enterprise State Roaming
- C. home folders
- D. known folder redirection in Microsoft OneDrive

**Answer: B**

**Explanation:**

Litware identifies the following device management requirements:

➤ Ensure that Microsoft Edge Favorites are accessible from all computers to which the developers sign in. Enterprise State Roaming allows for the synchronization of Microsoft Edge browser setting, including favorites and reading list, across devices.

Reference:

<https://docs.microsoft.com/en-us/azure/active-directory/devices/enterprise-state-roaming-windows-settings-refer>

**NEW QUESTION 119**

- (Exam Topic 1)

Which user can enroll Device6 in Intune?

- A. User4 and User2 only
- B. User4 and User 1 only
- C. User1, User2, User3, and User4
- D. User4. User Land User2 only

**Answer: B**

**NEW QUESTION 122**

- (Exam Topic 1)

User1 and User2 plan to use Sync your settings.

On which devices can the users use Sync your settings? To answer, select the appropriate options in the answer area.

NOTE: Each correct selection is worth one point.

**Answer Area**

User1:	<div><div>No devices</div><div>Device4 and Device5 only</div><div>Device1, Device2 and Device3 only</div><div>Device1, Device2, Device3, Device4, and Device5</div></div>
User2:	<div><div>No devices</div><div>Device4 and Device5 only</div><div>Device1, Device2 and Device3 only</div><div>Device1, Device2, Device3, Device4, and Device5</div></div>

- A. Mastered
- B. Not Mastered

**Answer: A**

**Explanation:**

Graphical user interface, text, application, email Description automatically generated

Reference:

<https://www.jeffgilb.com/managing-local-administrators-with-azure-ad-and-intune/>

**NEW QUESTION 127**

- (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
User1 can create a file named D:\Folder1\file1.txt on Device4 by using Notepad.	<input type="radio"/>	<input type="radio"/>
User2 can remove D:\Folder1 from the list of protected folders on Device2.	<input type="radio"/>	<input type="radio"/>
User3 can create a file named C:\Users\User3\Desktop\file1.txt on Device2 by running a custom Windows PowerShell script.	<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

NEW QUESTION 129

- (Exam Topic 1)

You implement Boundary1 based on the planned changes.

Which devices have a network boundary of 192.168.1.0/24 applied?

- A. Device2 only
- B. Device3 only
- C. Device 1, Device2, and Device5 only
- D. Device 1, Device2, Device3, and Device4 only

Answer: D

Explanation:

Reference:

<https://docs.microsoft.com/en-us/mem/intune/configuration/network-boundary-windows>

NEW QUESTION 130

- (Exam Topic 1)

Which devices are registered by using the Windows Autopilot deployment service?

- A. Device1 only
- B. Device3 only
- C. Device1 and Device3 only
- D. Device1, Device2, and Device3

Answer: C

Explanation:

Scenario: Windows Autopilot Configuration Assignments

Included groups: Group1

Excluded groups: Group2 Device1 is member of Group1.

Device2 is member of Group1 and member of Group2. Device3 is member of Group1.

Group1 and Group2 have a Membership type of Assigned.

Exclusion takes precedence over inclusion in the following same group type scenarios. Reference: <https://learn.microsoft.com/en-us/mem/intune/apps/apps-inc-exl-assignments>

NEW QUESTION 135

- (Exam Topic 1)

Which users can purchase and assign App1?

- A. User3 only
- B. User1 and User3 only
- C. User1, User2, User3, and User4
- D. User1, User3, and User4 only
- E. User3 and User4 only

Answer: B

Explanation:

Reference:

<https://docs.microsoft.com/en-us/microsoft-store/acquire-apps-microsoft-store-for-business> <https://docs.microsoft.com/en-us/microsoft-store/assign-apps-to-employees>

NEW QUESTION 139

- (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
<div><div></div><div></div><div></div></div>	<div><div></div><div></div><div></div></div>	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 141

- (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: C

Explanation:

Reference:

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

NEW QUESTION 144

- (Exam Topic 4)

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 146

- (Exam Topic 4)

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 149

- (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 153

- (Exam Topic 4)

You have an Azure Active Directory (Azure AD) tenant named contoso.com that contains a user named User1. User1 has a user principal name (UPN) of user1@contoso.com.

You join a Windows 10 device named Client1 to contoso.com.

You need to add User1 to the local Administrators group of Client1.

How should you complete the command? To answer, select the appropriate options in the answer area.

NOTE: Each correct selection is worth one point.

### Answer Area

net accounts
net localgroup
net user

Administrators /add "

AzureAD
CONTOSO
UPN

\user1@contoso.com"

- A. Mastered
- B. Not Mastered

**Answer: A**

**Explanation:**

### Answer Area

net accounts
net localgroup
net user

Administrators /add "

AzureAD
CONTOSO
UPN

\user1@contoso.com"

### NEW QUESTION 155

- (Exam Topic 4)

You have an Azure AD tenant that contains the devices shown in the following table. You purchase Windows 11 Enterprise E5 licenses.

Which devices can use Subscription Activation to upgrade to Windows 11 Enterprise?

- A. Device1 only
- B. Device1 and Device2 only
- C. Device1 and Device3 only
- D. Device1, Device2, Device3, and Device4

**Answer: B**



**NEW QUESTION 159**

- (Exam Topic 4)

You have a Microsoft 365 E5 subscription. The subscription contains 25 computers that run Windows 11 and are enrolled in Microsoft Intune. You need to onboard the devices to Microsoft Defender for Endpoint. What should you create in the Microsoft Intune admin center?

- A. an attack surface reduction (ASR) policy
- B. a security baseline
- C. an endpoint detection and response (EDR) policy
- D. an account protection policy
- E. an antivirus policy

**Answer: C**

**Explanation:**

To onboard the devices to Microsoft Defender for Endpoint, you need to create an endpoint detection and response (EDR) policy in the Microsoft Intune admin center. This policy enables EDR capabilities on devices that are enrolled in Intune and allows you to configure various settings for EDR functionality. You can then assign the policy to groups of users or devices. References:

<https://docs.microsoft.com/en-us/mem/intune/protect/edr-windows>

**NEW QUESTION 161**

- (Exam Topic 4)

You have a Microsoft 365 E5 subscription.

You create an app protection policy for Android devices named Policy1 as shown in the following exhibit.

[Home](#) > [Apps](#) >

## Create policy

✓ Basics

**2 Apps**

① Data protection

④ Access requirements

...

