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 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 3
- (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 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

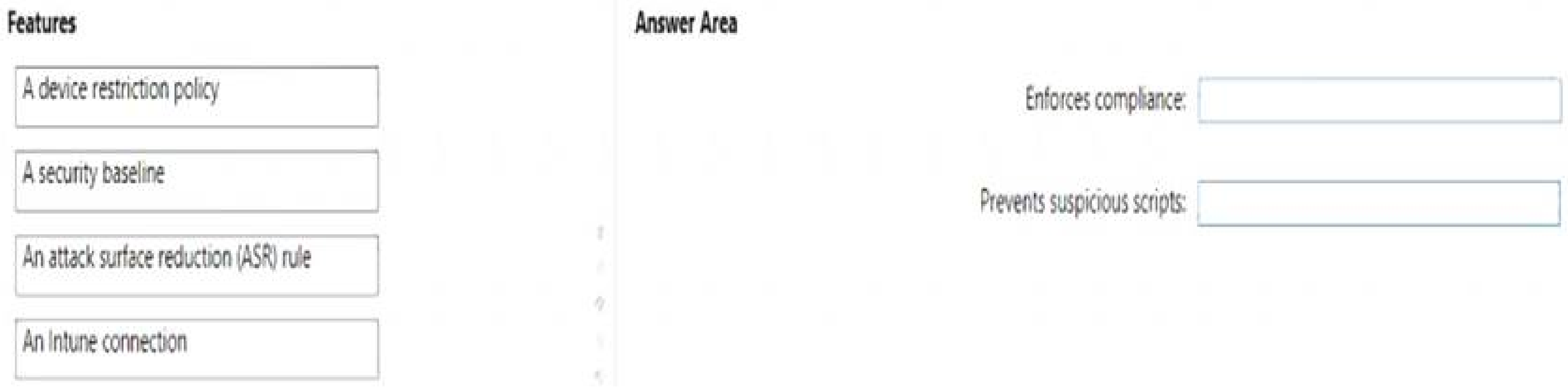
Explanation:
To ensure that users are not added automatically to the local Administrators group when they join their Windows 11 device to contoso.com, you should configure the Device settings in Azure AD. The Device settings allow you to manage which users can join devices to Azure AD and whether they 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 365 subscription that includes Microsoft Intune.
You need to implement a Microsoft Defender for Endpoint solution that meets the following requirements:
• Enforces compliance for Defender for Endpoint by using Conditional Access
• Prevents suspicious scripts from running on devices
What should you configure? To answer, drag the appropriate features to the correct requirements. Each feature may be used once, more than once, or not at all. You may need to drag the split bar between panes or scroll to view content.
NOTE: Each correct selection is worth one point.



Features

A device restriction policy

A security baseline

An attack surface reduction (ASR) rule

An Intune connection

Answer Area

Enforces compliance:

Prevents suspicious scripts:

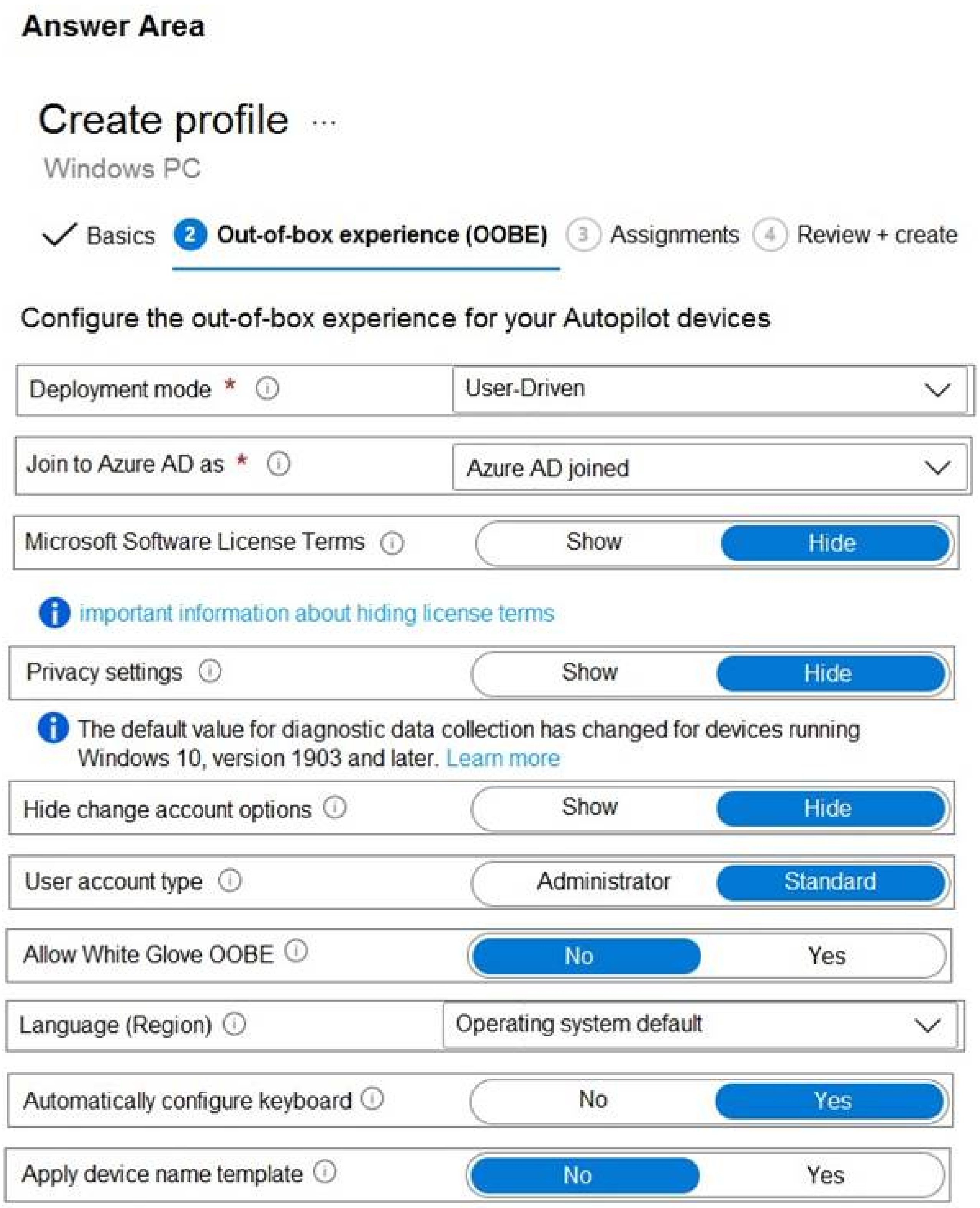
A. Mastered
B. Not Mastered

Answer: A

Explanation:
To enforce compliance for Defender for Endpoint by using Conditional Access, you need to configure an Intune connection in the Defender for Endpoint portal. This allows you to use Intune device compliance policies to evaluate the health and compliance status of devices that are enrolled in Defender for Endpoint. You can then use Conditional Access policies to block or allow access to cloud apps based on the device compliance status. References:
https://docs.microsoft.com/en-us/windows/security/threat-protection/microsoft-defender-atp/conditional-access
To prevent suspicious scripts from running on devices, you need to configure an attack surface reduction (ASR) rule in Intune. ASR rules are part of the endpoint protection settings that you can apply to devices by using device configuration profiles. You can use the ASR rule “Block Office applications from creating child processes” to prevent Office applications from launching child processes such as scripts or executables. References:
https://docs.microsoft.com/en-us/mem/intune/protect/endpoint-protection-windows-10#attack-surface-reduction

NEW QUESTION 6
- (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]

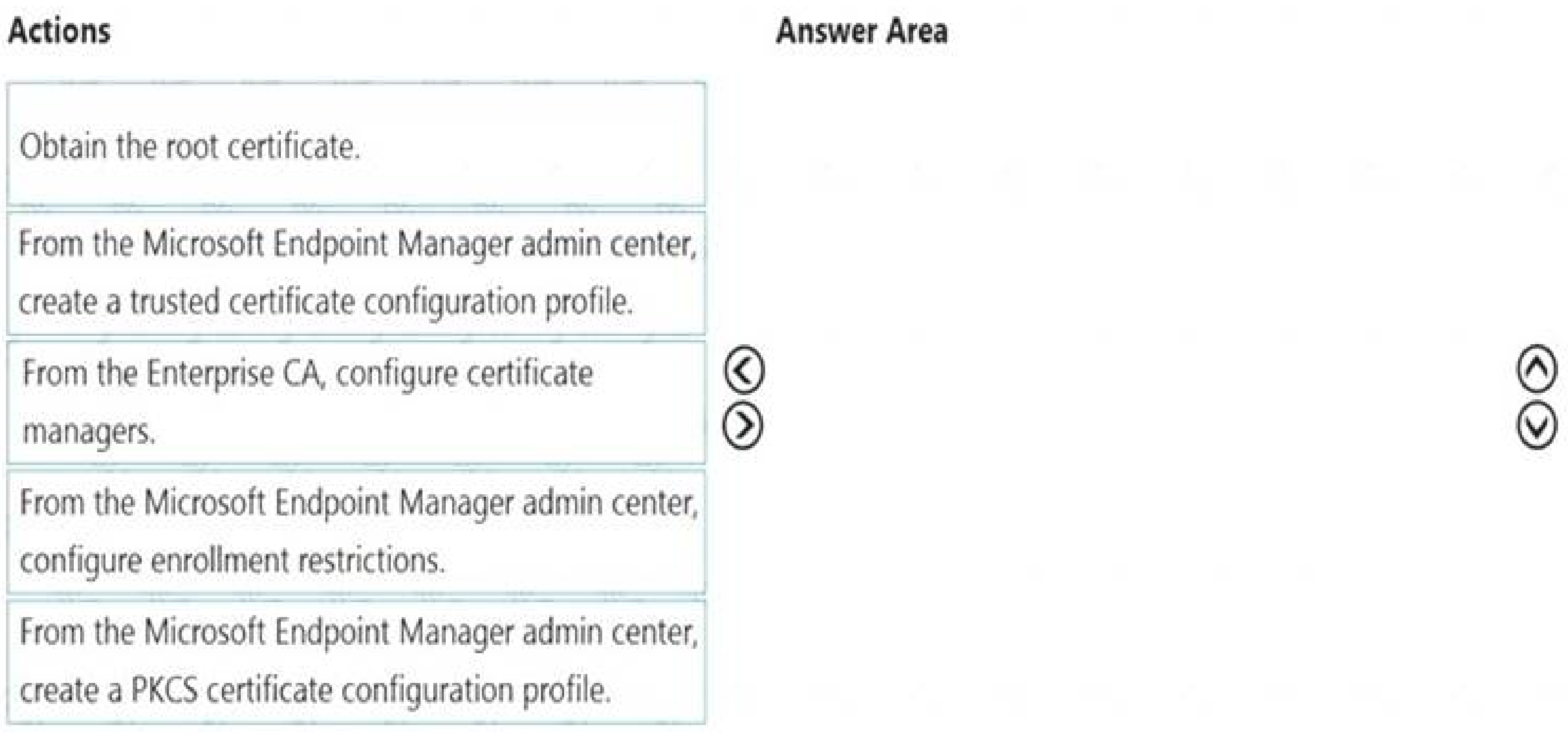
Apply device name template ⓘ: [✓ No] Yes

A. Mastered
B. Not Mastered

Answer: A

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

NEW QUESTION 7
- (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

Answer Area

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.

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 8
- (Exam Topic 4)
You have a Windows 10 device named Device! that is joined to Active Directory and enrolled in Microsoft Intune.
Device1 is managed by using Group Policy and Intune.
You need to ensure that the Intune settings override the Group Policy settings. What should you configure?

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

Answer: A

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

NEW QUESTION 9
- (Exam Topic 4)
You have a computer named Computer! that runs Windows 11.
A user named User1 plans to use Remote Desktop to connect to Computer1.
You need to ensure that the device of User1 is authenticated before the Remote Desktop connection is established and the sign in page appears.
What should you do on Computer1?

A. Turn on Reputation-based protection.
B. Enable Network Level Authentication (NLA).
C. Turn on Network Discovery.
D. Configure the Remote Desktop Configuration service.

Answer: B

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)
You have an Azure AD group named Group1. Group! contains two Windows 10 Enterprise devices named Device1 and Device2. You create a device configuration profile named Profile1. You assign Profile! to Group1. You need to ensure that Profile! applies to Device1 only. What should you modify in Profile 1?

A. Assignments
B. Settings
C. Scope (Tags)
D. Applicability Rules

Answer: D

Explanation:
To ensure that Profile1 applies to Device1 only, you need to modify the Applicability Rules in Profile1. You can use applicability rules to filter which devices receive a profile based on criteria such as device model, manufacturer, or operating system version. You can create an applicability rule that matches Device1's properties and excludes Device2's properties. References:
https://docs.microsoft.com/en-us/mem/intune/configuration/device-profile-assign#applicability-rules

NEW QUESTION 15
- (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

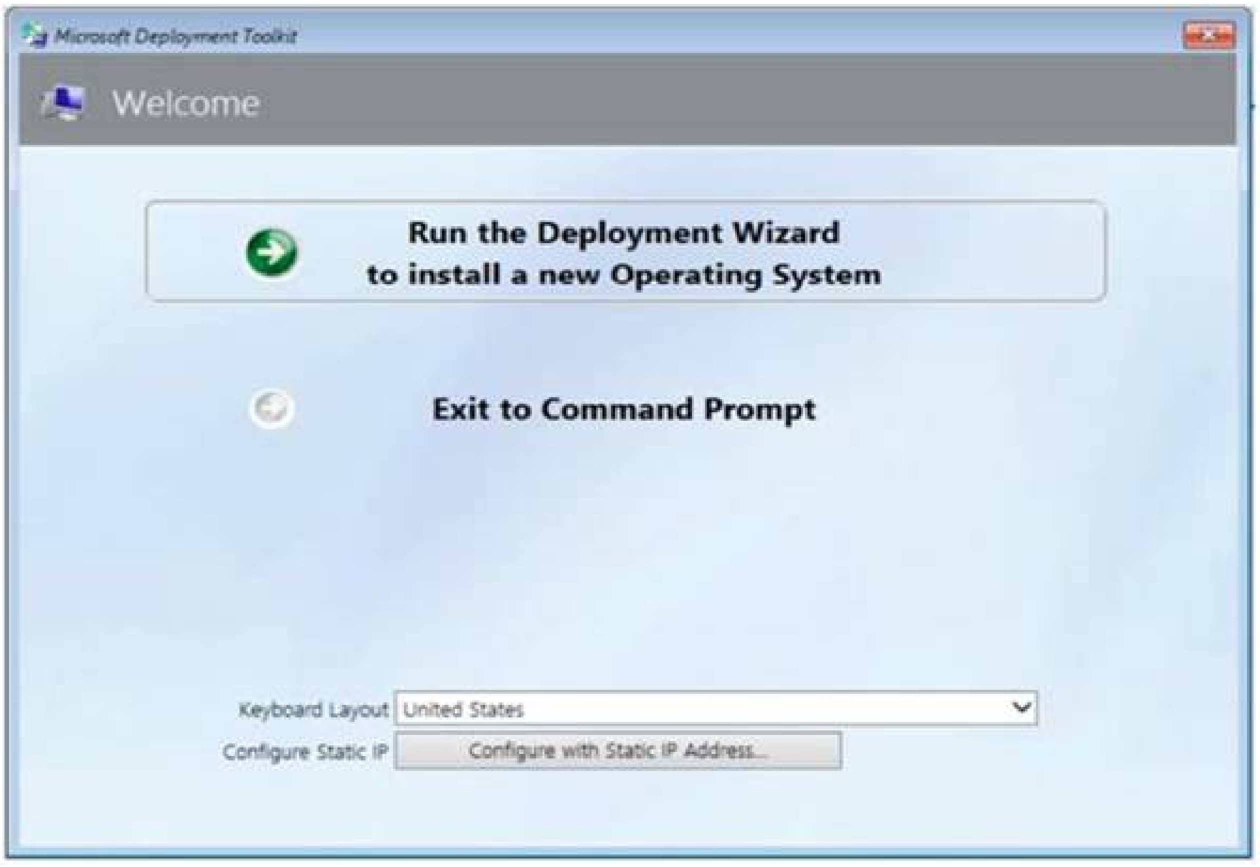
NEW QUESTION 19
- (Exam Topic 4)
You manage 1.000 devices by using Microsoft Intune. You review the Device compliance trends report. For how long will the report display trend data?

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 23
- (Exam Topic 4)
You have a Microsoft Deployment Toolkit (MDT) server named MDT1.
When computers start from the LiteTouchPE_x64.Iso image and connect to MDT1. the welcome screen appears as shown In the following exhibit.



Microsoft Deployment Toolkit

Welcome

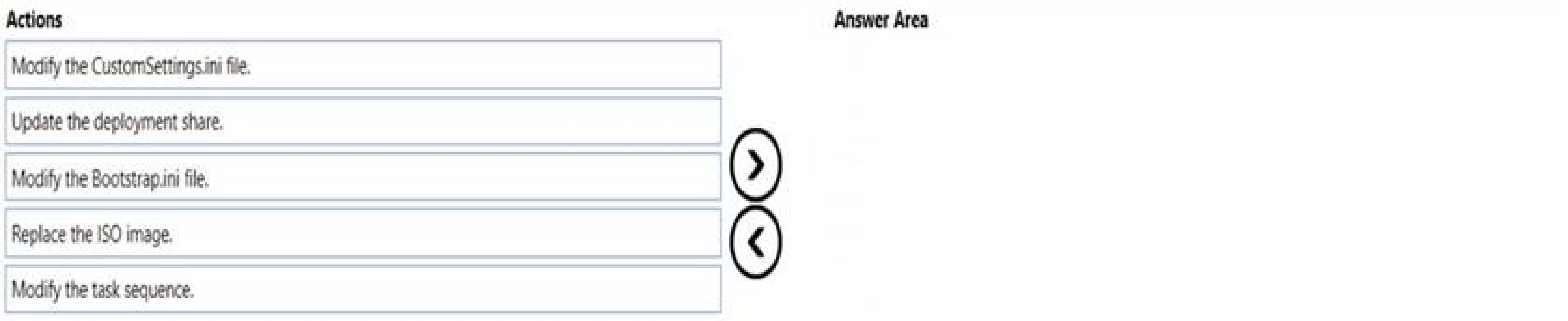
Run the Deployment Wizard
to install a new Operating System

Exit to Command Prompt

Keyboard Layout: United States

Configure Static IP: Configure with Static IP Address...

You need to prevent the welcome screen from appearing when the computers connect to MDT1.
Which three actions should you perform in sequence? To answer move the appropriate actions from the list of actions to the answer area and arrange them in the correct order.



Actions

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

Answer Area

A. Mastered
B. Not Mastered

Answer: A

Explanation:
Box 1: Modify the Bootstrap.ini file.
Add this to your bootstrap.ini file and then update the deployment share and use the new boot media created in that process:
SkipBDDWelcome=YES
Box 2: Modify the CustomSettings.ini file. SkipBDDWelcome
Indicates whether the Welcome to Windows Deployment wizard page is skipped.
For this property to function properly it must be configured in both CustomSettings.ini and BootStrap.ini. BootStrap.ini is processed before a deployment share (which contains CustomSettings.ini) has been selected.
Box 3: Update the deployment share. Reference:
https://docs.microsoft.com/en-us/mem/configmgr/mdt/toolkit-reference#table-6-deployment-wizard-pages

NEW QUESTION 25
- (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 26
- (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

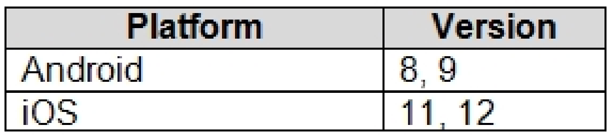
NEW QUESTION 29
- (Exam Topic 4)
You have a Microsoft 365 E5 subscription that contains 1,000 Windows 11 devices. All the devices are enrolled in Microsoft Intune.
You plan to integrate Intune with Microsoft Defender for Endpoint.
You need to establish a service-to-service connection between Intune and Defender for Endpoint. Which settings should you configure in the Microsoft Endpoint Manager admin center?

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

Answer: A

Explanation:
Microsoft Defender for Endpoint – Important Service and Endpoint Settings You Should Configure Right Now.
As a prerequisite, however, head to tenant administration > connectors and tokens > Microsoft Defender for Endpoint and confirm the connection is enabled. You previously set this up in the advanced settings of Microsoft 365 Defender.
Reference: https://petri.com/microsoft-defender-for-endpoint-which-settings-configure-right-now/

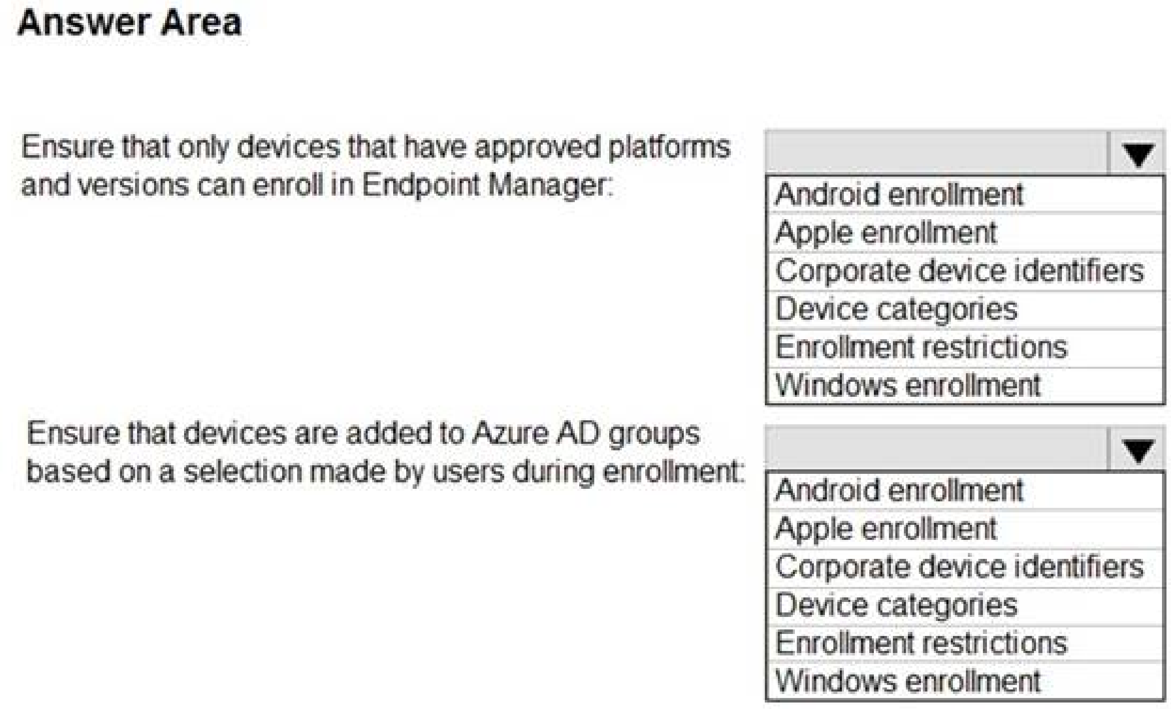
NEW QUESTION 33
- (Exam Topic 4)
You have a Microsoft 365 subscription.
You plan to enroll devices in Microsoft Endpoint Manager that have the platforms and versions shown in the following table.



