Exam Questions MD-102

Endpoint Administrator

https://www.2passeasy.com/dumps/MD-102/

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)
Your network contains an Active Directory domain named contoso.com. The domain contains two computers named Computer! and Computer2 that run Windows 10. On Computer1, you need to run the
Invoke-Command cmdlet to execute several PowerShell commands on Computed. What should you do first?

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

Answer: C

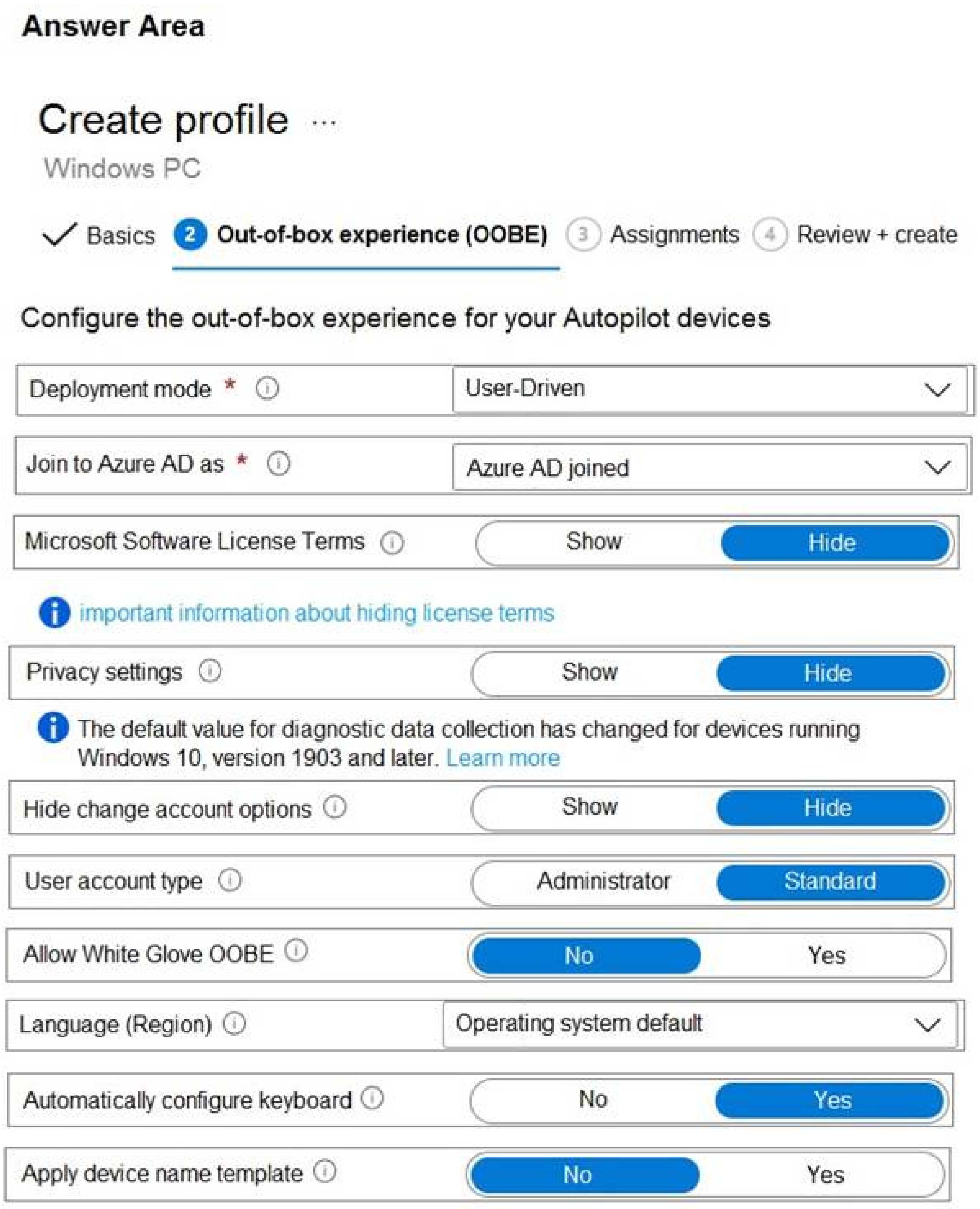
NEW QUESTION 3
- (Exam Topic 4)
You need to implement mobile device management (MDM) for personal devices that run Windows 11. The solution must meet the following requirements:
• Ensure that you can manage the personal devices by using Microsoft Intune.
• Ensure that users can access company data seamlessly 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 4
- (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

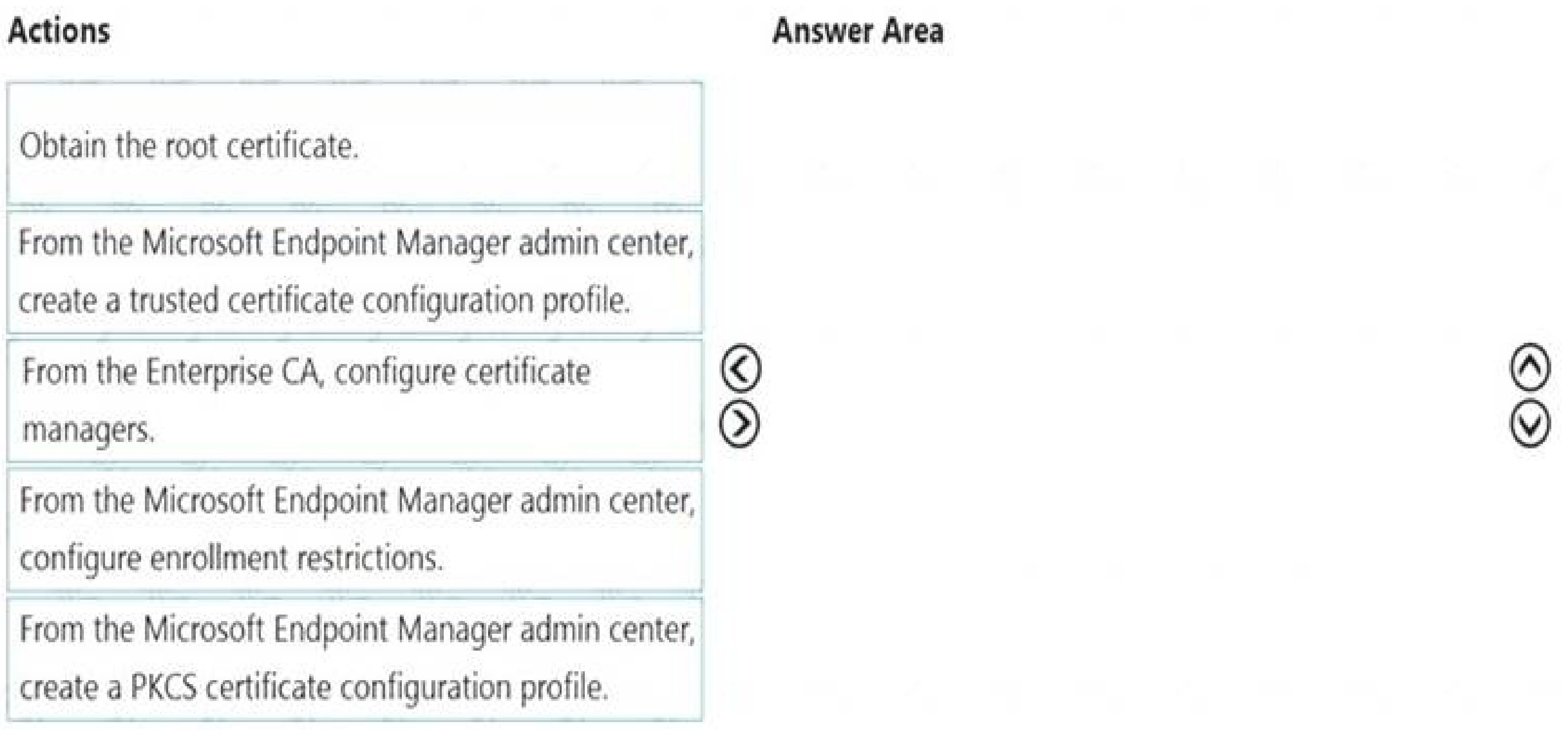
Hide change account options ⓘ	Show [✓ Hide]
User account type ⓘ	Administrator [✓ Standard]
Allow White Glove OOBE ⓘ	[✓ No] Yes
Language (Region) ⓘ	Operating system default
Automatically configure keyboard ⓘ	No [✓ Yes]
Apply device name template ⓘ	[✓ No] Yes

A. Mastered
B. Not Mastered

Answer: A

Explanation:
Reference:
https://docs.microsoft.com/en-us/mem/autopilot/profiles

NEW QUESTION 5
- (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.

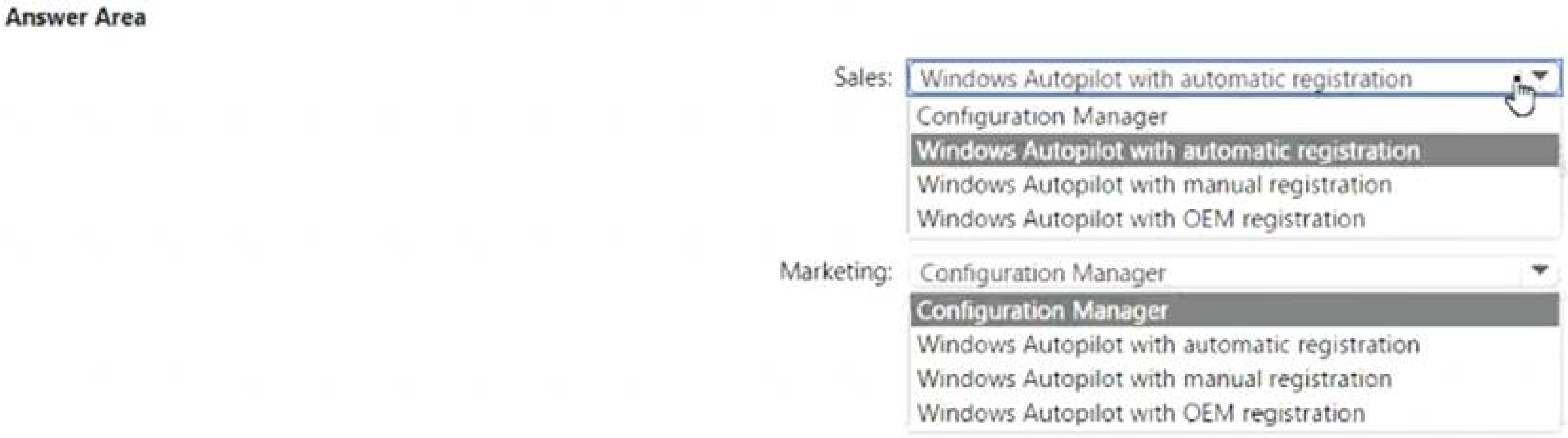
Answer Area

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 6
- (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

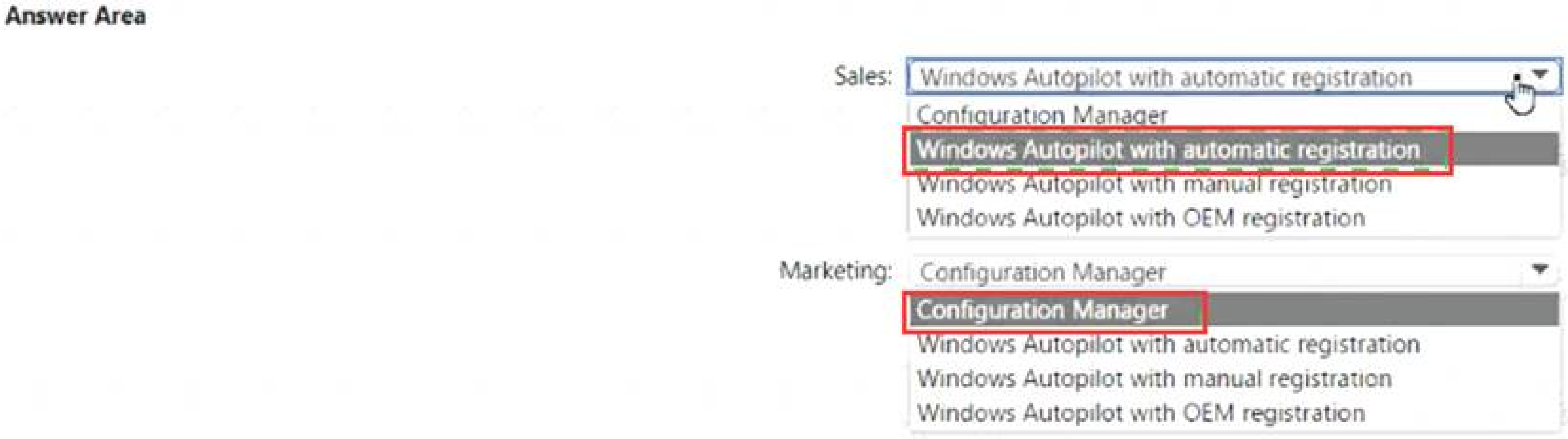
Sales: Windows Autopilot with automatic registration
- Configuration Manager
- Windows Autopilot with automatic registration
- Windows Autopilot with manual registration
- Windows Autopilot with OEM registration

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

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

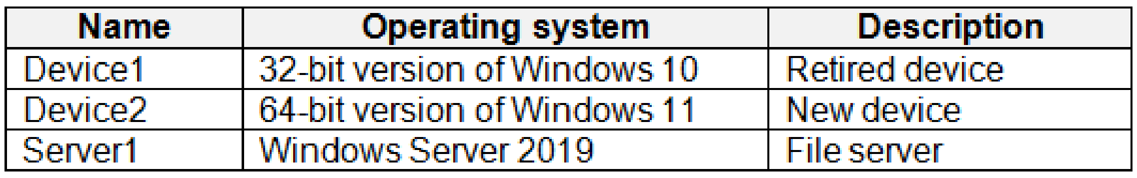
NEW QUESTION 7
- (Exam Topic 4)
You have a Microsoft 365 E5 subscription that contains 100 iOS devices enrolled in Microsoft Intune. You need to deploy a custom line-of-business (LOB) app to the devices by using Intune.
Which extension should you select for the app package file?

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

Answer: C

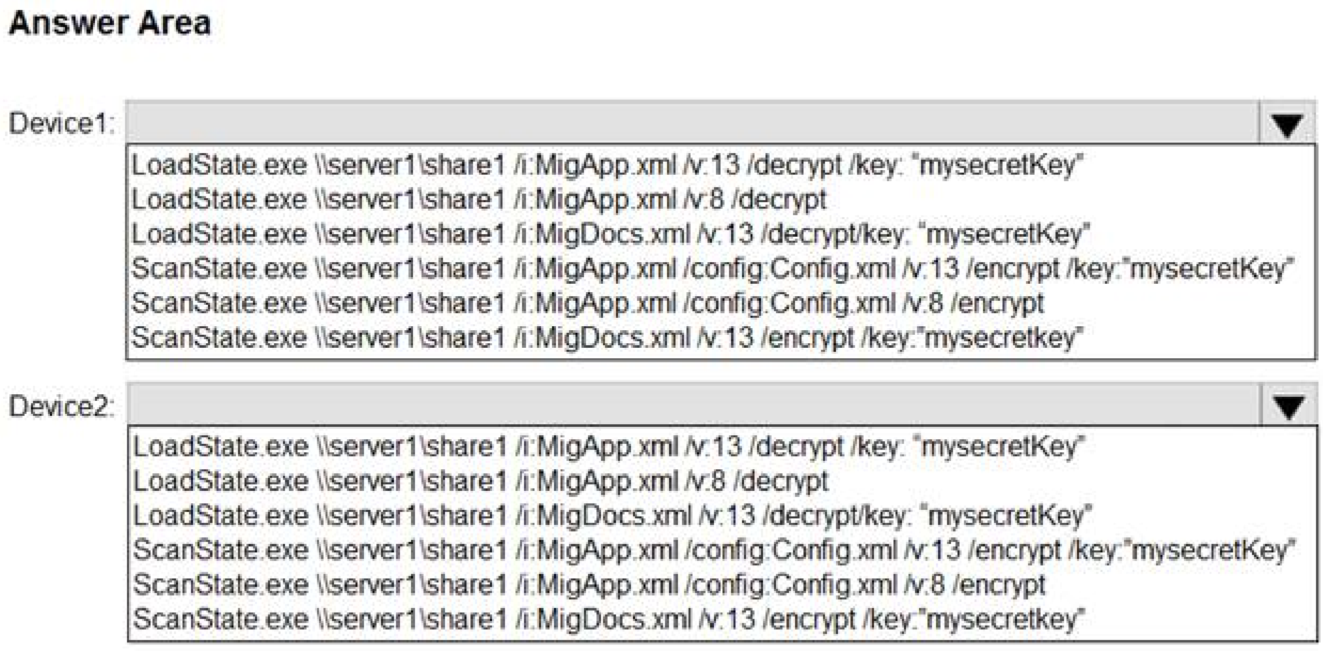
Explanation:
iOS/iPadOS LOB apps: Select Line-of-business app as the app type, select the App package file, and then enter an iOS/iPadOS installation file with the extension .ipa.
Reference:
https://docs.microsoft.com/en-us/mem/intune/apps/apps-add

NEW QUESTION 8
- (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"
```

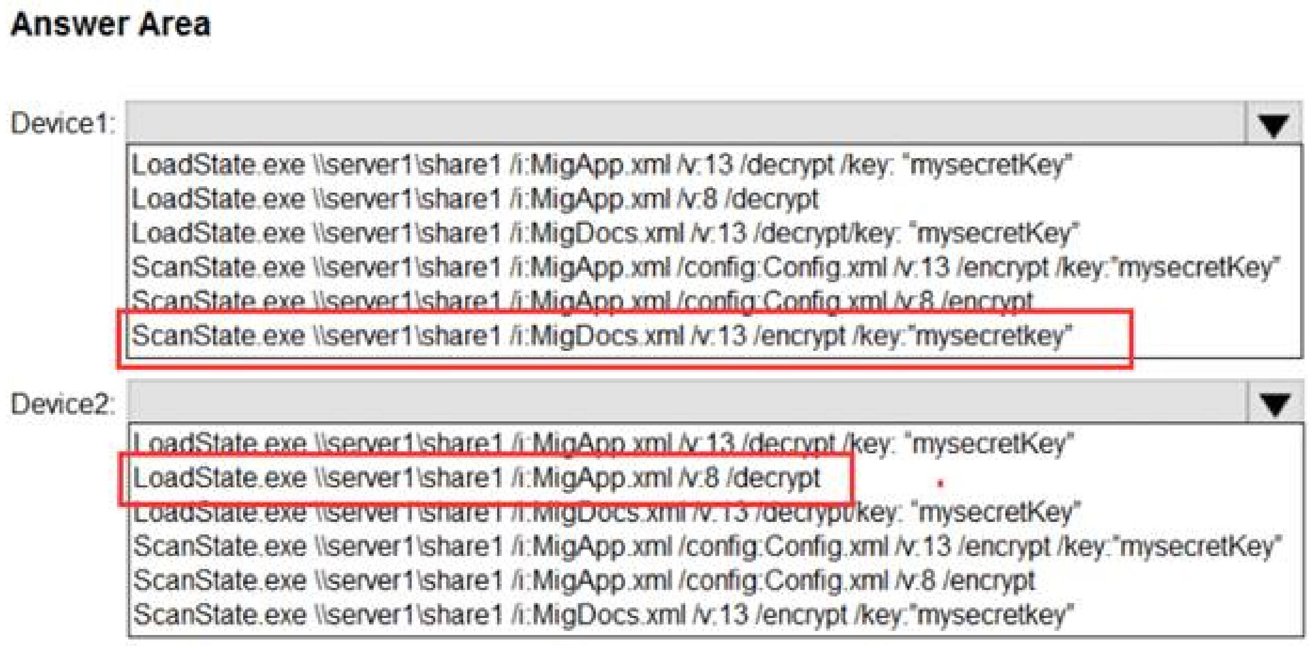
Device2:

```
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

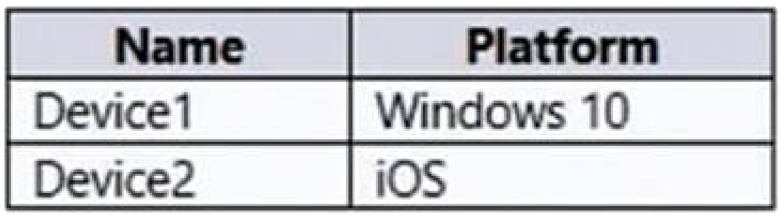
Device1:

```
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:

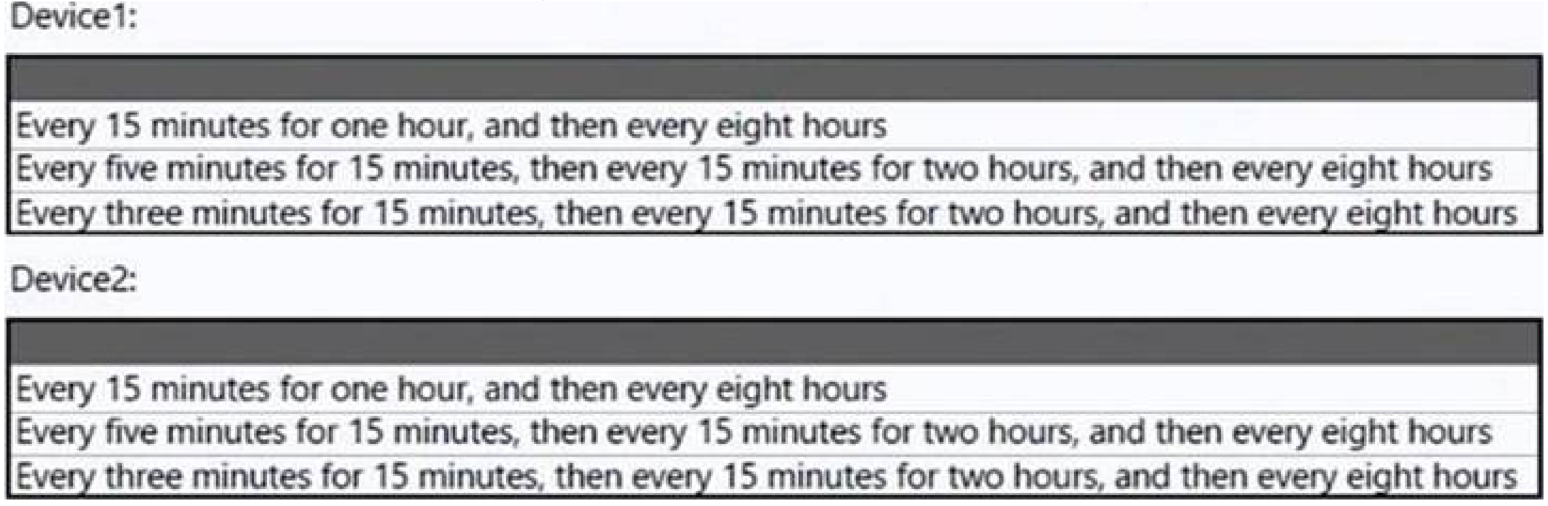
```
LoadState.exe \\server1\share1 /i:MigApp.xml /v:13 /decrypt /key: "mysecretKey"
LoadState.exe \\server1\share1 /i:MigApp.xml /v:8 /decrypt
LoadState.exe \\server1\share1 /i:MigDocs.xml /v:13 /decrypt/key: "mysecretKey"
ScanState.exe \\server1\share1 /i:MigApp.xml /config:Config.xml /v:13 /encrypt /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 9
- (Exam Topic 4)
You have a Microsoft 365 subscription that contains the devices shown in the following table.



Name	Platform
Device1	Windows 10
Device2	iOS

You plan to enroll the devices in Microsoft Intune.
How often will the compliance policy check-ins run after each device is enrolled in Intune? To answer, select the appropriate options in the answer area.
NOTE: Each correct selection is worth one point.



Device1:

Every 15 minutes for one hour, and then every eight hours
Every five minutes for 15 minutes, then every 15 minutes for two hours, and then every eight hours
Every three minutes for 15 minutes, then every 15 minutes for two hours, and then every eight hours

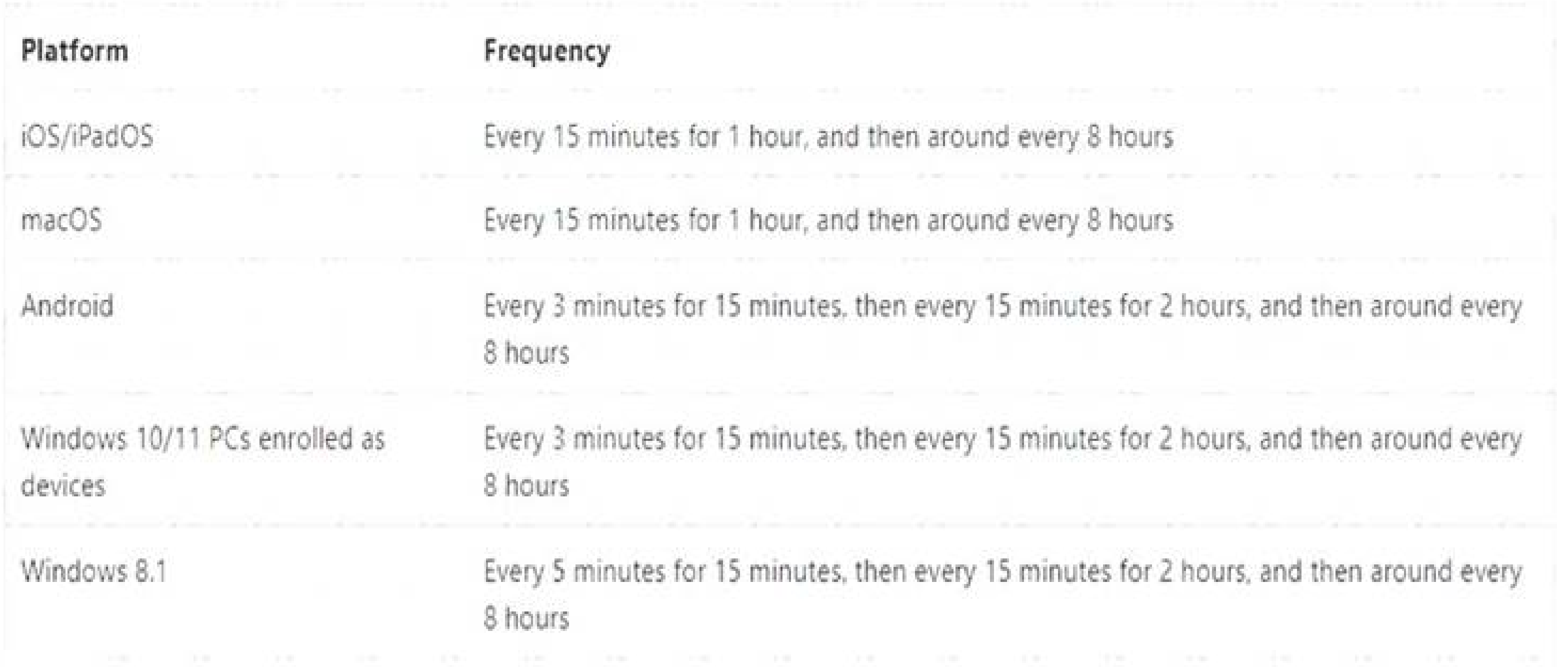
Device2:

Every 15 minutes for one hour, and then every eight hours
Every five minutes for 15 minutes, then every 15 minutes for two hours, and then every eight hours
Every three minutes for 15 minutes, then every 15 minutes for two hours, and then every eight hours

A. Mastered
B. Not Mastered

Answer: A

Explanation:
Box 1: Every three minutes for 15 minutes, then every 15 minutes for two hours, and then around every eight hours
If devices recently enroll, then the compliance, non-compliance, and configuration check-in runs more frequently. The check-ins are estimated at:
Windows 10: Every 3 minutes for 15 minutes, then every 15 minutes for 2 hours, and then around every 8 hours
Graphical user interface, text, application, email Description automatically generated



Platform	Frequency
iOS/iPadOS	Every 15 minutes for 1 hour, and then around every 8 hours
macOS	Every 15 minutes for 1 hour, and then around every 8 hours
Android	Every 3 minutes for 15 minutes, then every 15 minutes for 2 hours, and then around every 8 hours
Windows 10/11 PCs enrolled as devices	Every 3 minutes for 15 minutes, then every 15 minutes for 2 hours, and then around every 8 hours
Windows 8.1	Every 5 minutes for 15 minutes, then every 15 minutes for 2 hours, and then around every 8 hours

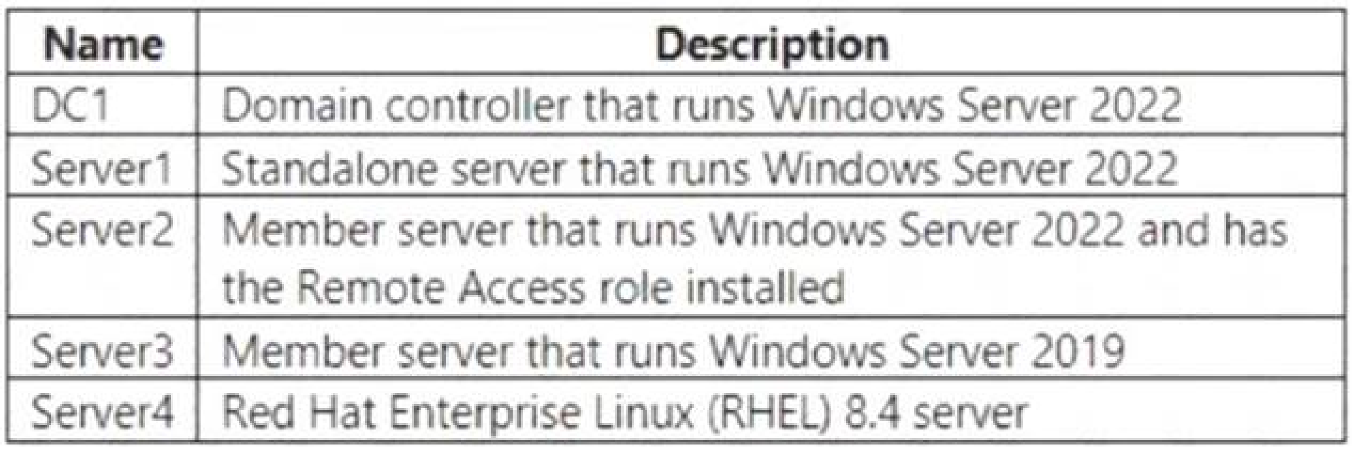
Box 2: Every 15 minutes for one hour, and then every eight hours iOS/iPadOS: Every 15 minutes for 1 hour, and then around every 8 hours
Reference: https://docs.microsoft.com/en-us/mem/intune/configuration/device-profile-troubleshoot

NEW QUESTION 10
- (Exam Topic 4)
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

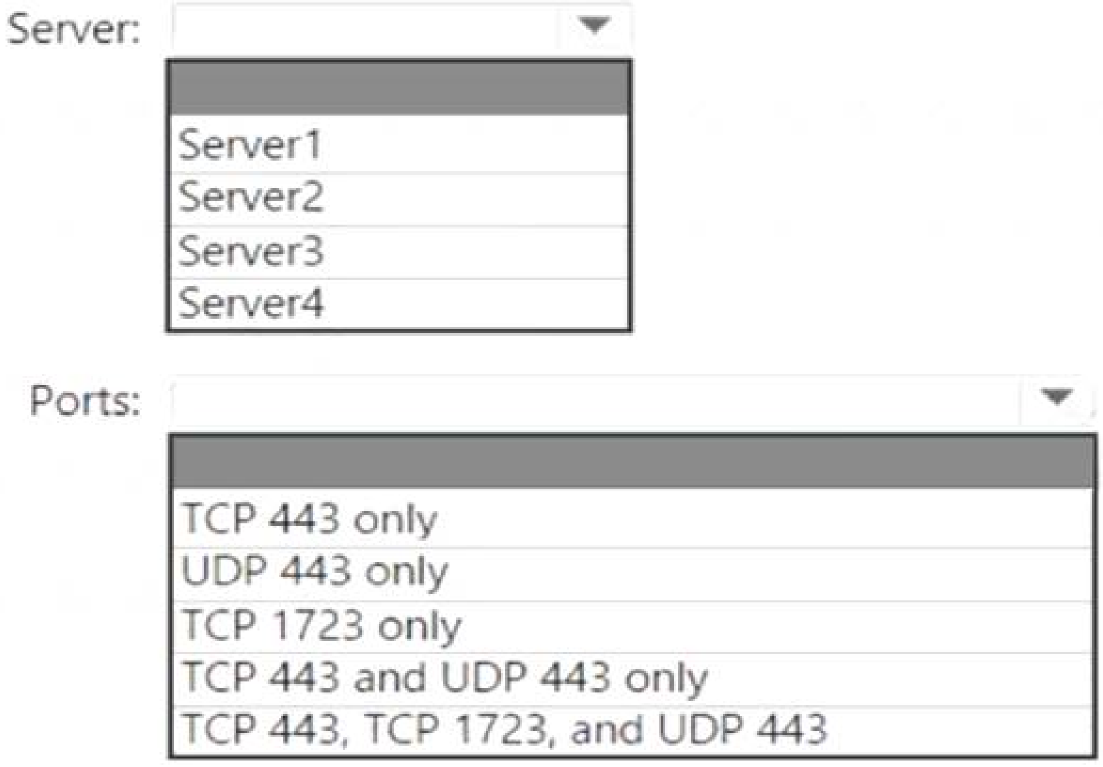
Answer: E

NEW QUESTION 10
- (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

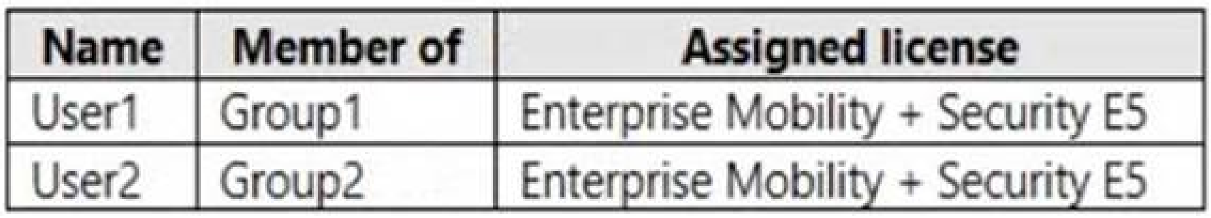
Ports:
- TCP 443 only
- UDP 443 only
- TCP 1723 only
- TCP 443 and UDP 443 only
- TCP 443, TCP 1723, and UDP 443

A. Mastered
B. Not Mastered

Answer: A

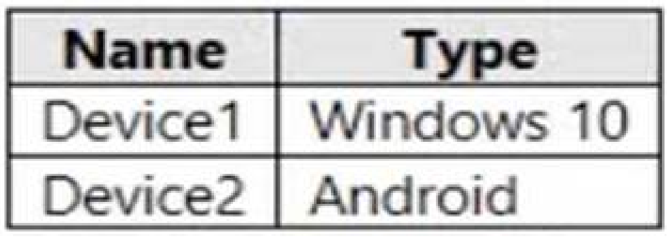
Explanation:
Box 1: Server4
Microsoft Tunnel is a VPN gateway solution for Microsoft Intune that runs in a container on Linux and allows access to on-premises resources from iOS/iPadOS and Android Enterprise devices using modern authentication and Conditional Access.
Box 2: TCP 443 and UDP 443 only
Some 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 15
- (Exam Topic 4)
You have an Azure Active Directory Premium Plan 2 subscription that contains the users shown in the following table.



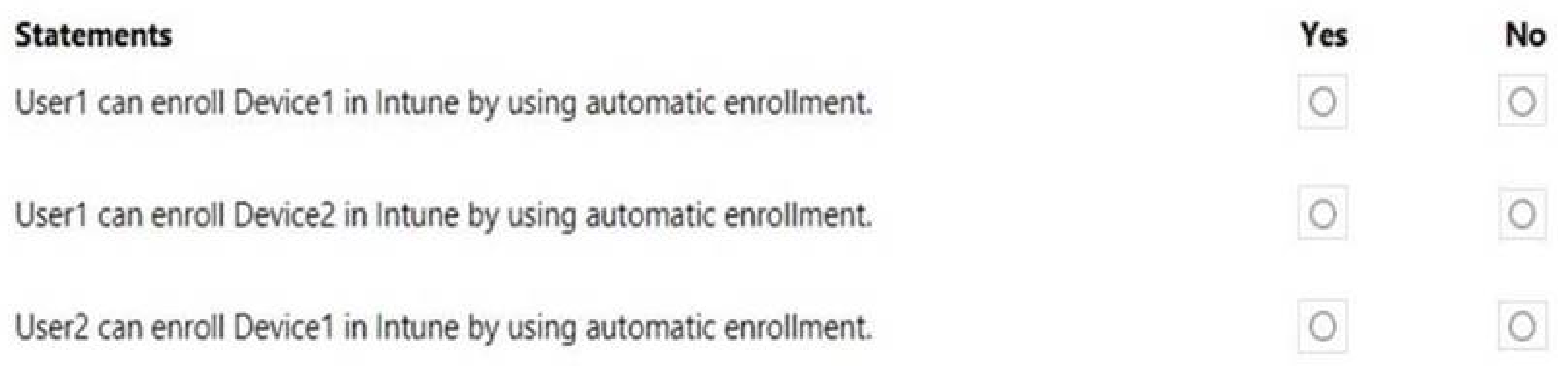
Name	Member of	Assigned license
User1	Group1	Enterprise Mobility + Security E5
User2	Group2	Enterprise Mobility + Security E5

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.