Choose how you want to apply this policy to apps on different devices. Then add at least one app.

Target to apps on all device types ⓘ

Yes No

Device types \* ⓘ

Unmanaged

Target policy to

All Apps

ⓘ

We'll continue to add managed apps to your policy as they become available in Intune. [View a list of apps that will be targeted](#)

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.

To apply Policy1 to an Android device, you must [answer choice].

- |   |
|---|
| install the Company Portal app on the device              |
| install the Microsoft Authenticator app on the device     |
| onboard the device to Microsoft Defender for Endpoint     |
| onboard the device to the Microsoft 365 compliance center |

When Policy1 is assigned, the policy will apply to [answer choice].

- |                   |
|-------------------|
| users only        |
| devices only      |
| users and devices |

- A. Mastered
- B. Not Mastered

**Answer: A**

**Explanation:**

Box 1: Install the Intune Company Portal app on the device

On Android, Android devices will prompt to install the Intune Company Portal app regardless of which Device type is chosen.

Box 2: Devices only

For Android devices, unmanaged devices are devices where Intune MDM management has not been detected. This includes devices managed by third-party MDM vendors.

Reference:

<https://docs.microsoft.com/en-us/mem/intune/apps/app-protection-policies#app-protection-policies-for-iosipado>



#### NEW QUESTION 162

- (Exam Topic 4)

You have a Microsoft 365 subscription.

You have 10 computers that run Windows 10 and are enrolled in mobile device management (MDM). You need to deploy the Microsoft 36S Apps for enterprise suite to all the computers.

What should you do?

- A. From the Microsoft Intune admin center, create a Windows 10 device profile.
- B. From Azure AD, add an app registration.
- C. From Azure A
- D. add an enterprise application.
- E. From the Microsoft Intune admin center, add an app.

**Answer: D**

#### Explanation:

To deploy Microsoft 365 Apps for enterprise to Windows 10 devices that are enrolled in Intune, you need to add an app of type “Windows 10 app (Win32)” in the Microsoft Intune admin center and configure the app settings. You can then assign the app to groups of users or devices. References:  
<https://docs.microsoft.com/en-us/mem/intune/apps/apps-win32-app-management>

#### NEW QUESTION 167

- (Exam Topic 4)

You have a Microsoft 365 subscription that uses Microsoft Intune Suite. You use Microsoft Intune to manage devices. Azure AD joined Windows devices enroll automatically in Intune. You have the devices shown in the following table.

Name	Operating system	Azure AD joined	Line-of-business (LOB) apps installed
Device1	64-bit version of Windows 10 Pro	Yes	No
Device2	32-bit version of Windows 10 Pro	No	Yes
Device3	64-bit version of Windows 10 Pro	No	Yes

You are preparing to upgrade the devices to Windows 11. All the devices are compatible with Windows 11. You need to evaluate Windows Autopilot and in-place upgrade as deployment methods to implement

Windows 11 Pro on the devices, while retaining all user settings and applications.

Which devices can be upgraded by using each method? To answer, select the appropriate options in the answer area.

NOTE: Each correct selection is worth one point.

**Answer Area**

Windows Autopilot:

In-place upgrade:

- A. Mastered
- B. Not Mastered

**Answer: A**

#### Explanation:

**Answer Area**

Windows Autopilot:

In-place upgrade:

#### NEW QUESTION 168

- (Exam Topic 4)

You have 1,000 computers that run Windows 10 and are members of an Active Directory domain. You need to capture the event logs from the computers to Azure.

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

#### Answer Area

Azure service to provision:

<input type="checkbox"/>
<input type="checkbox"/> An Azure Storage account
<input type="checkbox"/> Azure Cosmos DB
<input type="checkbox"/> Azure SQL Database
<input type="checkbox"/> Log Analytics

Action to perform on the computers:

<input type="checkbox"/>
<input type="checkbox"/> Create a collector-initiated subscription
<input type="checkbox"/> Install the Microsoft Monitoring Agent
<input type="checkbox"/> Enroll in Microsoft Intune
<input type="checkbox"/> Register to Azure Active Directory (Azure AD)

- A. Mastered
- B. Not Mastered

**Answer:** A

**Explanation:**

#### Answer Area

Azure service to provision:

<input type="checkbox"/>
<input type="checkbox"/> An Azure Storage account
<input type="checkbox"/> Azure Cosmos DB
<input type="checkbox"/> Azure SQL Database
<input checked="" type="checkbox"/> Log Analytics

Action to perform on the computers:

<input type="checkbox"/>
<input type="checkbox"/> Create a collector-initiated subscription
<input checked="" type="checkbox"/> Install the Microsoft Monitoring Agent
<input type="checkbox"/> Enroll in Microsoft Intune
<input type="checkbox"/> Register to Azure Active Directory (Azure AD)

#### NEW QUESTION 171

- (Exam Topic 4)

Note: This question is part of a series of questions that present the same scenario. Each question in the series contains a unique solution that might meet the stated goals. Some question sets might have more than one correct solution, while others might not have a correct solution.

After you answer a question in this section, you will NOT be able to return to it. As a result, these questions will not appear in the review screen.

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 the Authentication methods. Does this meet the goal?

- A. Yes
- B. No

**Answer:** B

#### NEW QUESTION 175

- (Exam Topic 4)

You are replacing 100 company-owned Windows devices.

You need to use the Microsoft Deployment Toolkit (MDT) to securely wipe and decommission the devices. The solution must meet the following requirements:

- Back up the user state.
- Minimize administrative effort.

Which task sequence template should you use?

- A. Standard Client Task Sequence
- B. Standard Client Replace Task Sequence
- C. Litetouch OEM Task Sequence
- D. Sysprep and Capture

Answer: B

#### NEW QUESTION 179

- (Exam Topic 4)

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

Name	Platform	Encryption	Secure Boot	Member of
Device1	Windows 10	Yes	No	Group1
Device2	Windows 10	No	Yes	Group2
Device3	Android	No	<i>Not applicable</i>	Group3

Intune includes the device compliance policies shown in the following table.

Name	Platform	Encryption	Secure Boot
Policy1	Windows 10	Not configured	Not configured
Policy2	Windows 10	Not configured	Required
Policy3	Windows 10	Required	Required
Policy4	Android	Not configured	<i>Not applicable</i>

The device compliance policies have the assignments shown in the following table.