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:

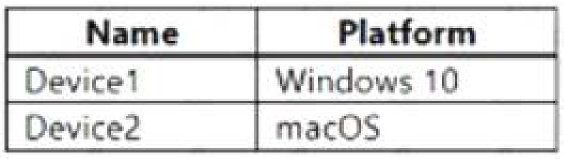
- Android enrollment
- Apple enrollment
- Corporate device identifiers
- Device categories
- Enrollment restrictions
- Windows enrollment

A. Mastered
B. Not Mastered

Answer: A

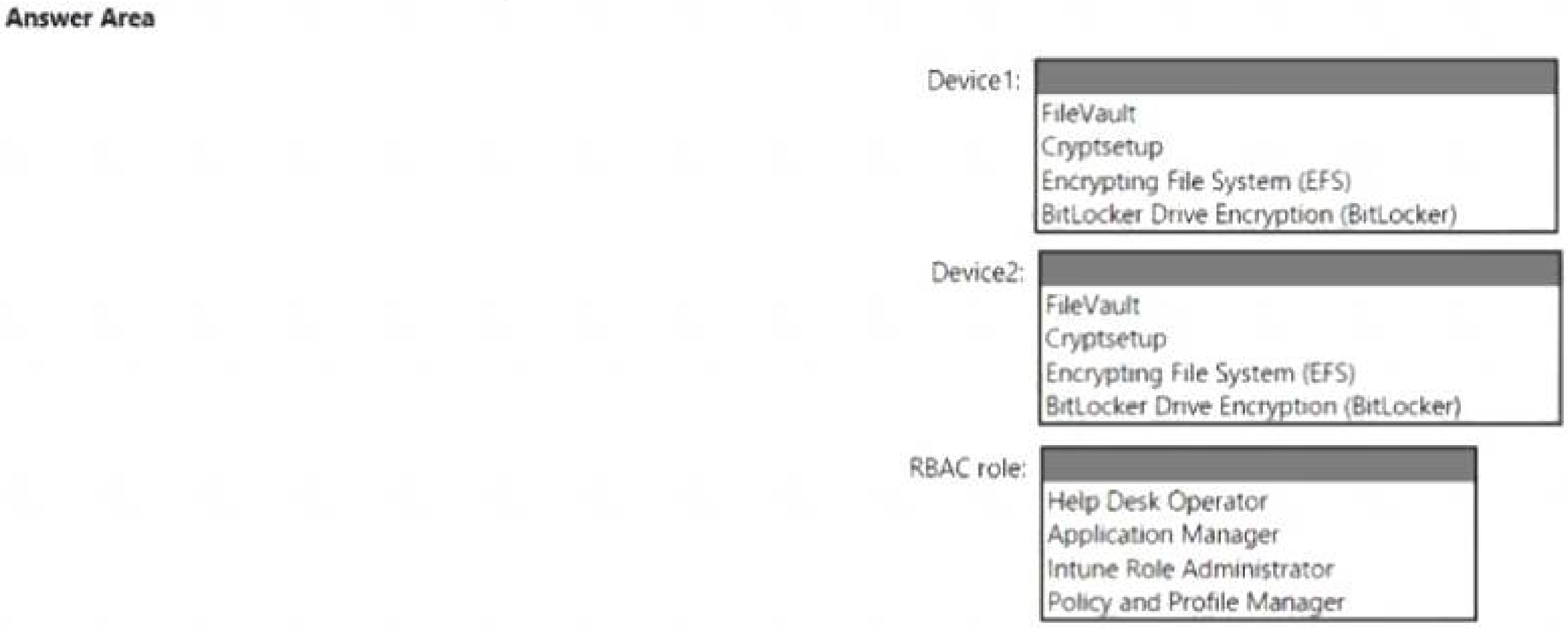
Explanation:
A screenshot of a computer Description automatically generated
Reference:
https://docs.microsoft.com/en-us/mem/intune/enrollment/enrollment-restrictions-set https://docs.microsoft.com/en-us/mem/intune/enrollment/device-group-mapping

NEW QUESTION 35
- (Exam Topic 4)
You have a Microsoft 365 tenant that uses Microsoft Intune and contains the devices shown in the following table.



Name	Platform
Device1	Windows 10
Device2	macOS

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



Answer Area

Device1:
- FileVault
- Cryptsetup
- Encrypting File System (EFS)
- BitLocker Drive Encryption (BitLocker)

Device2:
- FileVault
- Cryptsetup
- Encrypting File System (EFS)
- BitLocker Drive Encryption (BitLocker)

RBAC role:
- Help Desk Operator
- Application Manager
- Intune Role Administrator
- Policy and Profile Manager

A. Mastered
B. Not Mastered

Answer: A

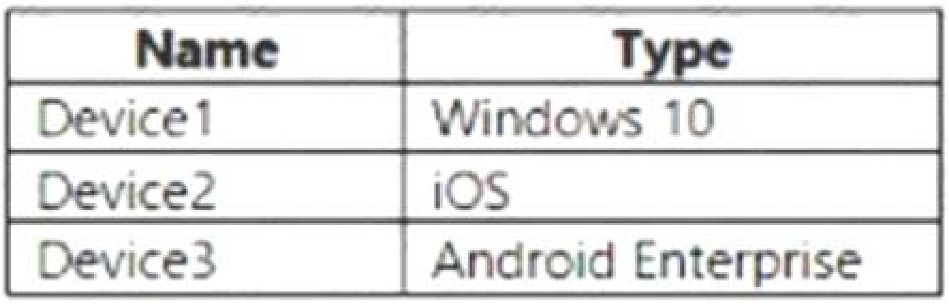
Explanation:
Graphical user interface, text, application Description automatically generated

NEW QUESTION 40
- (Exam Topic 4)
You have a Microsoft 365 subscription that uses Microsoft Intune.
You need to ensure that you can deploy apps to Android Enterprise devices. What should you do first?

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

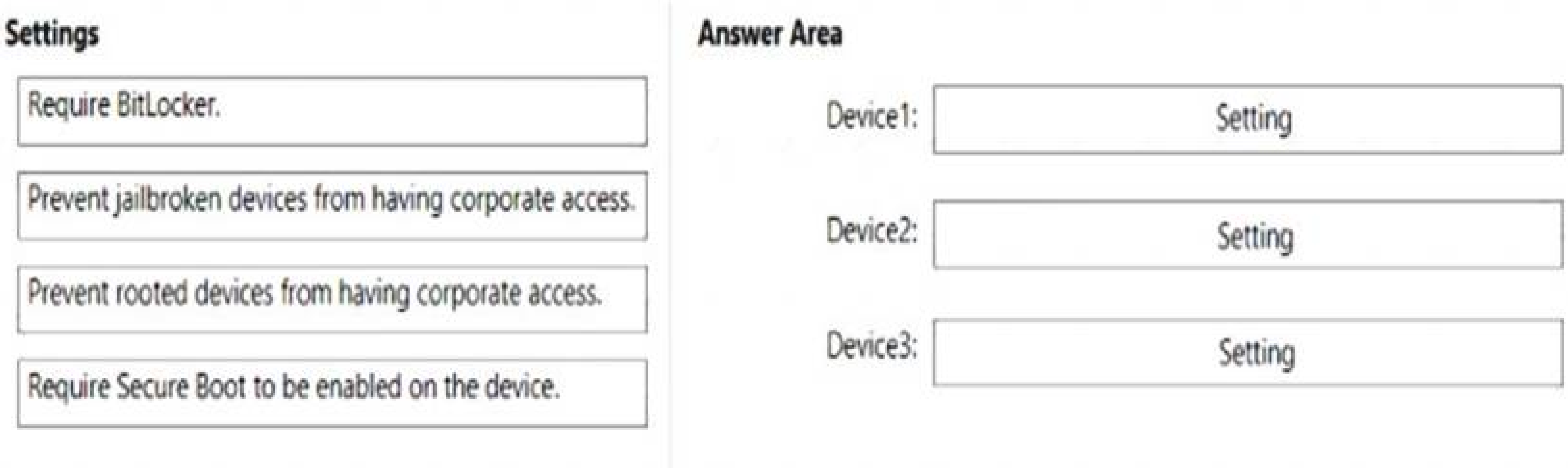
Answer: D

NEW QUESTION 45
- (Exam Topic 4)
You have a Microsoft 365 subscription that contains the devices shown in the following table.



Name	Type
Device1	Windows 10
Device2	iOS
Device3	Android Enterprise

You need to ensure that only devices running trusted firmware or operating system builds can access network resources.
Which compliance policy setting should you configure for each device? To answer, drag the appropriate settings to the correct devices. Each setting may be used once, more than once, or not at all. You may need to drag the split bar between panes or scroll to view content.
NOTE: Each correct selection is worth one point.



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

Answer Area

Device1: Setting
Device2: Setting
Device3: Setting

A. Mastered
B. Not Mastered

Answer: A

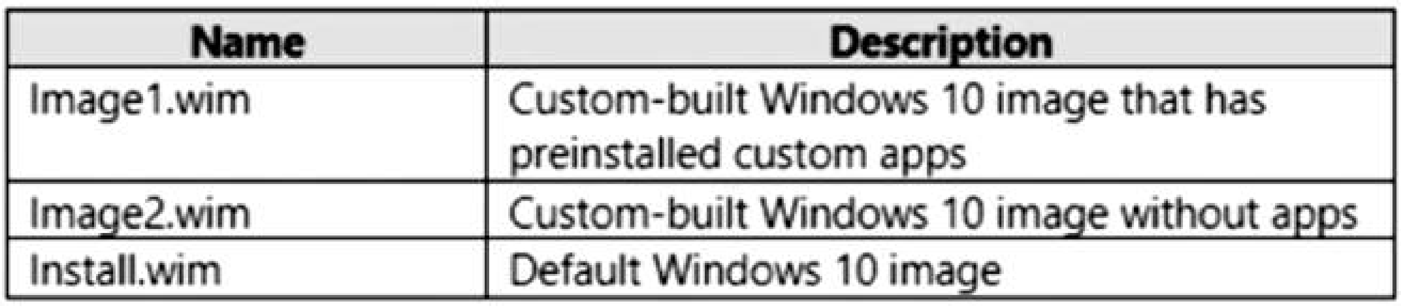
Explanation:
Box 1:
Device Compliance settings for Windows 10/11 in Intune
There are the different compliance settings you can configure on Windows devices in Intune. As part of your mobile device management (MDM) solution, use these settings to require BitLocker, set a minimum and maximum operating system, set a risk level using Microsoft Defender for Endpoint, and more.
Note: Windows Health Attestation Service evaluation rules Require BitLocker:
Windows BitLocker Drive Encryption encrypts all data stored on the Windows operating system volume. BitLocker uses the Trusted Platform Module (TPM) to help protect the Windows operating system and user
data. It also helps confirm that a computer isn't tampered with, even if its left unattended, lost, or stolen. If the computer is equipped with a compatible TPM, BitLocker uses the TPM to lock the encryption keys that protect the data. As a result, the keys can't be accessed until the TPM verifies the state of the computer.
Not configured (default) - This setting isn't evaluated for compliance or non-compliance.
Require - The device can protect data that's stored on the drive from unauthorized access when the system is off, or hibernates.
Box 2: Prevent jailbroken devices from having corporate access Device Compliance settings for iOS/iPadOS in Intune
There are different compliance settings you can configure on iOS/iPadOS devices in Intune. As part of your mobile device management (MDM) solution, use these settings to require an email, mark rooted (jailbroken) devices as not compliant, set an allowed threat level, set passwords to expire, and more.
Device Health Jailbroken devices
Supported for iOS 8.0 and later
Not configured (default) - This setting isn't evaluated for compliance or non-compliance. Block - Mark rooted (jailbroken) devices as not compliant.
Box 3: Prevent rooted devices from having corporate access. Device compliance settings for Android Enterprise in Intune
There are different compliance settings you can configure on Android Enterprise devices in Intune. As part of your mobile device management (MDM) solution, use these settings to mark rooted devices as not compliant, set an allowed threat level, enable Google Play Protect, and more.
Device Health - for Personally-Owned Work Profile Rooted devices
Not configured (default) - This setting isn't evaluated for compliance or non-compliance. Block - Mark rooted devices as not compliant.
Reference: https://docs.microsoft.com/en-us/mem/intune/protect/compliance-policy-create-windows https://docs.microsoft.com/en-us/mem/intune/protect/compliance-policy-create-android-for-work https://docs.microsoft.com/en-us/mem/intune/protect/compliance-policy-create-ios

NEW QUESTION 50
- (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

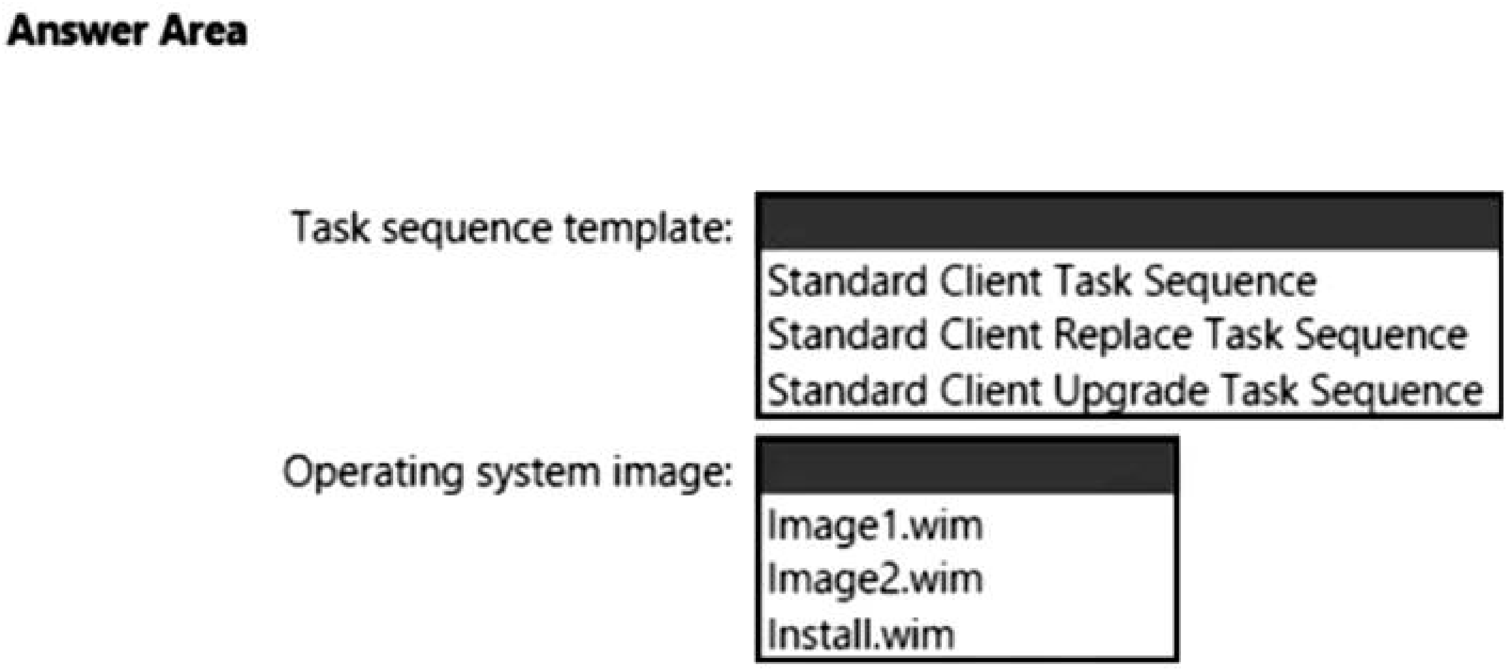
Answer: B

NEW QUESTION 54
- (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

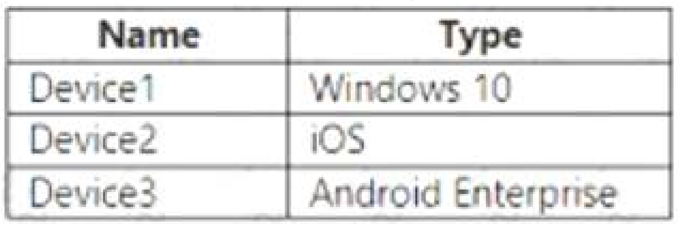
Operating system image:
- Image1.wim
- Image2.wim
- Install.wim

A. Mastered
B. Not Mastered

Answer: A

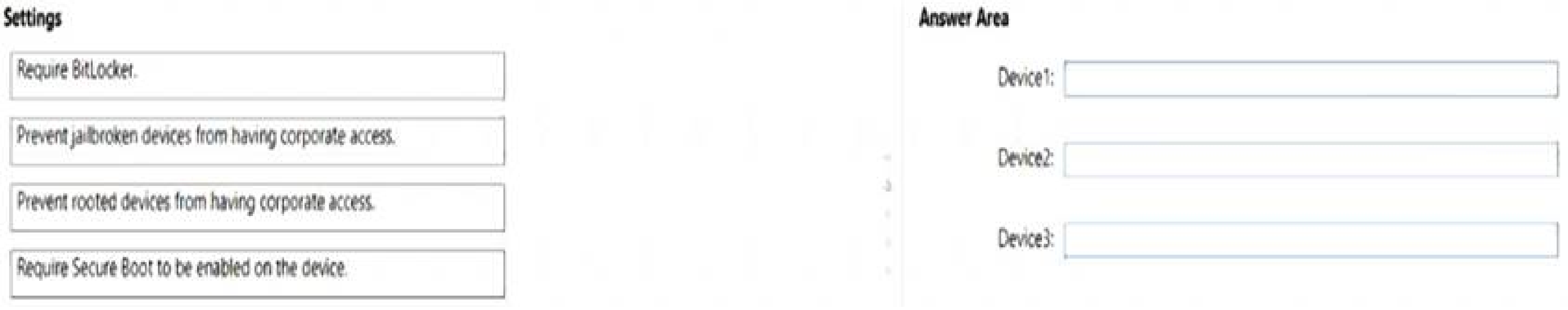
Explanation:
Box 1: Standard Client Upgrade Task Sequence
Use Template: Standard Client Upgrade Task Sequence
In-place upgrade is the preferred method to use when migrating from Windows 10 to a later release of Windows 10, and is also a preferred method for upgrading from Windows 7 or 8.1 if you do not 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 57
- (Exam Topic 4)
You have a Microsoft 365 subscription that contains the devices shown in the following table.



Name	Type
Device1	Windows 10
Device2	iOS
Device3	Android Enterprise

You need to ensure that only devices running trusted firmware or operating system build can access network resources.
Which compliance policy setting should you configure for each device? To answer, drag the appropriate settings to the correct devices. Each setting may be used once, more than once, or not at all. You may need to drag the split bar between panes or scroll to view content.
NOTE: Each correct selection is worth one point.



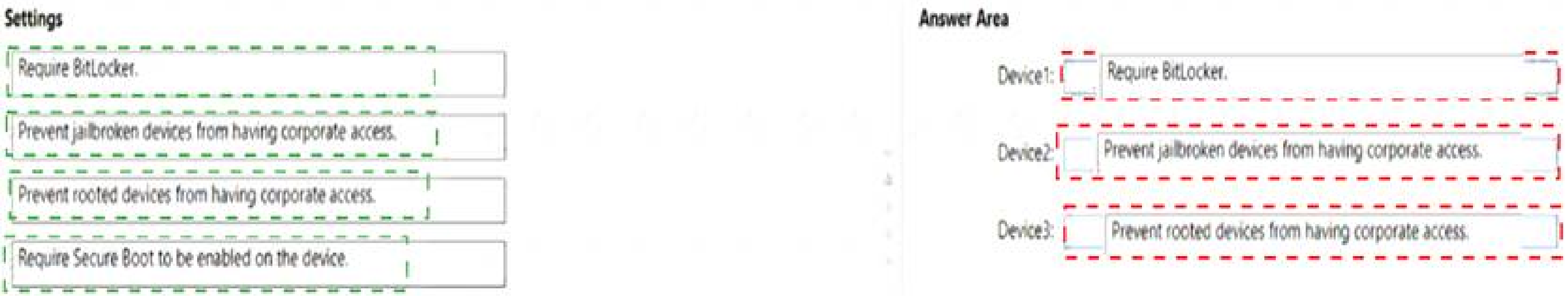
Settings
- Require BitLocker.
- Prevent jailbroken devices from having corporate access.
- Prevent rooted devices from having corporate access.
- Require Secure Boot to be enabled on the device.

Answer Area
- Device1:
- Device2:
- Device3:

A. Mastered
B. Not Mastered

Answer: A

Explanation:



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

Answer Area
- Device1: Require BitLocker.
- Device2: Prevent jailbroken devices from having corporate access.
- Device3: Prevent rooted devices from having corporate access.

NEW QUESTION 61
- (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 64
- (Exam Topic 4)
You have a Microsoft 365 subscription that uses Microsoft Intune Suite. You use Microsoft Intune to manage devices.
You plan to deploy two apps named App1 and App2 to all Windows devices. App1 must be installed before App2.
From the Intune admin center, you create and deploy two Windows app (Win32) apps. You need to ensure that App1 is installed before App2 on every device.
What should you configure?

A. the App1 deployment configurations
B. a dynamic device group
C. a detection rule
D. the App2 deployment configurations

Answer: C

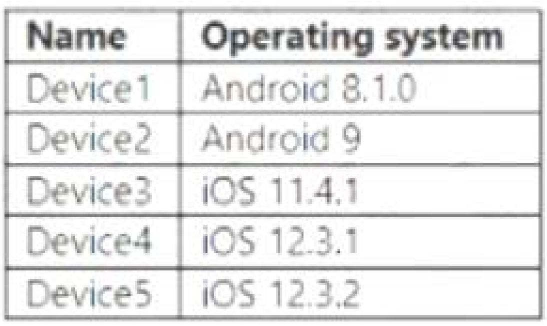
Explanation:
The correct answer is D because you can configure the dependencies for a Win32 app in the deployment configurations1. Dependencies are other Win32 apps that must be installed before your Win32 app can be installed1. You can add Win32 app dependencies only after your Win32 app has been added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

NEW QUESTION 68
- (Exam Topic 4)
You have a Microsoft 365 subscription.
You plan to use Windows Autopilot to provision 25 Windows 11 devices. You need to configure the Out-of-box experience (OOBE) settings.
What should you create in the Microsoft Intune admin center?

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

Answer: B

NEW QUESTION 73
- (Exam Topic 4)
You have a Microsoft Intune subscription.
You have devices enrolled in intune as shown in the following table.



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

An app named App1 is installed on each device.
What is the minimum number of app configuration policies required to manage Appl ?