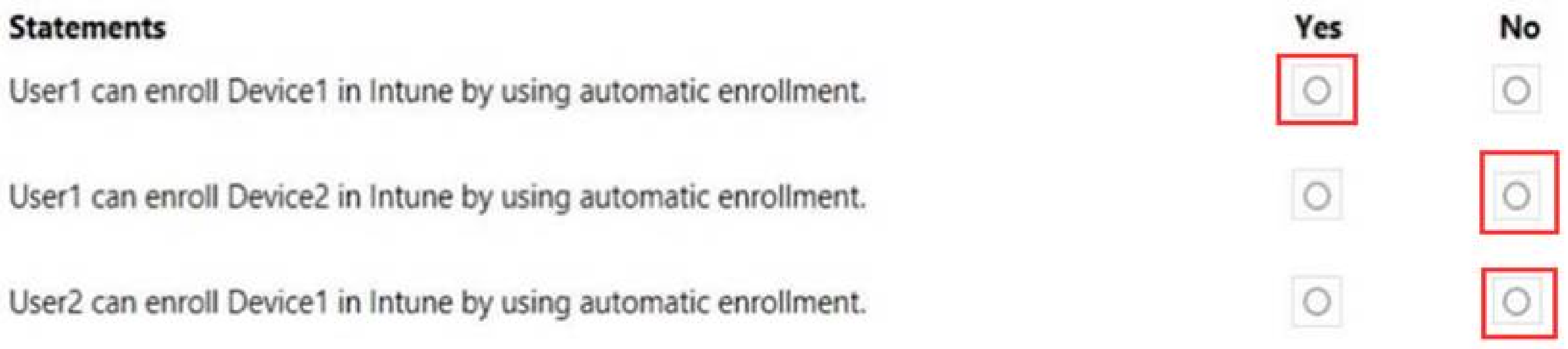


Statements	Yes	No
User1 can enroll Device1 in Intune by using automatic enrollment.	○	○
User1 can enroll Device2 in Intune by using automatic enrollment.	○	○
User2 can enroll Device1 in Intune by using automatic enrollment.	○	○

A. Mastered
B. Not Mastered

Answer: A

Explanation:



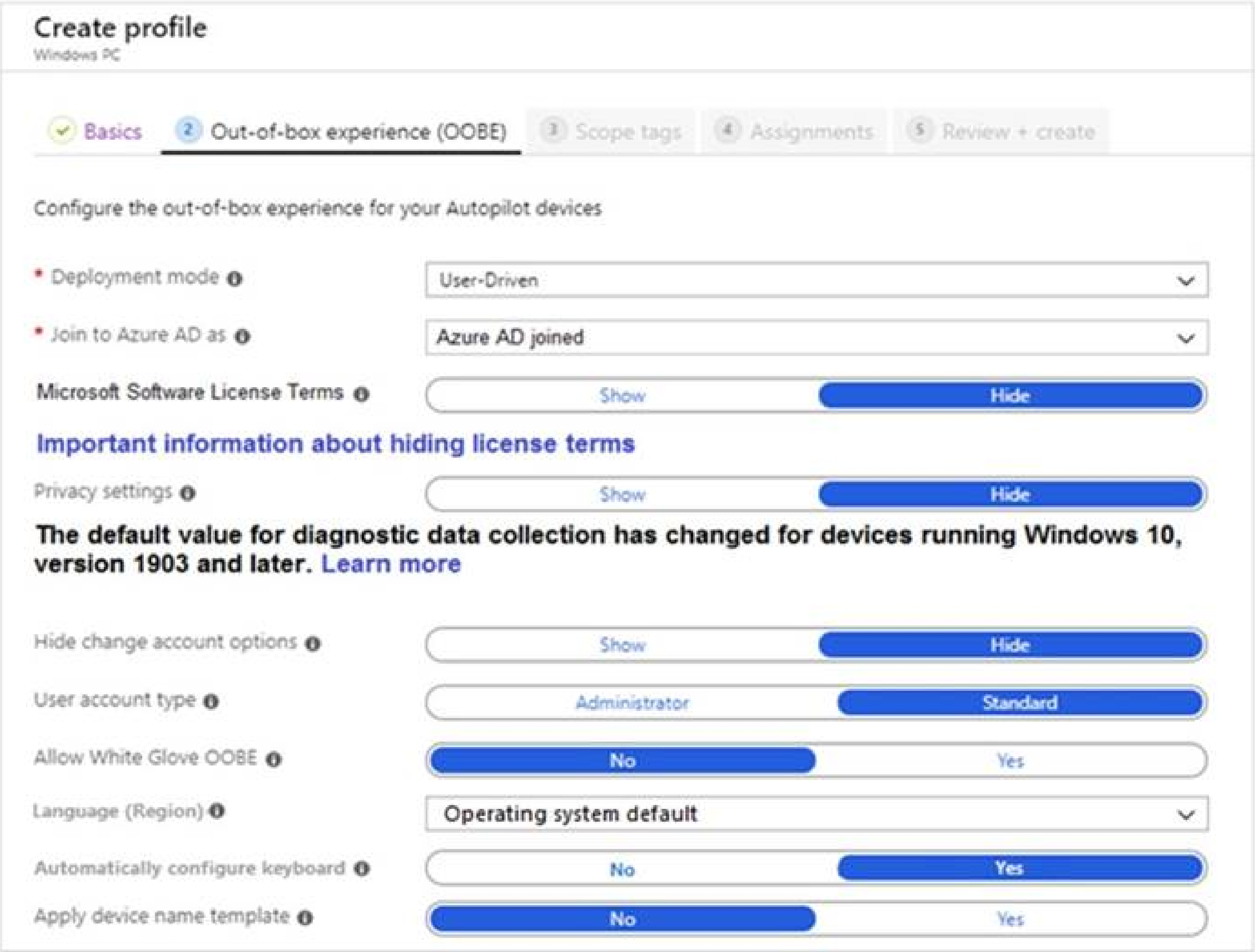
Statements	Yes	No
User1 can enroll Device1 in Intune by using automatic enrollment.	[✓ ○]	○
User1 can enroll Device2 in Intune by using automatic enrollment.	○	[✓ ○]
User2 can enroll Device1 in Intune by using automatic enrollment.	○	[✓ ○]

NEW QUESTION 19
- (Exam Topic 4)
Your company has 200 computers that run Windows 10. The computers are managed by using Microsoft Intune. Currently, Windows updates are downloaded without using Delivery Optimization. You need to configure the computers to use Delivery Optimization. What should you create in Intune?

A. a device compliance policy
B. a Windows 10 update ring
C. a device configuration profile
D. an app protection policy

Answer: C

NEW QUESTION 24
- (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	User-Driven
* Join to Azure AD as	Azure AD joined
Microsoft Software License Terms	Show [✓ Hide]

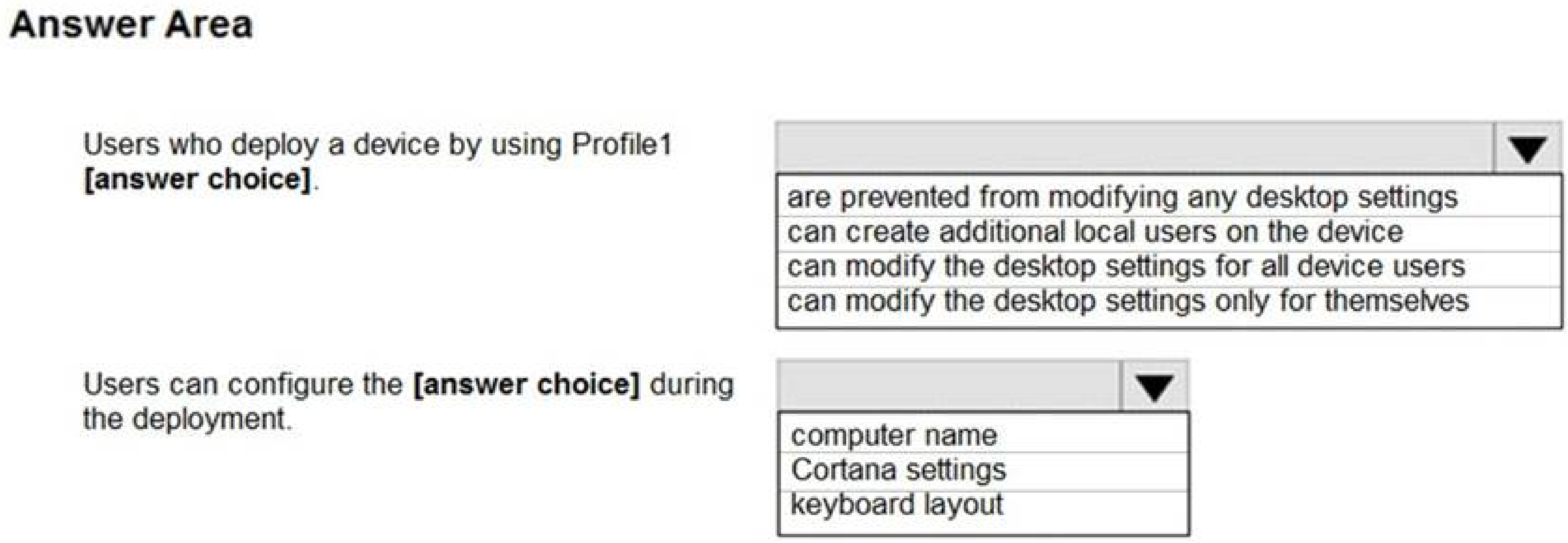
Important information about hiding license terms

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

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

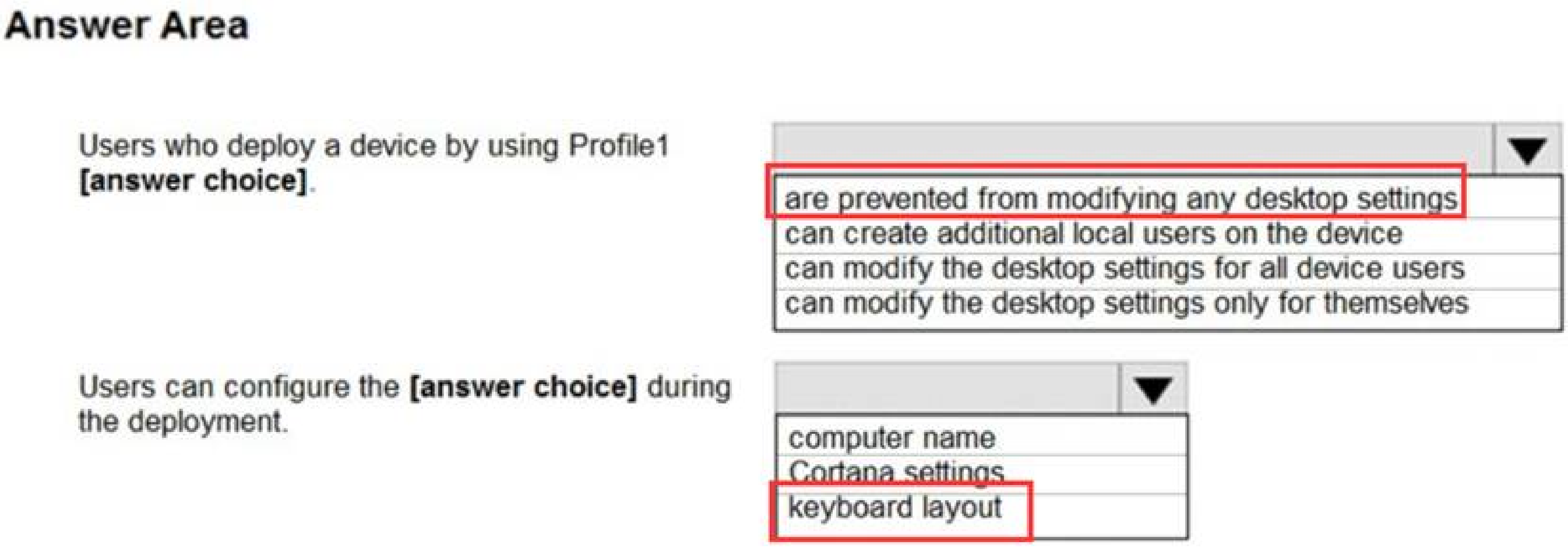
Users can configure the **[answer choice]** during the deployment.

- 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]**.

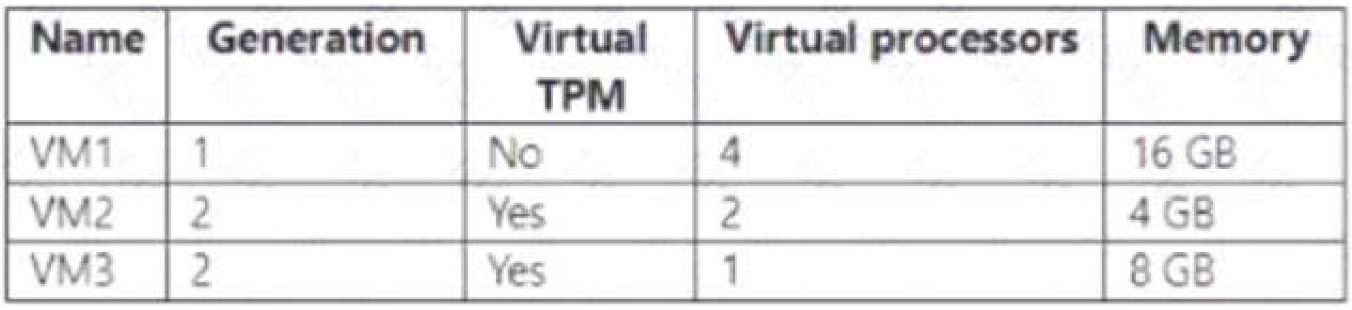
- [✓ are prevented from modifying any desktop settings]
- can create additional local users on the device
- can modify the desktop settings for all device users
- can modify the desktop settings only for themselves

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

- computer name
- Cortana settings
- [✓ keyboard layout]

NEW QUESTION 27

- (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. andVM3

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 and2 cores.

➤ A system firmware that supports UEFI
andSecure Boot.

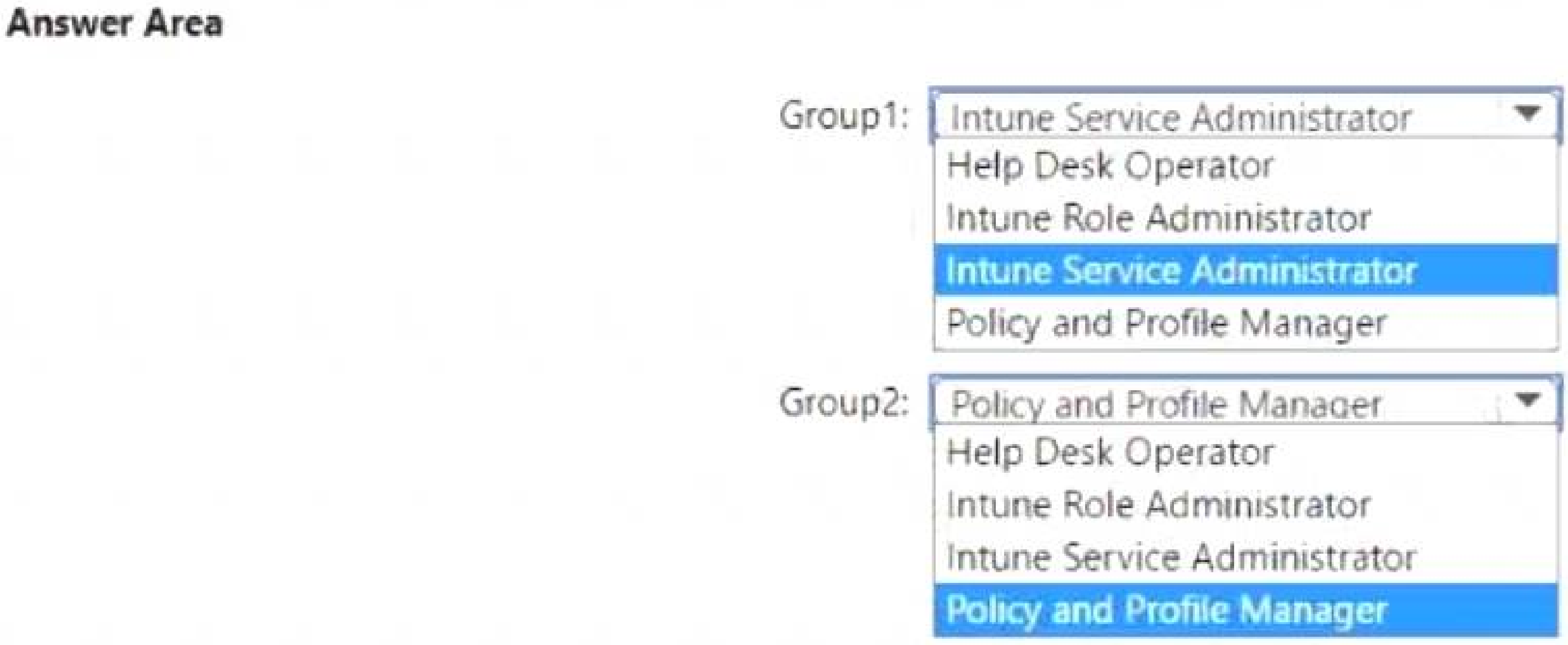
➤ A Trusted Platform Module (TPM)
version2.0
or higher.

➤ At least 4 GB

➤ At least 64 GB
of system memory (RAM). 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 30
- (Exam Topic 4)
You have a Microsoft 365 subscription that contains two security groups named Group1 and Group2. Microsoft 365 uses Microsoft Intune Suite.
You use Microsoft Intune to manage devices.
You need to assign roles in Intune to meet the following requirements:
• The members of Group1 must manage Intune roles and assignments.
• The members of Group2 must assign existing apps and policies to users and devices.
The solution must follow the principle of least privilege.
Which role should you assign to each group? To answer, select the appropriate options in the answer area. NOTE: Each correct selection is worth one point.



Answer Area

Group1: Intune Service Administrator ▼
Help Desk Operator
Intune Role Administrator
Intune Service Administrator
Policy and Profile Manager

Group2: Policy and Profile Manager ▼
Help Desk Operator
Intune Role Administrator
Intune Service Administrator
Policy and Profile Manager

A. Mastered
B. Not Mastered

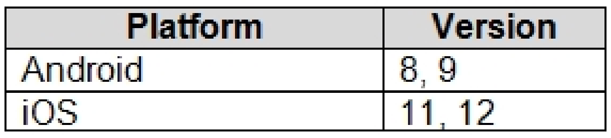
Answer: A

Explanation:
To assign roles in Intune to meet the requirements, you should assign the following roles to each group: Group1: Intune Role Administrator Group2: Help Desk Operator

➤ The Intune Role Administrator role is the only Intune role that can manage custom Intune roles and add assignments for built-in Intune roles1. This role meets the requirement for Group1 to manage Intune roles and assignments.

- The Help Desk Operator role can perform remote tasks on users and devices, and can assign applications or policies to users or devices1. This role meets the requirement for Group2 to assign existing apps and policies to users and devices.

NEW QUESTION 34
- (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.