Name	Assigned to
Policy1	Group1
Policy2	Group1, Group2
Policy3	Group3
Policy4	Group3

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
Device1 is marked as compliant.	<input type="radio"/>	<input type="radio"/>
Device2 is marked as compliant.	<input type="radio"/>	<input type="radio"/>
Device3 is marked as compliant.	<input type="radio"/>	<input type="radio"/>

- A. Mastered
- B. Not Mastered

Answer: A

#### Explanation:

Device1 is marked as compliant = No Device2 is marked as compliant = Yes Device3 is marked as comp  
= No

- Device1 is marked as noncompliant because it does not meet the minimum OS version requirement of Policy1, which is 11.0.0. Device1 has an OS version of 10.0.0, which is lower than the required version1.
- Device2 is marked as compliant because it meets all the requirements of Policy2, which are: minimum OS version of 10.0.0, password required, and encryption enabled. Device2 has an OS version of 11.0.0, a password set, and encryption enabled1.
- Device3 is marked as noncompliant because it does not meet the encryption requirement of Policy3, which is enabled. Device3 has encryption disabled1.

#### NEW QUESTION 182

- (Exam Topic 4)

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

You have 100 devices from users that left your company.

You need to repurpose the devices for new users by removing all the data and applications installed by the previous users. The solution must minimize administrative effort.

What should you do?

- A. Deploy a new configuration profile to the devices.
- B. Perform a Windows Autopilot reset on the devices.
- C. Perform an in-place upgrade on the devices.
- D. Perform a clean installation of Windows 11 on the devices.

Answer: B



### NEW QUESTION 183

- (Exam Topic 4)

You have a Microsoft 365 E5 subscription that contains a user named User1 and uses Microsoft Intune Suite. You use Microsoft Intune to manage devices. You have a device named Device1 that is enrolled in Intune.

You need to ensure that User1 can use Remote Help from the Intune admin center for Device1. Which three actions should you perform? Each correct answer presents part of the solution.

NOTE: Each correct selection is worth one point.

- A. Deploy the Remote Help app to Device1.
- B. Assign the Help Desk Operator role to User1.
- C. Assign the Intune Administrator role to User1.
- D. Assign a Microsoft 365 E5 license to User1.
- E. Rerun device onboarding on Device1.
- F. Assign the Remote Help add-on license to User1.

**Answer:** ABF

### NEW QUESTION 187

- (Exam Topic 4)

You have a Microsoft 365 subscription that contains a user named User1 and uses Microsoft Intune Suite. You use Microsoft Intune to manage devices that run Windows 11.

User1 provides remote support for 75 devices in the marketing department.

You need to add User1 to the Remote Desktop Users group on each marketing department device. What should you configure?

- A. an app configuration policy
- B. a device compliance policy
- C. an account protection policy
- D. a device configuration profile

**Answer:** D

### NEW QUESTION 189

- (Exam Topic 4)

You have a Microsoft 365 subscription that uses Microsoft Intune. You plan to manage Windows updates by using Intune.

You create an update ring for Windows 10 and later and configure the User experience settings for the ring as shown in the following exhibit.

**User experience settings**

Automatic update behavior ⓘ	Auto install and restart at maintenance time ▼
Active hours start * ⓘ	8 AM ▼
Active hours end * ⓘ	5 PM ▼
Restart checks ⓘ	<b>Allow</b> Skip
Option to pause Windows updates ⓘ	<b>Enable</b> Disable
Option to check for Windows updates ⓘ	<b>Enable</b> Disable
Change notification update level ⓘ	Use the default Windows Update notifications ▼
Use deadline settings ⓘ	<b>Allow</b> Not configured
Deadline for feature updates ⓘ	5 ✓
Deadline for quality updates ⓘ	2 ✓
Grace period ⓘ	1 ✓
Auto reboot before deadline ⓘ	<b>Yes</b> No

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**

Automatic restarts are blocked [answer choice].

A restart will be forced on a device [answer choice] after the deadline.

between 8 AM and 5 PM ▼
before 8 AM
<b>between 8 AM and 5 PM</b>
after 5 PM
5 days ▼
<b>1 day</b>
2 days
5 days

- A. Mastered
- B. Not Mastered



**Answer:** A

**Explanation:**  
Answer Area

Automatic restarts are blocked [answer choice].

A restart will be forced on a device [answer choice] after the deadline.

### NEW QUESTION 193

- (Exam Topic 4)

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

Name	Role
Admin1	Application admin
Admin2	Cloud application admin
Admin3	Office apps admin
Admin4	Security admin

In the Microsoft 365 Apps admin center, you create a Microsoft Office customization. Which users can download the Office customization file from the admin center?

- A. Admin1, Admin2, Admin3. and Admin4
- B. Admin1, Admin2, and Admin3 only
- C. Admin3 only
- D. Admin3 and Admin4 only
- E. Admin1 and Admin3 only

**Answer:** B

**Explanation:**

\* Admin1

An application admin has full access to enterprise applications, applications registrations, and application proxy settings.

\* Admin2

Mark your app as publisher verified.

In Azure AD this user must be a member of one of the following roles: Application Admin, Cloud Application Admin, or Global Admin.

\* Admin3

Office Apps admin - Assign the Office Apps admin role to users who need to do the following:

- Use the Office cloud policy service to create and manage cloud-based policies for Office
- Create and manage service requests
- Manage the What's New content that users see in their Office apps
- Monitor service health Reference:

Office Apps admin - Assign the Office Apps admin role to users who need to do the following <https://docs.microsoft.com/en-us/azure/active-directory/develop/mark-app-as-publisher-verified>

### NEW QUESTION 197

- (Exam Topic 4)

You have an Azure AD tenant named contoso.com that contains a user named User1. User1 has a user principal name (UPN) of user1@contoso.com.

You join a Windows 11 device named Client 1 to contoso.com. You need to add User1 to the local Administrators group of Client1.

How should you complete the command? To answer, select the appropriate options in the answer area. NOTE: Each correct selection is worth one point.

**Answer Area**

- A. Mastered
- B. Not Mastered

**Answer:** A

**Explanation:**

net localgroup Administrators /add "AzureAD\user1@contoso.com"

This command will add the Azure AD user with the UPN of user1@contoso.com to the local Administrators group of the device1. You need to use the AzureAD prefix and double backslashes to specify the user's domain2. You also need to enclose the user's name in quotation marks if it contains special characters like @1.

You can run this command from an elevated command prompt on Client1, or remotely by using PowerShell or other tools1. You can also use the Intune Role Administrator role or the Additional local administrators on all Azure AD joined devices setting to manage the local administrators group on Azure AD joined devices34.