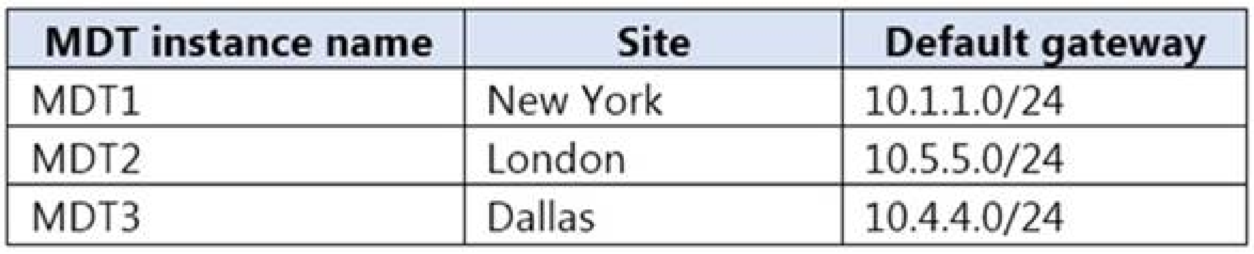
A. 1
B. 2
C. 3
D. 4
E. 5

Answer: B

Explanation:
The correct answer is B because you need to create two app configuration policies for managed devices, one for iOS/iPadOS devices and one for Android devices1. App configuration policies let you customize the settings of apps for iOS/iPadOS or Android devices1. The settings are assigned to user groups and applied when the app runs1. The app developer or supplier provides the configuration settings (keys and values) that are exposed to Intune1. You can't use a

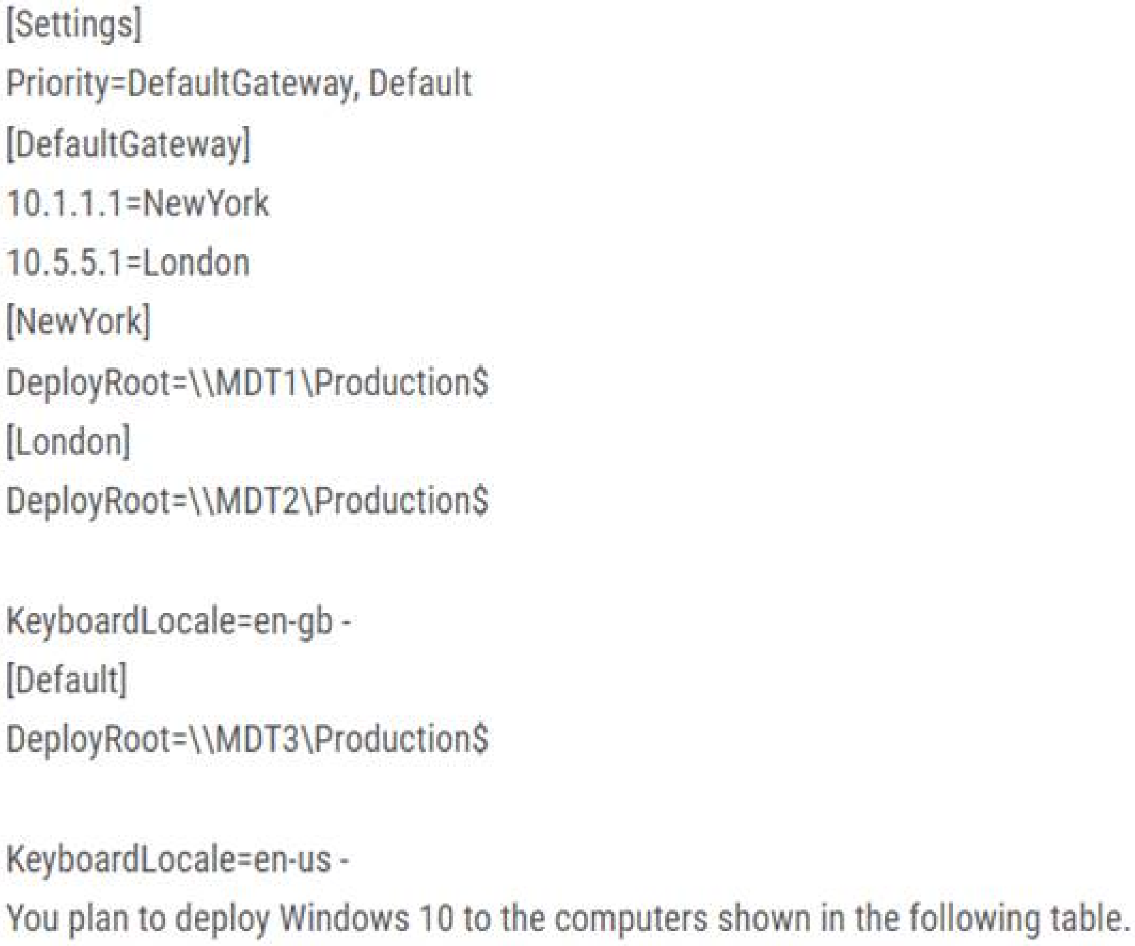
single app configuration policy for both iOS/iPadOS and Android devices because they have different configuration settings2. References: 1: App configuration policies for Microsoft Intune | Microsoft Learn https://learn.microsoft.com/en-us/mem/intune/apps/app-configuration-policies-overview 2: Add app configuration policies for managed iOS/iPadOS devices | Microsoft Learn https://learn.microsoft.com/en-us/mem/intune/apps/app-configuration-policies-use-ios

NEW QUESTION 77
- (Exam Topic 4)
You have the Microsoft Deployment Toolkit (MDT) installed in three sites as shown in the following table.



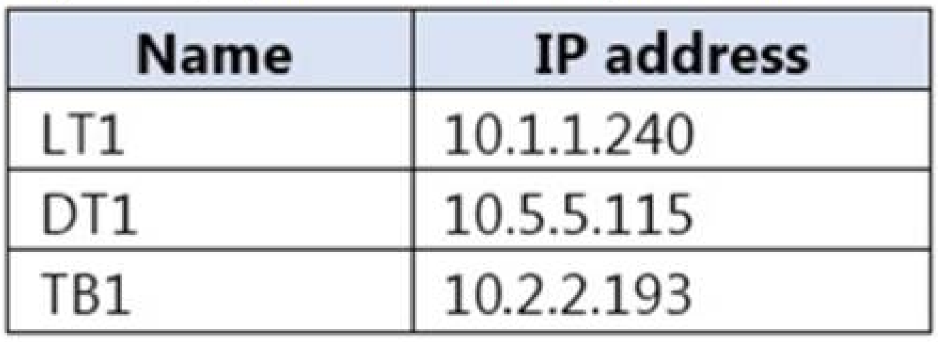
MDT instance name	Site	Default gateway
MDT1	New York	10.1.1.0/24
MDT2	London	10.5.5.0/24
MDT3	Dallas	10.4.4.0/24

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.