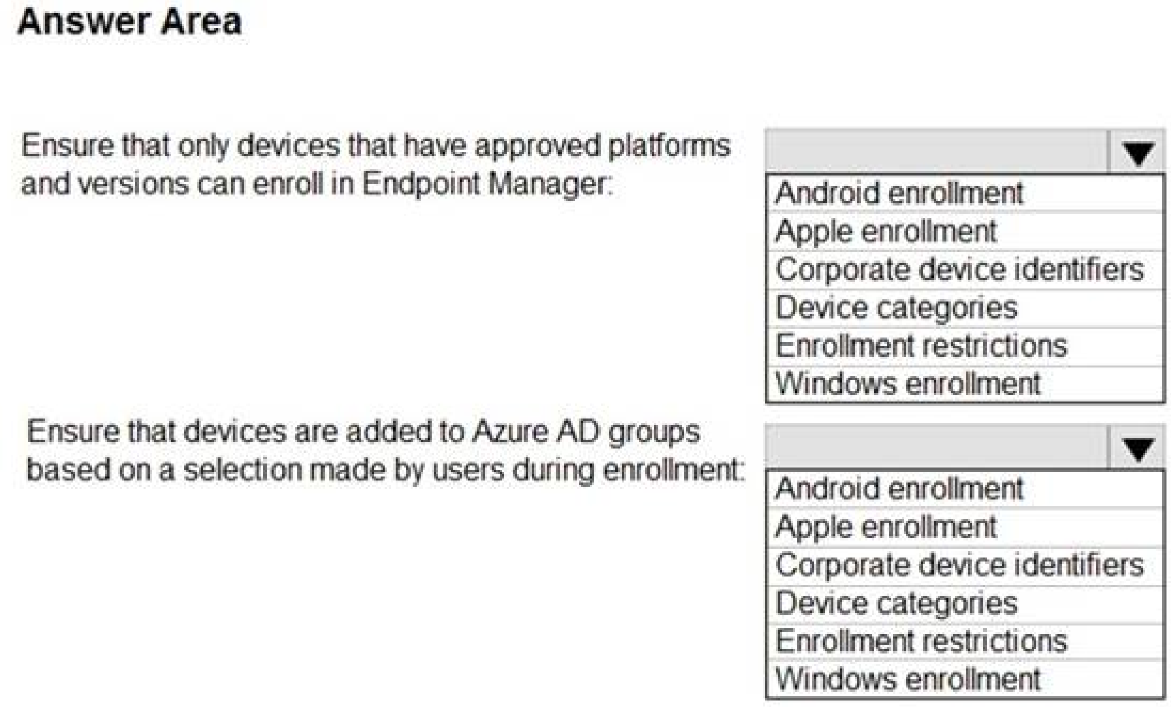


Platform	Version
Android	8, 9
iOS	11, 12

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:

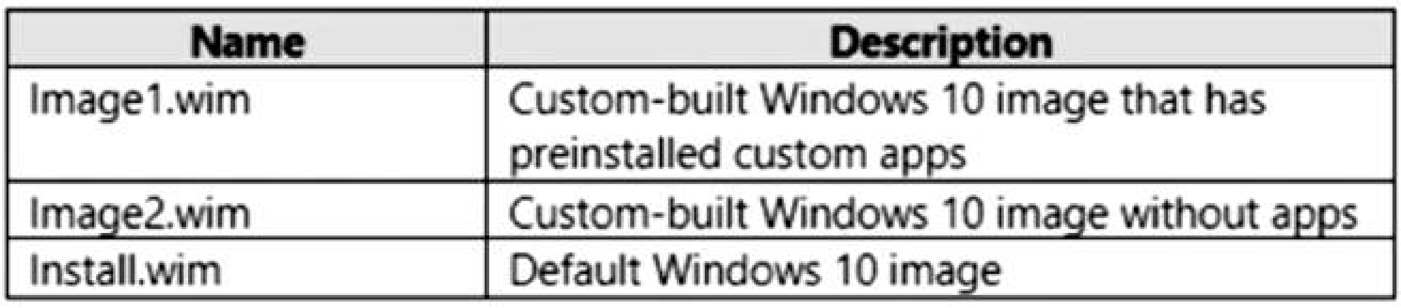
- Android enrollment
- Apple enrollment
- Corporate device identifiers
- Device categories
- Enrollment restrictions
- Windows enrollment

A. Mastered
B. Not Mastered

Answer: A

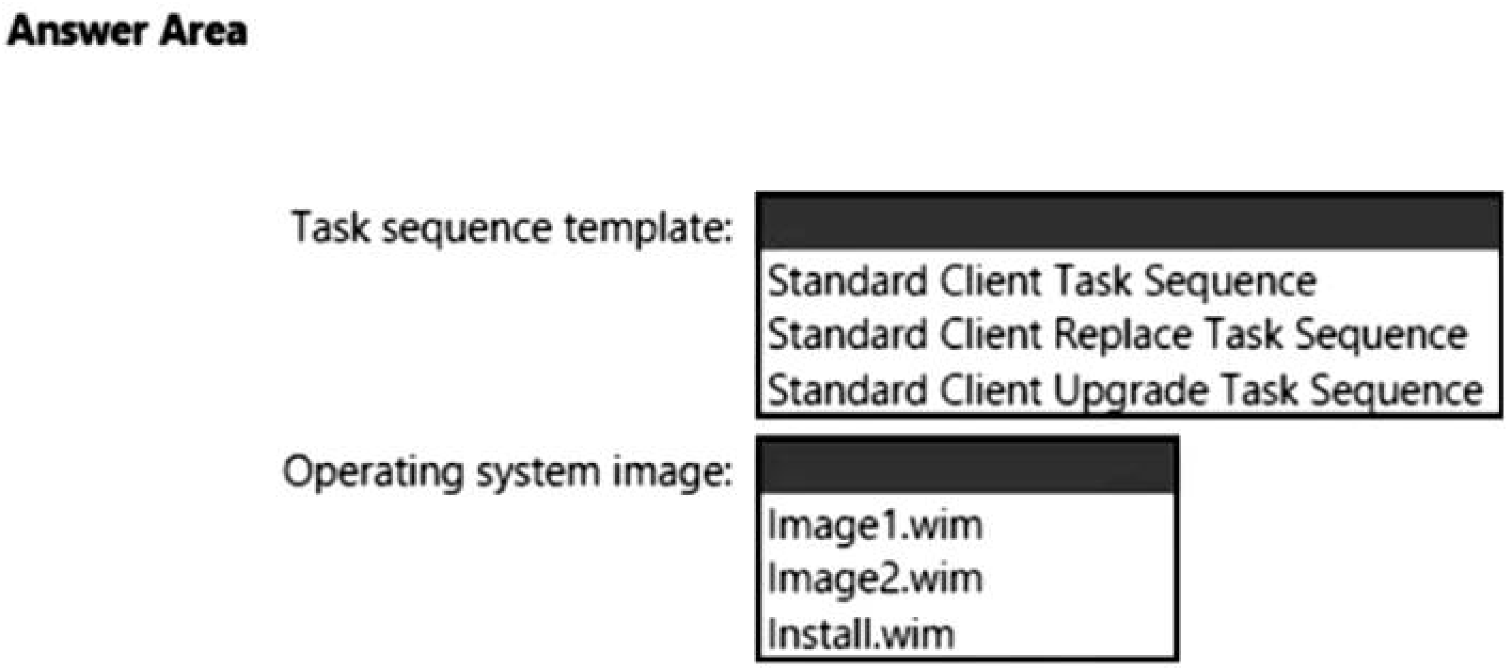
Explanation:
A screenshot of a computer Description automatically generated
Reference:
https://docs.microsoft.com/en-us/mem/intune/enrollment/enrollment-restrictions-set https://docs.microsoft.com/en-us/mem/intune/enrollment/device-group-mapping

NEW QUESTION 39
- (Exam Topic 4)
You have a Microsoft Deployment Toolkit (MDT) solution that is used to manage Windows 11 deployment tasks.
MDT contains the operating system images shown in the following table.



Name	Description
Image1.wim	Custom-built Windows 10 image that has preinstalled custom apps
Image2.wim	Custom-built Windows 10 image without apps
Install.wim	Default Windows 10 image

You need to perform a Windows 11 in-place upgrade on several computers that run Windows 10. From the Deployment Workbench, you open the New Task Sequence Wizard.
You need to identify which task sequence template and which operating system image to use for the task sequence. The solution must minimize administrative effort.
What should you identify? To answer, select the appropriate options in the answer area.
NOTE: Each correct selection is worth one point.



Answer Area

Task sequence template:
- Standard Client Task Sequence
- Standard Client Replace Task Sequence
- Standard Client Upgrade Task Sequence

Operating system image:
- Image1.wim
- Image2.wim
- Install.wim

A. Mastered
B. Not Mastered

Answer: A

Explanation:
Box 1: Standard Client Upgrade Task Sequence
Use Template: Standard Client Upgrade Task Sequence
In-place upgrade is the preferred method to use when migrating from Windows 10 to a later release of Windows 10, and is also a preferred method for upgrading from Windows 7 or 8.1 if you do not plan to significantly change the device's configuration or applications. MDT includes an in-place upgrade task sequence template that makes the process really simple.
Box 2: Install.wim
In-place upgrade differs from computer refresh in that you cannot use a custom image to perform the in-place upgrade. I
Reference:
https://docs.microsoft.com/en-us/windows/deployment/deploy-windows-mdt/upgrade-to-windows-10-with-the

NEW QUESTION 42
- (Exam Topic 4)
Your network contains an Active Directory domain. The domain contains a computer named Computer1 that runs Windows 8.1.
Computer1 has apps that are compatible with Windows 10.
You need to perform a Windows 10 in-place upgrade on Computer1.
Solution: You copy the Windows 10 installation media to a network share. You start Computer1 from Windows PE (WinPE), and then you run setup.exe from the network share.
Does this meet the goal?

A. Yes
B. No

Answer: B

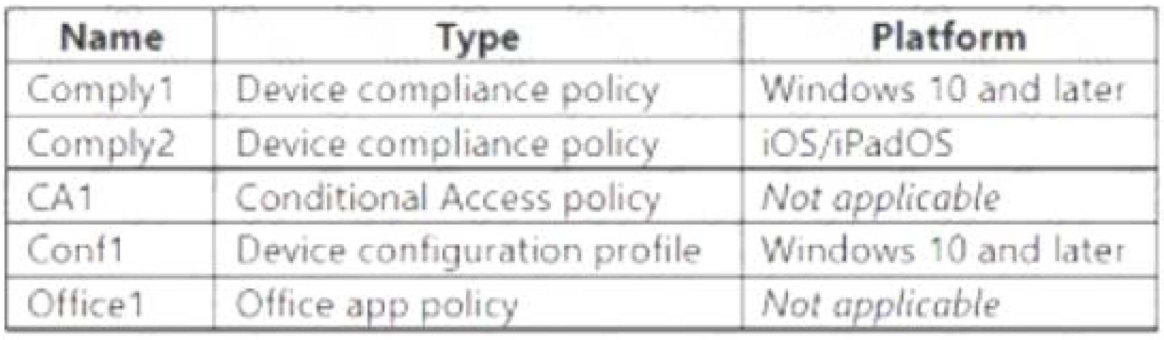
NEW QUESTION 43
- (Exam Topic 4)
Your company uses Microsoft Intune to manage devices.
You need to ensure that only Android devices that use Android work profiles can enroll in intune. Which two configurations should you perform in the device enrollment restrictions? Each correct answer
presents part 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 44
- (Exam Topic 4)
You have a Microsoft Intune deployment that contains the resources shown in the following table.



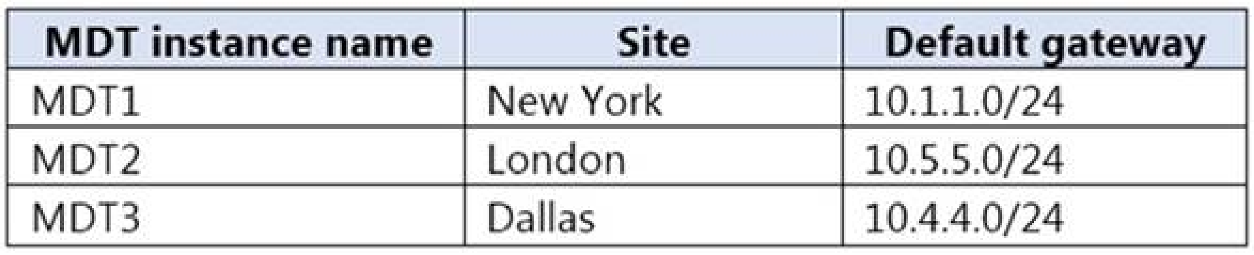
Name	Type	Platform
Comply1	Device compliance policy	Windows 10 and later
Comply2	Device compliance policy	iOS/iPadOS
CA1	Conditional Access policy	*Not applicable*
Conf1	Device configuration profile	Windows 10 and later
Office1	Office app policy	*Not applicable*

You create a policy set named Set1 and add Comply1 to Set1. Which additional resources can you add to Set1?

A. Conf1 only
B. Comply2 only
C. Comply2 and Conf1 only
D. CA1. Conf1. and Office 1 only
E. Comply2. CA1, Conf1. and Office1

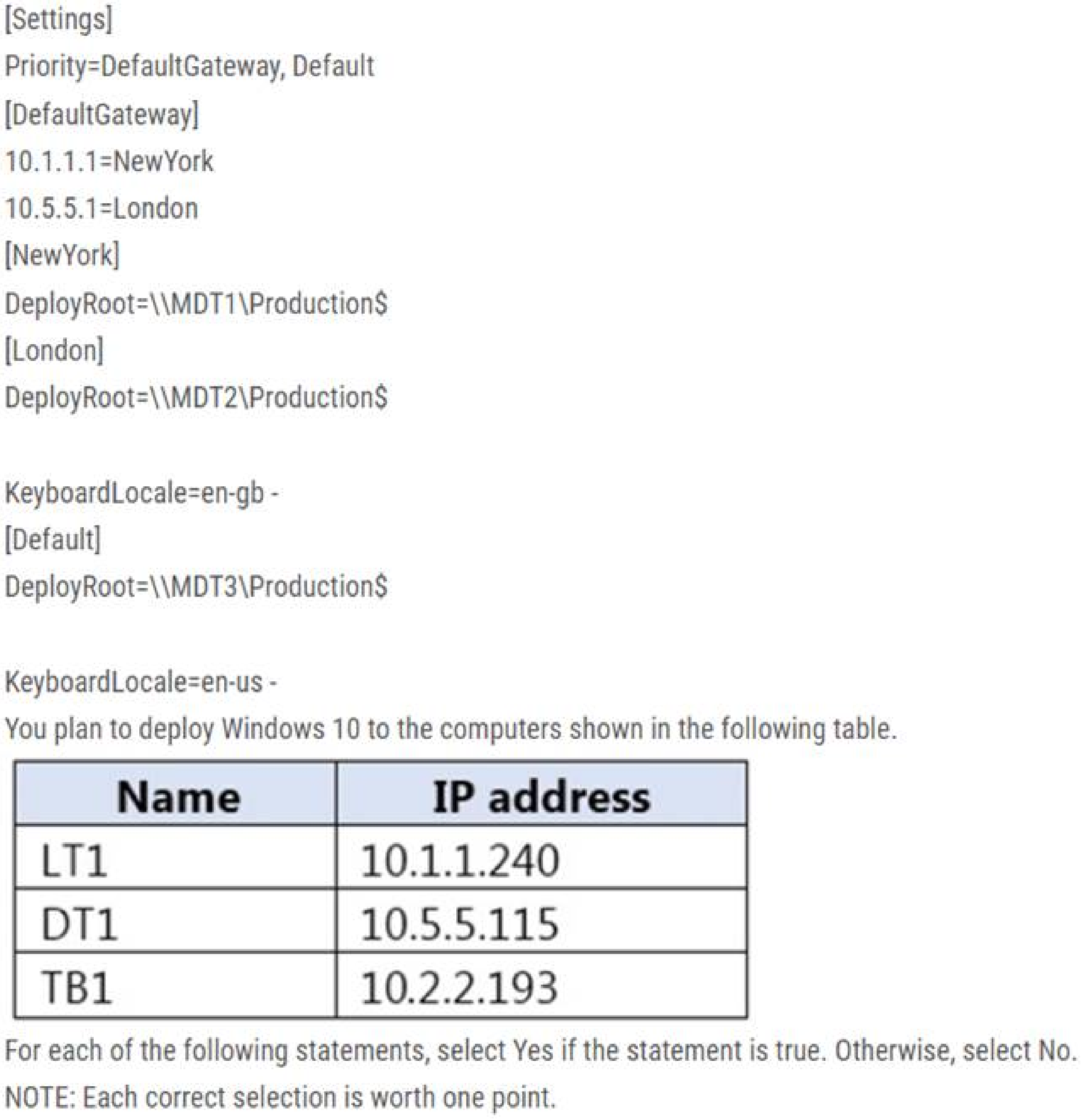
Answer: B

NEW QUESTION 49
- (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.