#### NEW QUESTION 201

- (Exam Topic 4)

Your network contains an Active Directory domain named adatum.com. The domain contains two computers named Computer1 and Computer2 that run Windows 10. Remote Desktop is enabled on Computer2.

The domain contains the user accounts shown in the following table.

Name	Member of
User1	Domain Admins
User2	Domain Users
User3	Domain Users

Computer2 contains the local groups shown in the following table.

Name	Members
Group1	ADATUM\User2 ADATUM\User3
Group2	ADATUM\User2
Group3	ADATUM\User3
Administrators	ADATUM\Domain Admins ADATUM\User3
Remote Desktop Users	Group1

The relevant user rights assignments for Computer2 are shown in the following table.

Policy	Security Setting
Allow log on through Remote Desktop Services	Administrators, Remote Desktop Users
Deny log on through Remote Desktop Services	Group2
Deny log on locally	Group3

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 can establish a Remote Desktop session to Computer2.	<input type="radio"/>	<input type="radio"/>
User2 can establish a Remote Desktop session to Computer2.	<input type="radio"/>	<input type="radio"/>
User3 can establish a Remote Desktop session to Computer2.	<input type="radio"/>	<input type="radio"/>

- A. Mastered
- B. Not Mastered

Answer: A

Explanation:

#### Answer Area

Statements	Yes	No
User1 can establish a Remote Desktop session to Computer2.	<input checked="" type="radio"/>	<input type="radio"/>
User2 can establish a Remote Desktop session to Computer2.	<input type="radio"/>	<input checked="" type="radio"/>
User3 can establish a Remote Desktop session to Computer2.	<input type="radio"/>	<input checked="" type="radio"/>

**NEW QUESTION 204**

- (Exam Topic 4)

You have an Azure AD tenant named contoso.com.

You have a workgroup computer named Computer1 that runs Windows 11. You need to add Computer1 to contoso.com.

What should you use?

- A. dsreecmd.exe
- B. Computer Management
- C. netdom.exe
- D. the Settings app

**Answer:** A

**NEW QUESTION 205**

- (Exam Topic 4)

You have a Microsoft 365 subscription that contains 1,000 iOS devices and includes Microsoft Intune. You need to prevent the printing of corporate data from managed apps on the devices, should you configure?

- A. an app configuration policy
- B. a security baseline
- C. an app protection policy
- D. an iOS app provisioning profile

**Answer:** C

**Explanation:**

An app protection policy is a set of rules that controls how data is accessed and handled by managed apps on mobile devices. App protection policies can prevent the printing of corporate data from managed apps on iOS devices by using the Restrict cut, copy, and paste with other apps setting. This setting can be configured to block printing from the iOS share menu. An app configuration policy is used to customize the behavior of a managed app, such as specifying a VPN profile or a web link. A security baseline is a collection of recommended security settings for Windows 10 devices that are managed by Intune. An iOS app provisioning profile is a file that contains information about the app's identity, entitlements, and distribution method

**NEW QUESTION 207**

- (Exam Topic 4)

You have a Microsoft 365 subscription that uses Microsoft Intune and contains 100 Windows 10 devices. You need to create Intune configuration profiles to perform the following actions on the devices:

- Deploy a custom Start layout.
- Rename the local Administrator account.

Which profile type template should you use for each action? To answer, select the appropriate options in the answer area. NOTE: Each correct selection is worth one point.

**Answer Area**

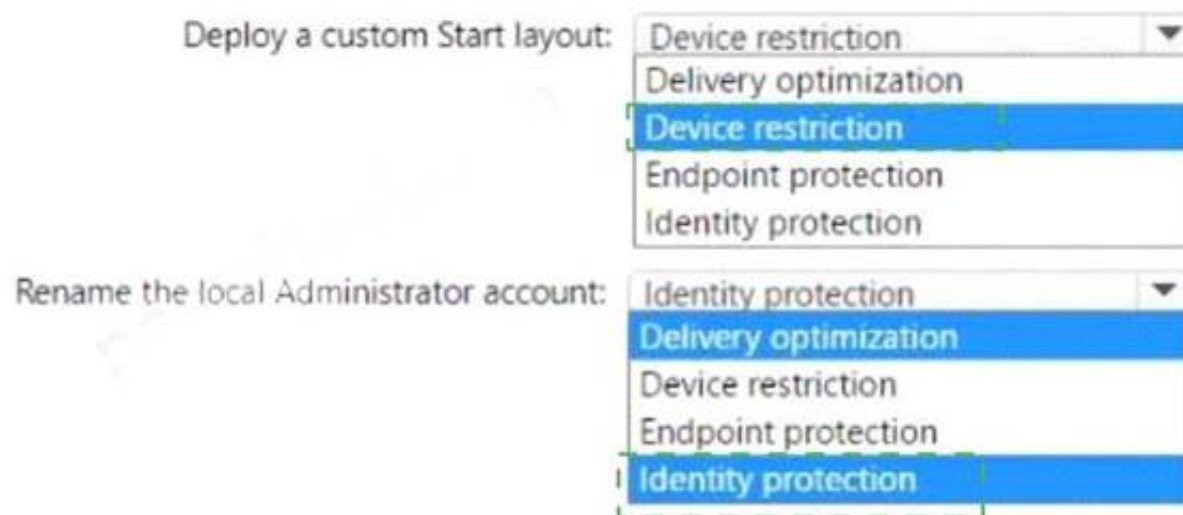
Deploy a custom Start layout:	<div>Device restriction</div> <div>Delivery optimization</div> <div>Device restriction</div> <div>Endpoint protection</div> <div>Identity protection</div>
Rename the local Administrator account:	<div>Identity protection</div> <div>Delivery optimization</div> <div>Device restriction</div> <div>Endpoint protection</div> <div>Identity protection</div>

- A. Mastered
- B. Not Mastered

**Answer:** A

**Explanation:**

## Answer Area



### NEW QUESTION 210

- (Exam Topic 4)

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 215

- (Exam Topic 4)

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

Name	Operating system	Azure AD status	Mobile device management (MDM)
Device1	Windows 8.1	Registered	None
Device2	Windows 10	Joined	None
Device3	Windows 10	Joined	Microsoft Intune

Contoso.com contains the Azure Active Directory groups shown in the following table.

Name	Members
Group1	Group2, Device1, Device3
Group2	Device2

You add a Windows Autopilot deployment profile. The profile is configured as shown in the following exhibit.



Create profile ...