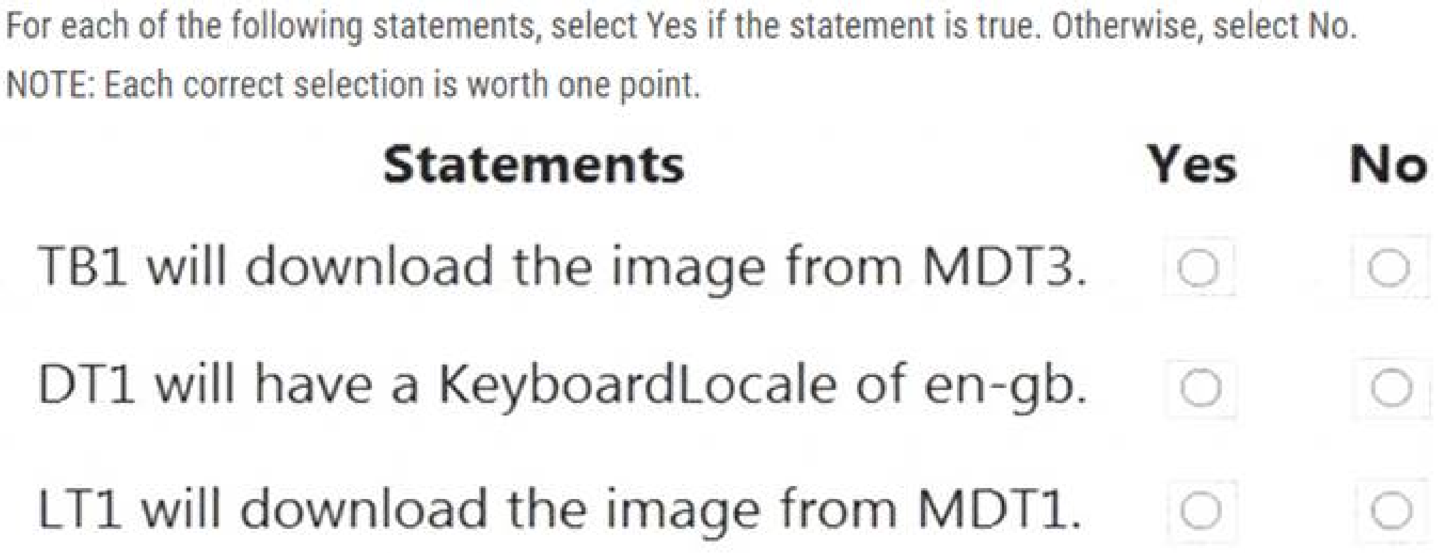


```
[Settings]
Priority=DefaultGateway, Default
[DefaultGateway]
10.1.1.1=NewYork
10.5.5.1=London
[NewYork]
DeployRoot=\\MDT1\Production$
[London]
DeployRoot=\\MDT2\Production$

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.

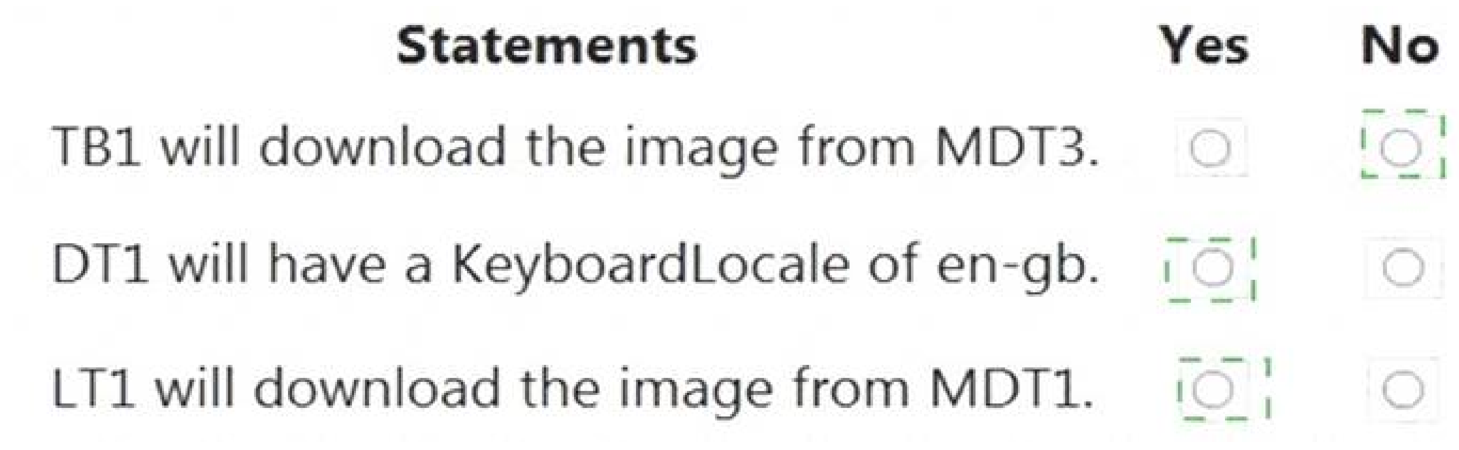
NOTE: Each correct selection is worth one point.

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 80
- (Exam Topic 2)
What should you configure to meet the technical requirements for the Azure AD-joined computers?

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

Answer: A

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

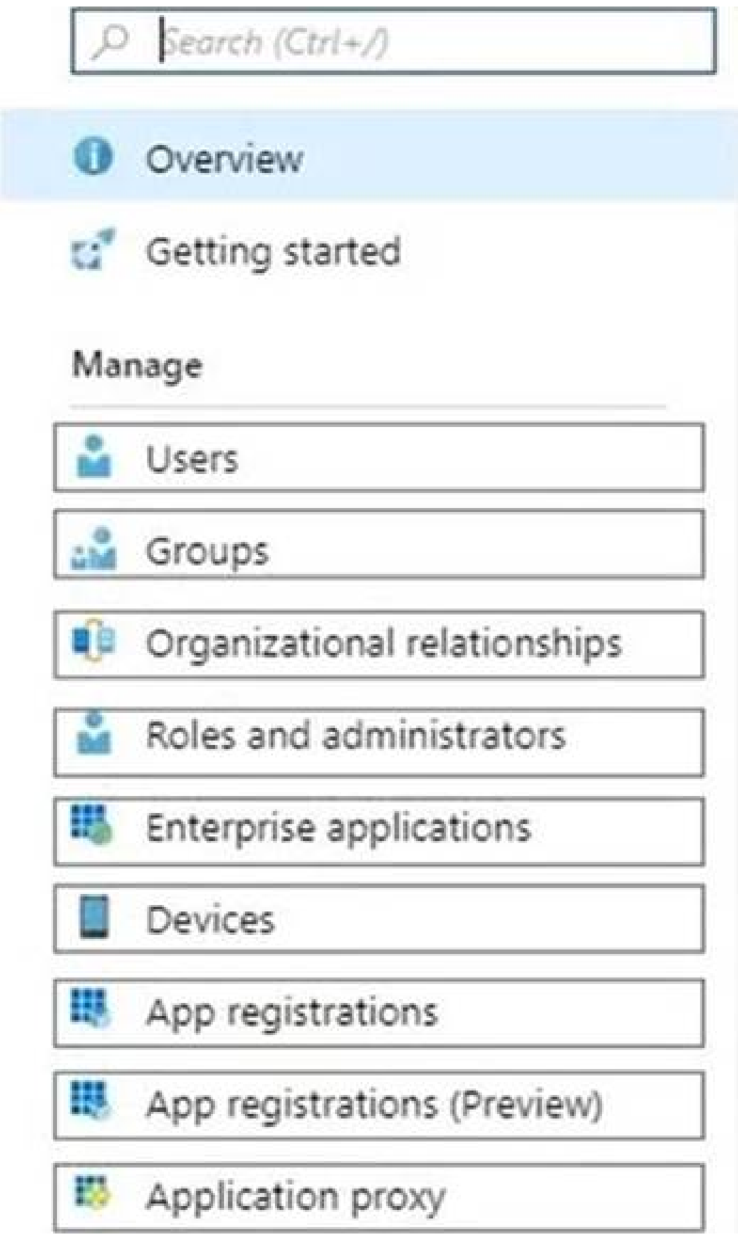
NEW QUESTION 84
- (Exam Topic 2)
What should you upgrade before you can configure the environment to support co-management?

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

Answer: B

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

NEW QUESTION 89
- (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.


Search (Ctrl+/)

Overview

Getting started

Manage

Users

Groups

Organizational relationships

Roles and administrators

Enterprise applications

Devices

App registrations

App registrations (Preview)

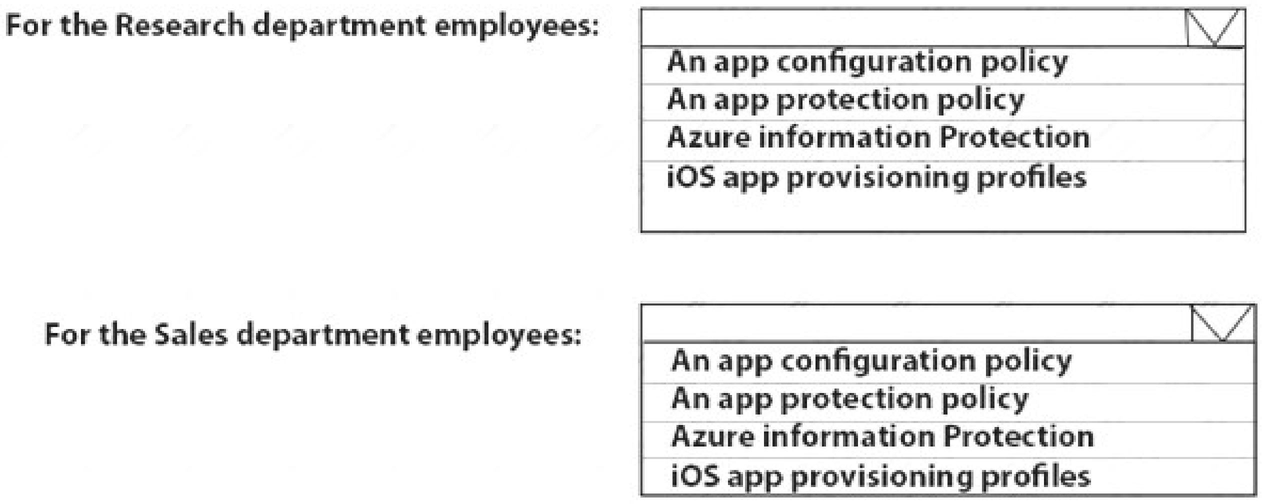
Application proxy

A. Mastered
B. Not Mastered

Answer: A

Explanation:
References:
https://docs.microsoft.com/en-us/windows/deployment/windows-autopilot/windows-autopilot-reset

NEW QUESTION 91
- (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 96
- (Exam Topic 2)
What should you use to meet the technical requirements for Azure DevOps?

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

Answer: C

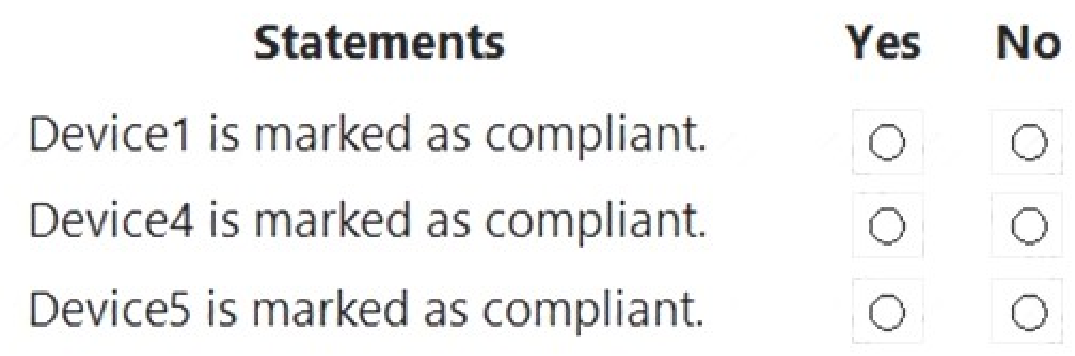
Explanation:
References:
https://docs.microsoft.com/en-us/azure/devops/organizations/accounts/manage-conditional-access? view=azure-devops

NEW QUESTION 100
- (Exam Topic 1)
Which user can enroll Device6 in Intune?

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

Answer: B

NEW QUESTION 104
- (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

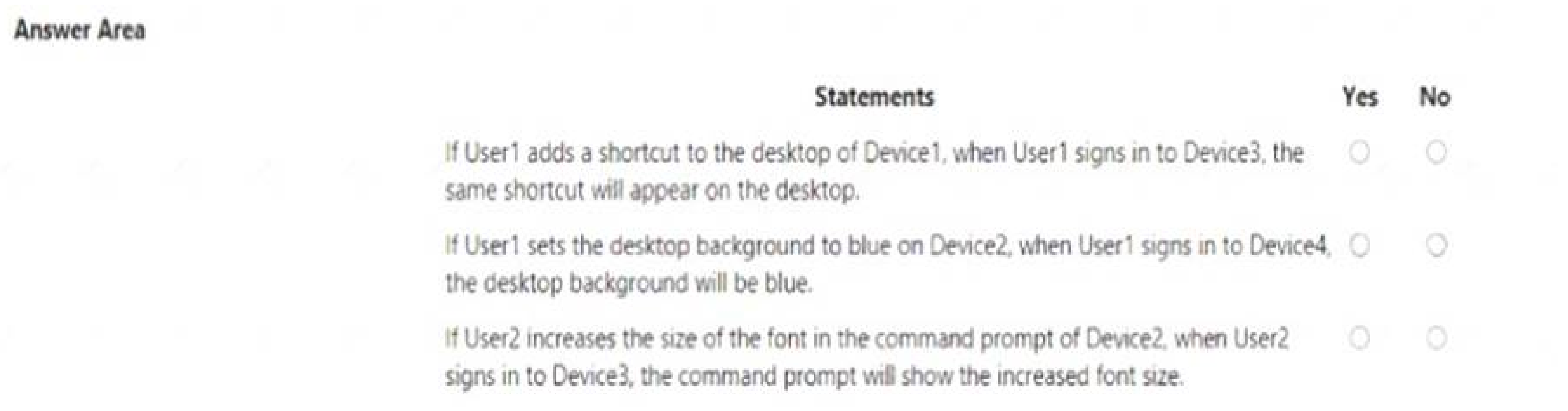
NEW QUESTION 108
- (Exam Topic 1)
Which users can purchase and assign App1?

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 111
- (Exam Topic 1)
For each of the following statements, select Yes if the statement is true. Otherwise, select No. NOTE: Each correct selection is worth one point.



Answer Area

Statements	Yes	No
If User1 adds a shortcut to the desktop of Device1, when User1 signs in to Device3, the same shortcut will appear on the desktop.	○	○
If User1 sets the desktop background to blue on Device2, when User1 signs in to Device4, the desktop background will be blue.	○	○
If User2 increases the size of the font in the command prompt of Device2, when User2 signs in to Device3, the command prompt will show the increased font size.	○	○

A. Mastered
B. Not Mastered

Answer: A

Explanation:
Text, letter Description automatically generated

NEW QUESTION 113
- (Exam Topic 1)
You need to ensure that computer objects can be created as part of the Windows Autopilot deployment. The solution must meet the technical requirements.
To what should you grant the right to create the computer objects?

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

Answer: C

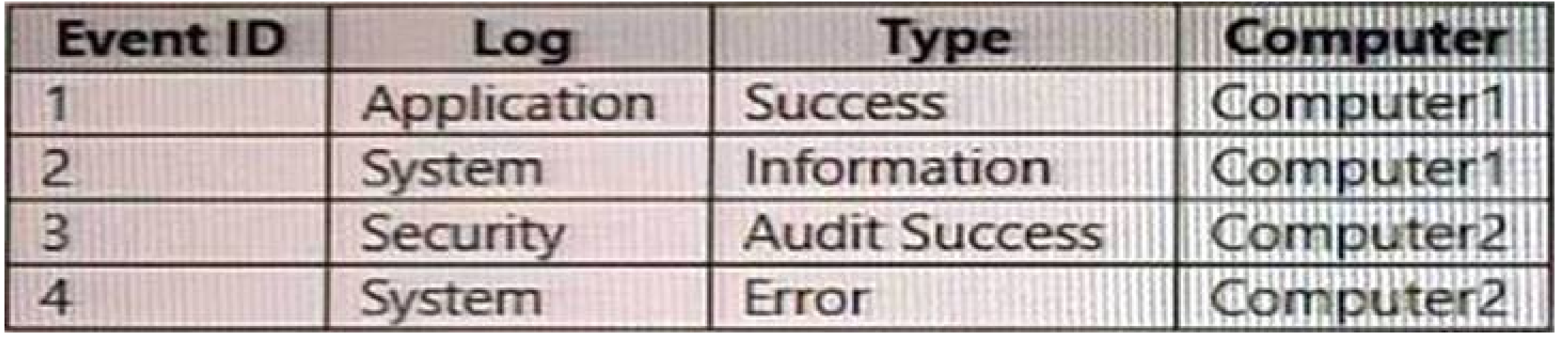
Explanation:
Reference:
https://blog.matrixpost.net/set-up-windows-autopilot-production-environment-part-2/

NEW QUESTION 118
- (Exam Topic 4)
Your company has an Azure AD tenant named contoso.com that contains several Windows 10 devices. When you join new Windows 10 devices to contoso.com, users are prompted to set up a four-digit pin. You need to ensure that the users are prompted to set up a six-digit pin when they join the Windows 10 devices to contoso.com.
Solution: From the Microsoft Entra admin center, you configure automatic mobile device management (MDM) enrollment. From the Microsoft Intune admin center, you create and assign a device restrictions profile.
Does this meet the goal?

A. Yes
B. No

Answer: B

NEW QUESTION 123
- (Exam Topic 4)
You have computer that run Windows 10 and connect to an Azure Log Analytics workspace. The workspace is configured to collect all available events from Windows event logs. The computers have the logged events shown in the following table.



Event ID	Log	Type	Computer
1	Application	Success	Computer1
2	System	Information	Computer1
3	Security	Audit Success	Computer2
4	System	Error	Computer2

Which events are collected in the Log Analytics workspace?

A. 1 only
B. 2 and 3 only
C. 1 and 3 only
D. 1, 2, and 4 on
E. 1, 2, 3, and 4

Answer: E

Explanation:
All events from Windows event logs are collected in the Log Analytics workspace, regardless of the event level or source. Therefore, events 1, 2, 3, and 4 are all

collected in the workspace. References: https://docs.microsoft.com/en-us/azure/azure-monitor/agents/data-sources-windows-events

NEW QUESTION 124
- (Exam Topic 4)
You have a Microsoft 365 E5 subscription that contains 10 Android Enterprise devices. Each device has a corporate-owned work profile and is enrolled in Microsoft Intune.
You need to configure the devices to run a single app in kiosk mode.
Which Configuration settings should you modify in the device restrictions profile?

A. General
B. Users and Accounts
C. System security
D. Device experience

Answer: D

Explanation:
To configure the devices to run a single app in kiosk mode, you need to modify the Device experience settings in the device restrictions profile. You can specify the app package name and activity name for the app that you want to run in kiosk mode. References:
https://docs.microsoft.com/en-us/mem/intune/configuration/device-restrictions-android-for-work#device-experie

NEW QUESTION 129
- (Exam Topic 4)
You have a Microsoft 365 subscription that uses Microsoft Intune Suite. You use Microsoft Intune to manage devices.
You have a Windows 11 device named Device1 that is enrolled in Intune. Device1 has been offline for 30 days.
You need to remove Device1 from Intune immediately. The solution must ensure that if the device checks in again, any apps and data provisioned by Intune are removed. User-installed apps, personal data, and
OEM-installed apps must be retained.
What should you use?

A. a Delete action
B. a Retire action
C. a Fresh Start action
D. an Autopilot Reset action

Answer: B

Explanation:
A retire action removes a device from Intune management and removes any apps and data provisioned by Intune. User-installed apps, personal data, and OEM-installed apps are retained. A retire action can be performed on devices that are offline for more than 30 days. References:
https://docs.microsoft.com/en-us/mem/intune/remote-actions/devices-wipe

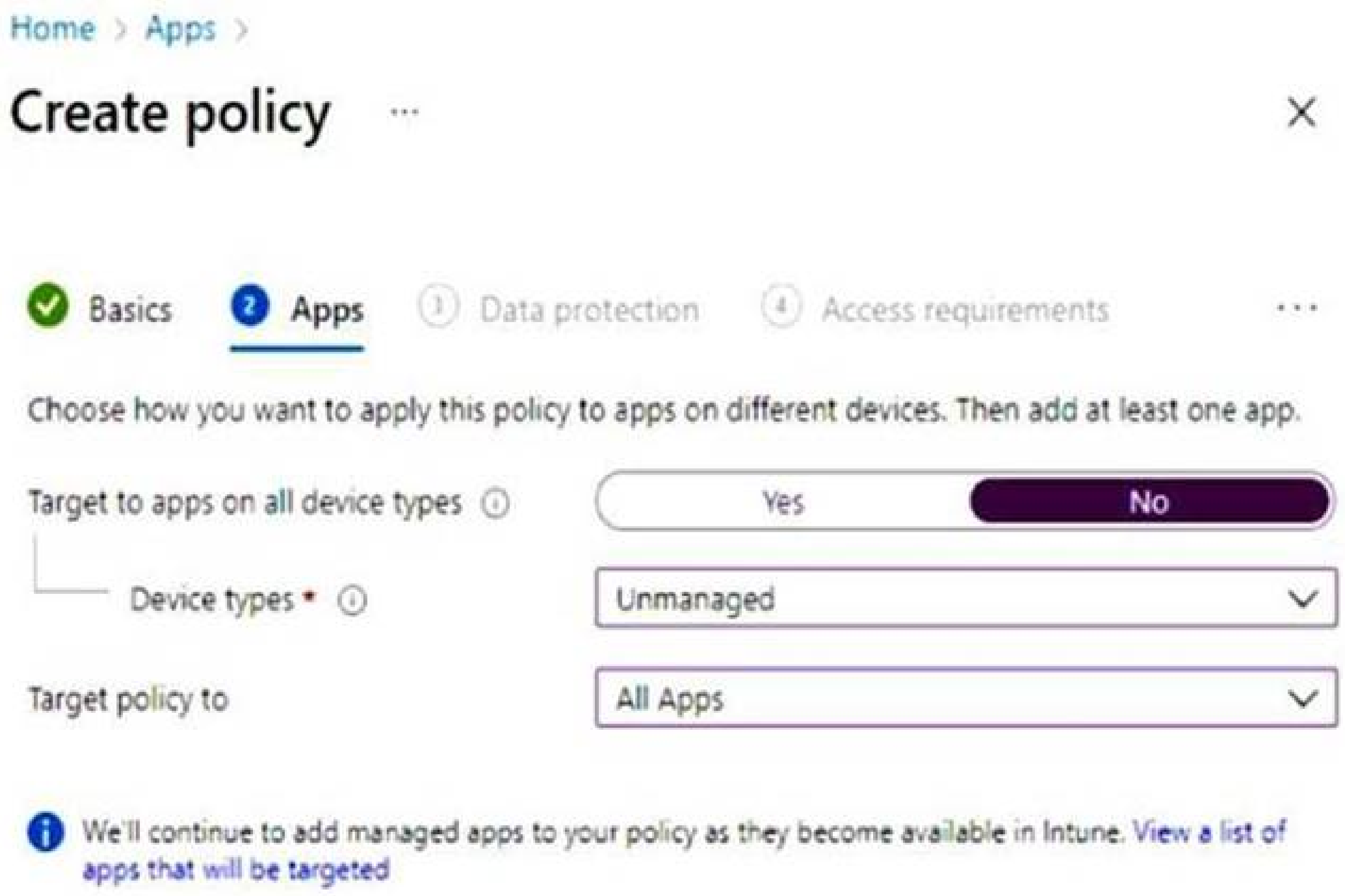
NEW QUESTION 134
- (Exam Topic 4)
You have a Microsoft 365 E5 subscription that contains a user named User! and a web app named Appl. App1 must only accept modern authentication requests.
You plan to create a Conditional Access policy named CAPolicy1 that will have the following settings:
• Assignments
° Users or workload identities: User1
° Cloud apps or actions: App1
• Access controls
° Grant: Block access
You need to block only legacy authentication requests to Appl. Which condition should you add to CAPolicy1?

A. Filter for devices
B. Device platforms
C. User risk
D. Sign-in risk
E. Client apps

Answer: E

Explanation:
you can use the client apps condition to block legacy authentication requests to App11. Legacy authentication is a term that refers to authentication protocols that do not support modern authentication features such as multi-factor authentication or conditional access2. Examples of legacy authentication protocols include Basic Authentication, Digest Authentication, NTLM, and Kerberos2. To block legacy authentication requests, you need to configure the client apps condition to include Other clients, which covers any client that uses legacy authentication protocols13. References: 1: Conditional Access: Block legacy authentication | Microsoft Learn https://learn.microsoft.com/en-us/mem/identity-protection/conditional-access/block-legacy-authentication 2:
What is legacy authentication? | Microsoft Learn