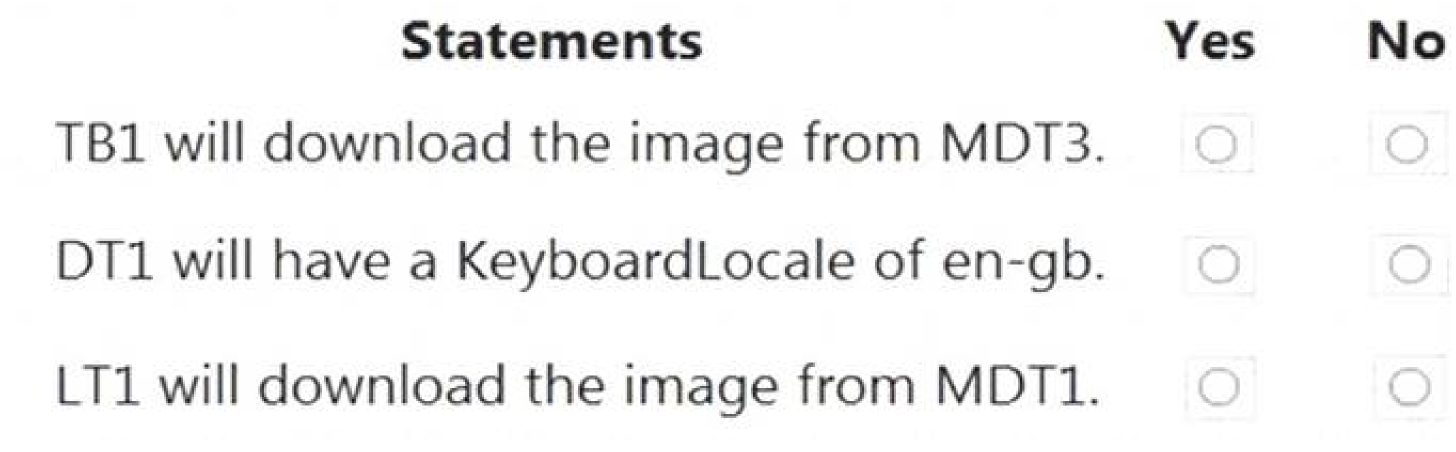
```
[Settings]
Priority=DefaultGateway, Default
[DefaultGateway]
10.1.1.1=NewYork
10.5.5.1=London
[NewYork]
DeployRoot=\\MDT1\Production$
[London]
DeployRoot=\\MDT2\Production$

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.

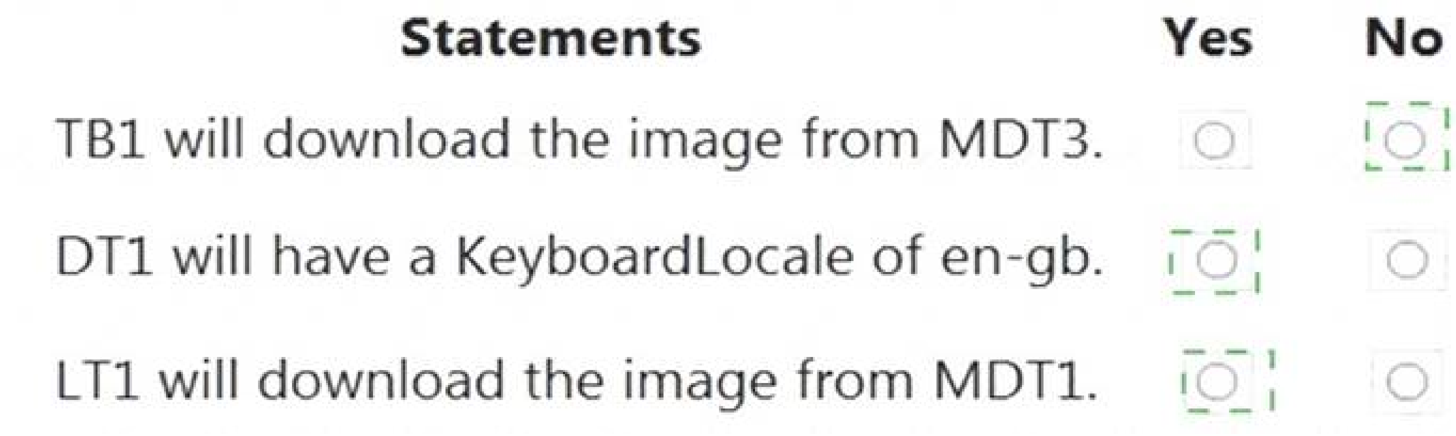


Statements	Yes	No
TB1 will download the image from MDT3.	○	○
DT1 will have a KeyboardLocale of en-gb.	○	○
LT1 will download the image from MDT1.	○	○

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 50
- (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

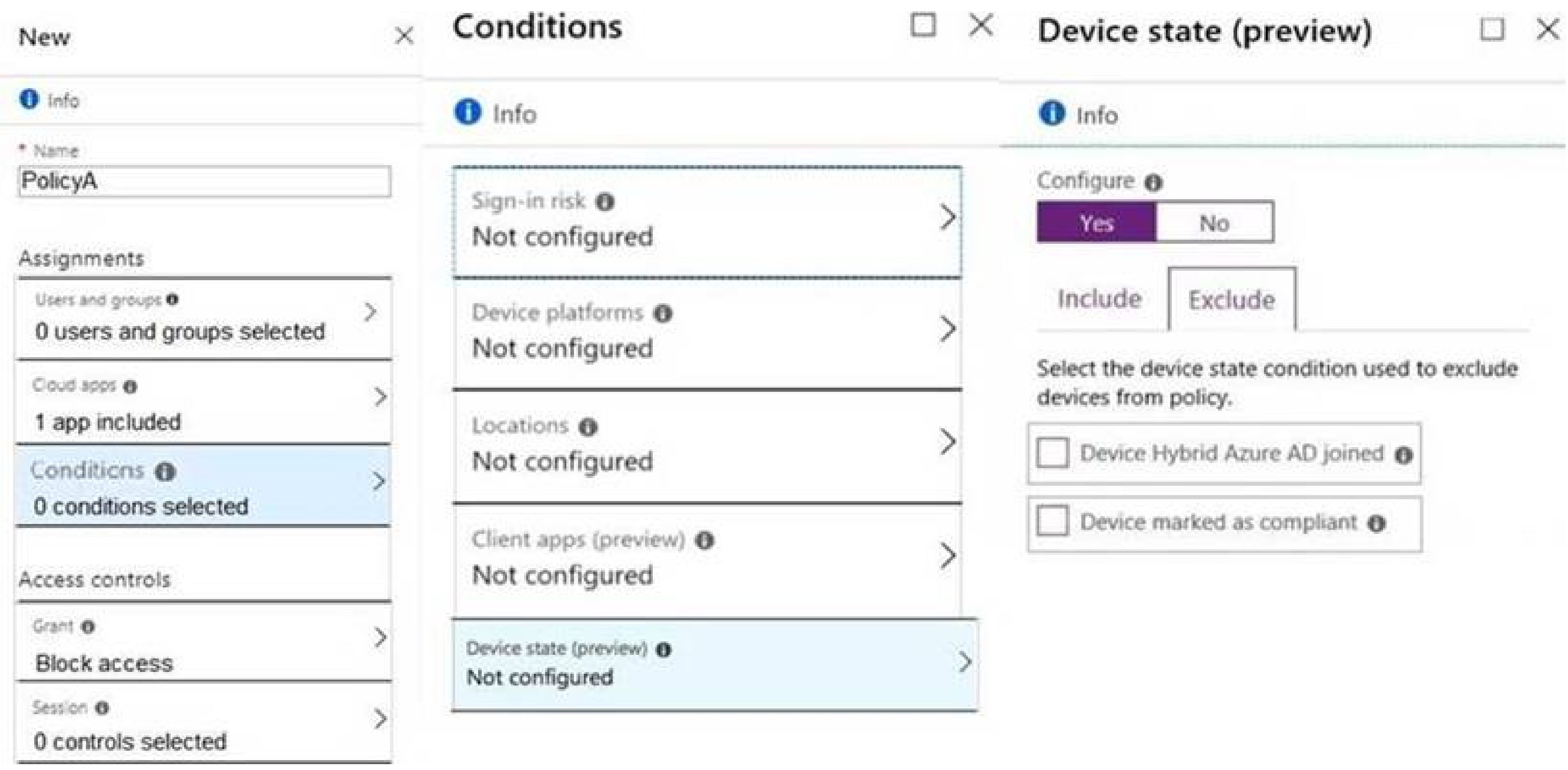
NEW QUESTION 53
- (Exam Topic 3)
You need to meet the requirements for the MKG department users. What should you do?

A. Assign the MKG department users the Purchaser role in Microsoft Store for Business
B. Download the APPX file for App1 from Microsoft Store for Business
C. Add App1 to the private store
D. Assign the MKG department users the Basic Purchaser role in Microsoft Store for Business
E. Acquire App1 from Microsoft Store for Business

Answer: E

Explanation:
References:
https://docs.microsoft.com/en-us/microsoft-store/distribute-apps-from-your-private-store Enable the users in the MKG department to use App1.
The private store is a feature in Microsoft Store for Business and Education that organizations receive during the signup process. When admins add apps to the private store, all employees in the organization can view and download the apps. Your private store is available as a tab in Microsoft Store app, and is usually named for your company or organization. Only apps with online licenses can be added to the private store.
Reference:
https://docs.microsoft.com/en-us/microsoft-store/distribute-apps-from-your-private-store

NEW QUESTION 55
- (Exam Topic 3)
You need a new conditional access policy that has an assignment for Office 365 Exchange Online. You need to configure the policy to meet the technical requirements for Group4.
Which two settings should you configure in the policy? To answer, select the appropriate settings in the answer area.
NOTE: Each correct selection is worth one point.



New

Info

* Name
PolicyA

Assignments

Users and groups
0 users and groups selected

Cloud apps
1 app included

Conditions
0 conditions selected

Access controls

Grant
Block access

Session
0 controls selected

Conditions

Info

Sign-in risk
Not configured

Device platforms
Not configured

Locations
Not configured

Client apps (preview)
Not configured

Device state (preview)
Not configured

Device state (preview)

Info

Configure
Yes | No

Include | Exclude

Select the device state condition used to exclude devices from policy.

□ Device Hybrid Azure AD joined

□ Device marked as compliant

A. Mastered
B. Not Mastered

Answer: A

Explanation:
The policy needs to be applied to Group4 so we need to configure Users and Groups. The Access controls are set to Block access
A screenshot of a computer Description automatically generated
We therefore need to exclude compliant devices. From the scenario:
➢ Ensure that the users in a group named Group4 can only access Microsoft Exchange Online from devices that are enrolled in Intune.
Note: When a device enrolls in Intune, the device information is updated in Azure AD to include the device compliance status. This compliance status is used by conditional access policies to block or allow access to e-mail and other organization resources.
References:
https://docs.microsoft.com/en-us/azure/active-directory/conditional-access/overview https://docs.microsoft.com/en-us/azure/active-directory/conditional-access/conditions https://docs.microsoft.com/en-us/intune/device-compliance-get-started

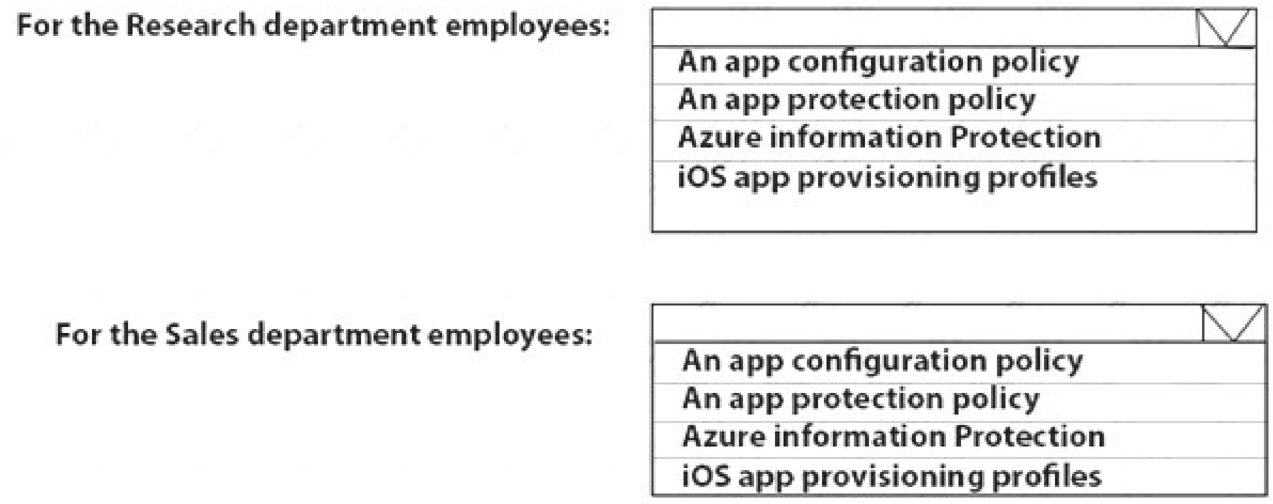
NEW QUESTION 56
- (Exam Topic 3)
You need to meet the technical requirements for the IT department. What should you do first?

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 57
- (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:
- An app configuration policy
- An app protection policy
- Azure information Protection
- iOS app provisioning profiles

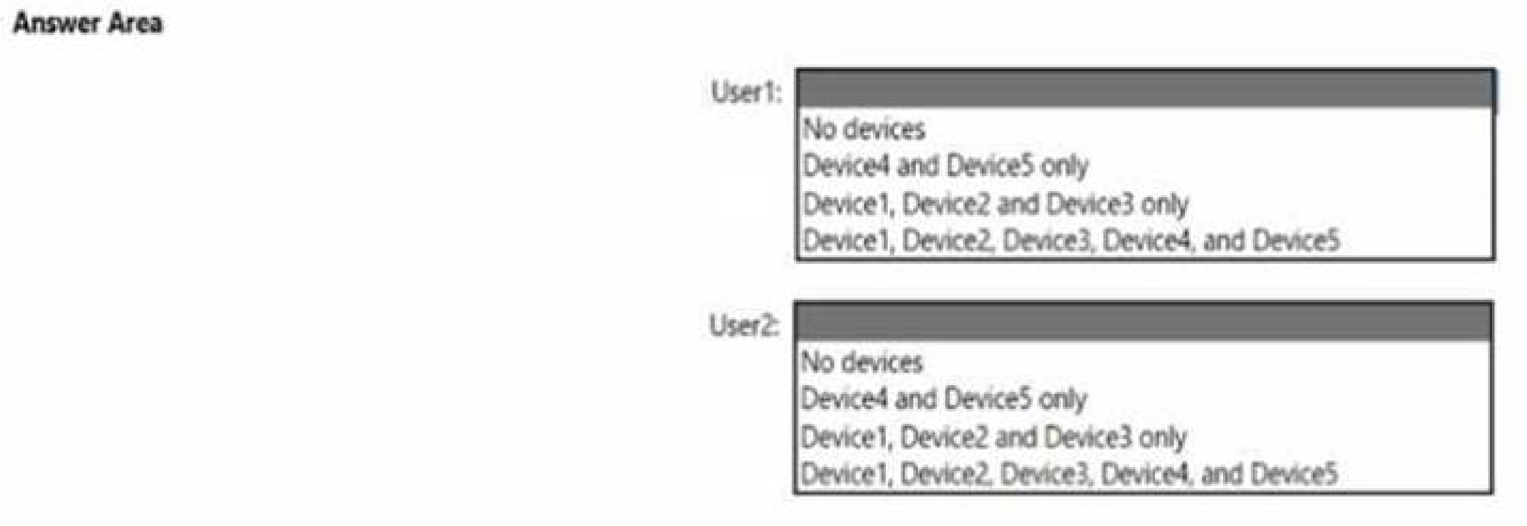
For the Sales department employees:
- An app configuration policy
- An app protection policy
- Azure information Protection
- iOS app provisioning profiles

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 58
- (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 63
- (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 68
- (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

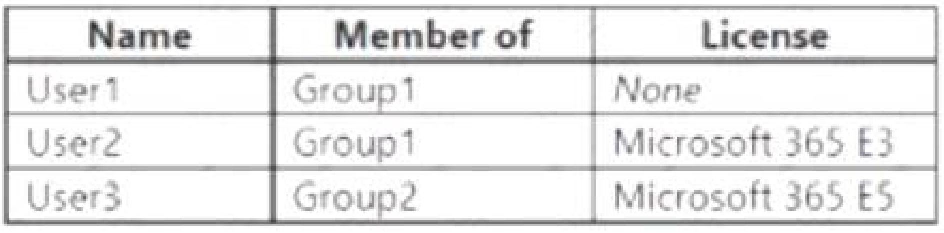
NEW QUESTION 72

- (Exam Topic 4)
You have two computers named Computer1 and Computed that run Windows 10. Computed has Remote Desktop enabled.
From Computer1, you connect to Computer2 by using Remote Desktop Connection.
You need to ensure that you can access the local drives on Computer1 from within the Remote Desktop session.
What should you do?

A. From Computer 2, configure the Remote Desktop settings.
