Microsoft

Exam Questions MD-102

Endpoint Administrator

NEW QUESTION 1
- (Exam Topic 4)
You have computers that run Windows 11 Pro. The computers are joined to Azure AD and enrolled in Microsoft Intune. You need to upgrade the computers to Windows 11 Enterprise. What should you configure in Intune?

A. a device compliance policy
B. a device cleanup rule
C. a device enrollment policy
D. a device configuration profile

Answer: D

NEW QUESTION 2
- (Exam Topic 4)
You have an Azure AD tenant that contains the users shown in the following table.

Name	Multi-factor authentication (MFA) status
User1	Disabled
User2	Enabled

You have the devices shown in the following table.

Name	Platform
Device1	Android
Device2	iOS

You have a Conditional Access policy named CAPolicy1 that has the following settings:
• Assignments
o Users or workload identities: User 1. User1
o Cloud apps or actions: Office 365 Exchange Online o Conditions: Device platforms: Windows, iOS
• Access controls
o Grant Require multi-factor authentication
You have a Conditional Access policy named CAPolicy2 that has the following settings:
Assignments
o Users or workload identities: Used, User2 o Cloud apps or actions: Office 365 Exch
o Conditions
Device platforms: Android, iOS Filter for devices
Device matching the rule: Exclude filtered devices from policy Rule syntax: device. displayName- contains "1"
Access controls Grant Block access
For each of the following statements, select Yes if the statement is true. Otherwise, select No.

Answer Area

Statements	Yes	No
If User1 connects to Microsoft Exchange Online from Device1, the user is prompted for MFA.	☉	☉
If User2 connects to Microsoft Exchange Online from Device1, the user is prompted for MFA.	☉	☉
User2 can access Microsoft Exchange Online from Device2.	☉	☉

A. Mastered
B. Not Mastered

Answer: A

Explanation:
A screen shot of a computer Description automatically generated with low confidence

NEW QUESTION 3
- (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 4
- (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 Selected1.
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 devices2.
⪢ 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 users3.
⪢ 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 role4.
References: Manage device identities using the Microsoft Entra admin center, Windows Autopilot, Provisioning packages for Windows 10, What are security defaults?

NEW QUESTION 5
- (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 6
- (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 7
- (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**
ⓘ important information about hiding license terms	
Privacy settings ⓘ	Show / **Hide**
ⓘ The default value for diagnostic data collection has changed for devices running Windows 10, version 1903 and later. Learn more	
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 8
- (Exam Topic 4)
You have a Windows 11 capable device named Device1 that runs the 64-bit version of Windows 10 Enterprise and has Microsoft Office 2019 installed. You have the Windows 11 Enterprise images shown in the following table.

Name	Platform	Description
Image1	x64	Custom Windows 11 image that has Office 2021 installed
Image2	x64	Default Windows 11 image created by Microsoft

Which images can be used to perform an in-place upgrade of Device1?

A. image1 only
B. Image2only
C. Image1 and Image2

Answer: B

NEW QUESTION 9
- (Exam Topic 4)
You have a Microsoft 365 subscription that uses Microsoft Intune.
You plan to use Windows Autopilot to provision 25 Windows 11 devices. You need to meet the following requirements during device provisioning:
• Display the progress of app and profile deployments.
• Join the devices to Azure AD.
What should you configure to meet each requirement? To answer drag the appropriate settings to the correct requirements. Each setting may be used once, more than once, or not at all. You may need to drag the split bar between panes or scroll to view content.
NOTE: Each correct selection is worth one point.

Settings

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

Answer Area

Display the progress of app and profile deployments: [   ]

Join the devices to Azure AD: [   ]

A. Mastered
B. Not Mastered

Answer: A

Explanation:

Settings

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

Answer Area

Display the progress of app and profile deployments: | Enrollment Status Page |

Join the devices to Azure AD: | Deployment Profiles |

NEW QUESTION 10
- (Exam Topic 4)
You have a Microsoft 365 E5 subscription that contains 100 iOS devices enrolled in Microsoft Intune. You need to deploy a custom line-of-business (LOB) app to the devices by using Intune.
Which extension should you select for the app package file?

A. .intunemac
B. apk
C. jpa
D. .appx

Answer: C

Explanation:
iOS/iPadOS LOB apps: Select Line-of-business app as the app type, select the App package file, and then enter an iOS/iPadOS installation file with the extension
.ipa.
Reference:
https://docs.microsoft.com/en-us/mem/intune/apps/apps-add

NEW QUESTION 10
- (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 12
- (Exam Topic 4)
You manage 1.000 devices by using Microsoft Intune. You review the Device compliance trends report. For how long will the report display trend data?

A. 30 days
B. 60 days
C. 90 days
D. 365 days

Answer: B

Explanation:
The Device compliance trends report shows the number of devices that are compliant, noncompliant, and not evaluated over time. The report displays trend data for the last 60 days by default, but you can change the time range to view data for the last 7, 14, or 30 days as well. The report does not show data for more than 60
days. References: [Device compliance trends report]

NEW QUESTION 13
- (Exam Topic 4)
Your company uses Microsoft Defender for Endpoint Microsoft Defender for Endpoint includes the device groups shown in the following table.

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

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

computer1

Actions ∨

Domain: adatum.com
OS: Windows10 64-bit (Build 17134)
Machine IP addresses >

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

Answer Area

Computer1 will be a member of:

Group3 only
Group4 only
Grou5 only
Group3, Group4, and Group5 only

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

Group1 only
Group2 only
Group1 and Group2 only
Group1, Group2, Group3, Group4, and Group5

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 15
- (Exam Topic 4)
You have a Microsoft 365 E5 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.		
If an iPadOS update becomes available on Thursday at 2 AM, the update is installed on Device2 automatically on Thursday.		
If an iPadOS update becomes available on Friday at 10 PM, the update is installed on Device3 automatically on Sunday.		