Windows PC

✓ Basics

✓ Out-of-box experience (OOBE)

✓ Assignments

1

 Review + create

Summary

Basics

Name

Profile1

Description

--

Convert all targeted devices to Autopilot

Yes

Device type

Windows PC

Out-of-box experience (OOBE)

Deployment mode

Self-Deploying (preview)

Join to Azure AD as

Azure AD joined

Skip AD connectivity check (preview)

No

Language (Region)

Operating system default

Automatically configure keyboard

Yes

Microsoft Software License Terms

Hide

Privacy settings

Hide

Hide change account options

Hide

User account type

Standard

Allow White Glove OOBE

No

Apply device name template

No

Assignments

Included groups

Group1

Excluded groups

--

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
If Device1 starts in Out of Box Experience (OOBE) mode, the device will be deployed by using Autopilot.	<input type="radio"/>	<input type="radio"/>
If Device2 starts in Out of Box Experience (OOBE) mode, the device will be deployed by using Autopilot.	<input type="radio"/>	<input type="radio"/>
If Device3 starts in Out of Box Experience (OOBE) mode, the device will be deployed by using Autopilot.	<input type="radio"/>	<input type="radio"/>

- A. Mastered
- B. Not Mastered

Answer: A

Explanation:

Box 1: No  
Device1 has no Mobile device Management (MDM) configured.  
Note: Device1 is running Windows 8.1, and is registered, but not joined. Device1 is in Group1.  
Profile1 is assigned to Group1. Box 2: No  
Device2 has no Mobile device Management (MDM) configured. Note: Device2 is running Windows 10, and is joined.  
Device2 is in Group2. Group2 is in Group1.  
Profile1 is assigned to Group1. Box 3: Yes  
Device3 has Mobile device Management (MDM) configured. Device3 is running Windows 10, and is joined

Device1 is in Group1.

Profile1 is assigned to Group1.

Mobile device management (MDM) enrollment: Once your Windows 10 device joins Azure AD, Autopilot ensures your device is automatically enrolled with MDMs such as Microsoft Intune. This program can automatically push configurations, policies and settings to the device, and install Office 365 and other business apps without you having to get IT admins to manually sort the device. Intune can also apply the latest updates from Windows Update for Business.

Reference: <https://xo.xello.com.au/blog/windows-autopilot>

#### NEW QUESTION 217

- (Exam Topic 4)

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

Name	Operating system	Azure AD join type
Device1	Windows 11 Pro	Joined
Device2	Windows 11 Pro	Registered
Device3	Windows 10 Pro	Joined
Device4	Windows 10 Pro	Registered

Which devices can be activated by using subscription activation?

- A. Device 1 only
- B. Device1 and Device2 only
- C. Device1 and Device3 only
- D. Device1, Device2. Device3, and Device4

**Answer: C**

#### NEW QUESTION 220

- (Exam Topic 4)

You have computers that run Windows 10 and are configured by using Windows AutoPilot. A user performs the following tasks on a computer named Computer1:

- Creates a VPN connection to the corporate network
- Installs a Microsoft Store app named App1
- Connects to a Wi-Fi network

You perform a Windows AutoPilot Reset on Computer1.

What will be the state of the computer when the user signs in? To answer, select the appropriate options in the answer area.

NOTE: Each correct selection is worth one point.

The Wi-Fi connection will be:

☐
☐
☐

☐ Removed
 ☐ Retained and the passphrase will be retained
 ☐ Retained but the passphrase will be reset

App1 will be:

☐
☐
☐

☐ Reinstalled at sign-in
 ☐ Removed
 ☐ Retained

The VPN connection will be:

☐
☐
☐

☐ Removed
 ☐ Retained and the credentials will be cached
 ☐ Retained but the credentials will be reset

- A. Mastered
- B. Not Mastered

**Answer: A**

**Explanation:**

Reference:

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

#### NEW QUESTION 225

- (Exam Topic 4)

You have a Microsoft 365 subscription that contains 1,000 Android devices enrolled in Microsoft Intune. You create an app configuration policy that contains the following settings:

- Device enrollment type: Managed devices
- Profile Type: All Profile Types
- Platform: Android Enterprise

Which two types of apps can be associated with the policy? Each correct answer presents a complete solution. NOTE: Each correct selection is worth one point.

- A. Built-in Android app
- B. Managed Google Play store app
- C. Web link
- D. Android Enterprise system app
- E. Android store app

**Answer:** BD

#### NEW QUESTION 229

- (Exam Topic 4)

You have a Microsoft 365 tenant that contains the objects shown in the following table. You are creating a compliance policy named Compliance1. Which objects can you specify in Compliance1 as additional recipients of noncompliance notifications?

- A. Group3 and Group4 only
- B. Group3, Group4, and Admin1 only
- C. Group1, Group2, and Group3 only
- D. Group1, Group2, Group3, and Group4 only
- E. Group1, Group2, Group3, Group4, and Admin1

**Answer:** C

#### Explanation:

Reference:

<https://www.ravenswoodtechnology.com/microsoft-intune-compliance-notifications/> <https://docs.microsoft.com/en-us/microsoft-365/admin/create-groups/compare-groups?view=o365-worldwide>