B. From Windows Defender Firewall on Computer 1, allow Remote Desktop.
C. From Windows Defender Firewall on Computer 2, allow File and Printer Sharing.
D. From Computer1, configure the Remote Desktop Connection settings.

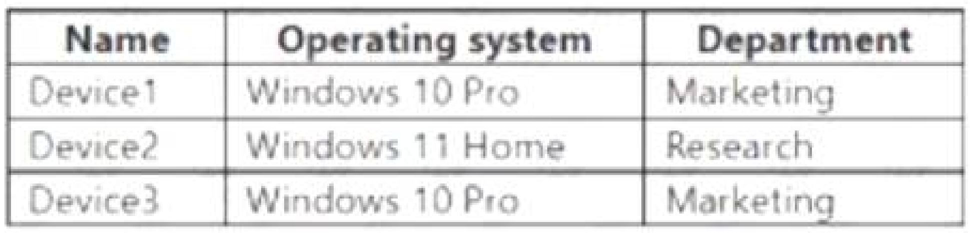
Answer: D

NEW QUESTION 73
- (Exam Topic 4)
You have a Microsoft 365 subscription that uses Microsoft Intune and contains the users shown in the following table.



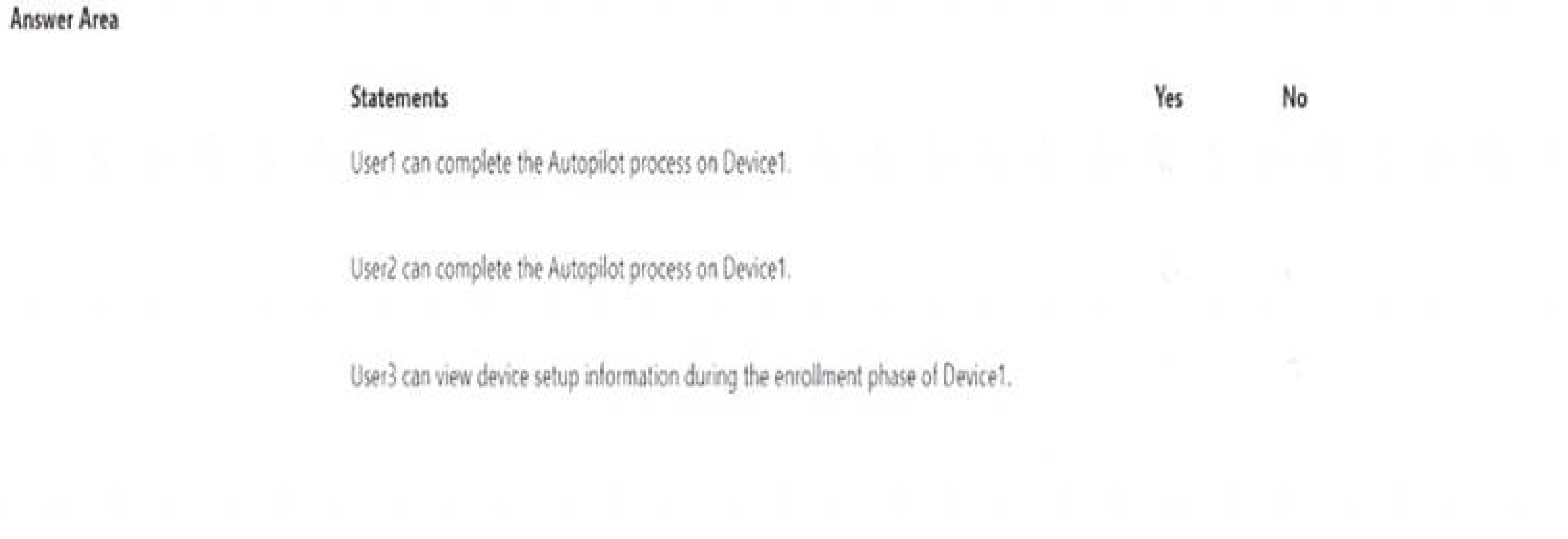
Name	Member of	License
User1	Group1	None
User2	Group1	Microsoft 365 E3
User3	Group2	Microsoft 365 E5

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.



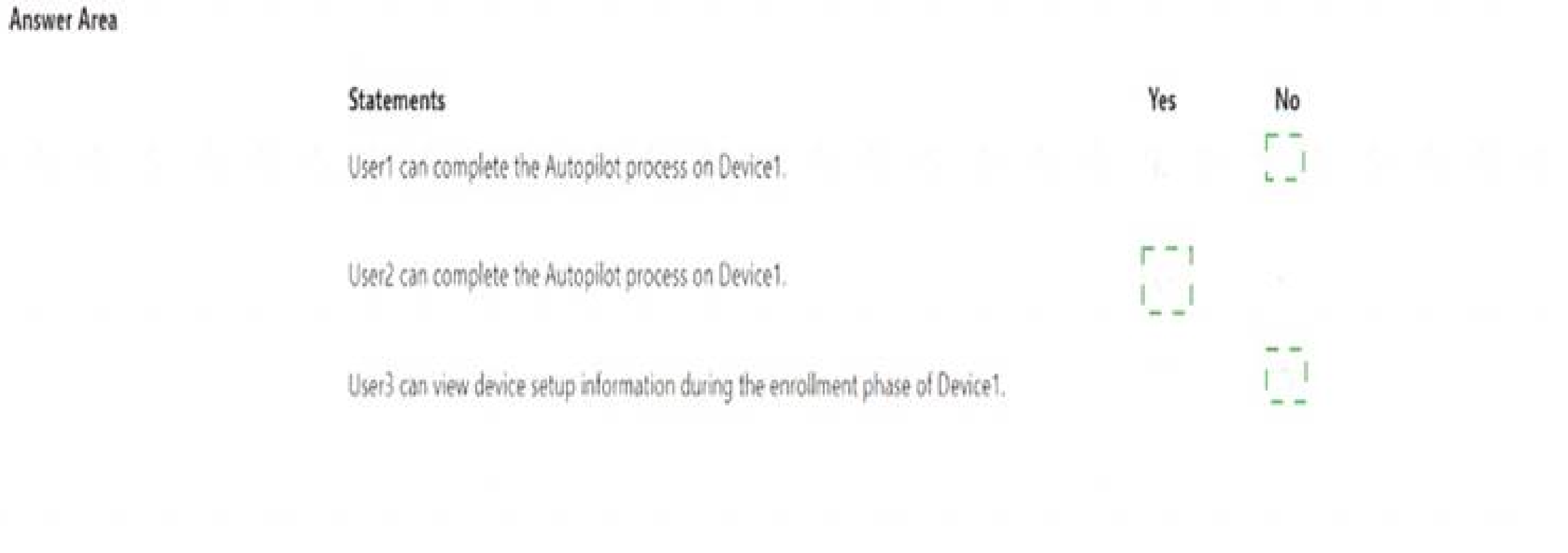
Answer Area

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 76
- (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 78
- (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 79
- (Exam Topic 4)
You have a Microsoft 365 subscription that uses Microsoft Intune Suite.
You use Microsoft Intune to manage devices.
You need to ensure that the startup performance of managed Windows 11 devices is captured and available for review in the Intune admin center.
What should you configure?

A. the Azure Monitor agent
B. a device compliance policy
C. a Conditional Access policy
D. an Intune data collection policy

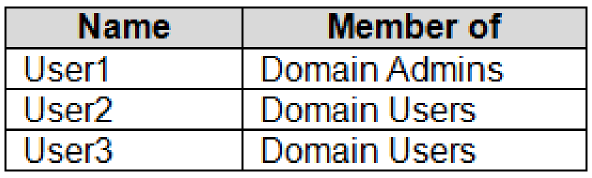
Answer: D

NEW QUESTION 82
- (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

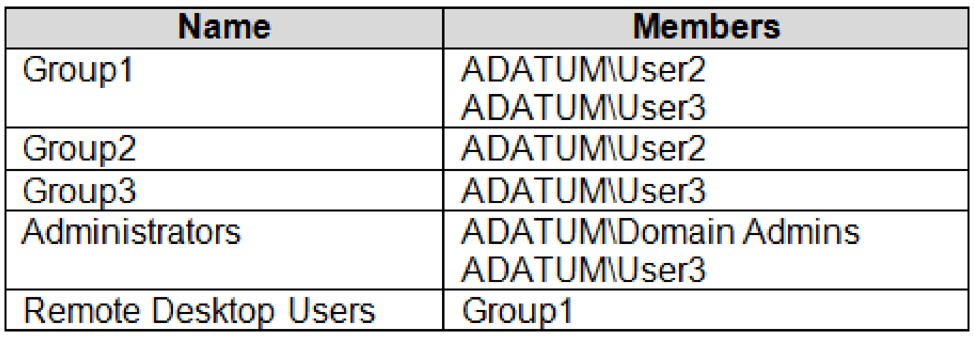
Answer: D

NEW QUESTION 84
- (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.



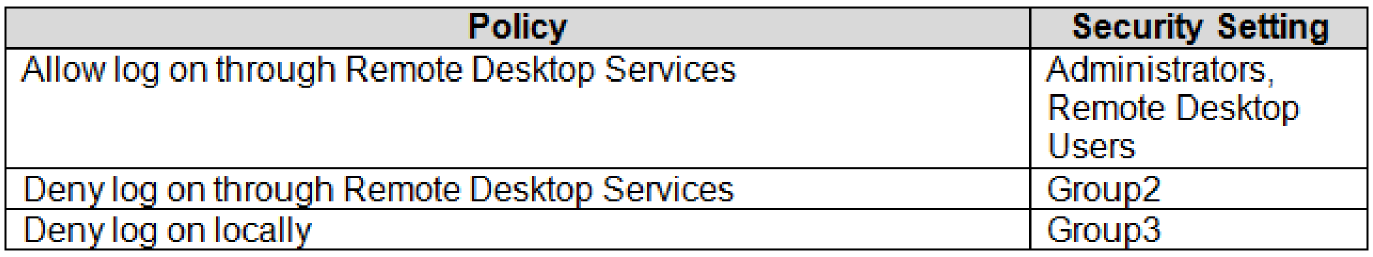
Name	Member of
User1	Domain Admins
User2	Domain Users
User3	Domain Users

Computer2 contains the local groups shown in the following table.



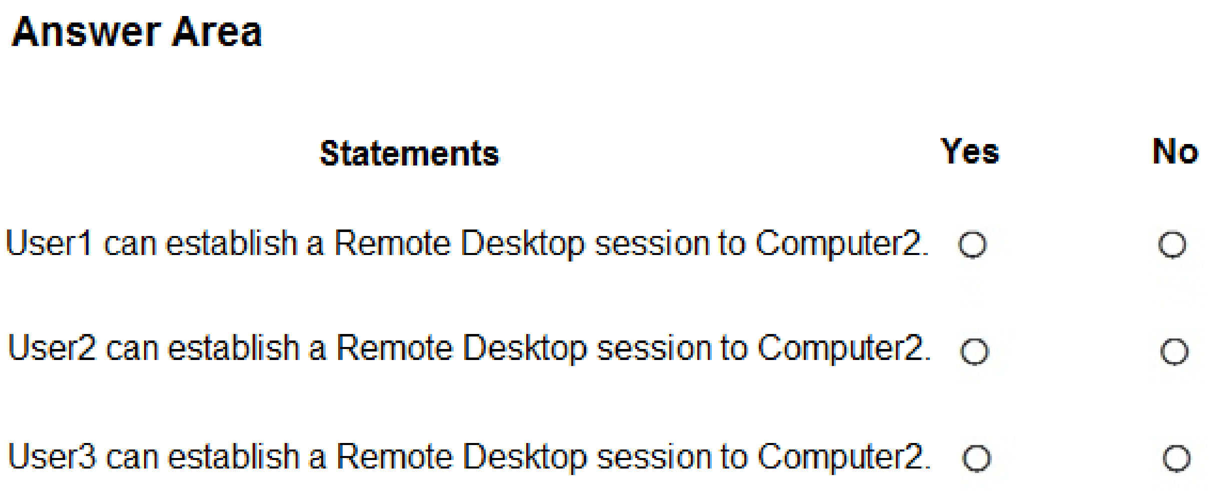
Name	Members
Group1	ADATUM\User2 ADATUM\User3
Group2	ADATUM\User2
Group3	ADATUM\User3
Administrators	ADATUM\Domain Admins ADATUM\User3
Remote Desktop Users	Group1

The relevant user rights assignments for Computed 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.



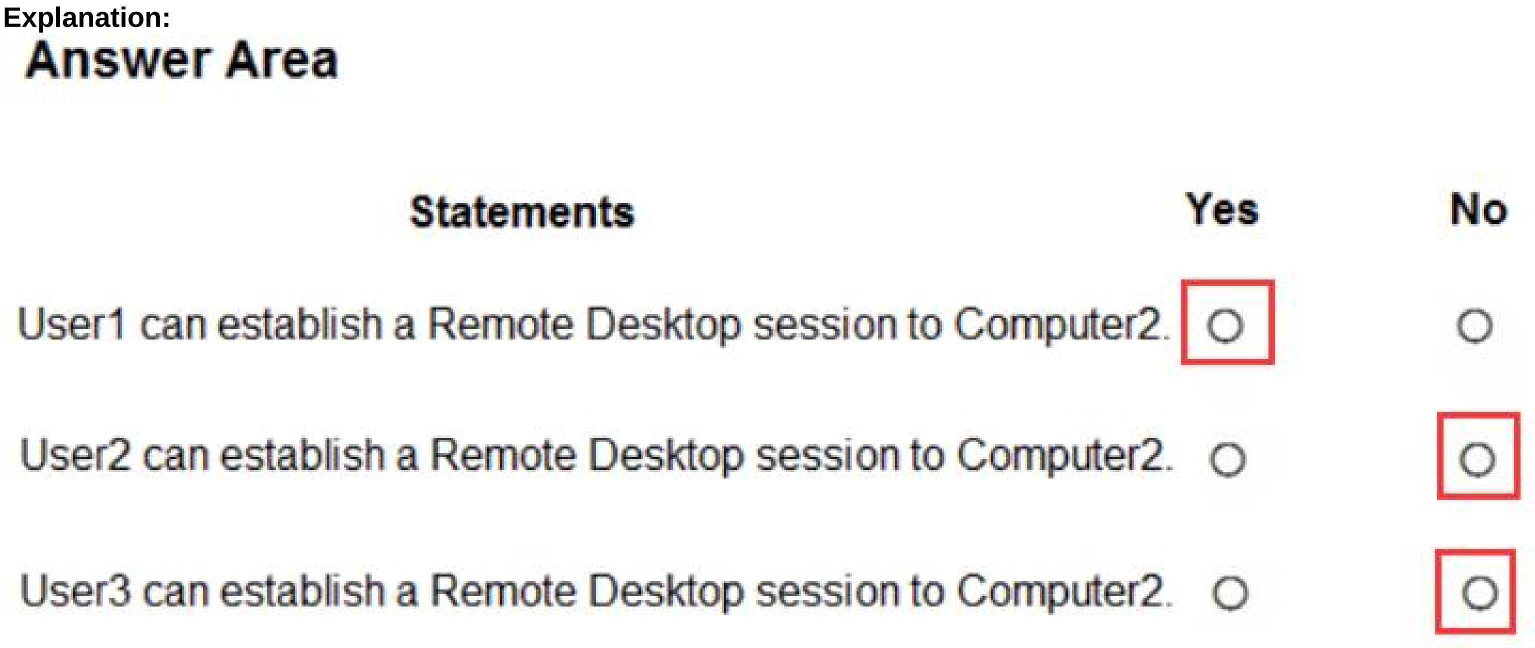
Answer Area

Statements	Yes	No
User1 can establish a Remote Desktop session to Computer2.	○	○
User2 can establish a Remote Desktop session to Computer2.	○	○
User3 can establish a Remote Desktop session to Computer2.	○	○

A. Mastered
B. Not Mastered

Answer: A

Explanation:



Answer Area

Statements	Yes	No
User1 can establish a Remote Desktop session to Computer2.	[✓ ○]	○
User2 can establish a Remote Desktop session to Computer2.	○	[✓ ○]
User3 can establish a Remote Desktop session to Computer2.	○	[✓ ○]

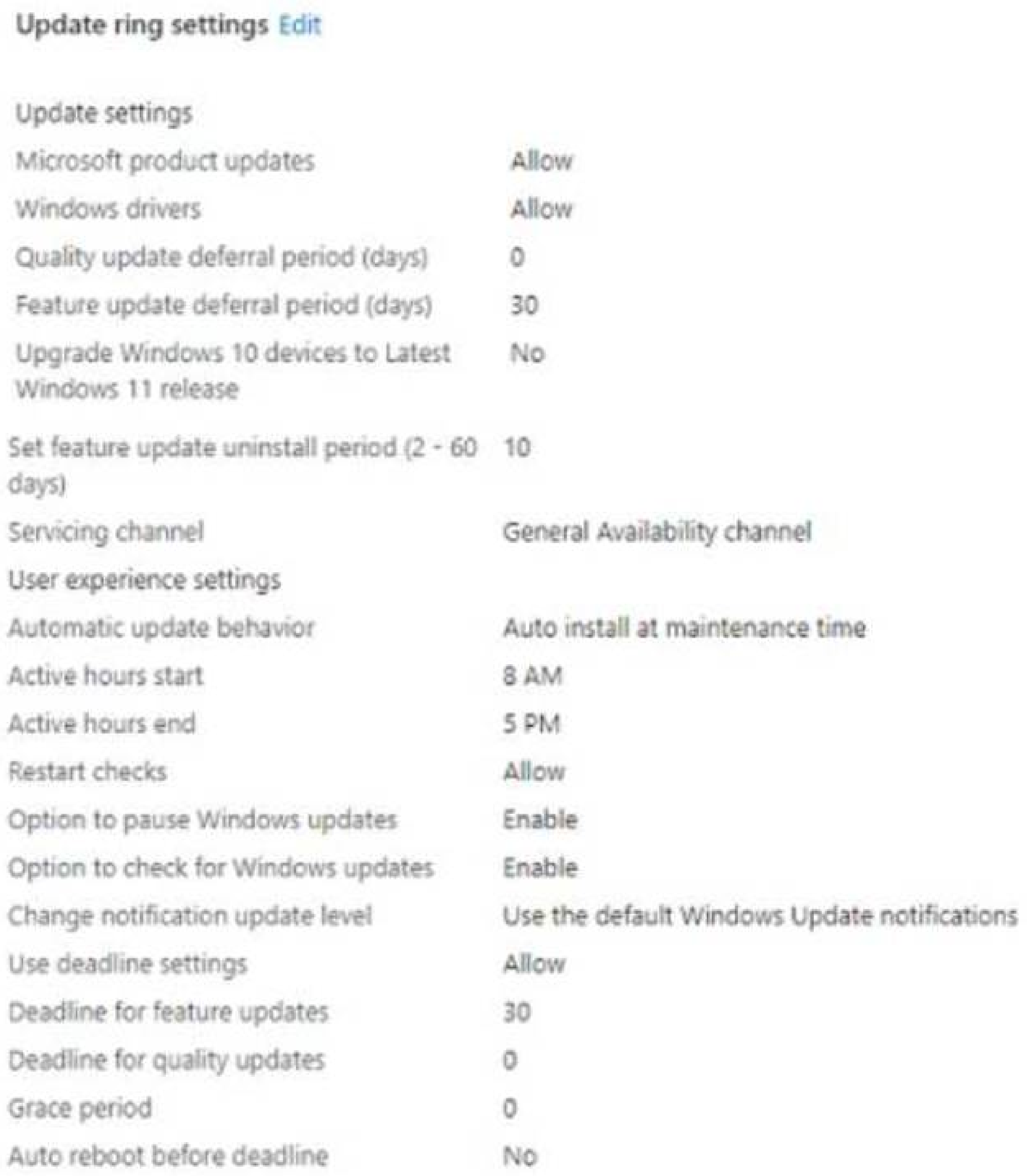
NEW QUESTION 86
- (Exam Topic 4)
You have a Microsoft 365 subscription that contains 1,000 iOS devices and includes Microsoft Intune. You need to prevent the printing of corporate data from managed apps on the devices, should you configure?

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

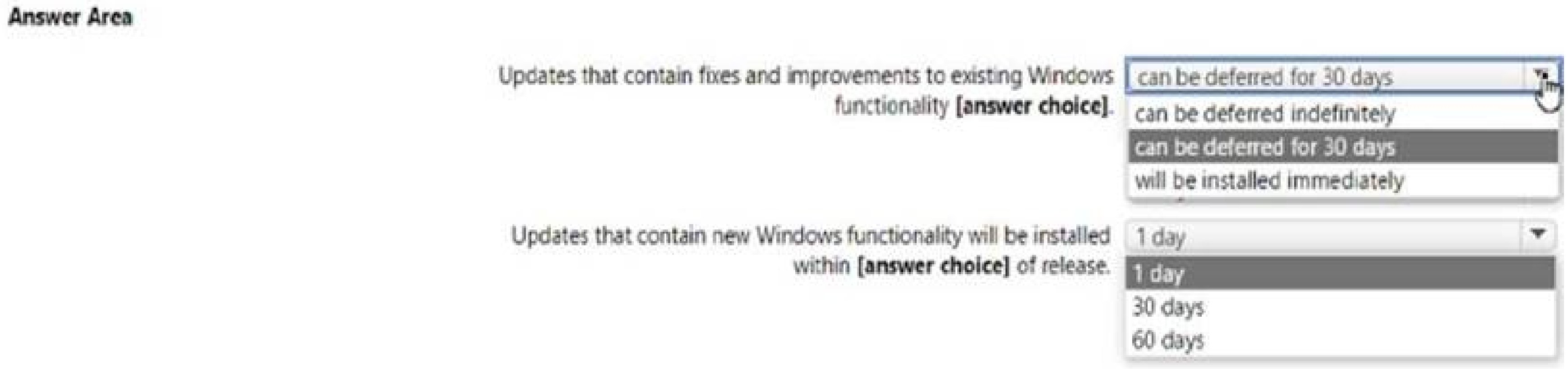
NEW QUESTION 91
- (Exam Topic 4)
You have a Microsoft 365 E5 subscription.
You create a new update rings policy named Policy1 as shown in the following exhibit.



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 95
- (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)

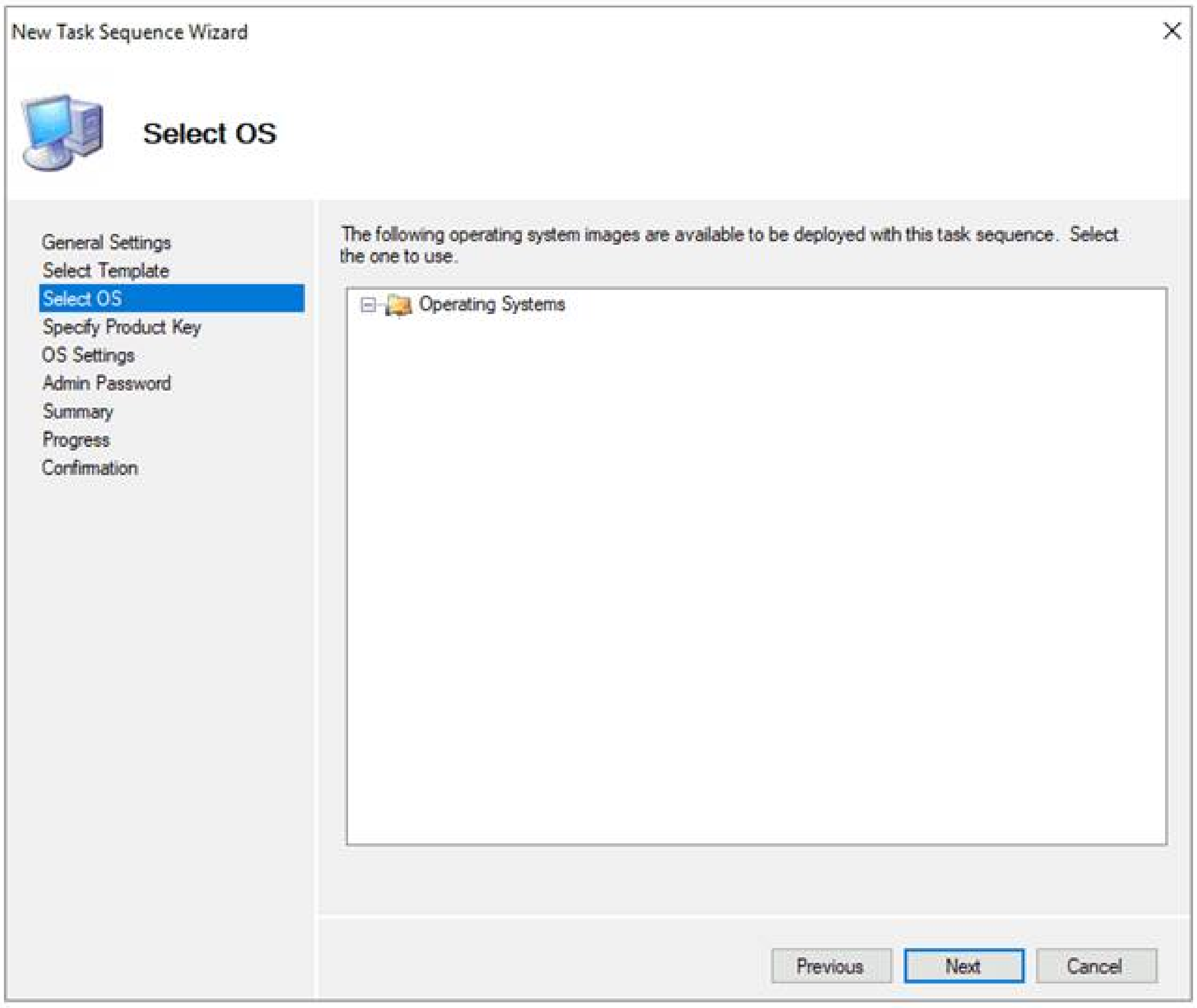
Answer: C

NEW QUESTION 97
- (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 100
- (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.



New Task Sequence Wizard

Select OS

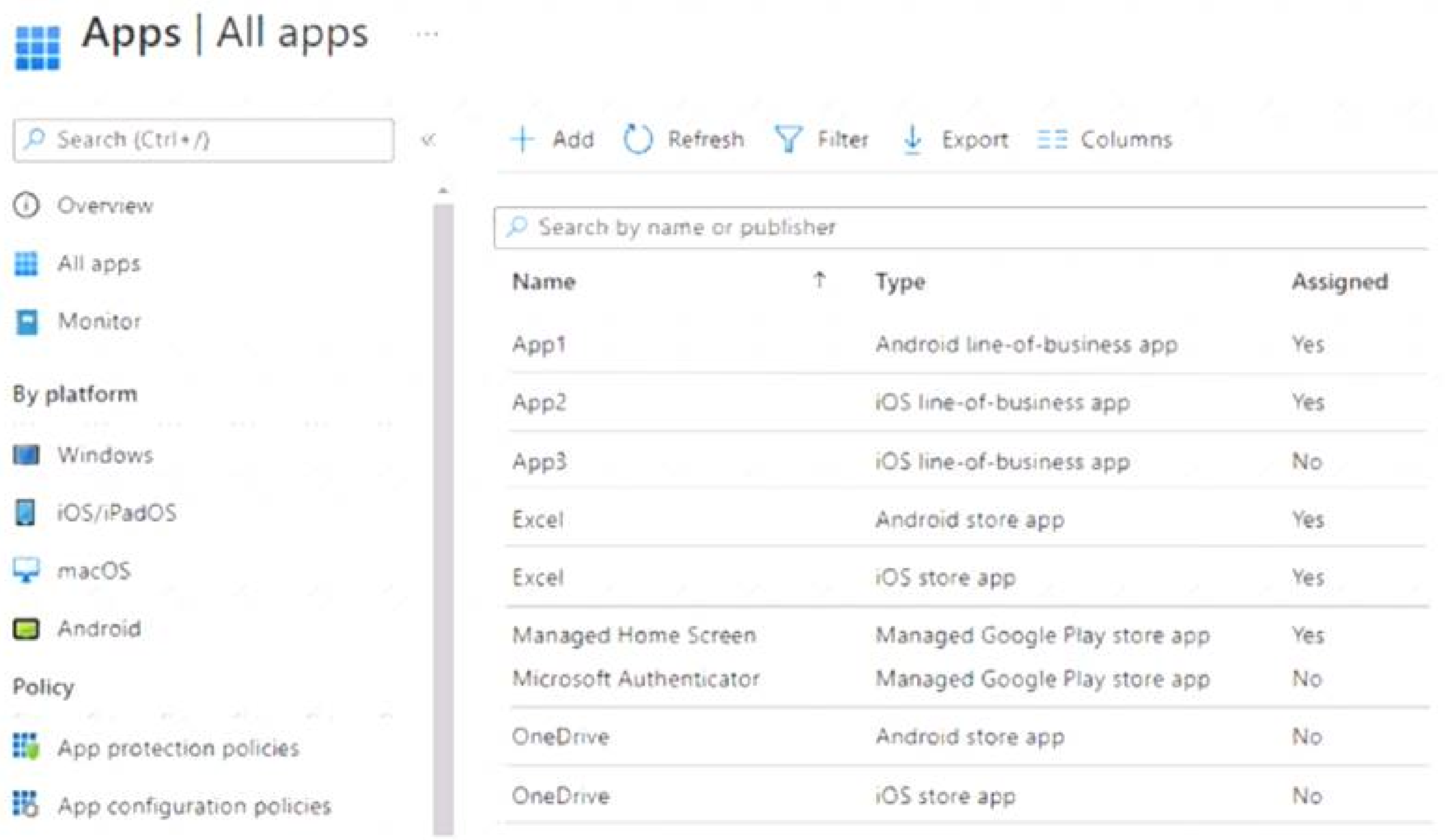
The following operating system images are available to be deployed with this task sequence. Select the one to use.

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 102
- (Exam Topic 4)
You have a Microsoft 365 ES subscription that uses Microsoft Intune. You have the apps shown in the following exhibit.

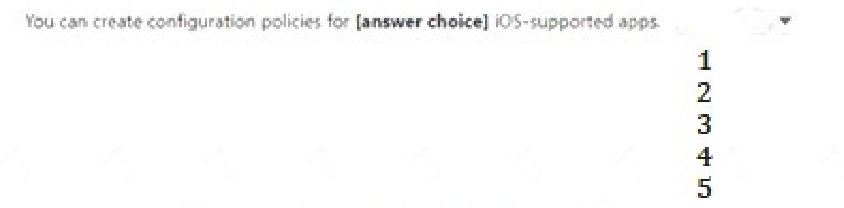


Apps | All apps ...

Name	Type	Assigned
App1	Android line-of-business app	Yes
App2	iOS line-of-business app	Yes
App3	iOS line-of-business app	No
Excel	Android store app	Yes
Excel	iOS store app	Yes
Managed Home Screen	Managed Google Play store app	Yes
Microsoft Authenticator	Managed Google Play store app	No
OneDrive	Android store app	No
OneDrive	iOS store app	No

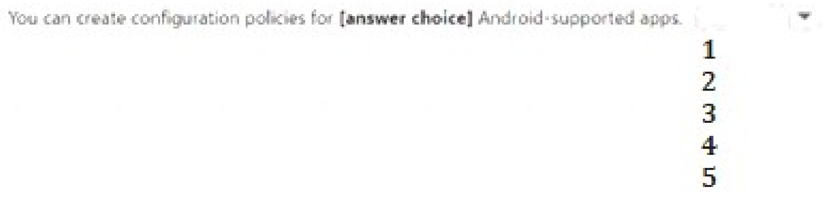
Use the drop-down menus to select the answer choice that completes each statement based upon the information presented in the graphic.

NOTE: Each correct selection is worth one point.



You can create configuration policies for **[answer choice]** iOS-supported apps.

1
2
3
4
5



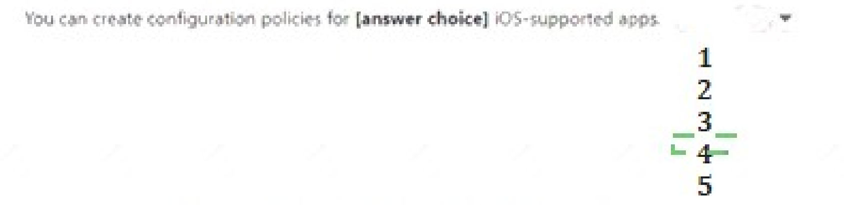
You can create configuration policies for **[answer choice]** Android-supported apps.

1
2
3
4
5

A. Mastered
B. Not Mastered

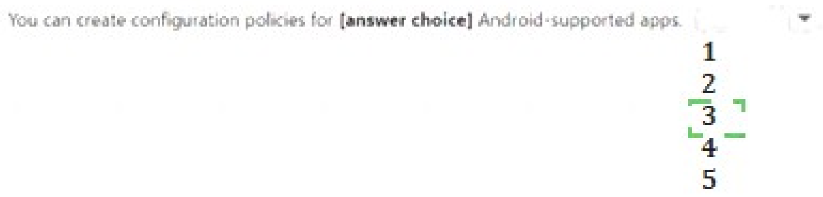
Answer: A

Explanation:



You can create configuration policies for **[answer choice]** iOS-supported apps.

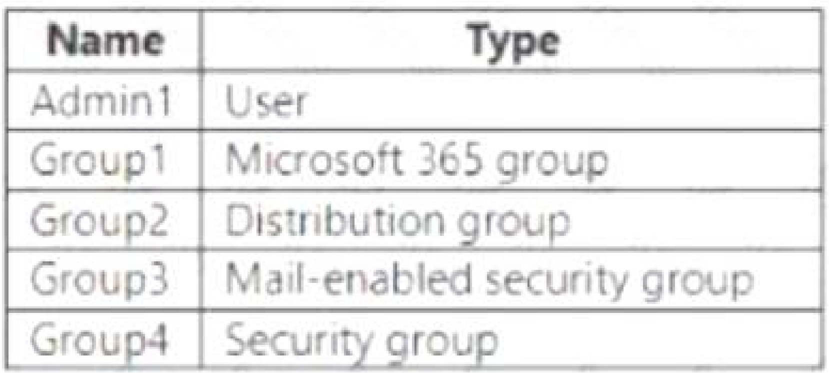
1
2
3
[✓ 4]
5



You can create configuration policies for **[answer choice]** Android-supported apps.

1