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.		☐
If an iPadOS update becomes available on Thursday at 2 AM, the update is installed on Device2 automatically on Thursday.		☐
If an iPadOS update becomes available on Friday at 10 PM, the update is installed on Device3 automatically on Sunday.		☐

NEW QUESTION 17
- (Exam Topic 4)

You have a computer named Computed that has Windows 10 installed. You create a Windows PowerShell script named config.psl.
You need to ensure that config.psl 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 18
- (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:

Server1
Server2
Server3
Server4

Ports:

TCP 443 only
UDP 443 only
TCP 1723 only
TCP 443 and UDP 443 only
TCP 443, TCP 1723, and UDP 443

A. Mastered
B. Not Mastered

Answer: A

Explanation:
Box 1: Server4
Microsoft Tunnel is a VPN gateway solution for Microsoft Intune that runs in a container on Linux and allows access to on-premises resources from iOS/iPadOS and Android Enterprise devices using modern authentication and Conditional Access.
Box 2: TCP 443 and UDP 443 only
Some traffic goes to your public facing IP address for the Tunnel. The VPN channel will use TCP, TLS, UDP, and DTLS over port 443.
By default, port 443 is used for both TCP and UDP, but this can be customized via the Intune Saerver Configuration – Server port setting. If changing the default port (443) ensure your inbound firewall rules are adjusted to the custom port.
Incorrect:
TCP 1723 is not used.
Reference: https://docs.microsoft.com/en-us/mem/intune/protect/microsoft-tunnel-overview

NEW QUESTION 22
- (Exam Topic 4)
You have following types of devices enrolled in Microsoft Intune:
• Windows 10

• Android
• iOS
For which types of devices can you create VPN profiles in Microsoft Intune admin center?

A. Windows 10 only
B. Windows 10 and Android only
C. Windows 10 and iOS only
D. Android and iOS only
E. Windows 10, Android, and iOS

Answer: E

NEW QUESTION 27
- (Exam Topic 4)
You have a Microsoft Deployment Toolkit (MDT) deployment share named Share 1. You add Windows 10 images to Share! as shown in the following table.

Name	In WIM file	Description
Image1	Install1.wim	Default Windows 10 Pro image from the Windows 10 installation media
Image2	Install1.wim	Default Windows 10 Enterprise image from the Windows 10 installation media
Image3	Install2.wim	Default Windows 10 Pro for Workstations image from the Windows 10 installation media
Image4	Custom1.wim	Custom Windows 10 Enterprise image without any additional applications
Image5	Custom2.wim	Custom Windows 10 Enterprise image that includes custom applications

Which images can be used in the Standard Client Task Sequence, and which images can be used in the Standard Client Upgrade Task Sequence?
NOTE: Each correct selection is worth one point.

Answer Area

Standard Client Task Sequence:

Image3 only
Image3, Image4, and Image5 only
Image1, Image2, and Image3 only
Image1, Image2, Image3, and Image4 only
Image1, Image2, Image3, Image4, and Image5

Standard Client Upgrade Task Sequence:

Image3 only
Image3, Image4, and Image5 only
Image1, Image2, and Image3 only
Image1, Image2, Image3, and Image4 only
Image1, Image2, Image3, Image4, and Image5

A. Mastered
B. Not Mastered

Answer: A

Explanation:

Answer Area

Standard Client Task Sequence:	
	Image3 only
	Image3, Image4, and Image5 only
	Image1, Image2, and Image3 only
	Image1, Image2, Image3, and Image4 only
	Image1, Image2, Image3, Image4, and Image5

Standard Client Upgrade Task Sequence:	
	Image3 only
	Image3, Image4, and Image5 only
	Image1, Image2, and Image3 only
	Image1, Image2, Image3, and Image4 only
	Image1, Image2, Image3, Image4, and Image5

NEW QUESTION 28
- (Exam Topic 4)
Your network contains an on-premises Active Directory Domain Services (AD DS) domain that syncs with an Azure AD tenant.
You have a Microsoft 365 subscription
You plan to use Windows Autopilot to deploy new Windows devices. You plan to create a deployment profile.
You need to ensure that The deployment meets the following requirements:
• Devices must be joined to AD DS regardless of their current working location.
• Users in the marketing department must have a line-of-business (LOB) app installed during the deployment. The solution must minimize administrative effort.
What should you do for each requirement? To answer, select the appropriate options in the answer area. NOTE: Each correct selection is worth one point.

Answer Area

Devices must be joined to AD DS regardless of their current working location:	Install the Intune connector for Active Directory. ▼
	Deploy Always On VPN.
	Install the Intune connector for Active Directory.
	Modify the Autopilot deployment profile.
	Edit the Co-management settings in Intune.

The marketing department users must have an LOB app installed during the deployment:	Modify the Autopilot deployment profile. ▼
	Modify the Autopilot deployment profile.
	Create a Microsoft Intune app deployment.
	Create a device configuration profile in Intune.

A. Mastered
B. Not Mastered

Answer: A

Explanation:
Answer Area

Devices must be joined to AD DS regardless of their current working location:	Install the Intune connector for Active Directory. ▼
	Deploy Always On VPN.
	Install the Intune connector for Active Directory.
	Modify the Autopilot deployment profile.
	Edit the Co-management settings in Intune.

The marketing department users must have an LOB app installed during the deployment:	Modify the Autopilot deployment profile. ▼
	Modify the Autopilot deployment profile.
	Create a Microsoft Intune app deployment.
	Create a device configuration profile in Intune.

NEW QUESTION 33
- (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.

Create profile
Windows PC

✓ Basics ② Out-of-box experience (OOBE) ③ Scope tags ④ Assignments ⑤ Review + create

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

* Deployment mode ❶	User-Driven ⌄
* Join to Azure AD as ❶	Azure AD joined ⌄
Microsoft Software License Terms ❶	Show / **Hide**

Important information about hiding license terms

Privacy settings ❶	Show / **Hide**

The default value for diagnostic data collection has changed for devices running Windows 10, version 1903 and later. Learn more

Hide change account options ❶	Show / **Hide**
User account type ❶	Administrator / **Standard**
Allow White Glove OOBE ❶	**No** / Yes
Language (Region) ❶	Operating system default ⌄
Automatically configure keyboard ❶	No / **Yes**
Apply device name template ❶	**No** / Yes

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 37

- (Exam Topic 4)
Your network contains an on-premises Active Directory domain. The domain contains two computers named Computer1 and Computer? 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 Computed?

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 42
- (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.