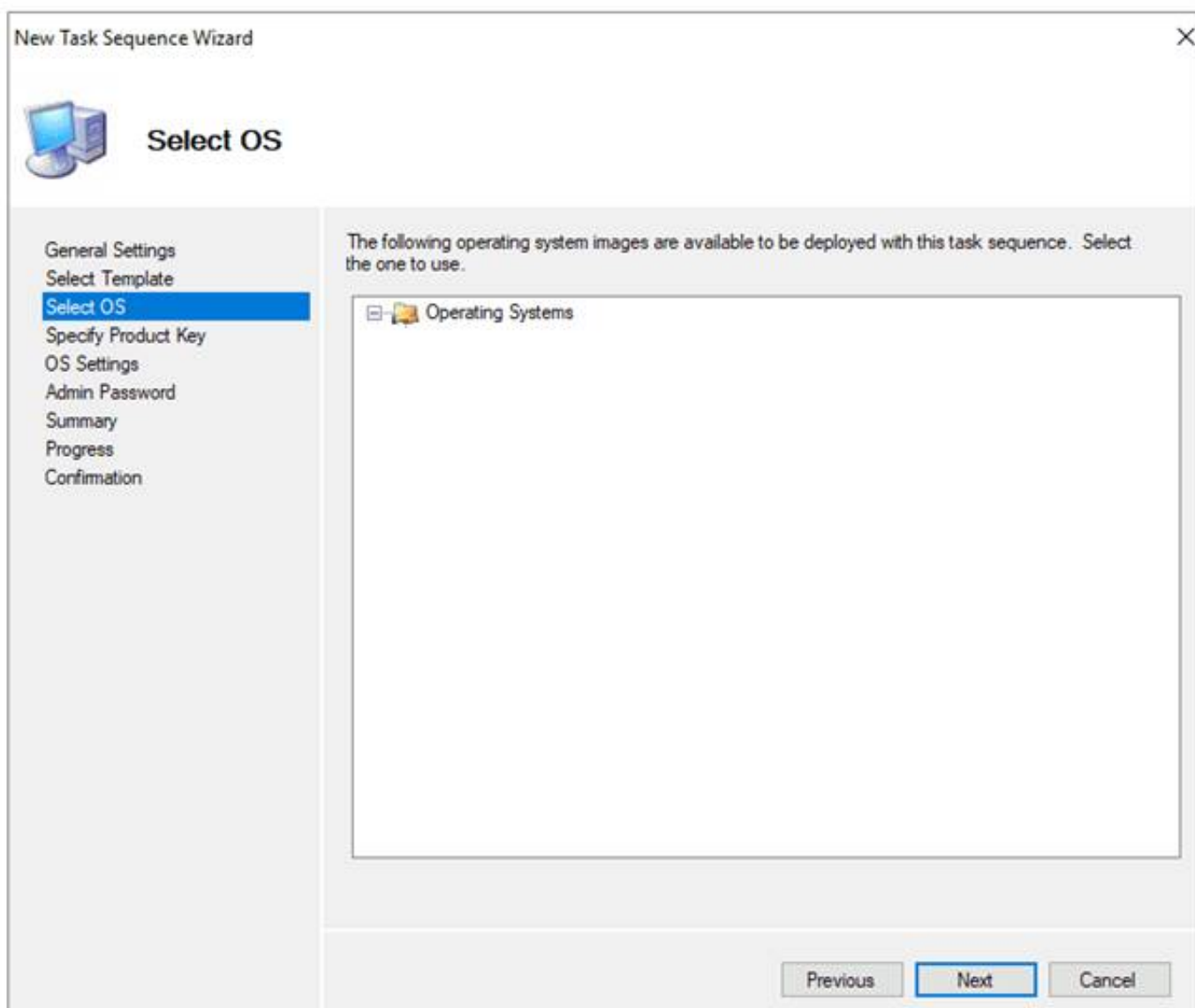
#### NEW QUESTION 234

- (Exam Topic 4)

You have a Microsoft Deployment Toolkit (MDT) deployment share.

From the Deployment Workbench, you open the New Task Sequence Wizard and select the Standard Client Upgrade Task Sequence task sequence template.

You discover that there are no operating system images listed on the Select OS page as shown in the following exhibit.



You need to be able to select an operating system image to perform a Windows 11 in-place upgrade. What should you do?

- A. Enable monitoring for the deployment share.
- B. Import a full set of source files.
- C. Import a custom image file.
- D. Run the Update Deployment Share Wizard

**Answer:** D

#### NEW QUESTION 239

- (Exam Topic 4)

You have a Microsoft 365 tenant that contains the objects shown in the following table.

Name	Type
Admin1	User
Group1	Microsoft 365 group
Group2	Distribution group
Group3	Mail-enabled security group
Group4	Security group

In the Microsoft Intune admin center, you are creating a Microsoft 365 Apps app named App1. To which objects can you assign App1?

- A. Group3 and Group4 only
- B. Admin1, Group3, and Group4 only
- C. Group1, Group3, and Group4 only
- D. Group1, Group2, Group3, and Group4 only
- E. Admin1, Group1, Group2, Group3, and Group4

**Answer: C**

**Explanation:**

In the Microsoft Intune admin center, you can assign apps to users or devices. Users can be assigned to apps by using user groups or individual user accounts. Devices can be assigned to apps by using device groups. In this scenario, the objects shown in the table are as follows:

- Admin1 is an individual user account that belongs to the Global administrators
- Group1 is a user group that contains 100 users.
- Group2 is a device group that contains 50 devices.
- Group3 is a user group that contains 200 users.
- Group4 is a device group that contains 150 devices.

role group.

Since App1 is a Microsoft 365 Apps app, it can only be assigned to users, not devices. Therefore, Group2 and Group4 are not valid objects for app assignment. Admin1 is also not a valid object for app assignment, because individual user accounts can only be used for testing purposes, not for production deployment. Therefore, the only valid objects for app assignment are Group1 and Group3, which are user groups.

**NEW QUESTION 241**

- (Exam Topic 4)

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.

**This site is not secure**

This might mean that someone's trying to fool you or steal any info you send to the server. You should close this site immediately.

 [Go to your Start page](#)

Details

Your PC doesn't trust this website's security certificate.

Error Code: DLG\_FLAGS\_INVALID\_CA

**Go on to the webpage** (Not recommended)

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 243**

- (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	Answer Area
Device Health	Requires BitLocker: <input type="text"/>
Device Properties	Requires a minimum operating system version: <input type="text"/>
Microsoft Defender for Endpoint	
System Security	

- A. Mastered  
B. Not Mastered

**Answer:** A

**Explanation:**

Settings	Answer Area
Device Health	Requires BitLocker: System Security
Device Properties	Requires a minimum operating system version: Device Properties
Microsoft Defender for Endpoint	
System Security	

#### NEW QUESTION 248

- (Exam Topic 4)

You have a Microsoft 365 E5 subscription that uses Microsoft Intune.

You add apps to Intune as shown in the following table.

Name	App type
App1	Android store app
App2	Android line-of-business app
App3	Managed Google Play app

You need to create an app configuration policy named Policy1 for the Android Enterprise platform. Which apps can you manage by using Policy1?

- A. App2 only  
B. App3 only  
C. App1 and App3 only  
D. App2 and App3 only  
E. App1, App2, and App3

**Answer:** D

#### NEW QUESTION 251

- (Exam Topic 4)

Your network contains an on-premises Active Directory domain named contoso.com that syncs to Azure AD. A user named User1 uses the domain-joined devices shown in the following table.

Name	Operating system
Device1	Windows 10 Pro
Device2	Windows 11 Pro

In the Microsoft Entra admin center, you assign a Windows 11 Enterprise E5 license to User1. You need to identify what will occur when User1 next signs in to the devices.