https://learn.microsoft.com/en-us/mem/identity-protection/conditional-access/legacy-authentication 3: Client apps condition in Azure Active Directory Conditional Access | Microsoft Learn https://learn.microsoft.com/en-us/mem/identity-protection/conditional-access/client-apps-condition

NEW QUESTION 137
- (Exam Topic 4)
You have a Microsoft 365 E5 subscription.
You create an app protection policy for Android devices named Policy1 as shown in the following exhibit.



Create policy

✓ Basics ❷ Apps ③ Data protection ④ Access requirements ···

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

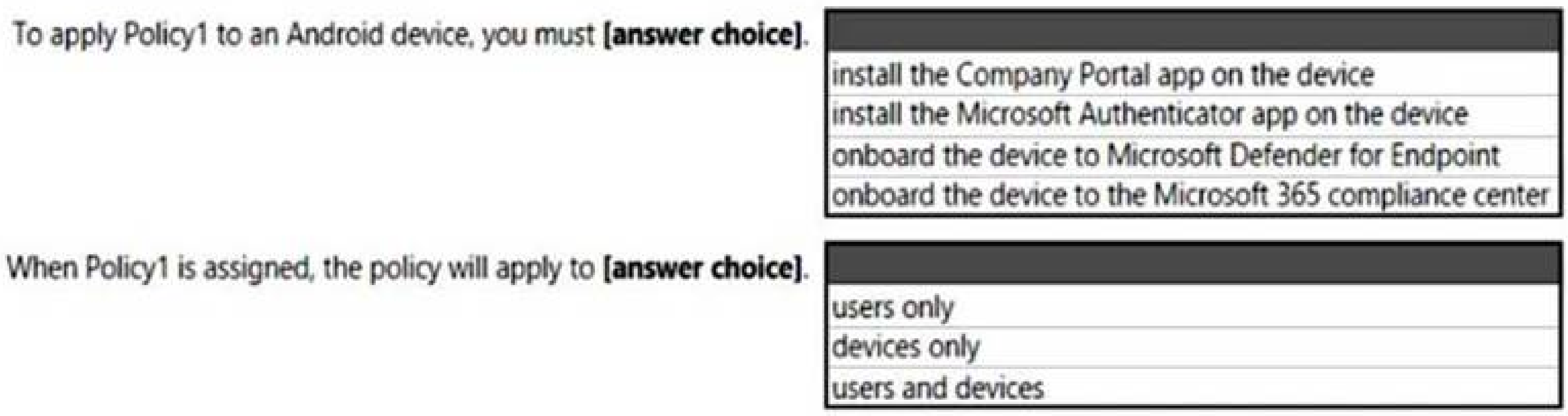
Target to apps on all device types: Yes [✓ No]

Device types *: Unmanaged

Target policy to: All Apps

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

Use the drop-down menus to select the answer choice that completes each statement based on the information presented in the graphic.
NOTE: Each correct selection is worth one point.



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

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

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

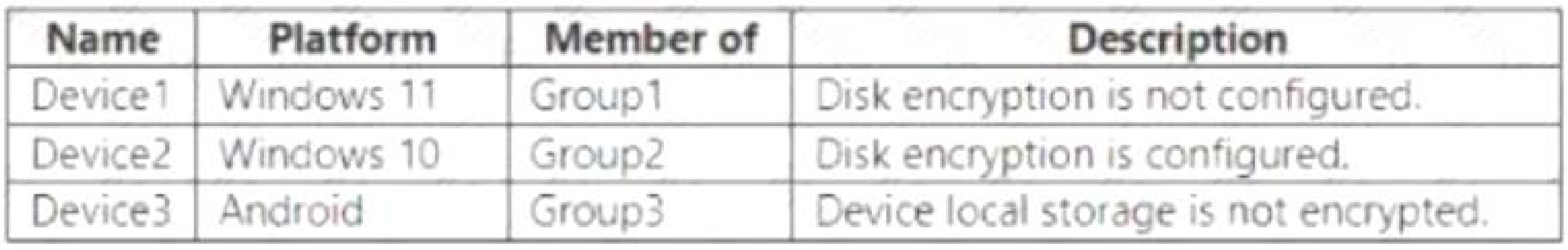
- users only
- devices only
- users and devices

A. Mastered
B. Not Mastered

Answer: A

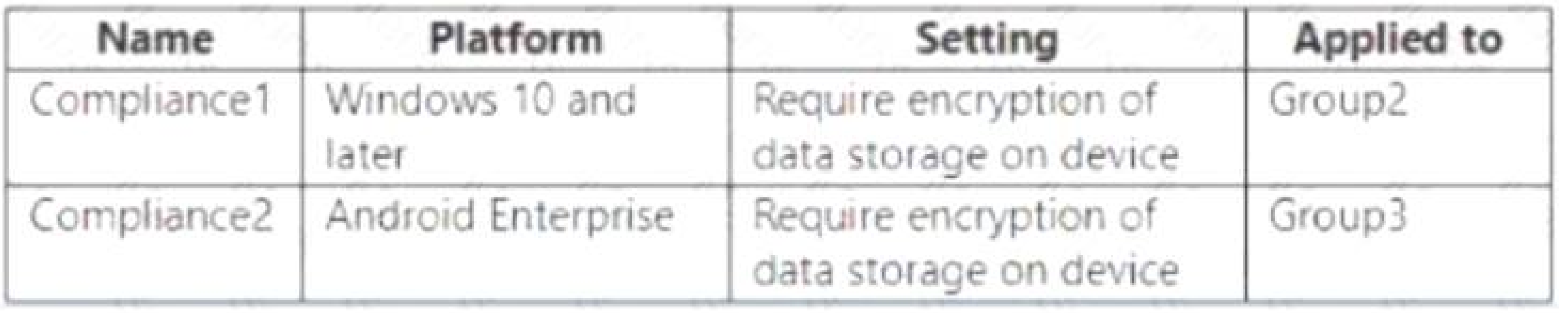
Explanation:
Box 1: Install the Intune Company Portal app on the device
On Android, Android devices will prompt to install the Intune Company Portal app regardless of which Device type is chosen.
Bix 2: Devices only
For Android devices, unmanaged devices are devices where Intune MDM management has not been detected. This includes devices managed by third-party MDM vendors.
Reference:
https://docs.microsoft.com/en-us/mem/intune/apps/app-protection-policies#app-protection-policies-for-iosipado

NEW QUESTION 142
- (Exam Topic 4)
You have a Microsoft 365 subscription that contains a user named User1. The subscription contains devices enrolled in Microsoft intune as shown in the following table.



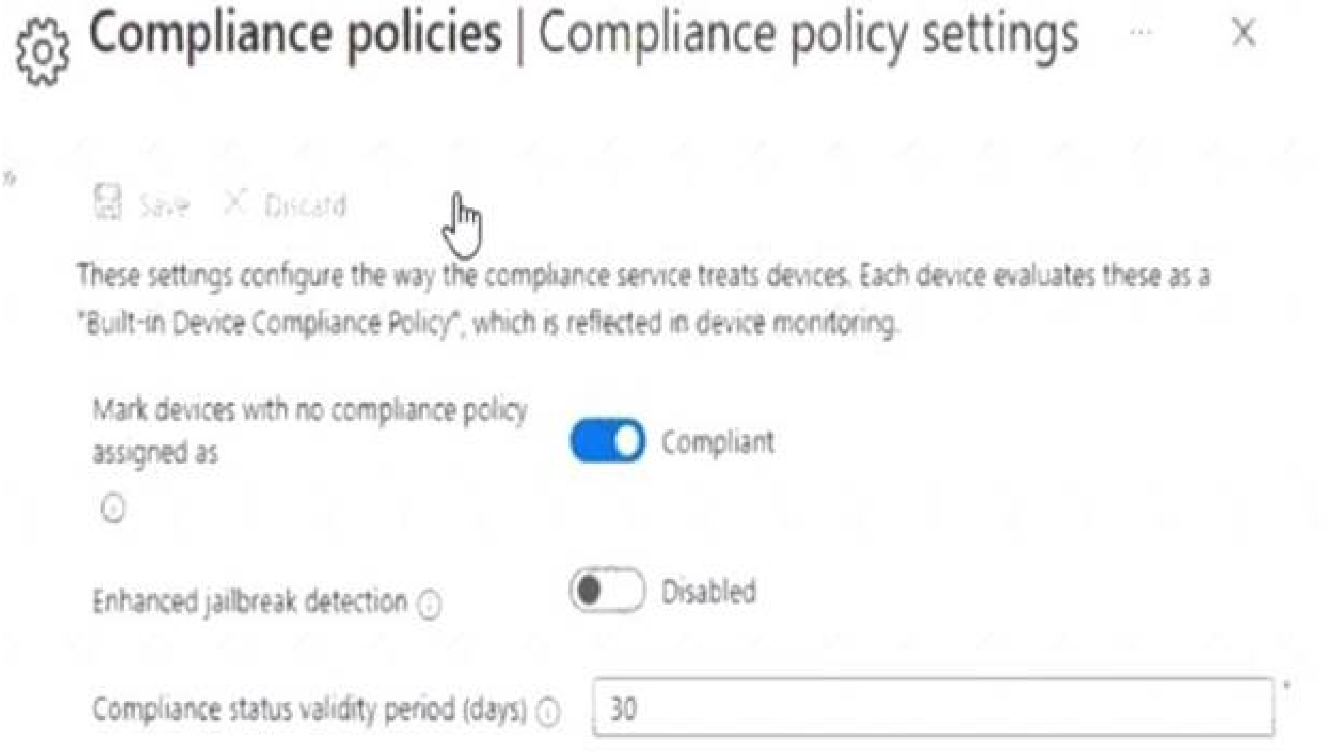
Name	Platform	Member of	Description
Device1	Windows 11	Group1	Disk encryption is not configured.
Device2	Windows 10	Group2	Disk encryption is configured.
Device3	Android	Group3	Device local storage is not encrypted.

Microsoft Edge is available on all the devices.
Intune has the device compliance policies shown in the following table.



Name	Platform	Setting	Applied to
Compliance1	Windows 10 and later	Require encryption of data storage on device	Group2
Compliance2	Android Enterprise	Require encryption of data storage on device	Group3

The Compliance policy settings are configured as shown in the exhibit. (Click the Exhibit tab.) You create the following Conditional Access policy:



Compliance policies | Compliance policy settings

These settings configure the way the compliance service treats devices. Each device evaluates these as a "Built-in Device Compliance Policy", which is reflected in device monitoring.

Mark devices with no compliance policy assigned as Compliant

Enhanced jailbreak detection Disabled

Compliance status validity period (days) 30

- Name: Policy1
- Assignments

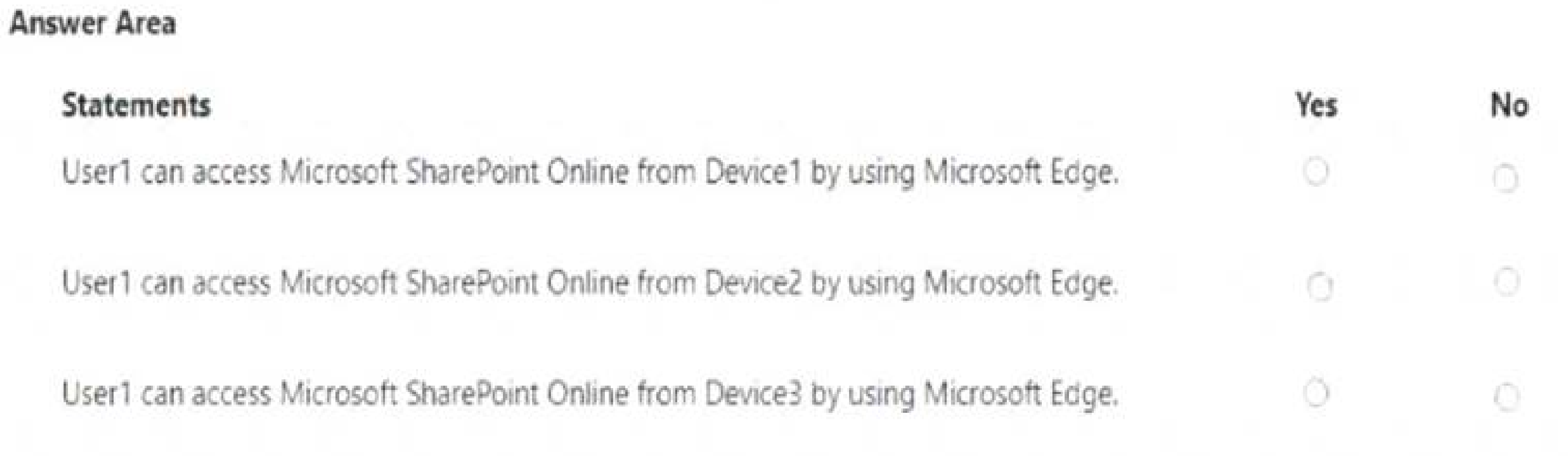
o Users and groups: User1
o Cloud apps or actions: Office 365 SharePoint Online

- Access controls

o Grant Require device to be marked as compliant

- Enable policy: On

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



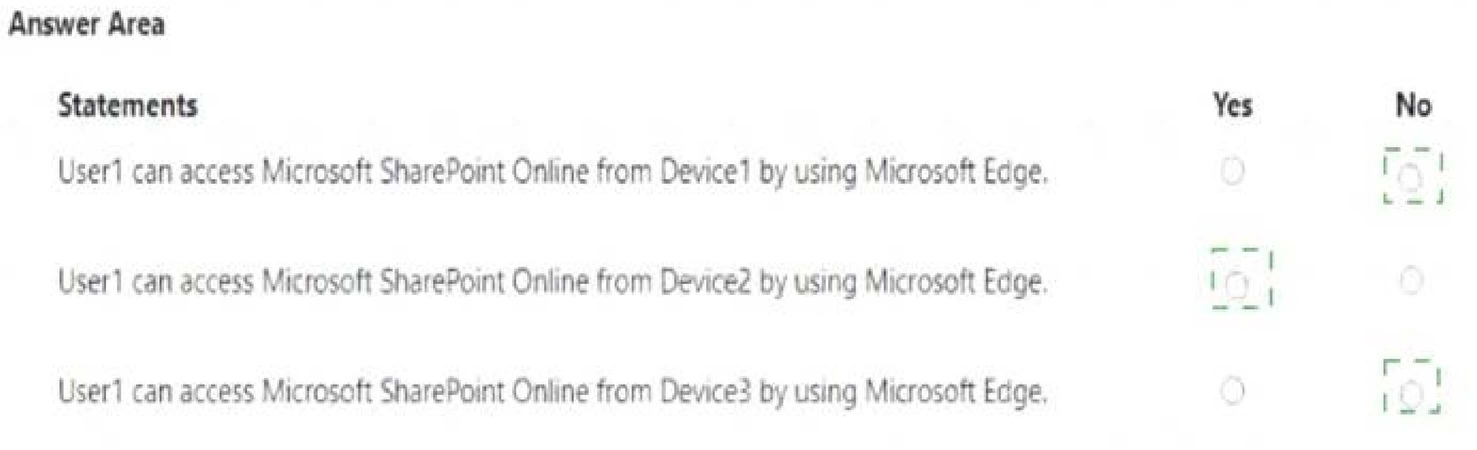
Answer Area

Statements	Yes	No
User1 can access Microsoft SharePoint Online from Device1 by using Microsoft Edge.	○	○
User1 can access Microsoft SharePoint Online from Device2 by using Microsoft Edge.	○	○
User1 can access Microsoft SharePoint Online from Device3 by using Microsoft Edge.	○	○

A. Mastered
B. Not Mastered

Answer: A

Explanation:



Answer Area

Statements	Yes	No
User1 can access Microsoft SharePoint Online from Device1 by using Microsoft Edge.	○	[✓ ○]
User1 can access Microsoft SharePoint Online from Device2 by using Microsoft Edge.	[✓ ○]	○
User1 can access Microsoft SharePoint Online from Device3 by using Microsoft Edge.	○	[✓ ○]

NEW QUESTION 143
- (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

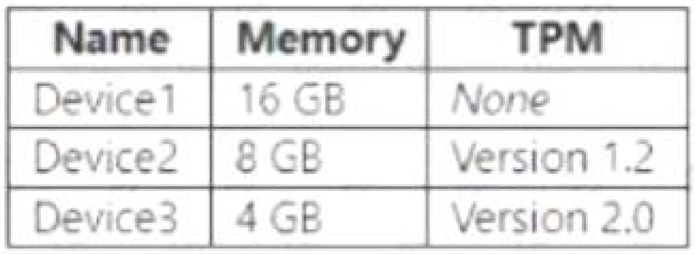
Answer: B

NEW QUESTION 147
- (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 150
- (Exam Topic 4)
You have an Azure AD tenant named contoso.com.
You plan to use Windows Autopilot to configure the Windows 10 devices shown in the following table.



Name	Memory	TPM
Device1	16 GB	None
Device2	8 GB	Version 1.2
Device3	4 GB	Version 2.0

Which devices can be configured by using Windows Autopilot self-deploying mode?

A. Device2 only
B. Device3 only
C. Device2 and Devnce3 only
D. Device 1, Device2, and Device3

Answer: C

Explanation:
Windows Autopilot self-deploying mode requires devices that have a firmware-embedded activation key for Windows 10 Pro or Windows 11 Pro. This feature allows devices to automatically activate Windows Enterprise edition using the subscription license assigned to the user. Device1 does not have a firmware-embedded activation key, so it cannot use self-deploying mode. Device2 and Device3 have firmware-embedded activation keys for Windows 10 Pro, so they can use self-deploying
mode. References: Windows Autopilot self-deploying mode (Public Preview), Deploy Windows Enterpris licenses

NEW QUESTION 151
- (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 152
- (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 154
- (Exam Topic 4)
You have an Azure AD tenant and 100 Windows 10 devices that are Azure AD joined and managed by using Microsoft Intune.
You need to configure Microsoft Defender Firewall and Microsoft Defender Antivirus on the devices. The solution must minimize administrative effort.

Which two actions should you perform? Each correct answer presents part of the solution. NOTE: Each correct selection is worth one point.

A. To configure Microsoft Defender Antivirus, create a Group Policy Object (GPO) and configure the Windows Defender Antivirus settings.
B. To configure Microsoft Defender Firewall, create a device configuration profile and configure the Device restrictions settings.
C. To configure Microsoft Defender Antivirus, create a device configuration profile and configure the Endpoint protection settings.
D. To configure Microsoft Defender Antivirus, create a device configuration profile and configure the Device restrictions settings.
E. To configure Microsoft Defender Firewall, create a device configuration profile and configure the Endpoint protection settings.
F. To configure Microsoft Defender Firewall, create a Group Policy Object (GPO) and configure Windows Defender Firewall with Advanced Security.

Answer: CE

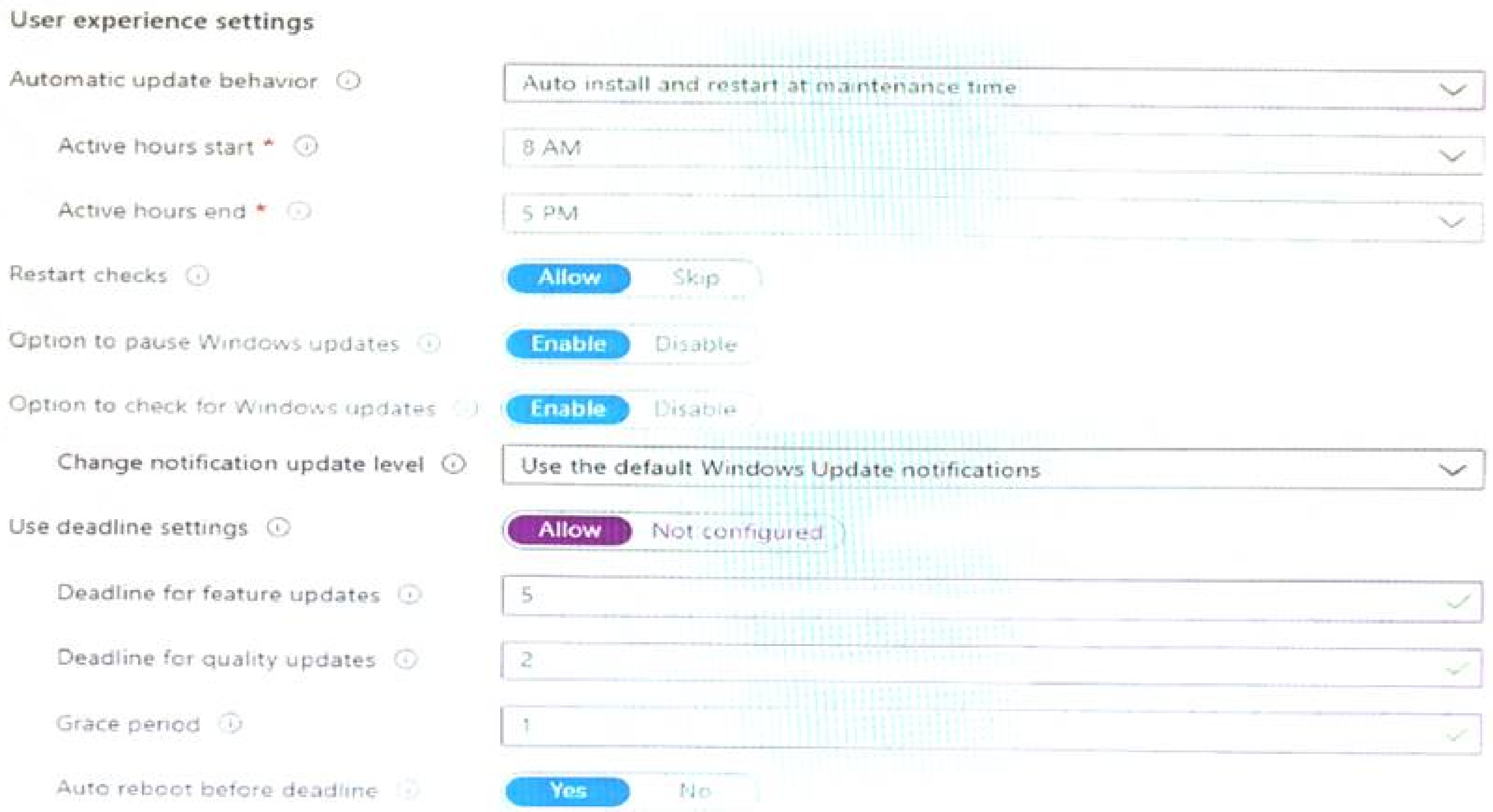
Explanation:
To configure Microsoft Defender Firewall and Microsoft Defender Antivirus on Azure AD joined devices that are managed by Intune, you need to create a device configuration profile and configure the Endpoint protection settings. You can use this profile to configure various settings for firewall and antivirus protection on the devices. References:
https://docs.microsoft.com/en-us/mem/intune/protect/endpoint-protection-windows-10

NEW QUESTION 159
- (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

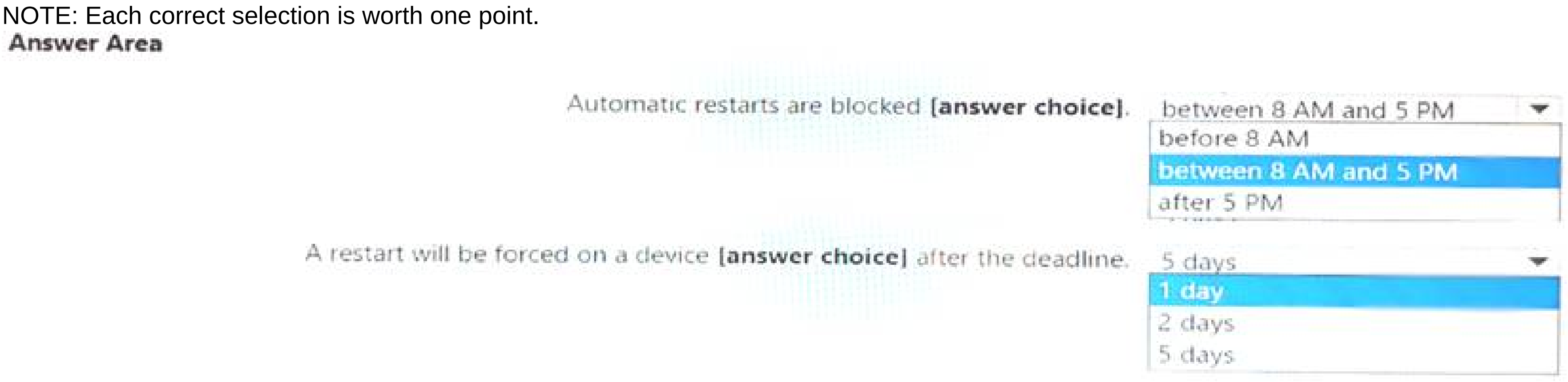
NEW QUESTION 164
- (Exam Topic 4)
You have a Microsoft 365 subscription that uses Microsoft Intune. You plan to manage Windows updates by using Intune.
You create an update ring for Windows 10 and later and configure the User experience settings for the ring as shown in the following exhibit.



User experience settings

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

Use the drop-down menus to select the answer choice that completes each statement based on the information presented in the graphic.
NOTE: Each correct selection is worth one point.



Answer Area

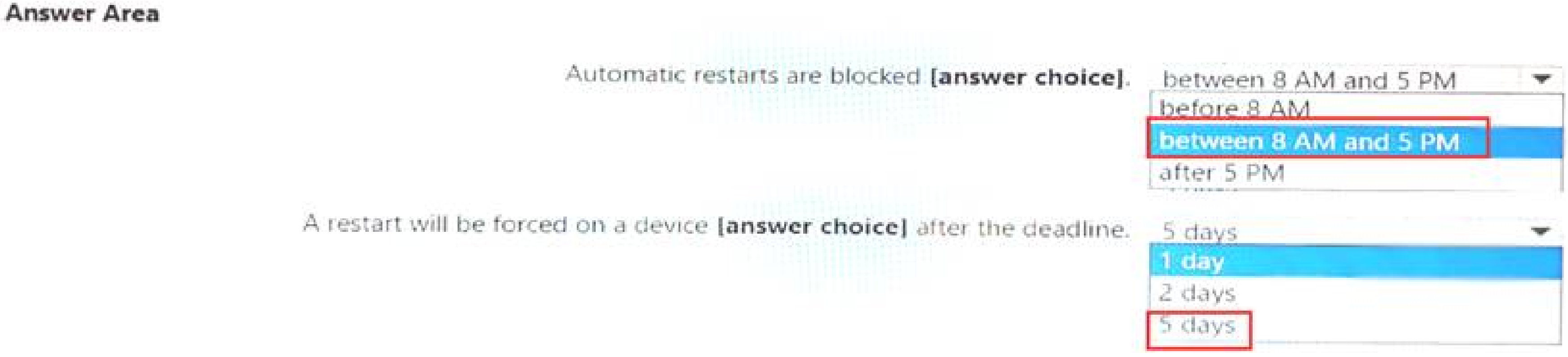
Automatic restarts are blocked **[answer choice]**. between 8 AM and 5 PM

A restart will be forced on a device **[answer choice]** after the deadline. 5 days

A. Mastered
B. Not Mastered

Answer: A

Explanation:



Answer Area