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
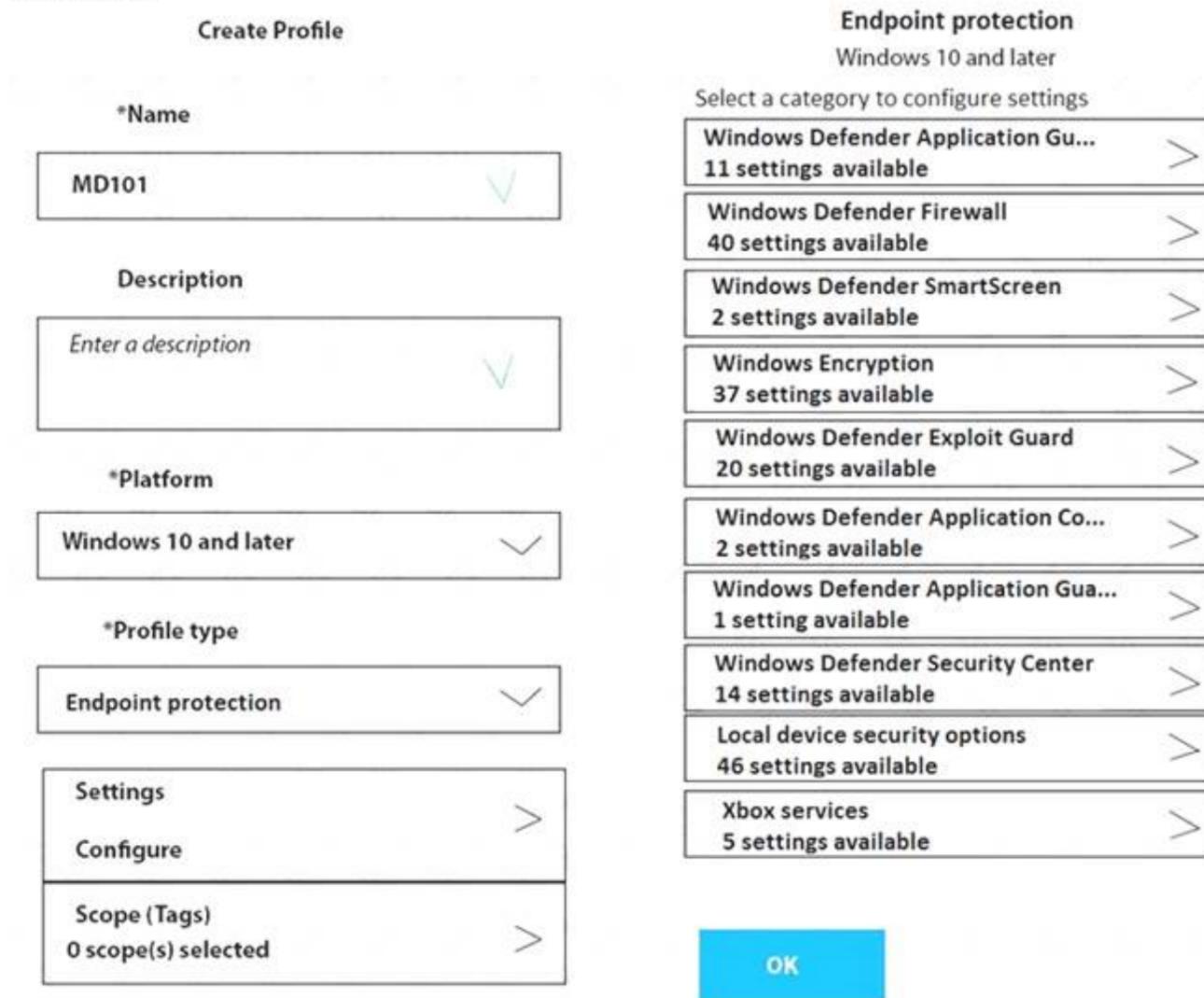
NEW QUESTION 44
- (Exam Topic 4)
You have a Microsoft 365 E5 subscription that contains 500 macOS devices enrolled in Microsoft Intune. You need to ensure that you can apply Microsoft Defender for Endpoint antivirus policies to the macOS
devices. The solution must minimize administrative effort.
What 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 45
- (Exam Topic 4)
You have a Microsoft 365 E5 subscription and 25 Apple iPads.
You need to enroll the iPads in Microsoft Intune by using the Apple Configurator enrollment method. What should you do first?

A. Upload a file that has the device identifiers for each iPad.
B. Modify the enrollment restrictions.
C. Configure an Apple MDM push certificate.
D. Add your user account as a device enrollment manager (DEM).

Answer: C

Explanation:
Reference:
https://www.manageengine.com/mobile-device-management/help/enrollment/mdm_creating_apns_certificate.ht Prerequisites for iOS enrollment Before you can enable iOS devices, complete the following steps: Make sure your device is eligible for Apple device enrollment. Set up Intune - These steps set up your Intune infrastructure. In particular, device enrollment requires that you set your MDM authority. Get an Apple MDM Push certificate - Apple requires a certificate to enable management of iOS and macOS devices.
https://docs.microsoft.com/en-gb/intune/enrollment/apple-mdm-push-certificate-get

NEW QUESTION 48
- (Exam Topic 4)
Your network contains an Active Directory domain.
You install the Microsoft Deployment Toolkit (MDT) on a server. You have a custom image of Windows 11.
You need to deploy the image to 100 devices by using MDT.
Which three actions should you perform in sequence? To answer, move answer area and arrange them in the correct order.

A. Mastered
B. Not Mastered

Answer: A

Explanation:
To deploy the Windows 11 image to 100 devices by using MDT, you should perform the following three actions in sequence:

➤ Install Windows Deployment Services (WDS) on the server. WDS is a role that enables you to deploy Windows operating systems over the network by using PXE boot and multicast technologies. You need to install WDS before you can enable multicast and configure the boot images for MDT. You can install WDS by using the Server Manager or PowerShell1.

➤ Create a deployment share on the server. A deployment share is a folder that contains the MDT files, scripts, applications, drivers, operating systems, and task sequences that you use to deploy Windows. You need to create a deployment share by using the MDT Deployment Workbench2.