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

Answer Area

Device1: Will activate as Windows 11 Enterprise  
Will activate as Windows 11 Enterprise  
Will not upgrade to Windows 11 Enterprise  
Will perform a clean installation of Windows 11 Enterprise  
Will perform an in-place upgrade to Windows 11 Enterprise

Device2: Will not upgrade to Windows 11 Enterprise  
Will activate as Windows 11 Enterprise  
Will not upgrade to Windows 11 Enterprise  
Will perform a clean installation of Windows 11 Enterprise  
Will perform an in-place upgrade to Windows 11 Enterprise

- A. Mastered  
B. Not Mastered

Answer: A

**Explanation:**

Device 1:

- > Will activate as Windows 11 Enterprise. According to Deploy Windows Enterprise licenses, Windo 11 Enterprise E5 license is a subscription license that can be assigned to users who have a supported and licensed version of Windows 10 Pro or Windows 11 Pro. Device 1 has Windows 11 Pro, so it meets the requirement. When User1 signs in to Device 1 with their Azure AD account, the device will automatically activate as Windows 11 Enterprise without changing the edition.
- > Will not activate as Windows 11 Enterprise. According to Deploy Windows Enterprise licenses, Windows 11 Enterprise E5 license is a subscription license that can be assigned to users who have a supported and licensed version of Windows 10 Pro or Windows 11 Pro. Device 2 has Windows 10 Home, so it does not meet the requirement. When User1 signs in to Device 2 with their Azure AD account, the device will not activate as Windows 11 Enterprise by subscription.

**NEW QUESTION 256**

- (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"/>

- A. Mastered  
B. Not Mastered

Answer: A

**Explanation:**

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

**NEW QUESTION 258**

- (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 261**

- (Exam Topic 4)

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 262**

- (Exam Topic 4)

You have a Microsoft 365 subscription that uses Microsoft Intune. You have five new Windows 11 Pro devices.

You need to prepare the devices for corporate use. The solution must meet the following requirements:

- Install Windows 11 Enterprise on each device.
- Install a Windows Installer (MSI) package named App1 on each device.
- Add a certificate named Certificate1 that is required by App1.
- Join each device to Azure AD.

Which three provisioning options can you use? Each correct answer presents a complete solution. NOTE: Each correct selection is worth one point.

- A. subscription activation
- B. a custom Windows image
- C. an in-place upgrade
- D. Windows Autopilot
- E. provisioning packages

**Answer:** BDE

**NEW QUESTION 266**

- (Exam Topic 4)

You have a Microsoft 365 subscription that includes Microsoft Intune.

You have an update ring named UpdateRing1 that contains the following settings:

- Automatic update behavior: Auto install and restart at a scheduled time
- Automatic behavior frequency: First week of the month



- Scheduled install day: Tuesday
- Scheduled install time: 3 AM

From the Microsoft Intune admin center, you select Uninstall for the feature updates of UpdateRing1. When will devices start to remove the feature updates?

- A. when a user approves the uninstall
- B. as soon as the policy is received
- C. next Tuesday
- D. the first Tuesday of the next month

**Answer: C**

#### NEW QUESTION 268

- (Exam Topic 4)

You have 200 computers that run Windows 10. The computers are joined to Azure AD and enrolled in Microsoft Intune. You need to set a custom image as the wallpaper and sign-in screen.

Which two settings should you configure in the Device restrictions configuration profile? To answer, select the appropriate settings in the answer area.

NOTE: Each correct selection is worth one point.

**Answer Area**

**Device restrictions**  
Windows 10 and later

1 Basics 2 **Configuration settings** 3 Assignments 4 Applicability Rules 5 Review + create

- App Store
- Cellular and connectivity
- Cloud and Storage
- Cloud Printer
- Control Panel and Settings
- Display
- General
- Locked Screen Experience** ✓
- Messaging
- Microsoft Edge Browser
- Network proxy
- Password
- Per-app privacy exceptions
- Personalization** ✓
- Printer
- Privacy
- Projection

Previous Next

- A. Mastered
- B. Not Mastered

**Answer: A**

**Explanation:**



Answer Area

## Device restrictions

Windows 10 and later

✓ Basics

**2 Configuration settings**

3 Assignments

4 Applicability Rules

5 Review + create

✓ App Store

✓ Cellular and connectivity

✓ Cloud and Storage

✓ Cloud Printer

✓ Control Panel and Settings

✓ Display

✓ General

**✓ Locked Screen Experience**

✓ Messaging

✓ Microsoft Edge Browser

✓ Network proxy

✓ Password

✓ Per-app privacy exceptions

**✓ Personalization**

✓ Printer

✓ Privacy

✓ Projection

Previous

Next

### NEW QUESTION 271

- (Exam Topic 4)

You have a Microsoft Intune subscription that has the following device compliance policy settings: Mark devices with no compliance policy assigned as: Compliant  
Compliance status validity period (days): 14

On January 1, you enroll Windows 10 devices in Intune as shown in the following table.

Name	BitLocker Drive Encryption (BitLocker)	Firewall	Scope (Tags)	Member of
Device1	Enabled	Off	Tag1	Group1
Device2	Disabled	On	Tag2	Group2

On January 4, you create the following two device compliance policies:

- Name: Policy1
- Platform: Windows 10 and later
- Require BitLocker: Require
- Mark device noncompliant: 5 days after noncompliance
- Scope (Tags): Tag1
- Name: Policy2
- Platform: Windows 10 and later
- Firewall: Require
- Mark device noncompliant: Immediately
- Scope (Tags): Tag2

On January 5, you assign Policy1 and Policy2 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
On January 7, Device1 is marked as compliant.	<input type="radio"/>	<input type="radio"/>
On January 8, Device1 is marked as compliant.	<input type="radio"/>	<input type="radio"/>
On January 8, Device2 is marked as compliant.	<input type="radio"/>	<input type="radio"/>

- A. Mastered  
B. Not Mastered

**Answer:** A

**Explanation:**

Box 1: No.

Policy1 and Policy2 apply to Group1 which Device1 is a member of. Device1 does not meet the firewall requirement in Policy2 so the device will immediately be marked as non-compliant.

Box 2: No

For the same reason as Box1. Box 3: Yes

Policy1 and Policy2 apply to Group1. Device2 is not a member of Group1 so the policies don't apply.

The Scope (tags) have nothing to do with whether the policy is applied or not. The tags are used in RBAC.

