Microsoft

Exam Questions MD-102

Endpoint Administrator

NEW QUESTION 1
- (Exam Topic 4)
You have a Microsoft 365 subscription that contains 100 devices enrolled in Microsoft Intune. You need to review the startup processes and how often each device restarts.
What should you use?

A. Endpoint analytics
B. Intune Data Warehouse
C. Azure Monitor
D. Device Management

Answer: B

NEW QUESTION 2
- (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?

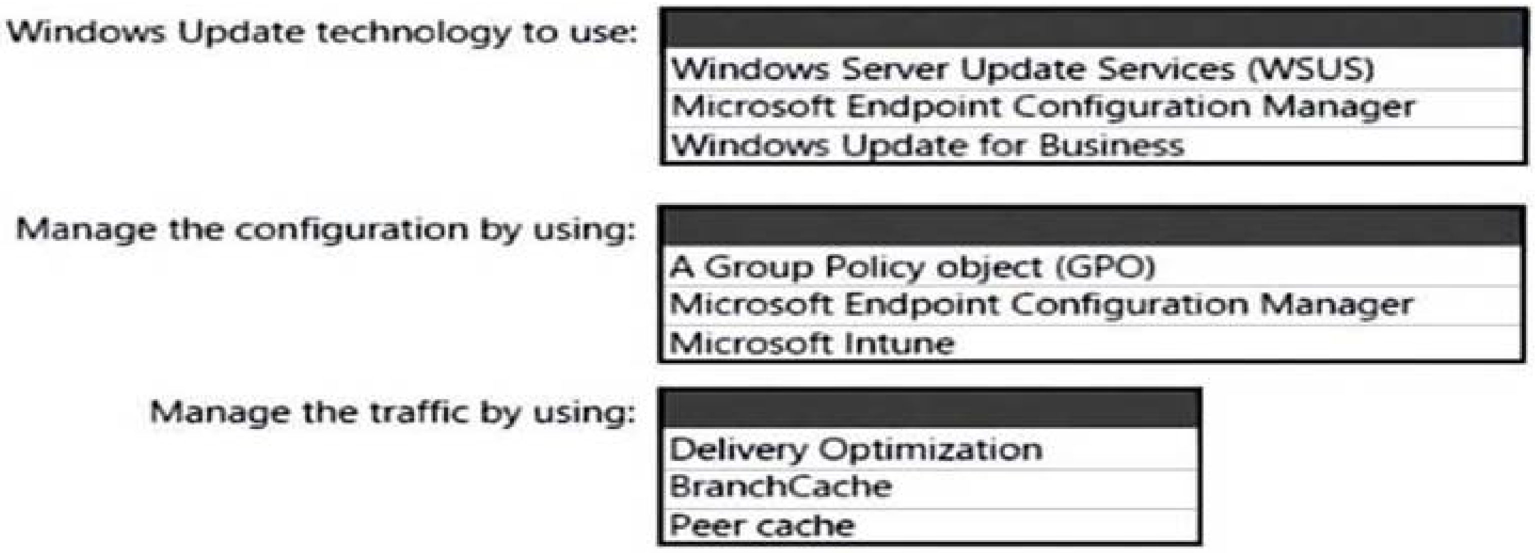
A. a device compliance policy
B. a device cleanup rule
C. a device enrollment policy
D. a device configuration profile

Answer: D

NEW QUESTION 3
- (Exam Topic 4)
You have 100 computers that run Windows 10. You have no servers. All the computers are joined to Microsoft Azure Active Directory (Azure AD).
The computers have different update settings, and some computers are configured for manual updates. You need to configure Windows Update. The solution must meet the following requirements:

- The configuration must be managed from a central location.
- Internet traffic must be minimized.
- Costs must be minimized.

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



Windows Update technology to use:
Windows Server Update Services (WSUS)
Microsoft Endpoint Configuration Manager
Windows Update for Business

Manage the configuration by using:
A Group Policy object (GPO)
Microsoft Endpoint Configuration Manager
Microsoft Intune

Manage the traffic by using:
Delivery Optimization
BranchCache
Peer cache

A. Mastered
B. Not Mastered

Answer: A

Explanation:
Box 1: Windows Server Update Services (WSUS)
Windows Server Update Services (WSUS) enables information technology administrators to deploy the latest Microsoft product updates. You can use WSUS to fully manage the distribution of updates that are released through Microsoft Update to computers on your network.
Windows Server Update Services is a built-in server role that includes the following enhancements: Can be added and removed by using the Server Manager Includes Windows PowerShell cmdlets to manage the most important administrative tasks in WSUS Etc.
Box 2: A Group Policy object
In an Active Directory environment, you can use Group Policy to define how computers and users can interact with Windows Update to obtain automatic updates from Windows Server Update Services (WSUS).
Box 3: BranchCache
BranchCache is a bandwidth-optimization feature that has been available since the Windows Server 2008 R2 and Windows 7 operating systems. Each client has a cache and acts as an alternate source for content that devices on its own network request. Windows Server Update Services (WSUS) and Microsoft Endpoint Manager can use BranchCache to optimize network bandwidth during update deployment, and it's easy to configure for either of them. BranchCache has two operating modes: Distributed Cache mode and Hosted Cache mode.
Reference: https://docs.microsoft.com/en-us/windows/deployment/update/waas-branchcache https://docs.microsoft.com/en-us/windows-server/administration/windows-server-update-services/deploy/4-conf