➤ Add the Windows 11 image and create a task sequence in the deployment share. An image is a file that contains a snapshot of a Windows installation. A task sequence is a set of steps that MDT executes to install Windows and configure the settings. You need to add the Windows 11 image by importing it from a source folder or a WIM file, and create a task sequence by using a template or customizing your own3.
These are the basic steps to prepare for deploying Windows 11 with MDT. For more details and guidance, you can refer to the web search results I found for you by using search_web("deploy Windows 11 image with MDT").

NEW QUESTION 51
- (Exam Topic 4)
You have a Microsoft 365 E5 subscription and 100 unmanaged iPad devices.
You need to deploy a specific iOS update to the devices. Users must be prevented from manually installing a more recent version of iOS.
Which two actions should you perform? Each correct answer presents part of the solution. NOTE: Each correct selection is worth one point.

A. Enroll the devices in Microsoft Intune by using the Intune Company Portal.
B. Create a compliance policy.
C. Enroll the devices in Microsoft Intune by using Apple Business Manager.
D. Create an iOS app provisioning profile.
E. Create a device configuration profile.

Answer: CE

Explanation:
To deploy a specific iOS update to the unmanaged iPad devices, you need to perform the following actions:

➤ Enroll the devices in Microsoft Intune by using Apple Business Manager. Apple Business Manager is a service that allows you to enroll and manage iOS/iPadOS devices in bulk. You can use Apple Business Manager to assign devices to Microsoft Intune and enroll them as supervised devices. Supervised devices are devices that have more management features and restrictions than unsupervised devices. You can also use Apple Business Manager to create device groups and assign roles and permissions12.

➤ Create a device configuration profile. A device configuration profile is a policy that you can create and assign in Microsoft Intune to configure settings on your devices. You can use a device configuration profile to manage software updates for iOS/iPadOS supervised devices. You can choose to deploy the latest update or an older update, specify a schedule for the update installation, and delay the visibility of software updates on the devices34.
The other options are not correct for this scenario because:

➤ Enrolling the devices in Microsoft Intune by using the Intune Company Portal is not suitable for unmanaged devices. The Intune Company Portal is an app that users can download and install on their personal or corporate-owned devices to enroll them in Microsoft Intune. However, this method requires user interaction and consent, and does not enroll the devices as supervised devices5.

➤ Creating a compliance policy is not necessary for this scenario. A compliance policy is a policy that you can create and assign in Microsoft Intune to evaluate and enforce compliance settings on your devices. You can use a compliance policy to check if the devices meet certain requirements, such as minimum OS version, encryption, or password settings. However, a compliance policy does not deploy or manage software updates on the devices6.

➤ Creating an iOS app provisioning profile is not relevant for this scenario. An iOS app provisioning profile is a file that contains information about the app and its distribution method. You can use an iOS app provisioning profile to deploy custom or line-of-business apps to your iOS/iPadOS devices by using Microsoft Intune. However, an iOS app provisioning profile does not affect the software updates on the devices7.
References: What is Apple Business Manager?, Enroll iOS/iPadOS devices in Intune, Manage iOS/iPadOS software update policies in Intune, Software updates planning guide and scenarios for supervised iOS/iPadOS devices in Microsoft Intune, Enroll your personal device in Intune, Device compliance policies in Microsoft Intune, Add an iOS app provisioning profile with Microsoft Intune

---

NEW QUESTION 54
- (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 network contains an Active Directory domain. The domain contains a computer named Computer1 that runs Windows 8.1.
Computer1 has apps that are compatible with Windows 10.
You need to perform a Windows 10 in-place upgrade on Computer1.
Solution: You copy the Windows 10 installation media to a Microsoft Deployment Toolkit (MDT) deployment
share. You create a task sequence, and then you run the MDT deployment wizard on Computer1. Does this meet the goal?

A. Yes
B. No

Answer: B

NEW QUESTION 57
- (Exam Topic 4)
You have devices enrolled in Microsoft Intune as shown in the following table.

Name	Platform
Device1	Windows 10
Device2	Windows 11
Device3	Android
Device4	iOS

On which devices can you apply app configuration policies?

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

Answer: D

Explanation:
The correct answer is D because app configuration policies can be applied to managed devices and managed apps1. Managed devices are enrolled and managed by Intune, while managed apps are integrated with Intune App SDK or wrapped using the Intune Wrapping Tool1. Device2, Device3, and Device4 are either enrolled in Intune or have managed apps installed, so they can receive app configuration policies2. Device1 is not enrolled in any MDM solution and does not have any managed apps installed, so it cannot receive app configuration policies2. References: 1: App configuration policies for Microsoft Intune | Microsoft Learn https://learn.microsoft.com/en-us/mem/intune/apps/app-configuration-policies-overview 2: Policy sets - Microsoft Intune | Microsoft Learn https://learn.microsoft.com/en-us/mem/intune/fundamentals/policy-sets

---

NEW QUESTION 60
- (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 62
- (Exam Topic 4)
You have a server named Server1 and computers that run Windows 8.1. Server1 has the Microsoft Deployment Toolkit (MDT) installed.
You plan to upgrade the Windows 8.1 computers to Windows 10 by using the MDT deployment wizard. You need to create a deployment share on Server1.
What should you do on Server1, and what are the minimum components you should add to the MDT deployment share? To answer, select the appropriate options in the answer area.
NOTE: Each correct selection is worth one point.

Answer Area

On Server1:	
	Import the Deployment Image Servicing and Management (DISM) PowerShell module.
	Import the WindowsAutopilotIntune Windows PowerShell module.
	Install the Windows Assessment and Deployment Kit (Windows ADK).
	Install the Windows Deployment Services server role.

Add to the MDT deployment share:	
	Windows 10 image and package only
	Windows 10 image and task sequence only
	Windows 10 image only
	Windows 10 image, task sequence, and package

A. Mastered
B. Not Mastered

Answer: A

Explanation:
Box 1: Install the Windows Deployment Services role. Install and initialize Windows Deployment Services (WDS) On the server:
Open an elevated Windows PowerShell prompt and enter the following command: Install-WindowsFeature -Name WDS -IncludeManagementTools
WDSUTIL /Verbose /Progress /Initialize-Server /Server:MDT01 /RemInst:"D:\RemoteInstall" WDSUTIL /Set-Server /AnswerClients:All
Box 2: Windows 10 image and task sequence only Create the reference image task sequence
In order to build and capture your Windows 10 reference image for deployment using MDT, you will create a task sequence.
Reference:
https://docs.microsoft.com/en-us/windows/deployment/deploy-windows-mdt/prepare-for-windows-deployment
https://docs.microsoft.com/en-us/windows/deployment/deploy-windows-mdt/create-a-windows-10-reference-im

NEW QUESTION 64
- (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 66
- (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 70
- (Exam Topic 2)
You need to meet the technical requirements for Windows AutoPilot.
Which two settings should you configure from the Azure Active Directory blade? To answer, select the appropriate settings in the answer area.
NOTE: Each correct selection is worth one point.