**NEW QUESTION 273**

- (Exam Topic 4)

Your network contains an Active Directory domain. The domain contains a computer named Computer1 that runs Windows 11. You need to enable the Windows Remote Management (WinRM) service on Computer1 and perform the following configurations:

- For the WinRM service, set Startup type to Automatic.
- Create a listener that accepts requests from any IP address.
- Enable a firewall exception for WS-Management communications. Which PowerShell cmdlet should you use?

- A. Connect-WSMan  
B. Enable-PSRemoting  
C. Invoke-WSManAction  
D. Enable-PSSessionConfiguration

**Answer:** B

**NEW QUESTION 274**

- (Exam Topic 4)

You have computers that run Windows 10 and are managed by using Microsoft Intune. Users store their files in a folder named D:\Folder1.

You need to ensure that only a trusted list of applications is granted write access to D:\Folder1. What should you configure in the device configuration profile?

- A. Microsoft Defender Exploit Guard  
B. Microsoft Defender Application Guard  
C. Microsoft Defender SmartScreen  
D. Microsoft Defender Application Control

**Answer:** A

**NEW QUESTION 276**

- (Exam Topic 4)

You have a Microsoft 365 subscription that includes Microsoft Intune. You have computers that run Windows 11 as shown in the following table.

Name	Azure AD status	Intune	BitLocker Drive Encryption (BitLocker)	Firewall
Computer1	Joined	Enrolled	Disabled	Enabled
Computer2	Registered	Enrolled	Enabled	Enabled
Computer3	Registered	Not enrolled	Enabled	Disabled

You have the groups shown in the following table.

Name	Members
Group1	Computer1, Computer2
Group2	Computer3

You create and assign the compliance policies shown in the following table.

Name	Configuration	Action for noncompliance	Assignment
Policy1	Require BitLocker to be enabled on the device.	Mark device as noncompliant after 10 days.	Group1
Policy2	Require firewall to be on and monitoring.	Mark device as noncompliant immediately.	Group2

The next day, you review the compliance status of the computers.

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	<div>YesNo</div>
The compliance status of Computer1 is In grace period.	<div><div></div><div></div></div>
The compliance status of Computer2 is Compliant.	<div><div></div><div></div></div>
The compliance status of Computer3 is Not compliant.	<div><div></div><div></div></div>

- A. Mastered  
B. Not Mastered

Answer: A

Explanation:

Answer Area	
Statements	<div>YesNo</div>
The compliance status of Computer1 is In grace period.	<div><div></div><div></div></div>
The compliance status of Computer2 is Compliant.	<div><div></div><div></div></div>
The compliance status of Computer3 is Not compliant.	<div><div></div><div></div></div>

#### NEW QUESTION 281

- (Exam Topic 4)

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

You have the devices shown in the following table.

Name	Operating system	Activation type
Device1	Windows 10 Pro for Workstation	Key
Device2	Windows 11 Pro	Key
Device3	Windows 11 Pro	Subscription

Which devices can be changed to Windows 11 Enterprise by using subscription activation?

- A. Device3 only  
B. Device2 and Device3 only  
C. Device 1 and Device2 only  
D. Device1, Device2, and Device3

Answer: A

#### NEW QUESTION 283

- (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
<div>Account protection</div>	<div>DEP: <div></div></div>
<div>App &amp; browser control</div>	<div>Mandatory ASLR: <div></div></div>
<div>Device security</div>	
<div>Virus &amp; threat protection</div>	

- A. Mastered  
B. Not Mastered



**Answer:** A

**Explanation:**

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.

**NEW QUESTION 287**

- (Exam Topic 4)

You have a Microsoft 365 subscription.

Users have iOS devices that are not enrolled in Microsoft 365 Device Management.

You create an app protection policy for the Microsoft Outlook app as shown in the exhibit. (Click the Exhibit tab.)

You need to configure the policy to meet the following requirements:

- Prevent the users from using the Outlook app if the operating system version is less than 12.0.0.
- Require the users to use an alphanumeric passcode to access the Outlook app.

What should you configure in an app protection policy for each requirement? To answer, select the appropriate options in the answer area.

NOTE: Each correct selection is worth one point.

**Answer Area**

Prevent the users from using Outlook if the operating system version is less than 12.0.0:

	▼
Access requirements	
Conditional launch	
Data protection	
Scope	

Require the users to use an alphanumeric passcode to access Outlook:

	▼
Access requirements	
Conditional launch	
Data protection	
Scope	



- A. Mastered  
B. Not Mastered

**Answer:** A

**Explanation:**

References:

<https://docs.microsoft.com/en-us/intune/app-protection-policy-settings-ios>

**NEW QUESTION 291**

- (Exam Topic 4)

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 296**

- (Exam Topic 4)

Your network contains an Active Directory domain named contoso.com. The domain contains a computer named Computer1 that runs Windows 10. You have the groups shown in the following table.

Name	Type	Location
Group1	Universal distribution group	Contoso.com
Group2	Global security group	Contoso.com
Group3	Group	Computer1
Group4	Group	Computer1

Which groups can you add to Group4?

- A. Group2only  
B. Group1 and Group2 only  
C. Group2 and Group3 only  
D. Group1, Group2, and Group3

**Answer:** C

**NEW QUESTION 297**

- (Exam Topic 4)

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

You plan to create Windows 11 device builds for the marketing and research departments The solution must meet the following requirements:

- Marketing department devices must support Windows Update for Business.
- Research department devices must have support for feature update versions for up to 36 months from release. What is the minimum Windows 11 edition required for each department? To answer, select the appropriate options in the answer area.

NOTE: Each correct selection is worth one point

**Answer Area**

Marketing:

Research:

- A. Mastered  
B. Not Mastered

**Answer:** A

**Explanation:**

Answer Area

Marketing:

Windows 11 Pro

Windows 11 Enterprise

Windows 11 Pro

Windows 11 Pro for Workstations

Research:

Windows 11 Enterprise

Windows 11 Enterprise

Windows 11 Pro

Windows 11 Pro for Workstations

NEW QUESTION 302

.....

## Thank You for Trying Our Product

\* 100% Pass or Money Back

All our products come with a 90-day Money Back Guarantee.

\* One year free update

You can enjoy free update one year. 24x7 online support.

\* Trusted by Millions

We currently serve more than 30,000,000 customers.

\* Shop Securely

All transactions are protected by VeriSign!

**100% Pass Your MD-102 Exam with Our Prep Materials Via below:**

<https://www.certleader.com/MD-102-dumps.html>