Automatic restarts are blocked [answer choice]. between 8 AM and 5 PM

- before 8 AM
- between 8 AM and 5 PM
- after 5 PM

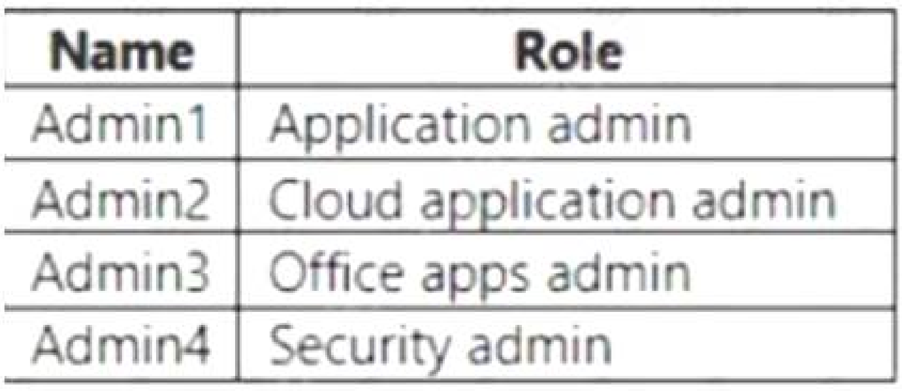
A restart will be forced on a device [answer choice] after the deadline. 5 days

- 1 day
- 2 days
- 5 days

NEW QUESTION 165

- (Exam Topic 4)

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



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

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

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

Answer: B

Explanation:

* Admin1

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

* Admin2

Mark your app as publisher verified.

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

* Admin3

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

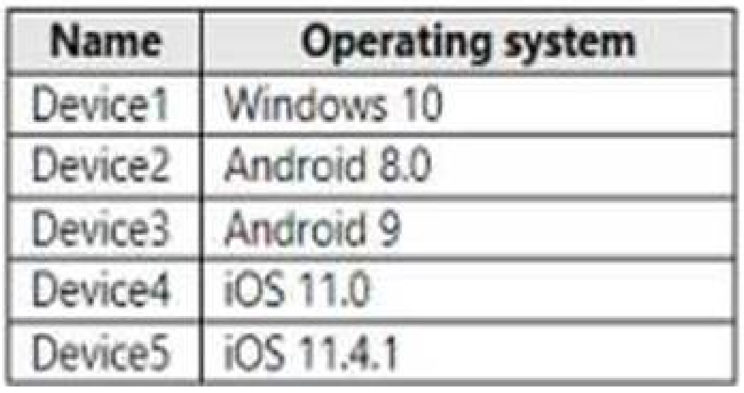
- Use the Office cloud policy service to create and manage cloud-based policies for Office
- Create and manage service requests
- Manage the What's New content that users see in their Office apps
- Monitor service health Reference:

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

NEW QUESTION 170

- (Exam Topic 4)

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



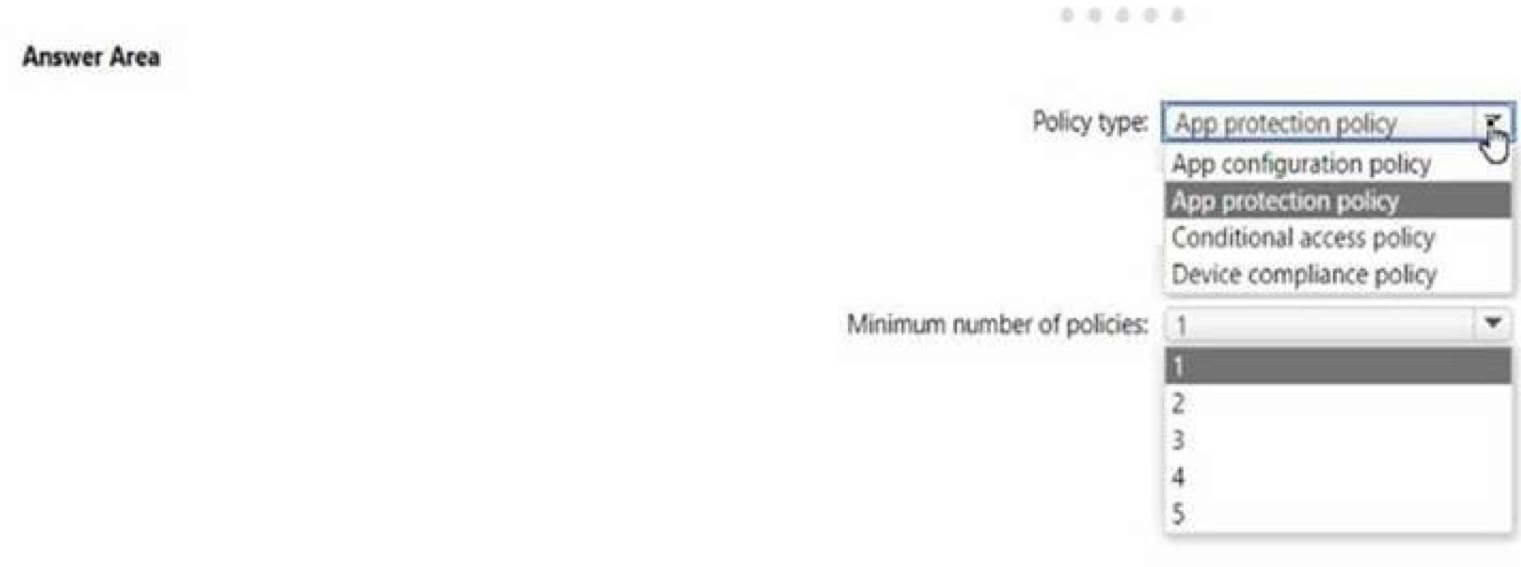
Name	Operating system
Device1	Windows 10
Device2	Android 8.0
Device3	Android 9
Device4	iOS 11.0
Device5	iOS 11.4.1

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

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

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

NOTE: Each correct selection is worth one point.



Answer Area

Policy type: App protection policy

Minimum number of policies: 1

A. Mastered
B. Not Mastered

Answer: A

Explanation:
of Corre Answer Only: The correct answer is app protection policy because it allows you to customize the settings of apps for iOS/iPadOS or Android devices1. One of the settings you can configure is Restrict cut, copy, and paste between other apps, which lets you prevent users from copying data from App1 and pasting the data into other apps2. You only need one policy to apply this setting to all devices that have App1 installe1d.
References: 1: App configuration policies for Microsoft Intune | Microsoft Learn https://learn.microsoft.com/en-us/mem/intune/apps/app-configuration-policies-overview 2: Troubleshoot restricting cut, copy, and paste between applications - Intune | Microsoft Learn
https://learn.microsoft.com/en-us/troubleshoot/mem/intune/app-protection-policies/troubleshoot-cut-copy-paste

NEW QUESTION 173
- (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

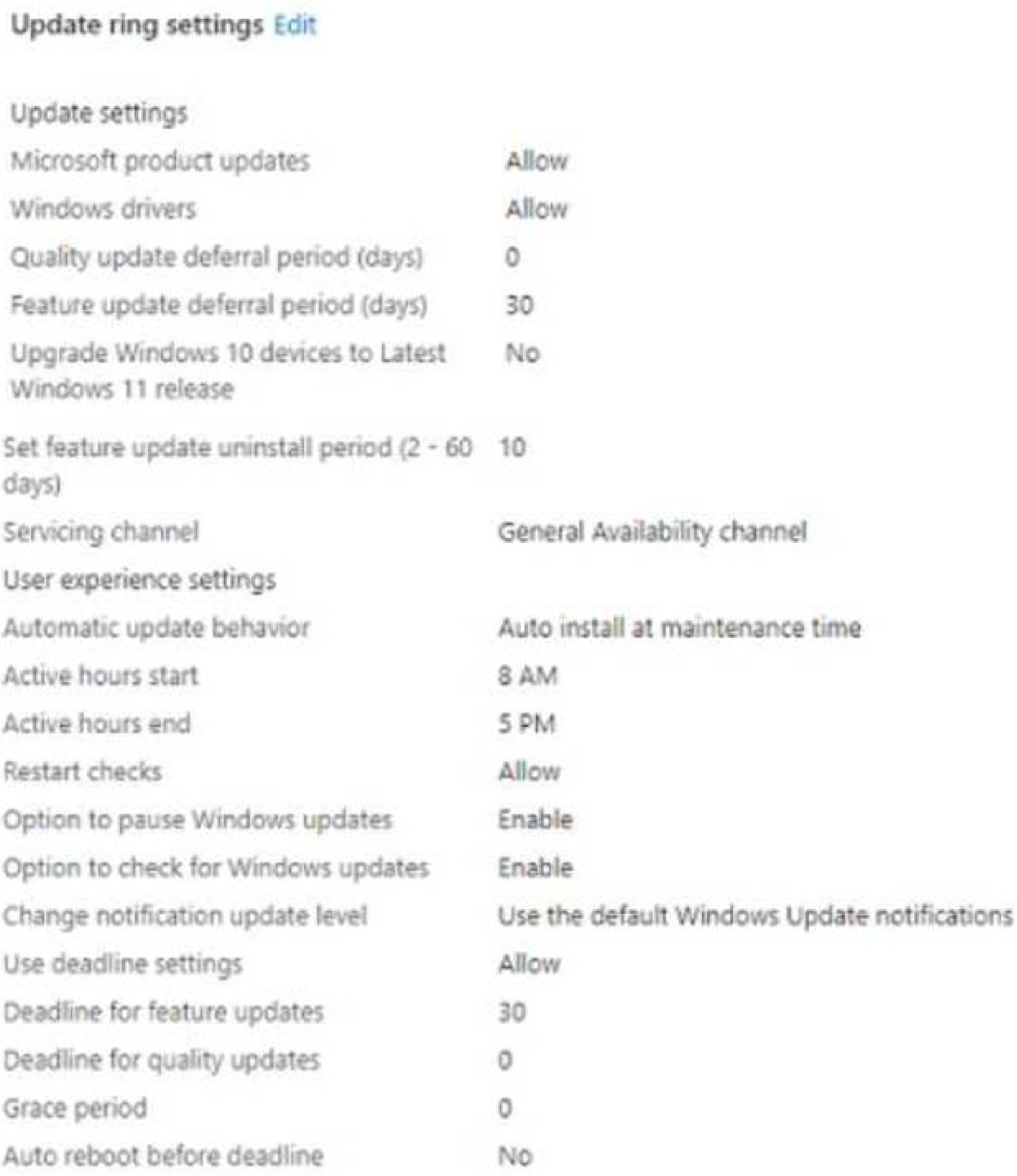
NEW QUESTION 176
- (Exam Topic 4)
You have a Microsoft 365 E5 subscription that contains 500 macOS devices enrolled in Microsoft Intune. You need to ensure that you can apply Microsoft Defender for Endpoint antivirus policies to the macOS
devices. The solution must minimize administrative effort.
What 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

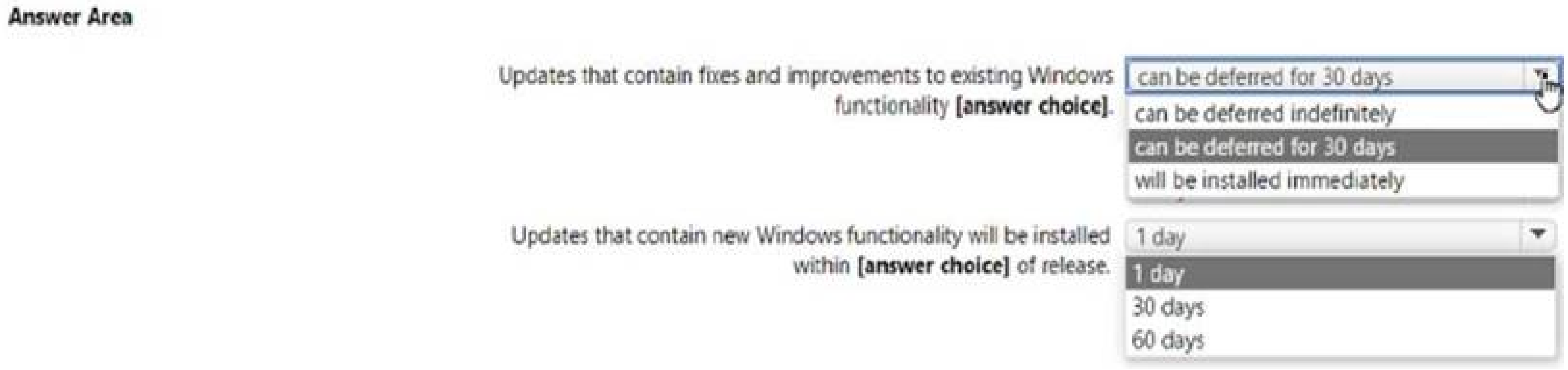
NEW QUESTION 180
- (Exam Topic 4)
You have a Microsoft 365 E5 subscription.
You create a new update rings policy named Policy1 as shown in the following exhibit.



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

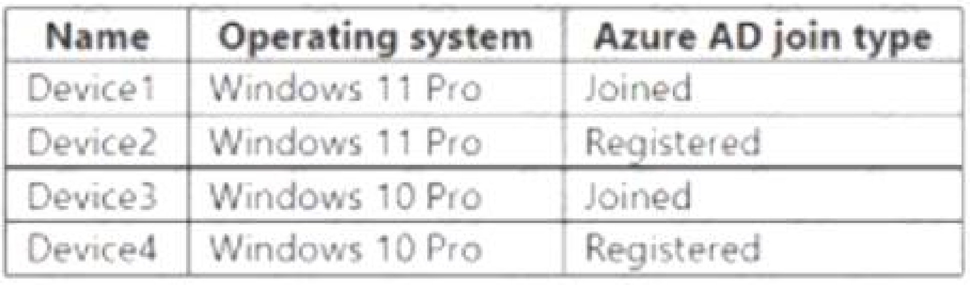
Explanation:
*Updates that contain fixes and improvements to existing Windows functionality can be deferred for 30 days. This is because the update rings policy named Policy1 has the “Quality updates deferral period (days)” setting set to 30. This means that quality updates, which include fixes and improvements 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 183
- (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 188
- (Exam Topic 4)
You have an Azure AD tenant that contains the devices shown in the following table.



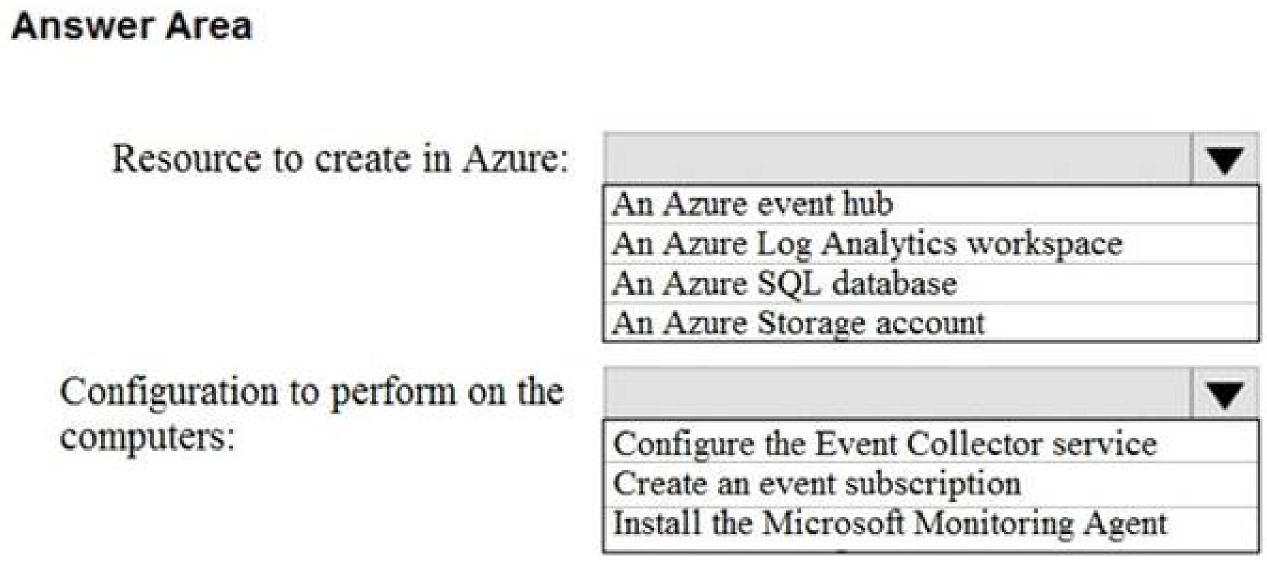
Name	Operating system	Azure AD join type
Device1	Windows 11 Pro	Joined
Device2	Windows 11 Pro	Registered
Device3	Windows 10 Pro	Joined
Device4	Windows 10 Pro	Registered

Which devices can be activated by using subscription activation?

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

Answer: C

NEW QUESTION 193
- (Exam Topic 4)
Your company has computers that run Windows 10 and are Microsoft Azure Active Directory (Azure AD)-joined.
The company purchases an Azure subscription.
You need to collect Windows events from the Windows 10 computers in Azure. The solution must enable you to create alerts based on the collected events.
What should you create in Azure and what should you configure on the computers? To answer, select the appropriate options in the answer area.
NOTE: Each correct selection is worth one point.



Answer Area

Resource to create in Azure:
- An Azure event hub
- An Azure Log Analytics workspace
- An Azure SQL database
- An Azure Storage account

Configuration to perform on the computers:
- Configure the Event Collector service
- Create an event subscription
- Install the Microsoft Monitoring Agent

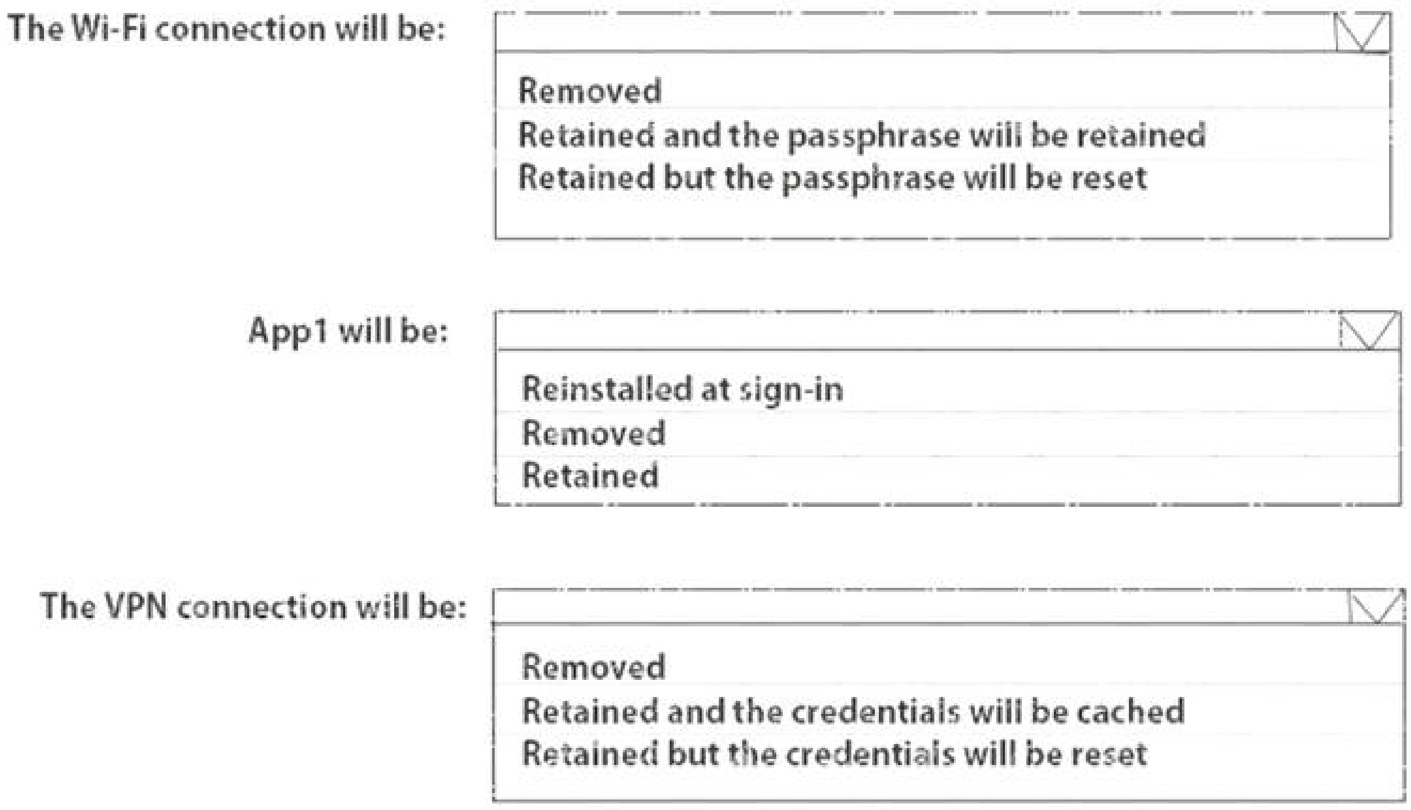
A. Mastered
B. Not Mastered

Answer: A

Explanation:
A screenshot of a computer Description automatically generated
Reference:
https://docs.microsoft.com/en-us/azure/azure-monitor/platform/log-analytics-agent

NEW QUESTION 198
- (Exam Topic 4)
You have computers that run Windows 10 and are configured by using Windows AutoPilot. A user performs the following tasks on a computer named Computer1:
- Creates a VPN connection to the corporate network
- Installs a Microsoft Store app named App1
- Connects to a Wi-Fi network

You perform a Windows AutoPilot Reset on Computer1.
What will be the state of the computer when the user signs in? To answer, select the appropriate options in the answer area.
NOTE: Each correct selection is worth one point.



The Wi-Fi connection will be:
- Removed
- Retained and the passphrase will be retained
- Retained but the passphrase will be reset

App1 will be:
- Reinstalled at sign-in
- Removed
- Retained

The VPN connection will be:
- Removed
- Retained and the credentials will be cached
- Retained but the credentials will be reset

A. Mastered
B. Not Mastered

Answer: A

Explanation:
Reference:
https://docs.microsoft.com/en-us/windows/deployment/windows-autopilot/windows-autopilot-reset

NEW QUESTION 202
- (Exam Topic 4)
You have a Microsoft 365 subscription that contains 1,000 Android devices enrolled in Microsoft Intune. You create an app configuration policy that contains the following settings:
• Device enrollment type: Managed devices
• Profile Type: All Profile Types
• Platform: Android Enterprise
Which two types of apps can be associated with the policy? Each correct answer presents a complete solution. NOTE: Each correct selection is worth one point.

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

Answer: BD

NEW QUESTION 206
- (Exam Topic 4)
You have a Microsoft 365 tenant that contains the objects shown in the following table. You are creating a compliance policy named Compliance1.
Which objects can you specify in Compliance1 as additional recipients of noncompliance notifications?

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

Answer: C

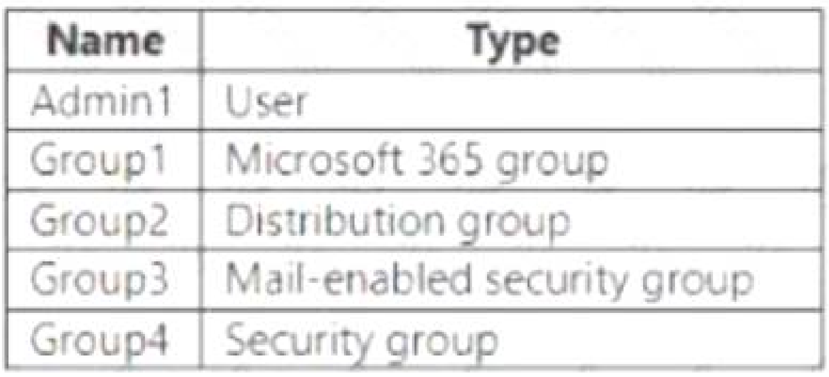
Explanation:
Reference:
https://www.ravenswoodtechnology.com/microsoft-intune-compliance-notifications/ https://docs.microsoft.com/en-us/microsoft-365/admin/create-groups/compare-groups?view=o365-worldwide

NEW QUESTION 209
- (Exam Topic 4)
You have a Microsoft 365 subscription.
You have devices enrolled in Microsoft Intune as shown in the following table. To which devices can you deploy apps by using Intune?

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

Answer: E

NEW QUESTION 210
- (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

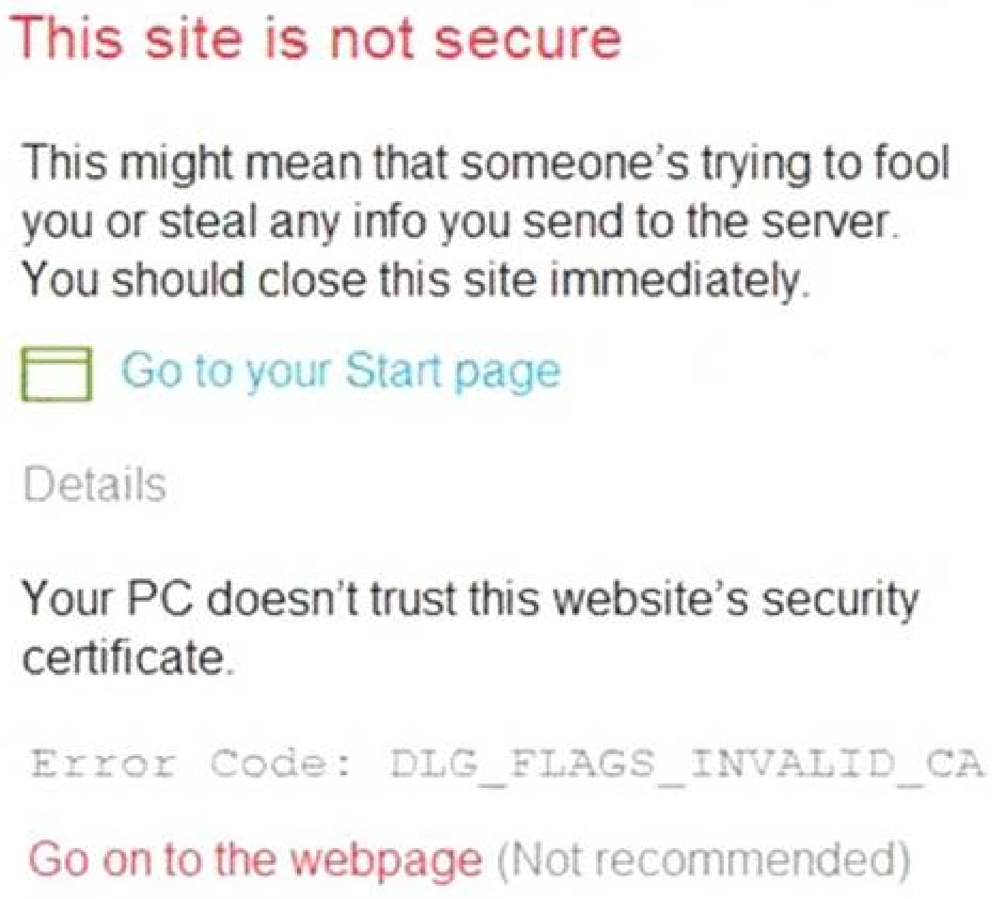
Answer: C

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 215
- (Exam Topic 4)
You use Windows Admin Center to remotely administer computers that run Windows 10.
When connecting to Windows Admin Center, you receive the message shown in the following exhibit.



This site is not secure

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

Go to your Start page

Details

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