A. Mastered
B. Not Mastered

Answer: A

Explanation:
References:
https://docs.microsoft.com/en-us/windows/deployment/windows-autopilot/windows-autopilot-reset
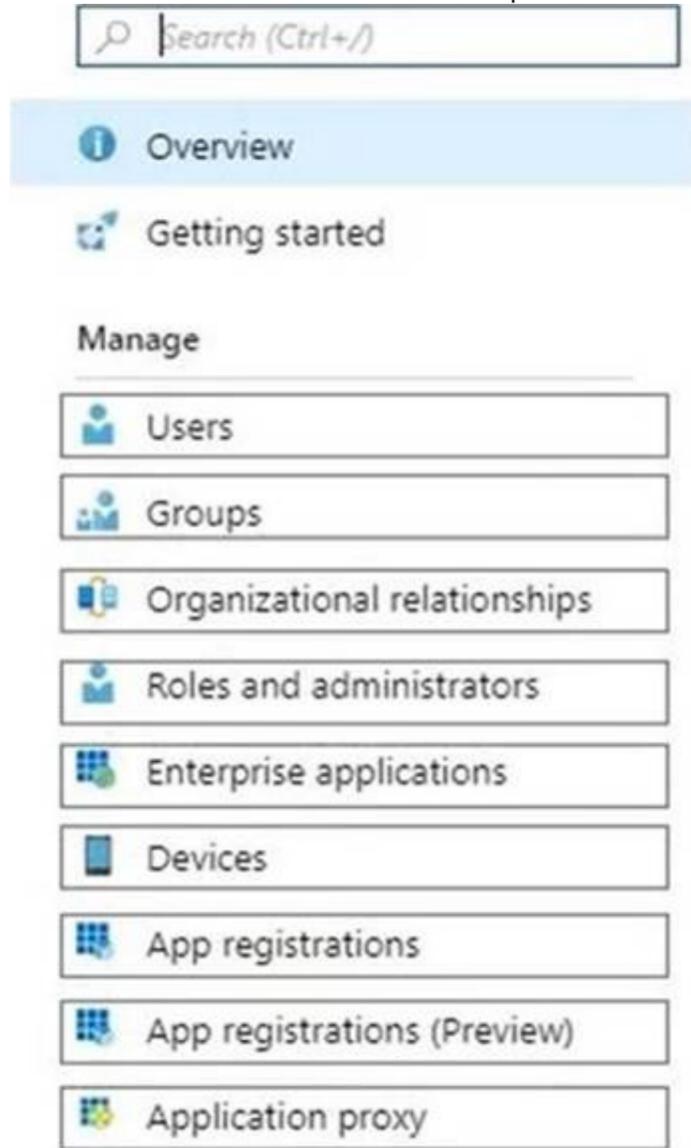
NEW QUESTION 71
- (Exam Topic 1)
User1 and User2 plan to use Sync your settings.
On which devices can the users use Sync your settings? To answer, select the appropriate options in the answer area.
NOTE: Each correct selection is worth one point.

Answer Area

User1:
- No devices
- Device4 and Device5 only
- Device1, Device2 and Device3 only
- Device1, Device2, Device3, Device4, and Device5

User2:
- No devices
- Device4 and Device5 only
- Device1, Device2 and Device3 only
- Device1, Device2, Device3, Device4, and Device5

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 74
- (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 77
- (Exam Topic 1)
For each of the following statements, select Yes if the statement is true. Otherwise, select No.
NOTE: Each correct selection is worth one point.

Statements	Yes	No
Device1 is marked as compliant.	○	○
Device4 is marked as compliant.	○	○
Device5 is marked as compliant.	○	○

A. Mastered
B. Not Mastered

Answer: A

Explanation:
Text Description automatically generated

NEW QUESTION 80
- (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 81
- (Exam Topic 4)
Your network contains an Active Directory domain. Active Directory is synced with Microsoft Azure Active
Directory (Azure AD).
There are 500 Active Directory domain-joined computers that run Windows 10 and are enrolled in Microsoft Intune.
You plan to implement Microsoft Defender Exploit Guard.
You need to create a custom Microsoft Defender Exploit Guard policy, and then distribute the policy to all the computers.

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

Answer Area

Tool to use to configure the settings: ▼

| Security & Compliance in Microsoft 365 |
| Windows Security app |
| Microsoft Endpoint Manager admin center |

Distribution method: ▼

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

A. Mastered
B. Not Mastered

Answer: A

Explanation:
A screenshot of a computer Description automatically generated
Reference:
https://docs.microsoft.com/en-us/windows/security/threat-protection/microsoft-defender-atp/import-export-expl https://docs.microsoft.com/en-us/intune/endpoint-protection-windows-10
https://docs.microsoft.com/en-us/windows/security/threat-protection/microsoft-defender-atp/enable-exploit-prot

NEW QUESTION 84
- (Exam Topic 4)
You have a Microsoft 365 tenant that uses Microsoft Intune to manage personal and corporate devices. The tenant contains three Windows 10 devices as shown in the following exhibit.

Name	Enabled	OS	Version	Join Type	Owner	MDM	Compliant
LON-CL2	✔ Yes	Windows	10.0.17763.615	Azure AD registered	User2	Microsoft Intune	✔ Yes
LON-CL4	✔ Yes	Windows	10.0.17763.107	Azure AD joined	User1	Microsoft Intune	✔ Yes

How will Intune classify each device after the devices are enrolled in Intune automatically? To answer, select the appropriate options in the answer area.
NOTE: Each correct selection is worth one point.