2
[✓ 3]
4
5

NEW QUESTION 104
- (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, andGroup4

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.

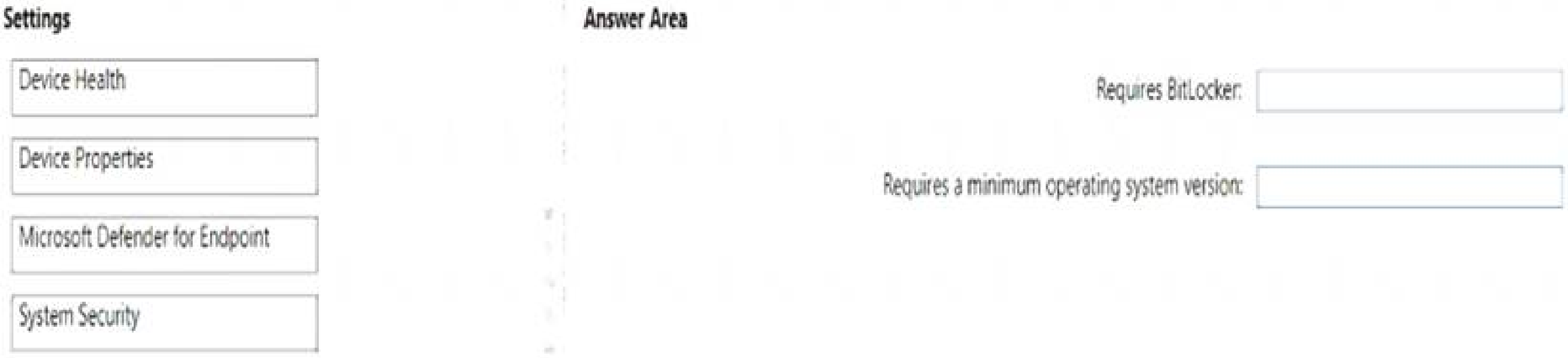
role group.
Since App1 is a Microsoft 365 Apps app, it can only be assigned to users, not devices. Therefore, Group2 and Group4 are not valid objects for app assignment. Admin1 is also not a valid object for app assignment, because individual user accounts can only be used for testing purposes, not for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

NEW QUESTION 107
- (Exam Topic 4)
You have a Microsoft 365 subscription that uses Microsoft Intune Suite.
You use Microsoft Intune to manage devices. All devices are in the same time zone. You create an update rings policy and assign the policy to all Windows devices.
On the November 1, you pause the update rings policy. All devices remain online.
Without further modification to the policy, on which date will the devices next attempt to update?

A. December 1
B. December 6
C. November 15
D. November 22

Answer: C

NEW QUESTION 109
- (Exam Topic 4)
You have a Microsoft 365 subscription. The subscription contains computers that run Windows 11 and are enrolled in Microsoft Intune. You need to create a compliance policy that meets the following requirements:
• Requires BitLocker Drive Encryption (BitLocker) on each device
• Requires a minimum operating system version
Which setting of the compliance policy should you configure for each requirement? To answer, drag the appropriate settings to the correct requirements. Each setting may be used once, more than once, or not at all. You may need to drag the split bar between panes or scroll to view content.
NOTE: Each correct selection is worth one point,



Settings

Device Health

Device Properties

Microsoft Defender for Endpoint

System Security

Answer Area

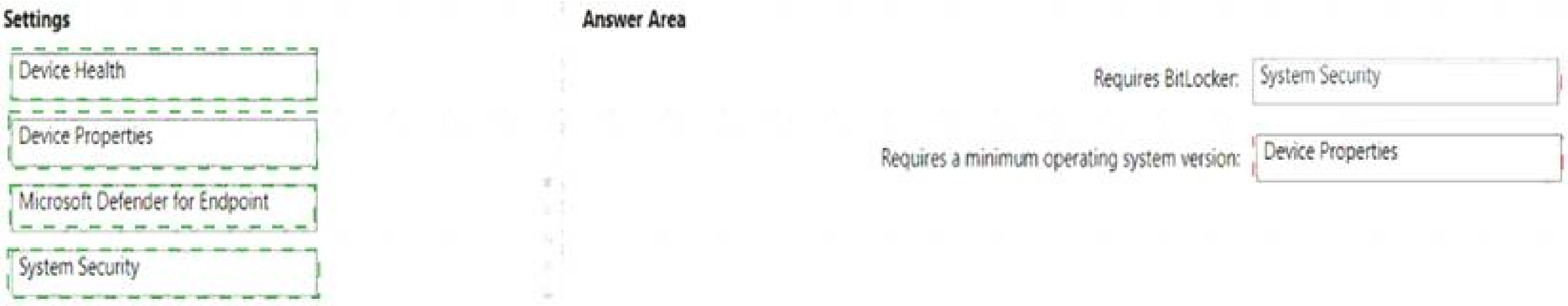
Requires BitLocker:

Requires a minimum operating system version:

A. Mastered
B. Not Mastered

Answer: A

Explanation:



Settings

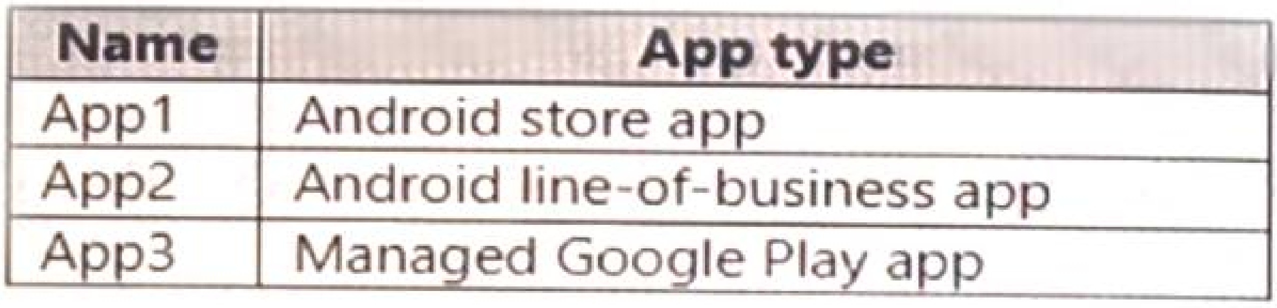
- Device Health
- Device Properties
- Microsoft Defender for Endpoint
- System Security

Answer Area

Requires BitLocker: System Security

Requires a minimum operating system version: Device Properties

NEW QUESTION 114
- (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.



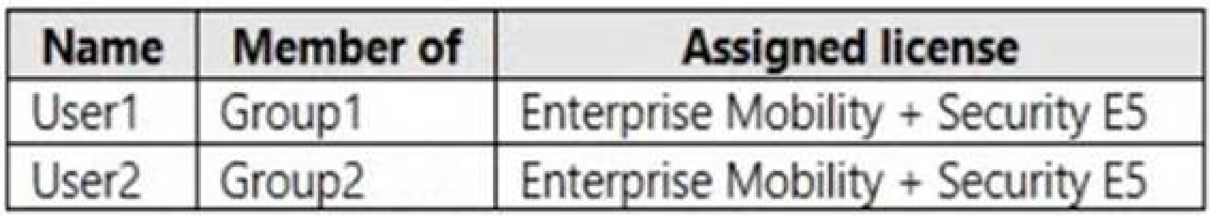
Name	App type
App1	Android store app
App2	Android line-of-business app
App3	Managed Google Play app

You need to create an app configuration policy named Policy1 for the Android Enterprise platform. Which apps can you manage by using Policyl1?

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

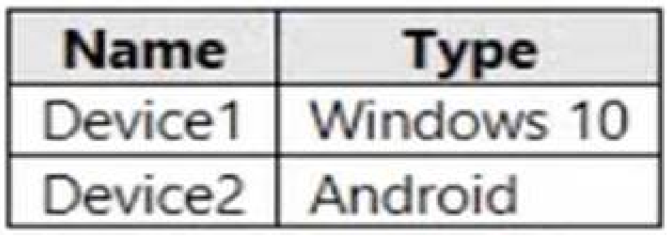
Answer: D

NEW QUESTION 118
- (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.

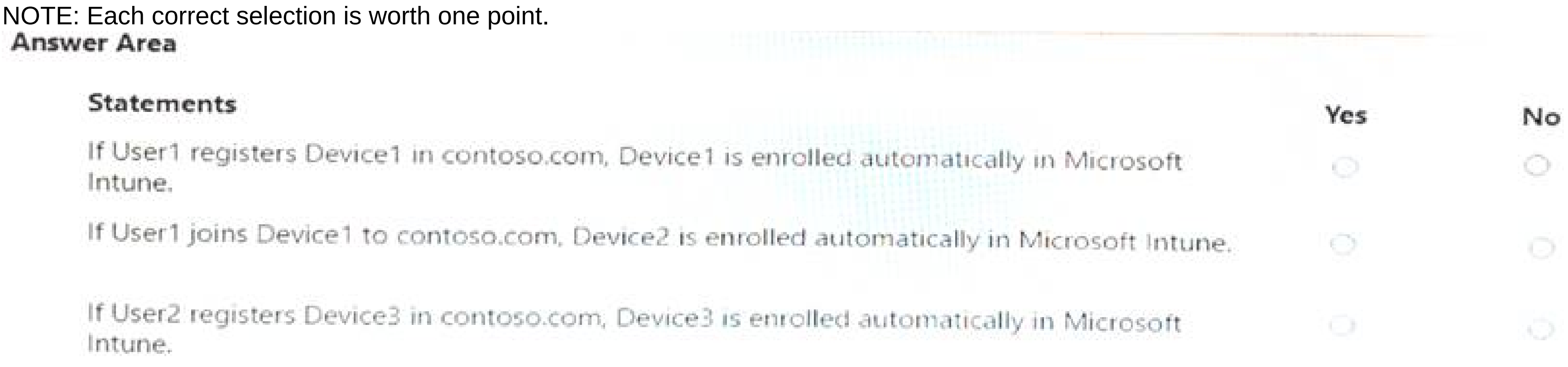


Name	Type
Device1	Windows 10
Device2	Android

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

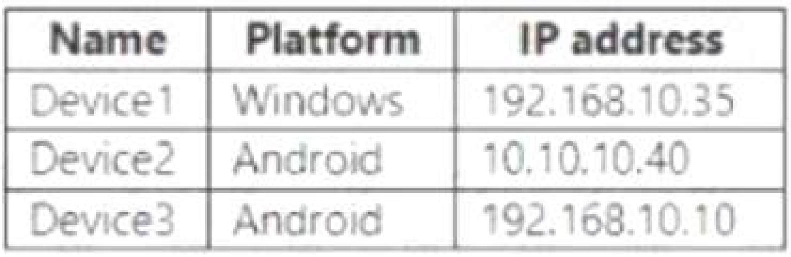
Statements	Yes	No
If User1 registers Device1 in contoso.com, Device1 is enrolled automatically in Microsoft Intune.	○	○
If User1 joins Device1 to contoso.com, Device2 is enrolled automatically in Microsoft Intune.	○	○
If User2 registers Device3 in contoso.com, Device3 is enrolled automatically in Microsoft Intune.	○	○

A. Mastered
B. Not Mastered

Answer: A

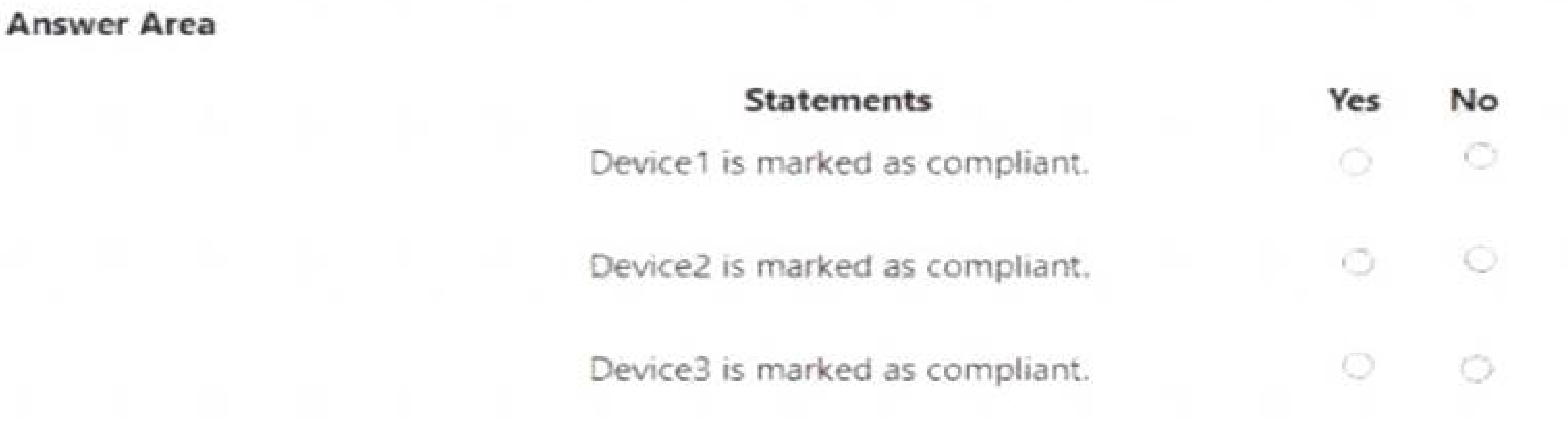
Explanation:
Reference: https://docs.microsoft.com/en-us/mem/intune/enrollment/android-enroll https://powerautomate.microsoft.com/fr-fr/blog/mam-flow-mobile/

NEW QUESTION 120
- (Exam Topic 4)
You have devices that are not rooted enrolled in Microsoft Intune as shown in the following table.



Name	Platform	IP address
Device1	Windows	192.168.10.35
Device2	Android	10.10.10.40
Device3	Android	192.168.10.10

The devices are members of a group named Group1.
In Intune, you create a device compliance location that has the following configurations:
• Name: Network1
• IPv4 range: 192.168.0.0/16
In Intune. you create a device compliance policy for the Android platform. The policy has the following configurations:
• Name: Policy1
• Device health: Rooted devices: Block
• Locations: Location: Network1
• Mark device noncompliant: Immediately
• Assigned: Group1
The Intune device compliance policy has the following configurations:
• Mark devices with no compliance policy assigned as: Compliant
• Enhanced jailbreak detection: Enabled
• Compliance status validity period (days): 20
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 compliant. = No

➢ Device1 is marked as noncompliant because it is rooted and the device compliance policy Policy1 blocks rooted devices under the Device health setting1.

➢ Device2 is marked as compliant because it is not rooted and it is within the network location Network1 that is specified in the device compliance policy Policy11.

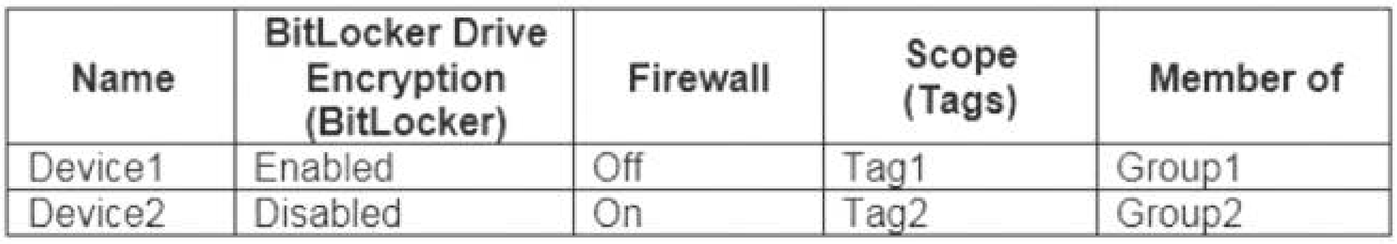