```
Error Code: DLG_FLAGS_INVALID_CA
```

Go on to the webpage (Not recommended)

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

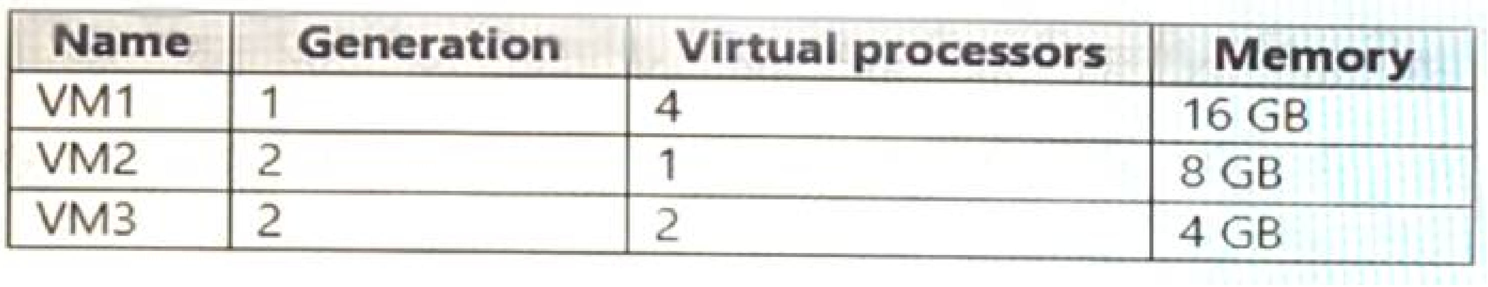
A. Personal
B. Trusted Root Certification Authorities
C. Client Authentication Issuers

Answer: B

NEW QUESTION 216

- (Exam Topic 4)

You have a Hyper-V host that contains the virtual machines shown in the following table.



Name	Generation	Virtual processors	Memory
VM1	1	4	16 GB
VM2	2	1	8 GB
VM3	2	2	4 GB

On which virtual machines can you install Windows 11?

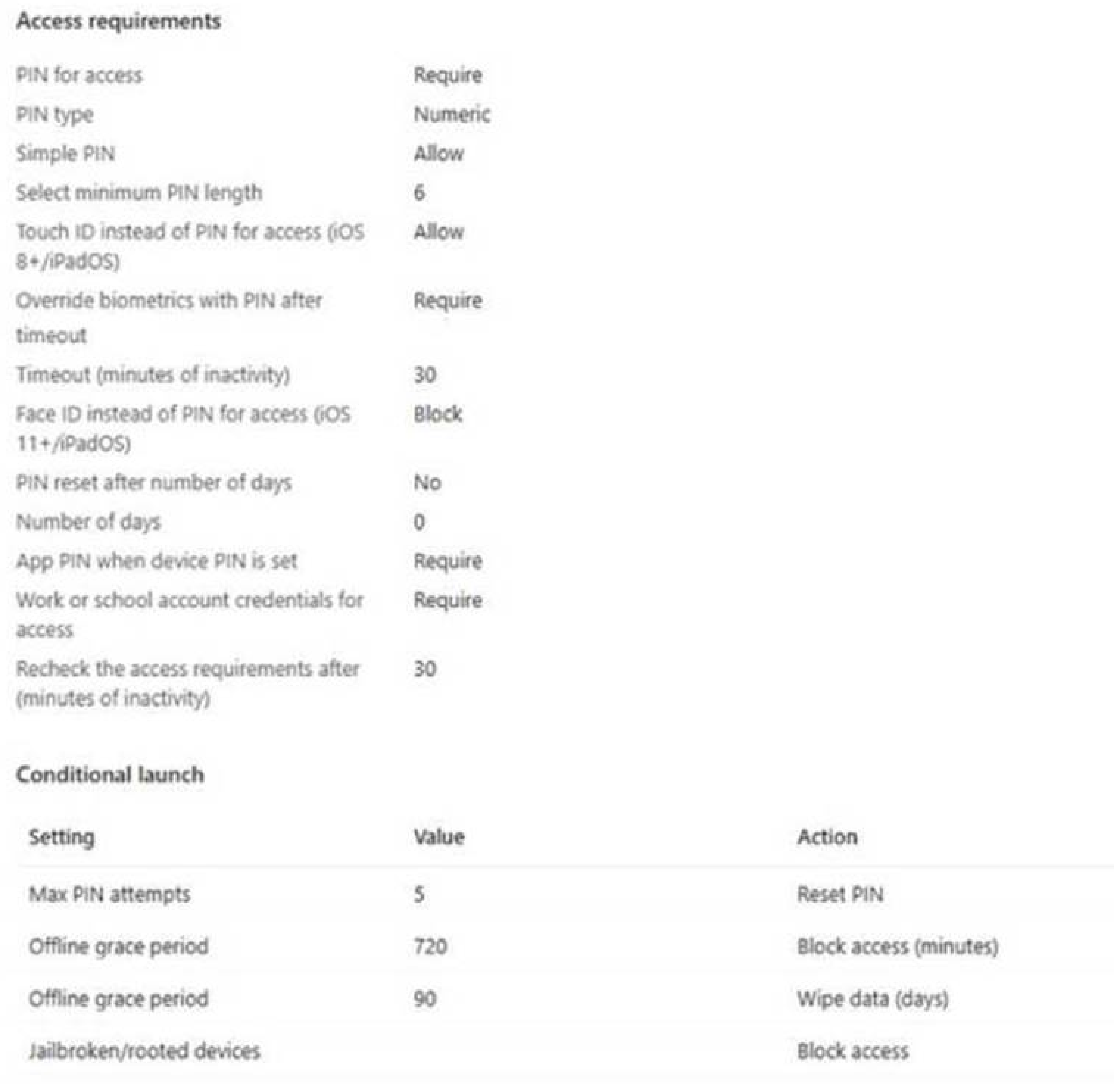
A. VM1 only
B. VM3only
C. VM1 and VM2 only
D. VM2 and VM3 only
E. VM1, VM2, and VM3

Answer: E

NEW QUESTION 217

- (Exam Topic 4)

You have a Microsoft 365 subscription.
You use Microsoft Intune Suite to manage devices.
You have the iOS app protection policy shown in the following exhibit.



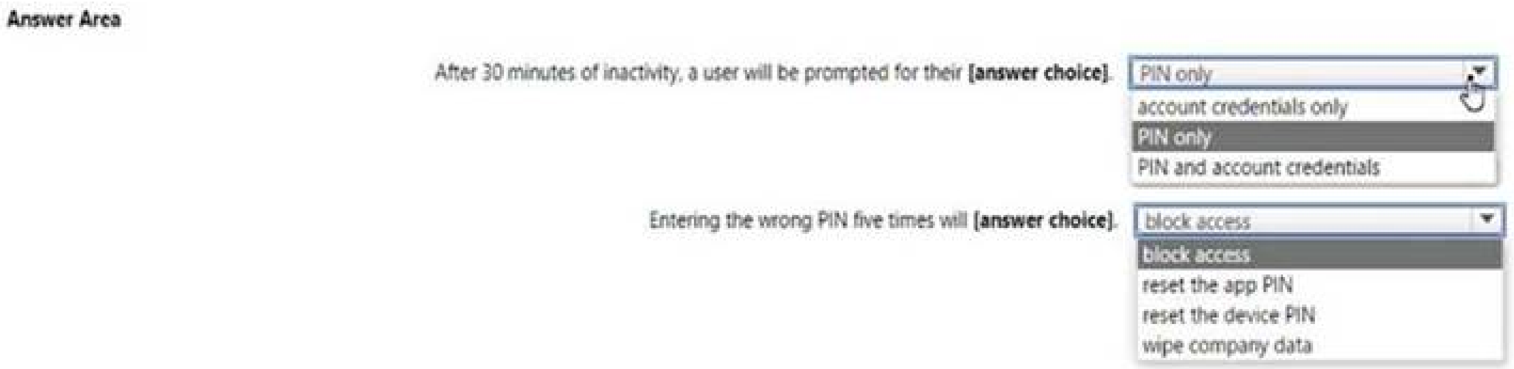
Access requirements

PIN for access	Require
PIN type	Numeric
Simple PIN	Allow
Select minimum PIN length	6
Touch ID instead of PIN for access (iOS 8+/iPadOS)	Allow
Override biometrics with PIN after timeout	Require
Timeout (minutes of inactivity)	30
Face ID instead of PIN for access (iOS 11+/iPadOS)	Block
PIN reset after number of days	No
Number of days	0
App PIN when device PIN is set	Require
Work or school account credentials for access	Require
Recheck the access requirements after (minutes of inactivity)	30

Conditional launch

Setting	Value	Action
Max PIN attempts	5	Reset PIN
Offline grace period	720	Block access (minutes)
Offline grace period	90	Wipe data (days)
Jailbroken/rooted devices		Block access

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

After 30 minutes of inactivity, a user will be prompted for their **[answer choice]**. PIN only

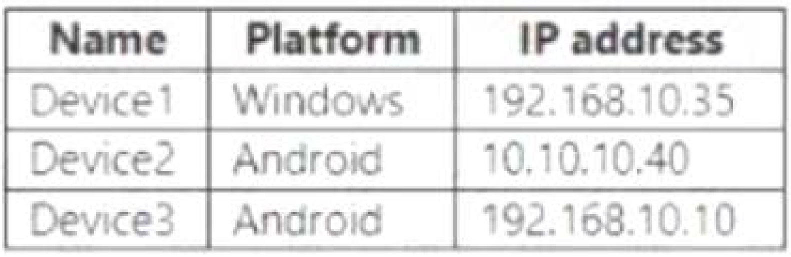
Entering the wrong PIN five times will **[answer choice]**. block access

A. Mastered
B. Not Mastered

Answer: A

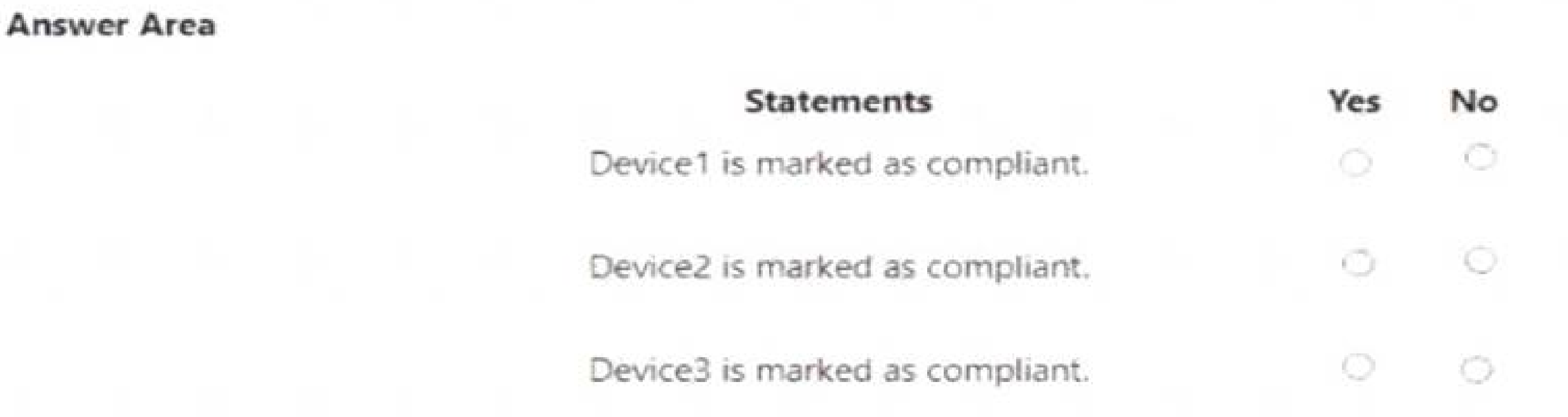
Explanation:
Box 1 = PIN only
Box 2 = reset the PIN app
iOS/iPadOS app protection policy settings - Microsoft Intune | Microsoft Learn https://learn.microsoft.com/en-us/mem/intune/apps/app-protection-policy-settings-ios

NEW QUESTION 218
- (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.	○	○

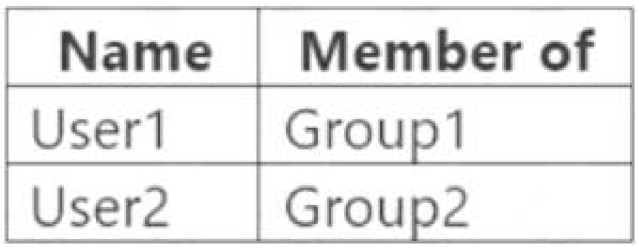
A. Mastered
B. Not Mastered

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.

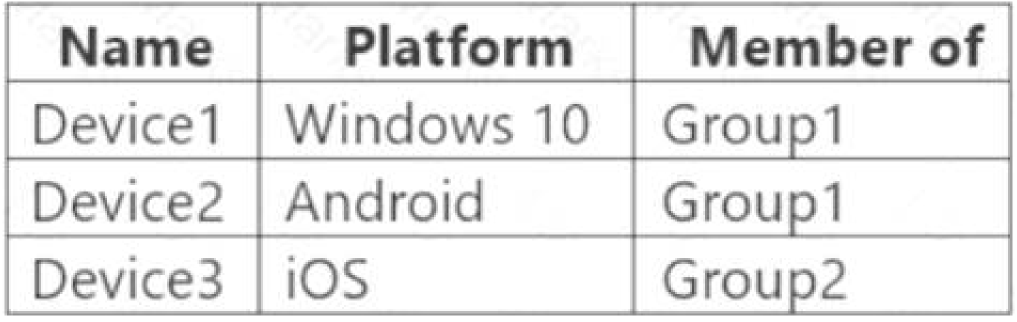
NEW QUESTION 219

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



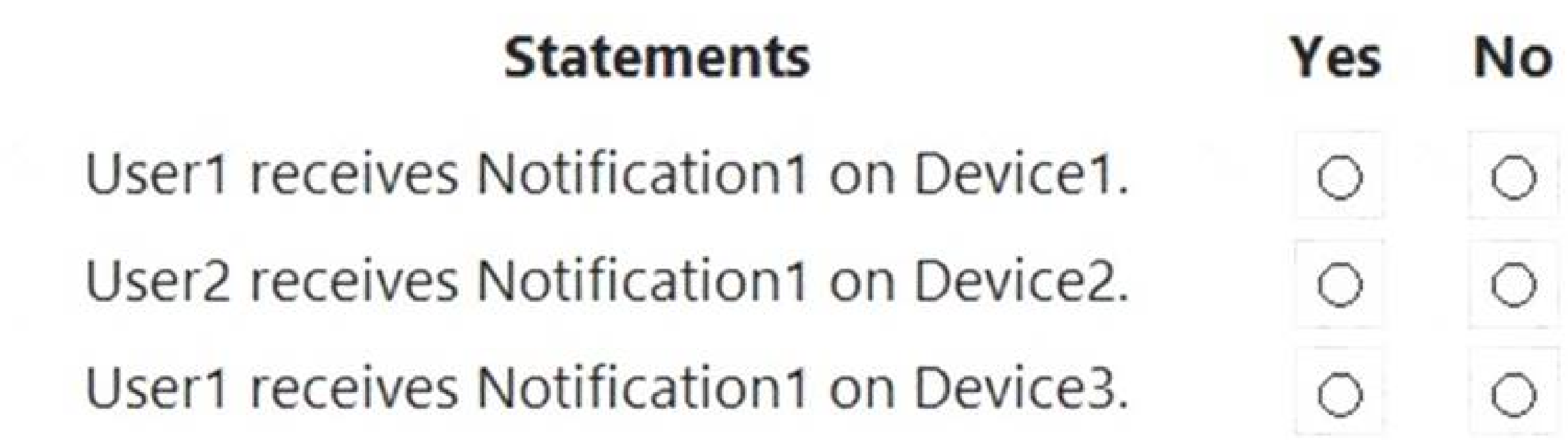
Name	Member of
User1	Group1
User2	Group2

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



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

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



Statements	Yes	No
User1 receives Notification1 on Device1.	○	○
User2 receives Notification1 on Device2.	○	○
User1 receives Notification1 on Device3.	○	○

A. Mastered
B. Not Mastered

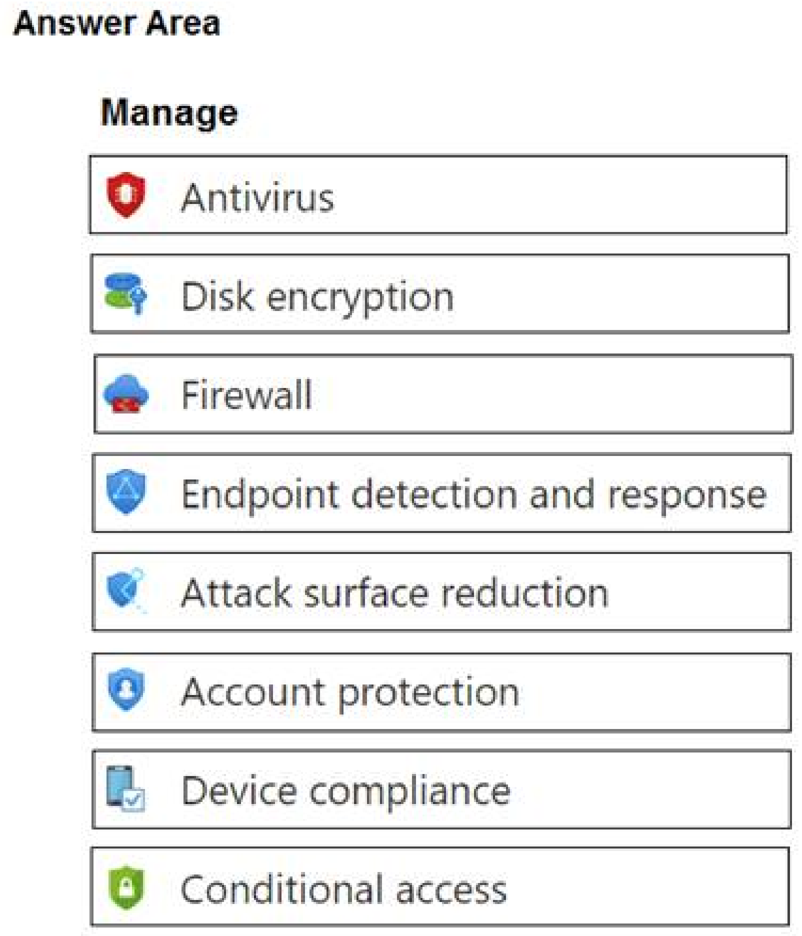
Answer: A

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

NEW QUESTION 223
- (Exam Topic 4)
You have a Microsoft 365 E5 subscription that contains 100 Windows 10 devices enrolled in Microsoft Intune. You need to create Endpoint security policies to meet the following requirements:

- Hide the Firewall & network protection area in the Windows Security app.
- Disable the provisioning of Windows Hello for Business on the devices.

Which two policy types should you use? To answer, select the policies in the answer area.
NOTE: Each correct selection is worth one point.



Answer Area

Manage

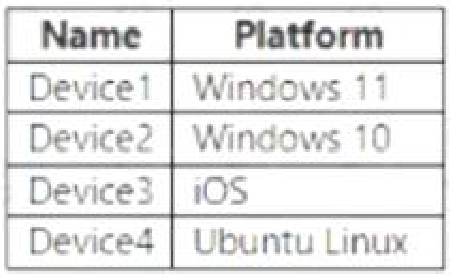
- Antivirus
- Disk encryption
- Firewall
- Endpoint detection and response
- Attack surface reduction
- Account protection
- Device compliance
- Conditional access

A. Mastered
B. Not Mastered

Answer: A

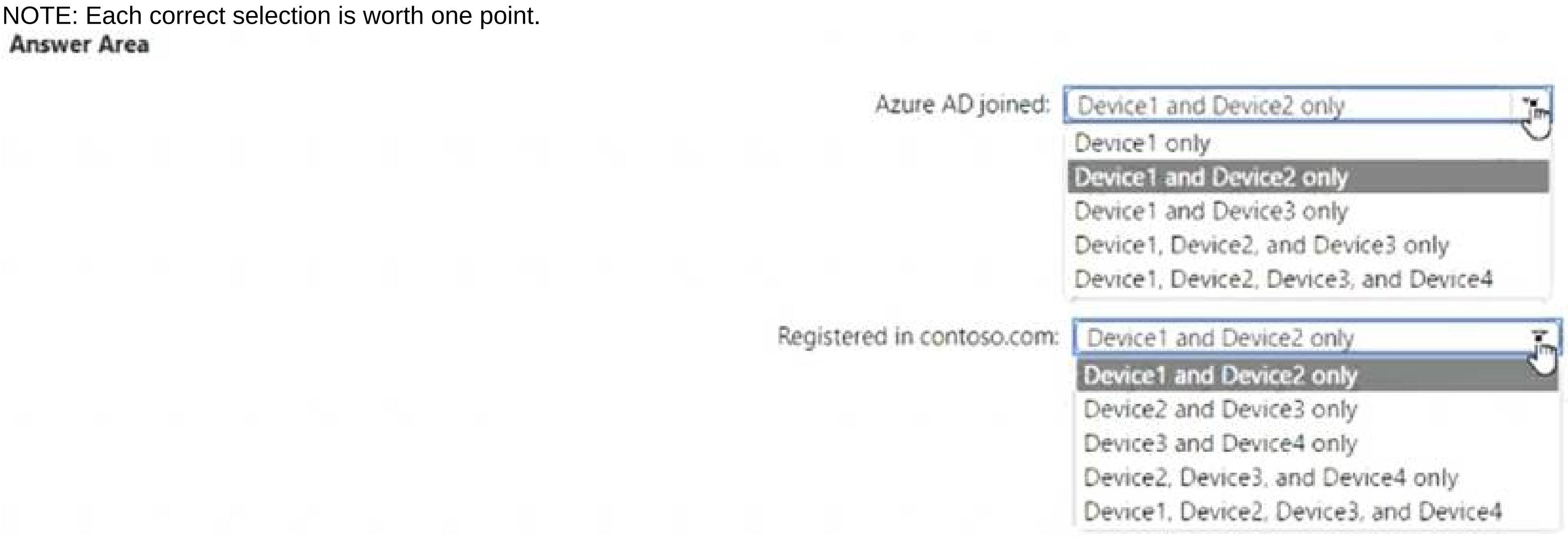
Explanation:
Graphical user interface, application Description automatically generated
In the Antivirus policy settings, you can hide the Firewall and network protection area in the Windows Security app.
Windows Hello for Business settings are configured in Identity protection. Reference:
https://docs.microsoft.com/en-us/mem/intune/protect/antivirus-security-experience-windows-settings https://docs.microsoft.com/en-us/mem/intune/protect/identity-protection-windows-settings

NEW QUESTION 227
- (Exam Topic 4)
You have an Azure AD tenant named contoso.com. You have the devices shown in the following table.



Name	Platform
Device1	Windows 11
Device2	Windows 10
Device3	iOS
Device4	Ubuntu Linux

Which devices can be Azure AD joined, and which devices can be registered in contoso.com? To answer, select the appropriate options in the answer area.
NOTE: Each correct selection is worth one point.



Answer Area

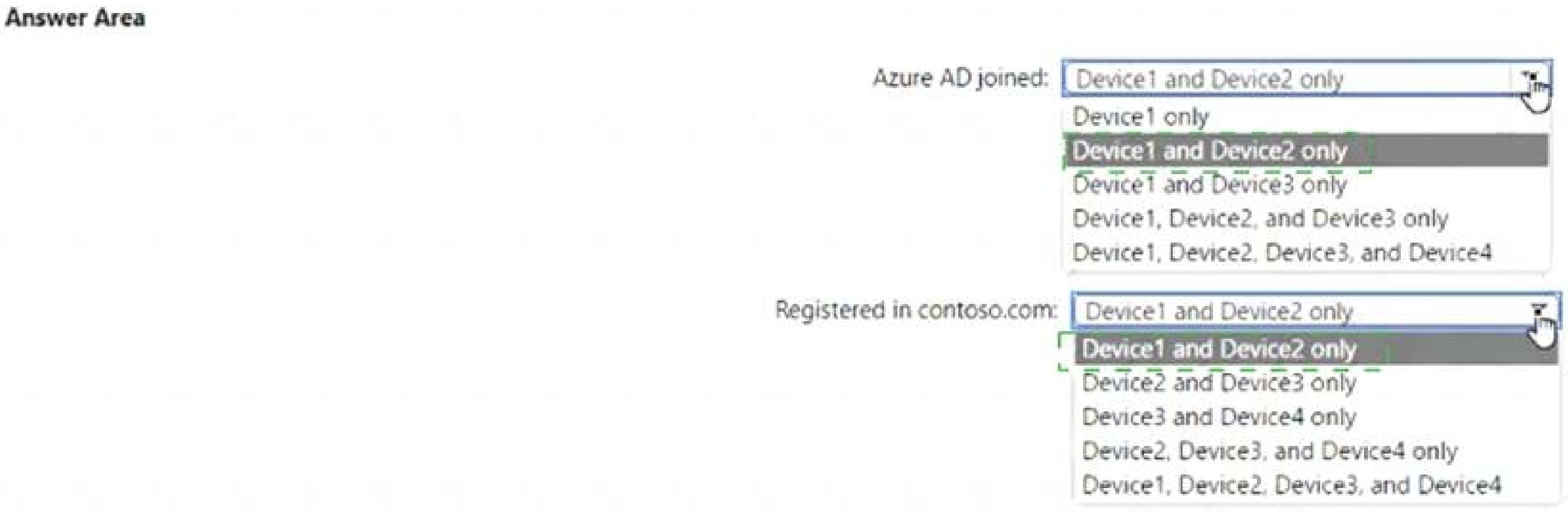
Azure AD joined: Device1 and Device2 only
Device1 only
Device1 and Device2 only
Device1 and Device3 only
Device1, Device2, and Device3 only
Device1, Device2, Device3, and Device4

Registered in contoso.com: Device1 and Device2 only
Device1 and Device2 only
Device2 and Device3 only
Device3 and Device4 only
Device2, Device3, and Device4 only
Device1, Device2, Device3, and Device4

A. Mastered
B. Not Mastered

Answer: A

Explanation:



Answer Area

Azure AD joined: Device1 and Device2 only

- Device1 only
- Device1 and Device2 only
- Device1 and Device3 only
- Device1, Device2, and Device3 only
- Device1, Device2, Device3, and Device4

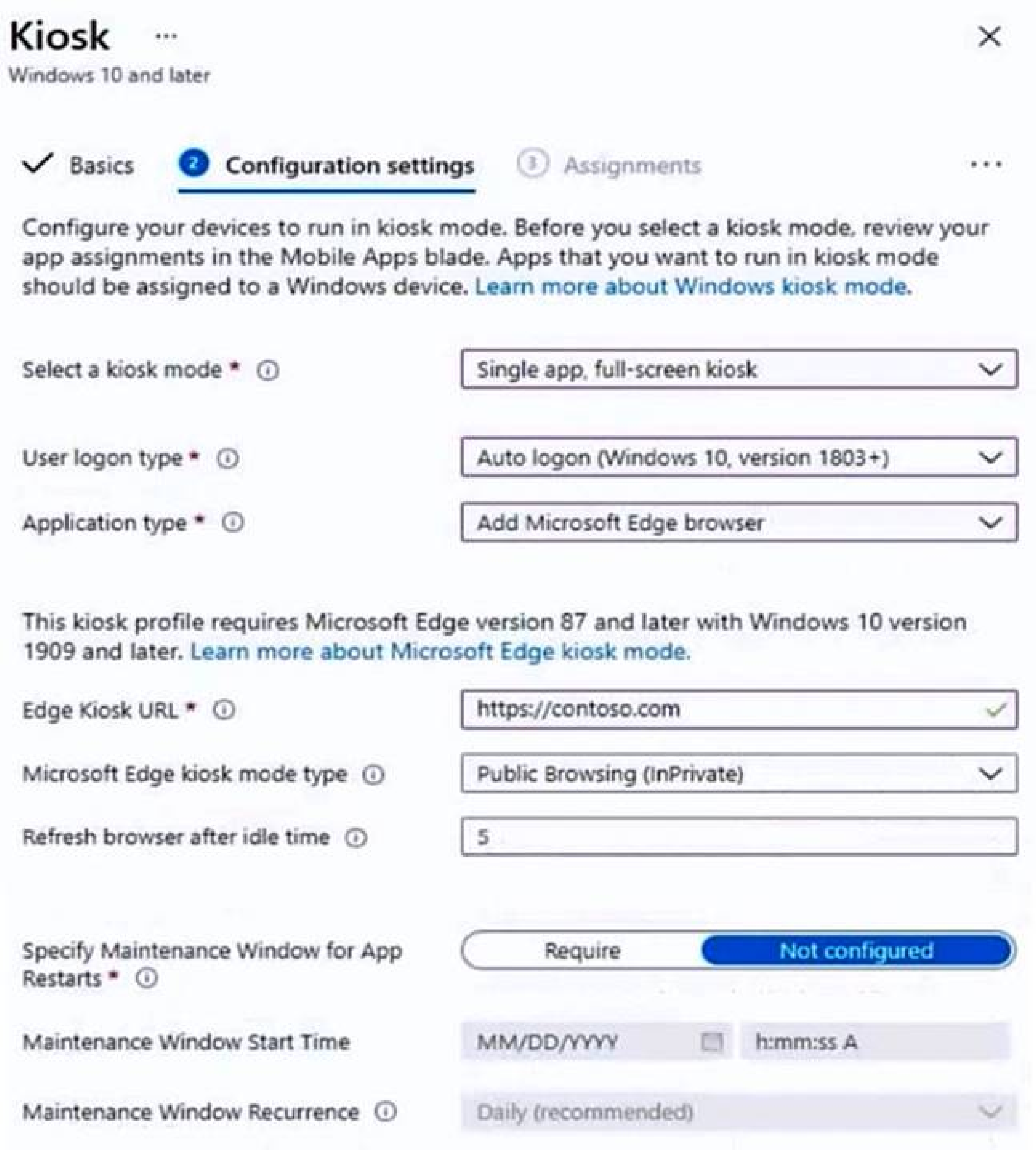
Registered in contoso.com: Device1 and Device2 only

- Device1 and Device2 only
- Device2 and Device3 only
- Device3 and Device4 only
- Device2, Device3, and Device4 only
- Device1, Device2, Device3, and Device4

NEW QUESTION 231

- (Exam Topic 4)

You have the device configuration profile shown in the following exhibit.



Kiosk ...

Windows 10 and later

✓ Basics ② Configuration settings ③ Assignments ...

Configure your devices to run in kiosk mode. Before you select a kiosk mode, review your app assignments in the Mobile Apps blade. Apps that you want to run in kiosk mode should be assigned to a Windows device. Learn more about Windows kiosk mode.

Select a kiosk mode * ⓘ: Single app, full-screen kiosk

User logon type * ⓘ: Auto logon (Windows 10, version 1803+)

Application type * ⓘ: Add Microsoft Edge browser