Answer Area

Identified by Intune as a personal device: ▼

| LON-CL2 only |
| LON-CL4 only |
| Both LON-CL2 and LON-CL4 |
| Neither LON-CL2 or LON-CL4 |

Identified by Intune as a corporate device: ▼

| LON-CL2 only |
| LON-CL4 only |
| Both LON-CL2 and LON-CL4 |
| Neither LON-CL2 or LON-CL4 |

A. Mastered
B. Not Mastered

Answer: A

Explanation:
Table Description automatically generated
Reference:
https://docs.microsoft.com/en-us/azure/active-directory/devices/concept-azure-ad-join https://docs.microsoft.com/en-us/azure/active-directory/devices/concept-azure-ad-register

NEW QUESTION 87
- (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 89
- (Exam Topic 4)
You have a Microsoft 365 subscription that uses Microsoft Intune and contains the users shown in the following table.

Name	Member of	License
User1	Group1	None
User2	Group1	Microsoft 365 E3
User3	Group2	Microsoft 365 E5

Group2 has been assigned in the Enrollment Status Page. You have the devices shown in the following table.

Name	Operating system	Department
Device1	Windows 10 Pro	Marketing
Device2	Windows 11 Home	Research
Device3	Windows 10 Pro	Marketing

You capture and upload the hardware IDs of the devices in the marketing department. You configure Windows Autopilot.
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 complete the Autopilot process on Device1.		
User2 can complete the Autopilot process on Device1.		
User3 can view device setup information during the enrollment phase of Device1.		

A. Mastered
B. Not Mastered

Answer: A

Explanation:
Answer Area

Statements	Yes	No
User1 can complete the Autopilot process on Device1.		☐
User2 can complete the Autopilot process on Device1.	☐	
User3 can view device setup information during the enrollment phase of Device1.		☐

NEW QUESTION 92
- (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 96
- (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	Not applicable	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	Not applicable

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.	○	○
Device2 is marked as compliant.	○	○
Device3 is marked as compliant.	○	○

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 97
- (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 100
- (Exam Topic 4)
You have an Azure AD tenant named contoso.com that contains a user named Used. User! 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
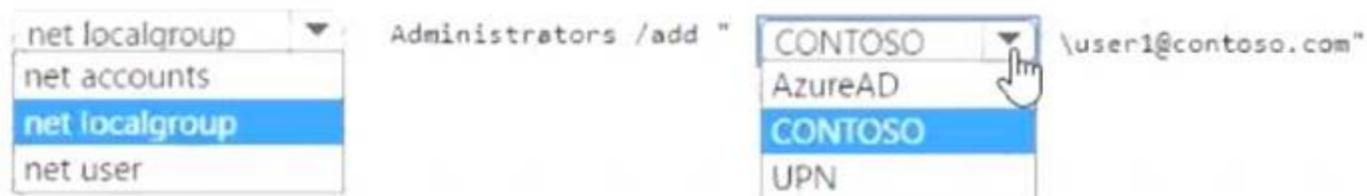
A. Mastered
B. Not Mastered

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 101
- (Exam Topic 4)
You have a hybrid deployment of Azure AD that contains 50 Windows 10 devices. All the devices are enrolled in Microsoft Intune.
You discover that Group Policy settings override the settings configured in Microsoft Intune policies. You need to ensure that the settings configured in Microsoft Intune override the Group Policy settings. What should you do?

A. From Group Policy Management Editor, configure the Computer Configuration settings in the Default Domain Policy.
B. From the Microsoft Intune admin center, create a custom device profile.
C. From the Microsoft Intune admin center, create an Administrative Templates device profile.
D. From Group Policy Management Editor, configure the User Configuration settings in the Default Domain Policy.

Answer: C

NEW QUESTION 106
- (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: [Device restriction ▼]
- Delivery optimization
- **Device restriction**
- Endpoint protection
- Identity protection

Rename the local Administrator account: [Identity protection ▼]
- **Delivery optimization**
- Device restriction
- Endpoint protection
- **Identity protection**

A. Mastered
B. Not Mastered

Answer: A

Explanation:

Answer Area

Deploy a custom Start layout: [Device restriction ▼]
- Delivery optimization
- **Device restriction**
- Endpoint protection
- Identity protection

Rename the local Administrator account: [Identity protection ▼]
- **Delivery optimization**
- Device restriction
- Endpoint protection
- **Identity protection**

NEW QUESTION 107
- (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 111
- (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   🔵 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.	○	○
If Device2 starts in Out of Box Experience (OOBE) mode, the device will be deployed by using Autopilot.	○	○
If Device3 starts in Out of Box Experience (OOBE) mode, the device will be deployed by using	○	○

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 115
- (Exam Topic 4)
You have a Microsoft 365 E5 subscription.
You create a new update rings policy named Policy1 as shown in the following exhibit.

Update ring settings Edit

Update settings	
Microsoft product updates	Allow
Windows drivers	Allow
Quality update deferral period (days)	0
Feature update deferral period (days)	30
Upgrade Windows 10 devices to Latest Windows 11 release	No
Set feature update uninstall period (2 - 60 days)	10
Servicing channel	General Availability channel

User experience settings	
Automatic update behavior	Auto install at maintenance time
Active hours start	8 AM
Active hours end	5 PM
Restart checks	Allow
Option to pause Windows updates	Enable
Option to check for Windows updates	Enable
Change notification update level	Use the default Windows Update notifications
Use deadline settings	Allow
Deadline for feature updates	30
Deadline for quality updates	0
Grace period	0
Auto reboot before deadline	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

Updates that contain fixes and improvements to existing Windows functionality [answer choice].

- can be deferred for 30 days ▼
  - can be deferred indefinitely
  - can be deferred for 30 days
  - will be installed immediately

Updates that contain new Windows functionality will be installed within [answer choice] of release.