➢ Device3 is marked as noncompliant because it is outside the network location Network1 that is specified in the device compliance policy Policy11. The device compliance location setting requires devices to be in a specific network range to be compliant2.

NEW QUESTION 123
- (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 127
- (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.

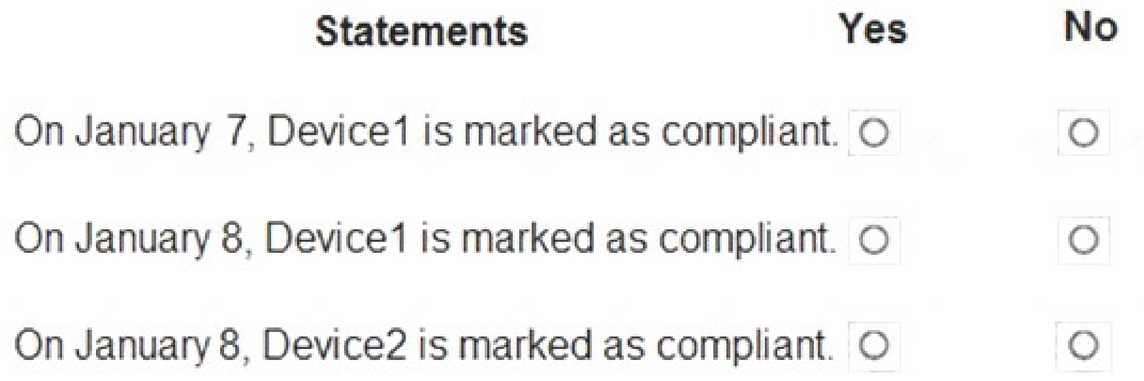


Name	BitLocker Drive Encryption (BitLocker)	Firewall	Scope (Tags)	Member of
Device1	Enabled	Off	Tag1	Group1
Device2	Disabled	On	Tag2	Group2

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.	○	○
On January 8, Device1 is marked as compliant.	○	○
On January 8, Device2 is marked as compliant.	○	○

A. Mastered
B. Not Mastered

Answer: A

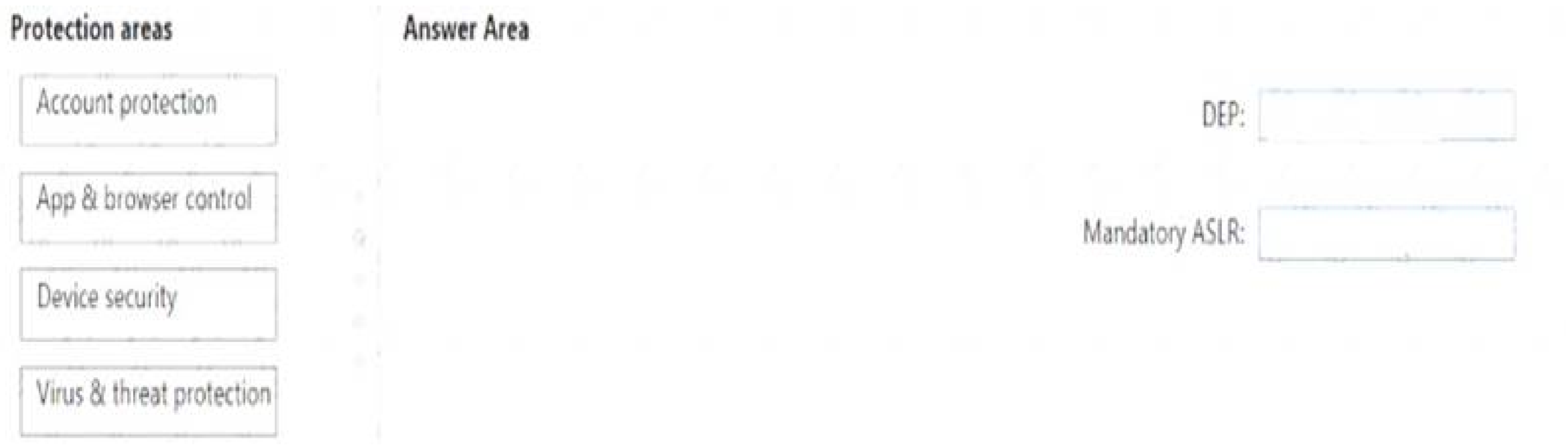
Explanation:
Box 1: No.
Policy1 and Policy2 apply to Group1 which Device1 is a member of. Device1 does not meet the firewall requirement in Policy2 so the device will immediately be marked as non-compliant.
Box 2: No
For the same reason as Box1. Box 3: Yes
Policy1 and Policy2 apply to Group1. Device2 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 132
- (Exam Topic 4)
You use Microsoft Defender for Endpoint to protect computers that run Windows 10.
You need to assess the differences between the configuration of Microsoft Defender for Endpoint and the Microsoft-recommended configuration baseline.
Which tool should you use?

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

Answer: B

NEW QUESTION 137
- (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

- Account protection
- App & browser control
- Device security
- Virus & threat protection

Answer Area

DEP:

Mandatory ASLR:

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.

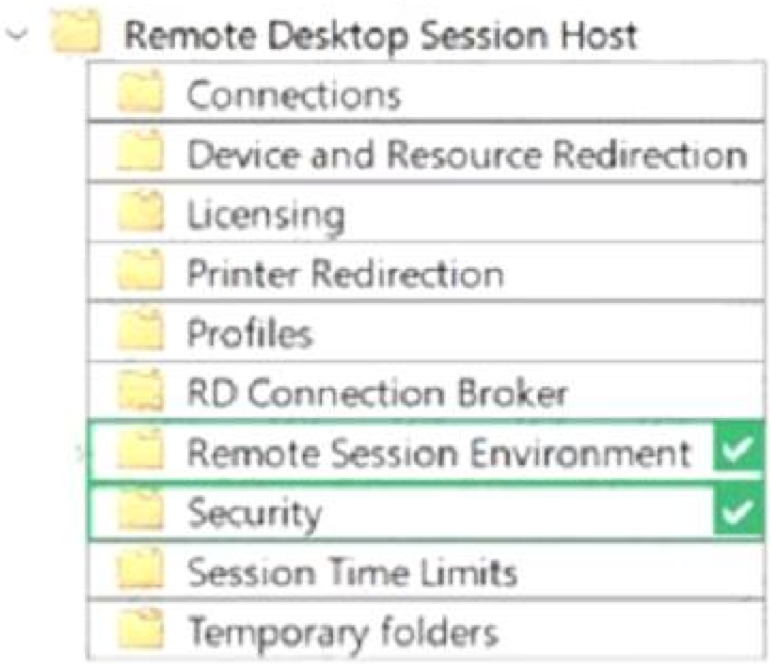
NEW QUESTION 141
- (Exam Topic 4)
You have a Microsoft 365 subscription that contains 500 computers that run Windows 11. The computers are Azure AD joined and are enrolled in Microsoft Intune.
You plan to manage Microsoft Defender Antivirus on the computers. You need to prevent users from disabling Microsoft Defender Antivirus, What should you do?

A. From the Microsoft Intune admin center, create a security baseline.
B. From the Microsoft 365 Defender portal, enable tamper protection.
C. From the Microsoft Intune admin center, create an account protection policy.
D. From the Microsoft Intune admin center, create an endpoint detection and response (EDR) policy.

Answer: B

Explanation:
Tamper protection is a feature of Microsoft Defender Antivirus that prevents users or malicious software from disabling or modifying the antivirus settings. Tamper protection can be enabled from the Microsoft 365 Defender portal for devices that are Azure AD joined and enrolled in Microsoft Intune. This will prevent users from turning off Microsoft Defender Antivirus or changing its configuration through Windows Security, PowerShell, Registry, or Group Policy. References: [Enable tamper protection]

NEW QUESTION 145
- (Exam Topic 4)
Your network contains an Active Directory domain. The domain contains 1.000 computers that run Windows 11.
You need to configure the Remote Desktop settings of all the computers. The solution must meet the following requirements:
• Prevent the sharing of clipboard contents.
• Ensure that users authenticate by using Network Level Authentication (NLA).
Which two nodes of the Group Policy Management Editor should you use? To answer, select the appropriate nodes in the answer area. NOTE: Each correct selection is worth one point.



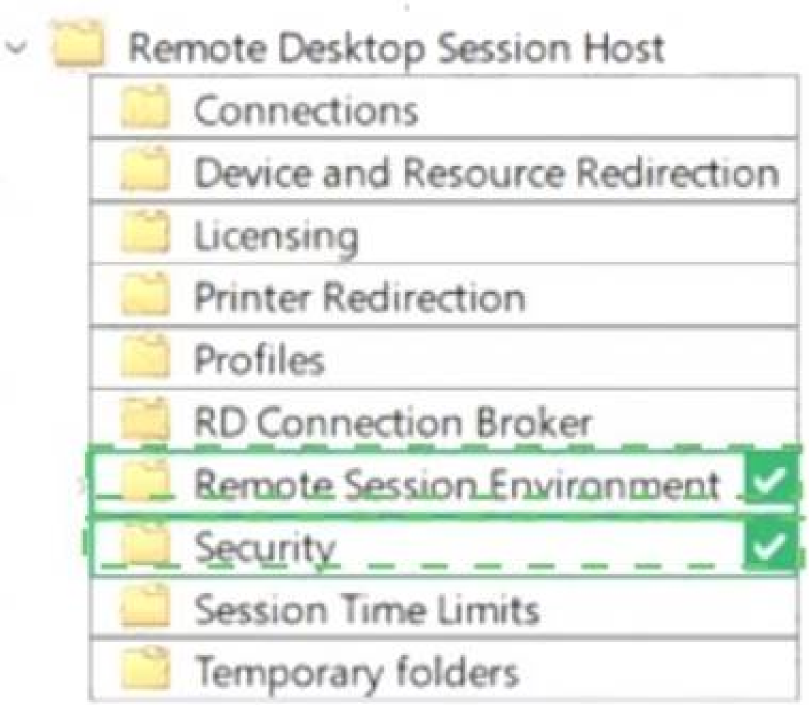
Remote Desktop Session Host

- Connections
- Device and Resource Redirection
- Licensing
- Printer Redirection
- Profiles
- RD Connection Broker
- Remote Session Environment ✓
- Security ✓
- Session Time Limits
- Temporary folders

A. Mastered
B. Not Mastered

Answer: A

Explanation:



- Remote Desktop Session Host
  - Connections
  - Device and Resource Redirection
  - Licensing
  - Printer Redirection
  - Profiles
  - RD Connection Broker
  - Remote Session Environment ✓
  - Security ✓
  - Session Time Limits
  - Temporary folders

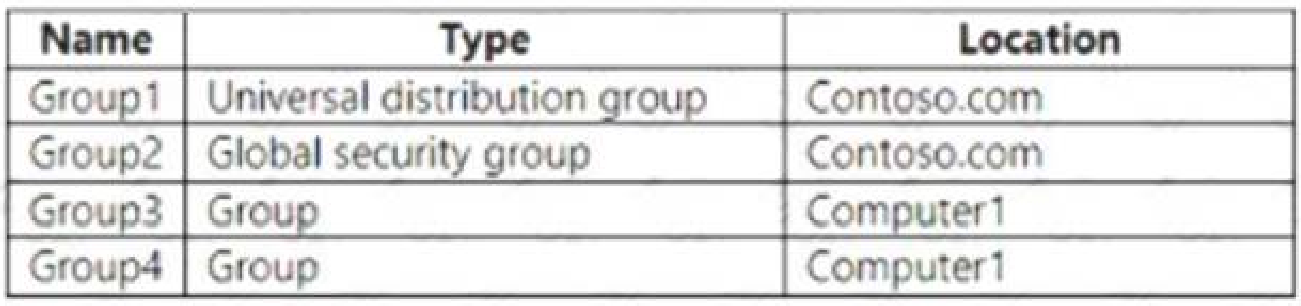
NEW QUESTION 148
- (Exam Topic 4)
You have a Microsoft 365 subscription.
You need provide a user the ability to disable Security defaults and principle of least privilege. Which role should you assign to the user?

A. Global Administrator
B. Conditional Access Administrator
C. Security Administrator
D. Intune Administrator

Answer: B

Explanation:
To enable or disable security defaults in your directory, sign in to theAzure portalas a security administrator, Conditional Access administrator, or global administrator.
Note: Conditional Access Administrator
Users with this role have the ability to manage Azure Active Directory Conditional Access settings.
Reference:
https://docs.microsoft.com/en-us/azure/active-directory/fundamentals/concept-fundamentals-security-defaults

NEW QUESTION 150
- (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 151
......