This kiosk profile requires Microsoft Edge version 87 and later with Windows 10 version 1909 and later. Learn more about Microsoft Edge kiosk mode.

Edge Kiosk URL * ⓘ: https://contoso.com ✓

Microsoft Edge kiosk mode type ⓘ: Public Browsing (InPrivate)

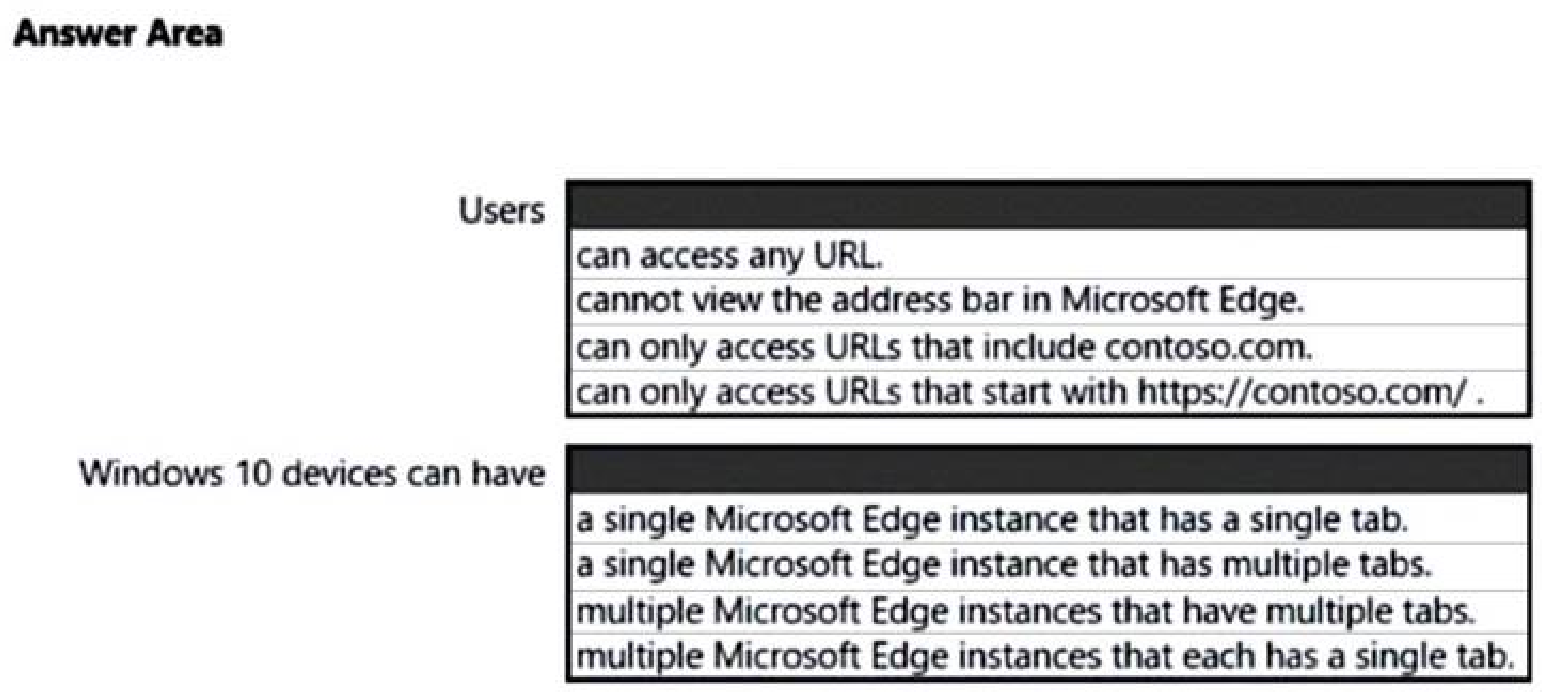
Refresh browser after idle time ⓘ: 5

Specify Maintenance Window for App Restarts * ⓘ: Require [✓ Not configured]

Maintenance Window Start Time: MM/DD/YYYY h:mm:ss A

Maintenance Window Recurrence ⓘ: Daily (recommended)

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
- can access any URL.
- cannot view the address bar in Microsoft Edge.
- can only access URLs that include contoso.com.
- can only access URLs that start with https://contoso.com/ .

Windows 10 devices can have
- a single Microsoft Edge instance that has a single tab.
- a single Microsoft Edge instance that has multiple tabs.
- multiple Microsoft Edge instances that have multiple tabs.
- multiple Microsoft Edge instances that each has a single tab.

A. Mastered
B. Not Mastered

Answer: A

Explanation:
Users can only access URLs that start with https://contoso.com/ Windows 10 and later devices can have multiple Microsoft Edge instances that each has a single tab
he device configuration profile shown in the exhibit is a kiosk browser profile that configures Microsoft Edge to run in kiosk mode. The profile has the following settings:

- Kiosk mode: Enabled
- Kiosk type: Multi-app
- Allowed URLs: https://contoso.com/*
- Address bar: Disabled

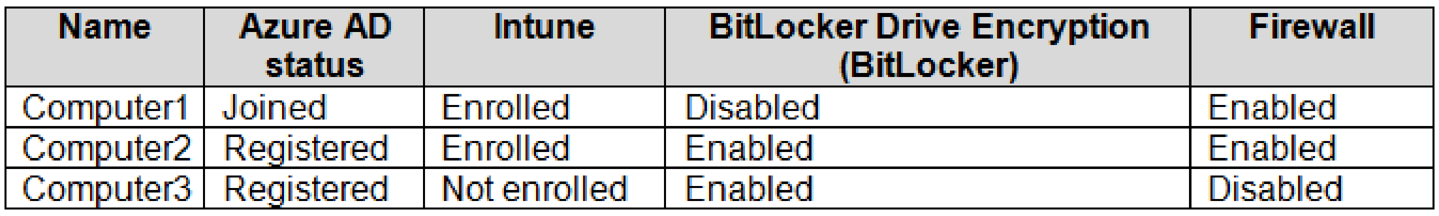
These settings mean that users can only access URLs that start with https://contoso.com/ and cannot view the address bar in Microsoft Edge. The kiosk type of Multi-app allows users to open multiple instances of Microsoft Edge, but each instance can only have a single tab. Therefore, users cannot access any URL, cannot view the address bar in Microsoft Edge, and can have multiple Microsoft Edge instances that each has a single tab. References: https://docs.microsoft.com/en-us/mem/intune/configuration/kiosk-settings#kiosk-browser-settings

NEW QUESTION 236
- (Exam Topic 4)
You have computers that run Windows 10 and are managed by using Microsoft Intune. Users store their files in a folder named D:\Folder1.
You need to ensure that only a trusted list of applications is granted write access to D:\Folder1. What should you configure in the device configuration profile?

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

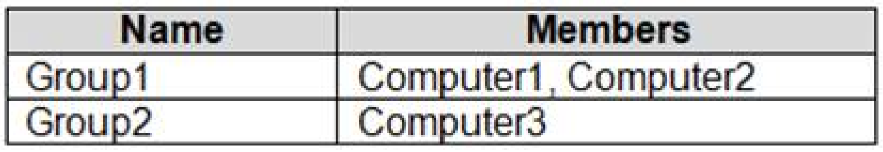
Answer: A

NEW QUESTION 240
- (Exam Topic 4)
You have a Microsoft 365 subscription that includes Microsoft Intune. You have computers that run Windows 11 as shown in the following table.



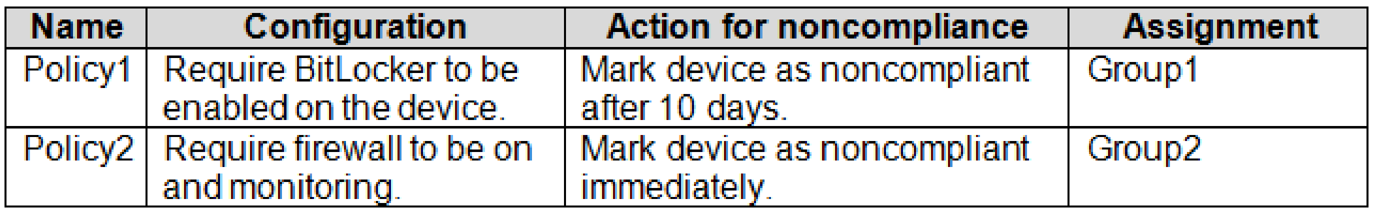
Name	Azure AD status	Intune	BitLocker Drive Encryption (BitLocker)	Firewall
Computer1	Joined	Enrolled	Disabled	Enabled
Computer2	Registered	Enrolled	Enabled	Enabled
Computer3	Registered	Not enrolled	Enabled	Disabled

You have the groups shown in the following table.



Name	Members
Group1	Computer1, Computer2
Group2	Computer3

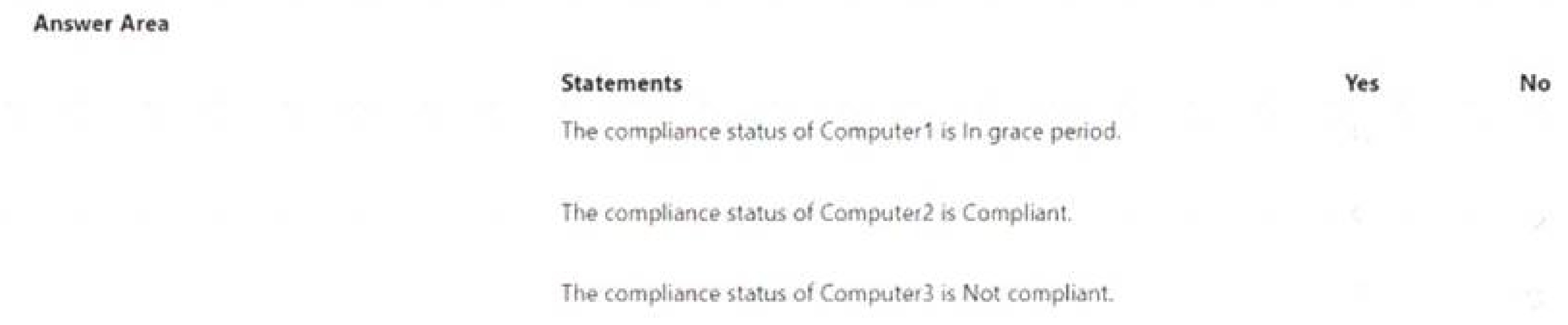
You create and assign the compliance policies shown in the following table.



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

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

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



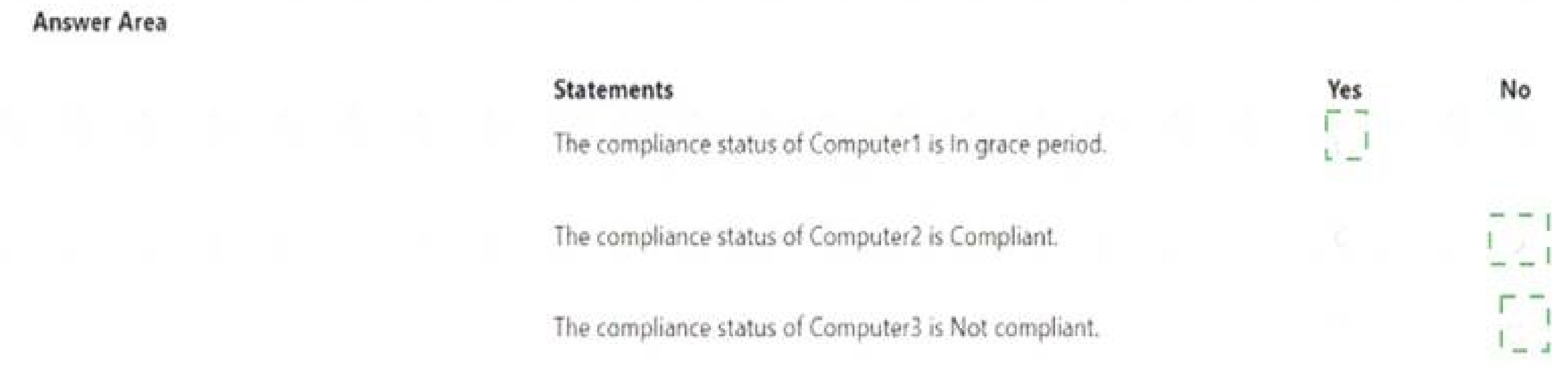
Answer Area

Statements	Yes	No
The compliance status of Computer1 is In grace period.	○	○
The compliance status of Computer2 is Compliant.	○	○
The compliance status of Computer3 is Not compliant.	○	○

A. Mastered
B. Not Mastered

Answer: A

Explanation:



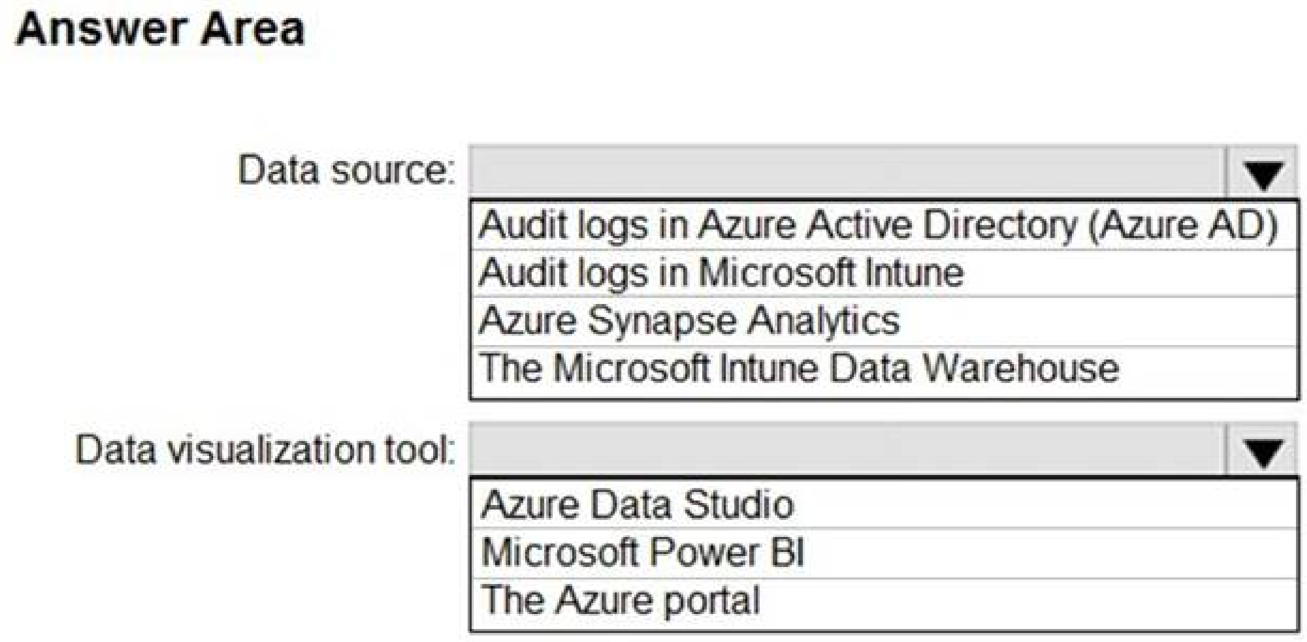
Answer Area

Statements	Yes	No
The compliance status of Computer1 is In grace period.	✓	
The compliance status of Computer2 is Compliant.		✓
The compliance status of Computer3 is Not compliant.		✓

NEW QUESTION 243
- (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

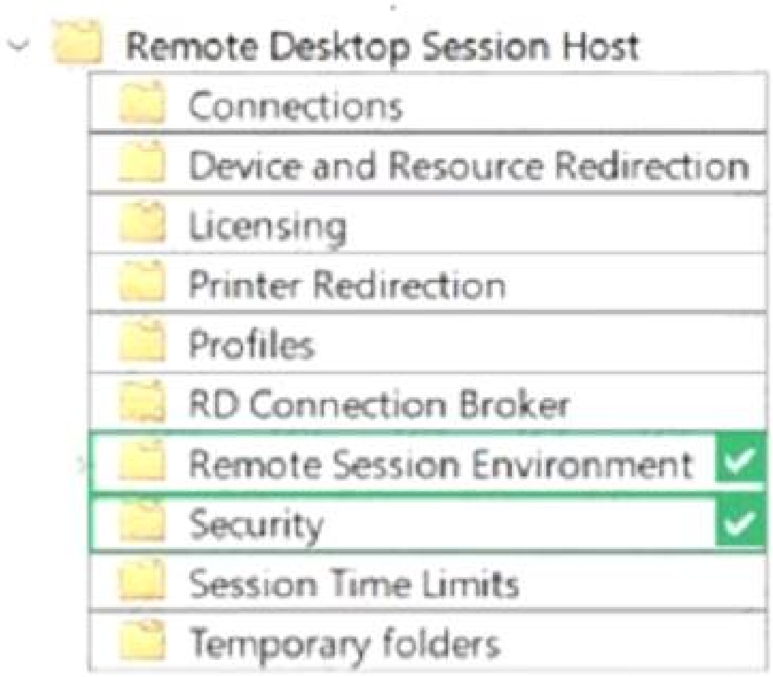
NEW QUESTION 247
- (Exam Topic 4)
You have a Microsoft Deployment Toolkit (MDT) deployment share named DS1.
in the Out-of-Box Drivers node, you create folders that contain drivers for different hardware models.
You need to configure the Inject Drivers MDT task to use PnP detection to install the drivers 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 249
- (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.

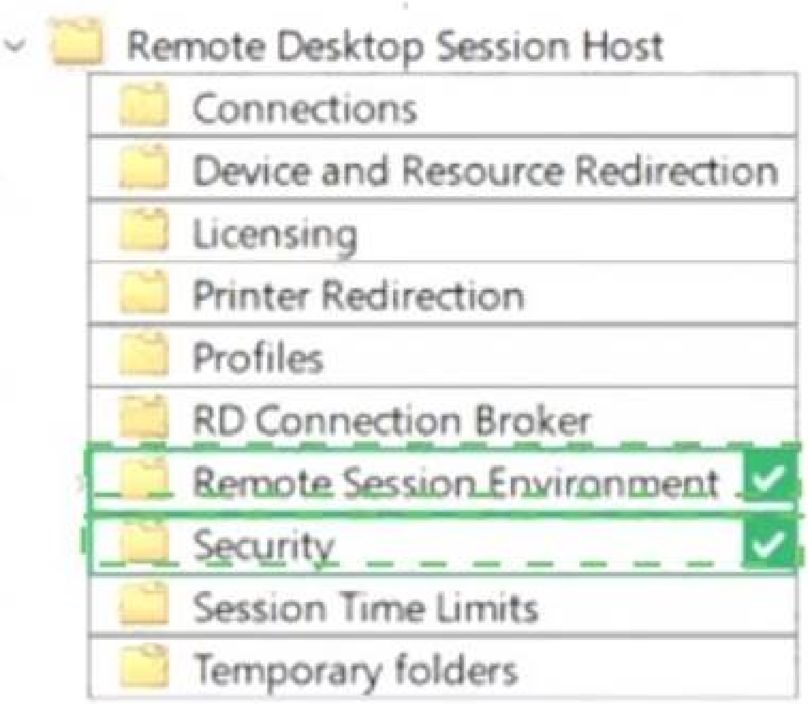


Remote Desktop Session Host
- Connections
- Device and Resource Redirection
- Licensing
- Printer Redirection
- Profiles
- RD Connection Broker
- Remote Session Environment ✓
- Security ✓
- Session Time Limits
- Temporary folders

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 254
- (Exam Topic 4)
You have a Microsoft 365 subscription that contains a user named User1. User! is assigned a Windows 10/11 Enterprise E3 license. You use Microsoft Intune Suite to manage devices. User1 activates the following devices:
• Device1: Windows 11 Enterprise
• Device2: Windows 10 Enterprise
• Device3: Windows 11 Enterprise
How many more devices can User1 activate?

A. 2
B. 3
C. 7
D. 8

Answer: A

NEW QUESTION 257

- (Exam Topic 4)

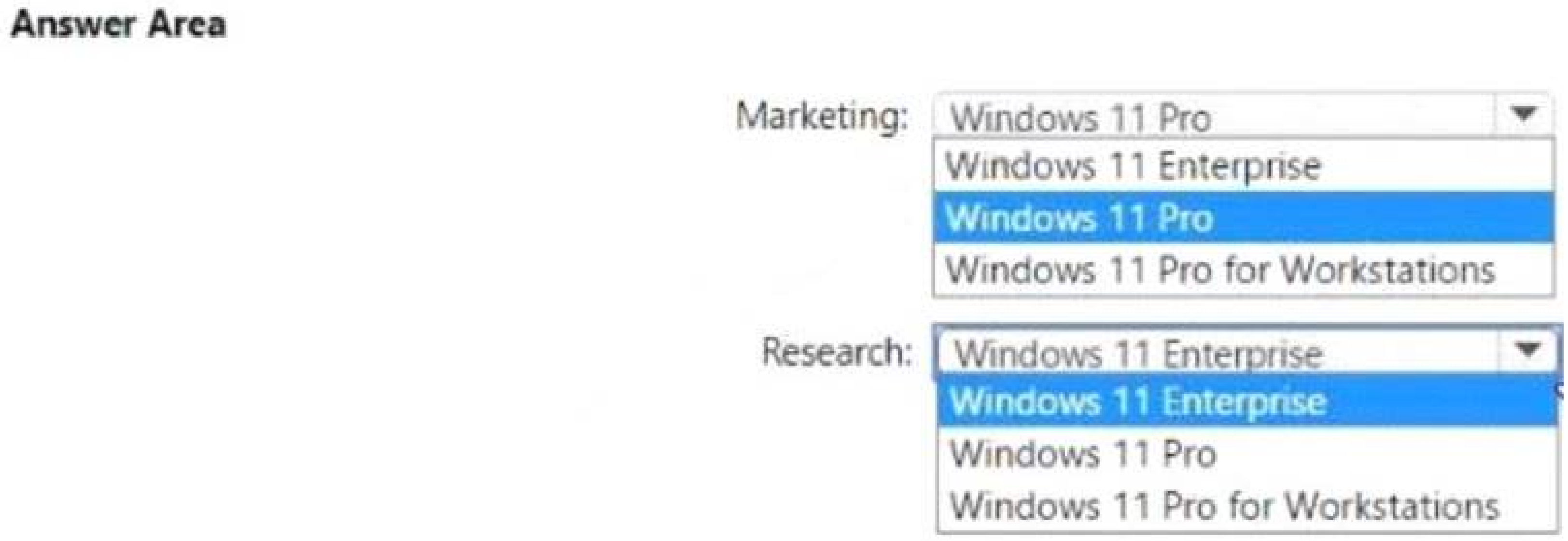
You have a Microsoft 365 subscription that uses Microsoft Intune Suite. You use Microsoft Intune to manage devices.

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

• Marketing department devices must support Windows Update for Business.

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

NOTE: Each correct selection is worth one point


Answer Area

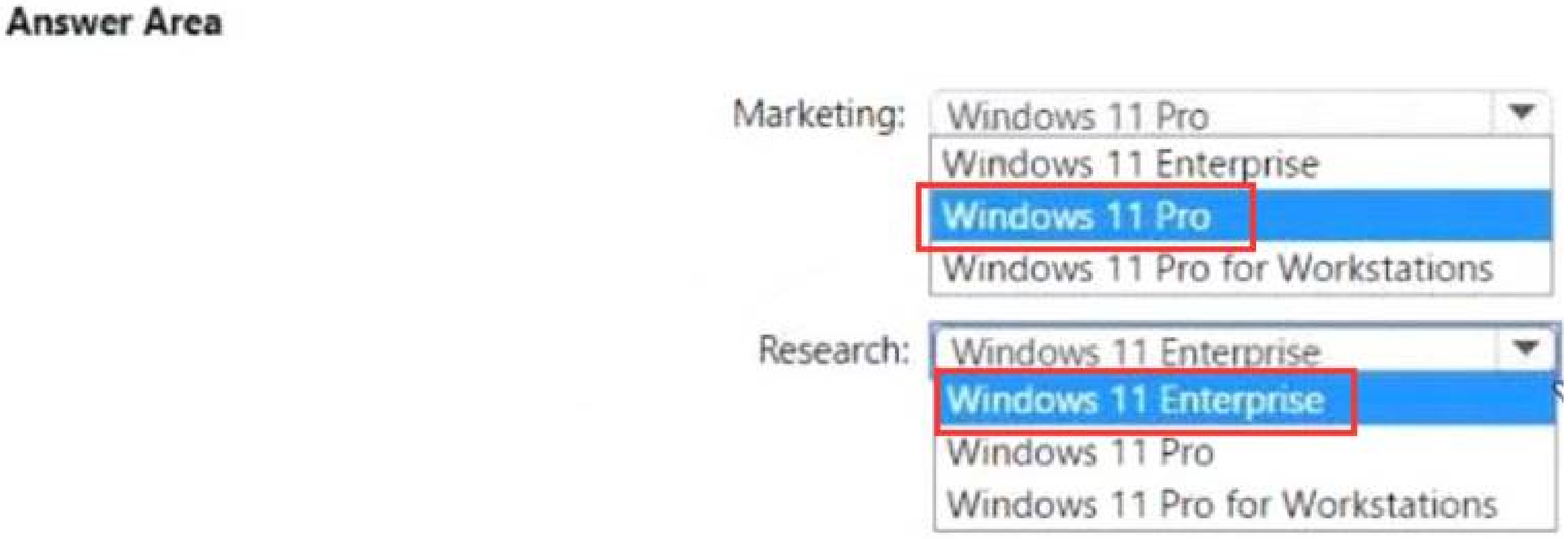
Marketing: Windows 11 Pro
- Windows 11 Enterprise
- Windows 11 Pro
- Windows 11 Pro for Workstations

Research: Windows 11 Enterprise
- Windows 11 Enterprise
- Windows 11 Pro
- Windows 11 Pro for Workstations

A. Mastered
B. Not Mastered

Answer: A

Explanation:


Answer Area

Marketing: Windows 11 Pro
- Windows 11 Enterprise
- Windows 11 Pro
- Windows 11 Pro for Workstations

Research: Windows 11 Enterprise
- Windows 11 Enterprise
- Windows 11 Pro
- Windows 11 Pro for Workstations

NEW QUESTION 259

......

Relate Links

100% Pass Your MD-102 Exam with Exambible Prep Materials

https://www.exambible.com/MD-102-exam/

Contact us

We are proud of our high-quality customer service, which serves you around the clock 24/7.

Viste - https://www.exambible.com/