- 1 day ▼
  - 1 day
  - 30 days
  - 60 days

A. Mastered
B. Not Mastered

Answer: A

Explanation:
*Updates that contain fixes and improvements to existing Windows functionality can be deferred for 30 days. This is because the update rings policy named Policy1 has the "Quality updates deferral period (days)" setting set to 30. This means that quality updates, which include fixes and improvements to existing Windows functionality, can be deferred for up to 30 days from the date they are released by Microsoft. After 30 days, the devices will automatically install the quality updates. References:
https://docs.microsoft.com/en-us/mem/intune/protect/windows-update-for-business-configure
*Updates that contain new Windows functionality will be installed within 60 days of release.
This is because the update rings policy named Policy1 has the "Feature updates deferral period (days)" setting set to 60. This means that feature updates, which include new Windows functionality, can be deferred for up to 60 days from the date they are released by Microsoft. After 60 days, the devices will automatically install the feature updates. References:
https://docs.microsoft.com/en-us/mem/intune/protect/windows-update-for-business-configure

NEW QUESTION 120
- (Exam Topic 4)
You have an on-premises server named Server! that hosts a Microsoft Deployment Toolkit (MDT) deployment share named MDT1. You need to ensure that MDT1 supports multicast deployments. What should you install on Server1?

A. Multipath I/O (MPIO)
B. Multipoint Connector
C. Windows Deployment Services (WDS)
D. Windows Server Update Services (WSUS)

Answer: C

NEW QUESTION 125
- (Exam Topic 4)
You use the Microsoft Deployment Toolkit (MDT) to deploy Windows 11.
You create a new task sequence by using the Standard Client Task Sequence template to deploy Windows 11 Enterprise to new computers. The computers have a single hard disk.
You need to modify the task sequence to create a system volume and a data volume.
Which phase should you modify in the task sequence?

A. Initialization
B. State Restore
C. Preinstall
D. Postinstall

Answer: C

NEW QUESTION 128
- (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.
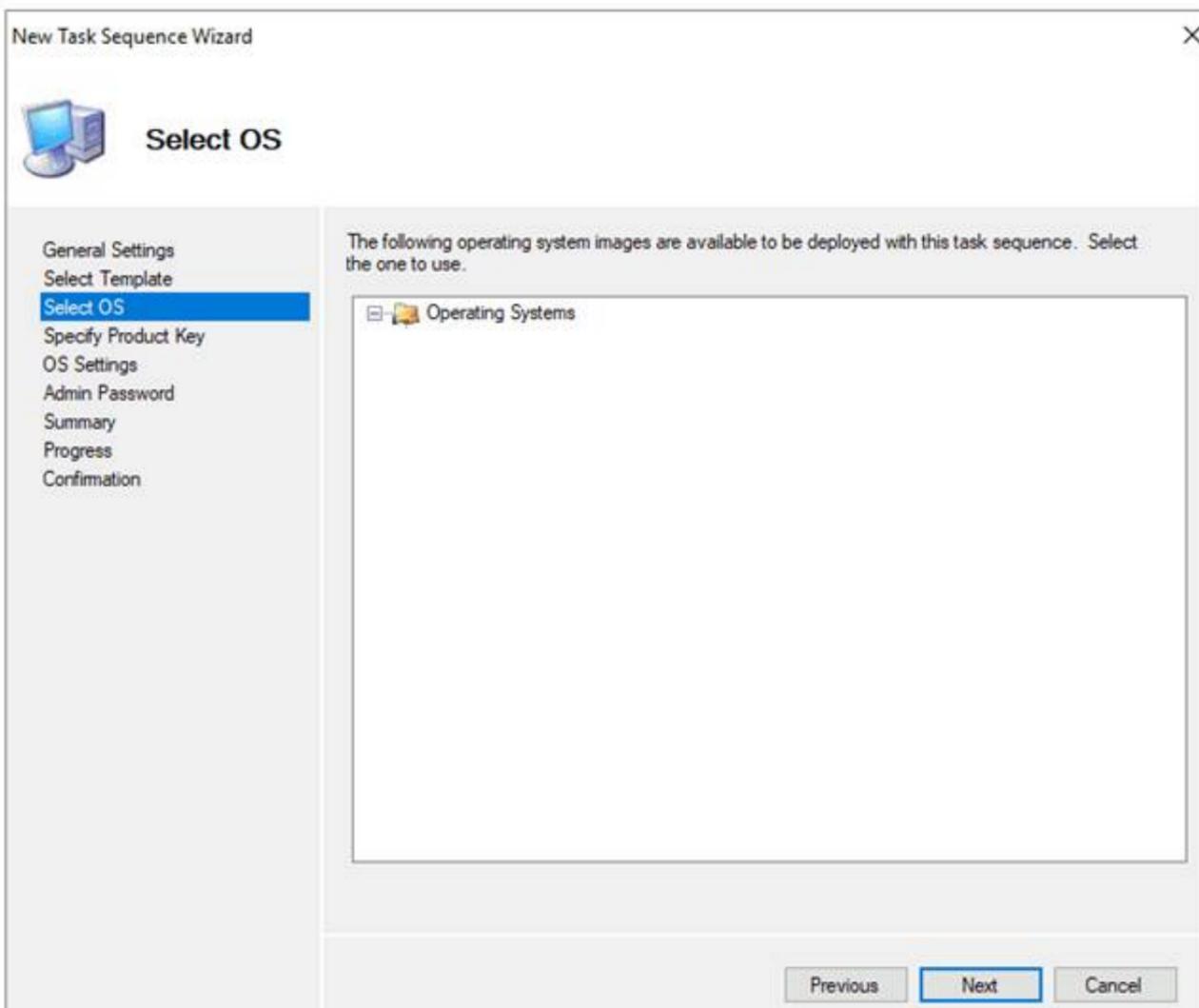
You need to be able to select an operating system image to perform a Windows 11 in-place upgrade. What should you do?

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 132
- (Exam Topic 4)
You have a Microsoft 365 ES subscription that uses Microsoft Intune. You have the apps shown in the following exhibit.

Use the drop-down menus to select the answer choice that completes each statement based upon the information presented in the graphic.

NOTE: Each correct selection is worth one point.

A. Mastered
B. Not Mastered

Answer: A

Explanation:

NEW QUESTION 136
- (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,

A. Mastered
B. Not Mastered

Answer: A

Explanation:

NEW QUESTION 137
- (Exam Topic 4)
You have 200 computers that run Windows 10 and are joined to an Active Directory domain.
You need to enable Windows Remote Management (WinRM) on all the computers by using Group Policy. Which three actions should you perform? Each correct answer presents part of the solution.
NOTE: Each correct selection is worth one point.

A. Enable the Allow Remote Shell access setting.
B. Enable the Allow remote server management through WinRM setting.
C. Set the Startup Type of the Windows Remote Management (WS-Management) service to Automatic.
D. Enable the Windows Defender Firewall: Allow inbound Remote Desktop exceptions setting.
E. Set the Startup Type of the Remote Registry service to Automatic
F. Enable the Windows Defender Firewall: Allow inbound remote administration exception setting.

Answer: BCF

Explanation:
To enable WinRM on domain computers using Group Policy, you need to perform the following actions:

> Enable the Allow remote server management through WinRM setting under Computer Configuration > Policies > Administrative Templates > Windows Components > Windows Remote Management (WinRM) > WinRM Service. This setting allows you to specify the IP address ranges that can connect to the WinRM service.

> Set the Startup Type of the Windows Remote Management (WS-Management) service to Automatic under Computer Configuration > Preferences > Control Panel Settings > Services. This setting ensures that the WinRM service starts automatically on the computers.

> Enable the Windows Defender Firewall: Allow inbound remote administration exception setting under Computer Configuration > Policies > Security Settings > Windows Firewall and Advanced Security > Windows Firewall and Advanced Security > Inbound Rules. This setting creates a firewall rule that allows incoming TCP connections on port 5985 for WinRM. References: How to Enable WinRM via Group Policy, Installation and configuration for Windows Remote Management

NEW QUESTION 142
- (Exam Topic 4)
You have a Microsoft 365 E5 subscription that contains a user named User1. You need to perform the following tasks for User1:

> Set the Usage location to Canada.

> Configure the Phone and Email authentication contact info for self-service password reset (SSPR). Which two settings should you configure in the Azure Active Directory admin center? To answer, select the
appropriate settings in the answer area.
NOTE: Each correct selection is worth one point.

Manage

👤	Profile
🟦	Custom security attributes (Preview)
👥	Assigned roles
🖥	Administrative units
👥	Groups
▦	Applications
👤	Licenses
🖥	Devices
🔑	Azure role assignments
🛡	Authentication methods

A. Mastered
B. Not Mastered

Answer: A

Explanation:
Graphical user interface, application Description automatically generated

NEW QUESTION 144
- (Exam Topic 4)
Your network contains an on-premises Active Directory domain and an Azure AD tenant.
The Default Domain Policy Group Policy Object (GPO) contains the settings shown in the following table.

Name	GPO value
LockoutBadCount	0
MaximumPasswordAge	42
MinimumPasswordAge	1
MinimumPasswordLength	7
PasswordComplexity	True
PasswordHistorySize	24

Which device configuration profile type template should you use?

A. Administrative Templates
B. Endpoint protection
C. Device restrictions
D. Custom

Answer: A

Explanation:
To configure the settings shown in the table, you need to use the Administrative Templates device configuration profile type template. This template allows you to configure hundreds of settings that are also available in Group Policy. You can use this template to configure settings such as password policies, account lockout policies, and audit policies. References:
https://docs.microsoft.com/en-us/mem/intune/configuration/administrative-templates-windows

NEW QUESTION 147
- (Exam Topic 4)
You install a feature update on a computer that runs Windows 10. How many days do you have to roll back the update?

A. 5
B. 10

C. 14
D. 30

Answer: B

NEW QUESTION 149
- (Exam Topic 4)
You use Microsoft Endpoint Manager to manage Windows 10 devices.
You are designing a reporting solution that will provide reports on the following:

> Compliance policy trends

> Trends in device and user enrolment

> App and operating system version breakdowns of mobile devices

You need to recommend a data source and a data visualization tool for the design.
What should you recommend? To answer, select the appropriate options in the answer area. NOTE: Each correct selection is worth one point.

Answer Area

Data source:
- Audit logs in Azure Active Directory (Azure AD)
- Audit logs in Microsoft Intune
- Azure Synapse Analytics
- The Microsoft Intune Data Warehouse

Data visualization tool:
- Azure Data Studio
- Microsoft Power BI
- The Azure portal

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/developer/reports-nav-create-intune-reports https://docs.microsoft.com/en-us/mem/intune/developer/reports-proc-get-a-link-powerbi

NEW QUESTION 153
- (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 155
- (Exam Topic 4)
You have a hybrid Azure AD tenant.
You configure a Windows Autopilot deployment profile as shown in the following exhibit.

Create profile
Windows PC

✓ Basics ② Out-of-box experience (OOBE) ③ Scope tags ④ Assignments ⑤ Review + create

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

* Deployment mode ❶	User-Driven ⌄
* Join to Azure AD as ❶	Azure AD joined ⌄
Microsoft Software License Terms ❶	Show / **Hide**

❶ Important information about hiding license terms

Privacy settings ❶	Show / **Hide**

❶ The default value for diagnostic data collection has changed for devices running Windows 10, version 1903 and later. Learn more

Hide change account options ❶	Show / **Hide**
User account type ❶	Administrator / **Standard**
Allow White Glove OOBE ❶	**No** / Yes
Apply device name template ❶	**No** / Yes

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

To apply the profile to a new computer, you must first
- join the device to Azure AD
- enroll the device in Microsoft Intune
- import a CSV file into Windows Autopilot

When the Windows Autopilot profile is applied to a computer, the computer will be
- joined to Azure AD only
- registered in Azure AD only
- joined to Active Directory only
- joined to Active Directory and registered in Azure AD

A. Mastered
B. Not Mastered

Answer: A

Explanation:

Answer Area

To apply the profile to a new computer, you must first
- join the device to Azure AD
- enroll the device in Microsoft Intune
- **import a CSV file into Windows Autopilot**

When the Windows Autopilot profile is applied to a computer, the computer will be
- joined to Azure AD only
- registered in Azure AD only
- joined to Active Directory only
- **joined to Active Directory and registered in Azure AD**

NEW QUESTION 157
- (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 159
......

Thank You for Trying Our Product

We offer two products:

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

2nd - Questons and Answers in PDF Format

MD-102 Practice Exam Features:

* MD-102 Questions and Answers Updated Frequently

* MD-102 Practice Questions Verified by Expert Senior Certified Staff

* MD-102 Most Realistic Questions that Guarantee you a Pass on Your FirstTry

* MD-102 Practice Test Questions in Multiple Choice Formats and Updatesfor 1 Year

100% Actual & Verified — Instant Download, Please Click
Order The MD-102 Practice Test Here