NEW QUESTION 4

- (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 5
- (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 6
- (Exam Topic 4)
You have a Microsoft Azure subscription that contains an Azure Log Analytics workspace.
You deploy a new computer named Computer1 that runs Windows 10. Computer1 is in a workgroup. You need to ensure that you can use Log Analytics to query events from Computer1.
What should you do on Computer1?

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

Answer: D

NEW QUESTION 7
- (Exam Topic 4)
You need to implement mobile device management (MDM) for personal devices that run Windows 11. The solution must meet the following requirements:
• Ensure that you can manage the personal devices by using Microsoft Intune.
• Ensure that users can access company data seamlessly from their personal devices.
• Ensure that users can only sign in to their personal devices by using their personal account What should you use to add the devices to Azure AD?

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

Answer: A

Explanation:
To implement MDM for personal devices that run Windows 11, you should use Azure AD registered. Azure AD registered devices are devices that are connected to your organization’s resources using a personal device and a personal account. You can manage these devices by using Microsoft Intune and enable seamless access to company data. Users can only sign in to their personal devices by using their personal account, not their organizational account. Azure AD registered devices support Windows 10 or newer, iOS, Android, macOS, and Ubuntu 20.04/22.04 LTS1.
The other options are not suitable for this scenario because:
➢ Hybrid Azure AD join is for corporate-owned and managed devices that are joined to both on-premises Active Directory and Azure AD. Users can sign in to these devices by using their organizational account that exists in both directories2.
➢ AD joined is for devices that are joined only to on-premises Active Directory. These devices are not managed by Microsoft Intune and do not have access to cloud resources3.
References: What are Azure AD registered devices?, What are hybrid Azure AD joined devices?, What is Active Directory domain join?

NEW QUESTION 8

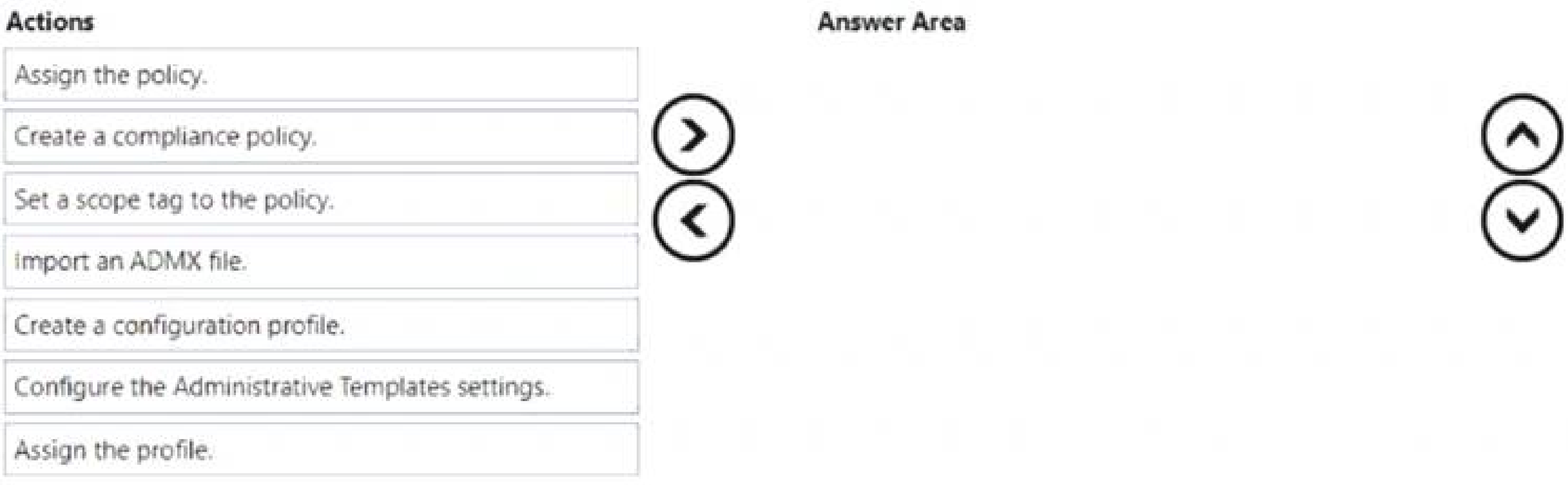
- (Exam Topic 4)

You have an on-premises Active Directory domain that syncs to Azure AD tenant.

The tenant contains computers that run Windows 10. The computers are hybrid Azure AD joined and enrolled in Microsoft Intune. The Microsoft Office settings on the computers are configured by using an Group Policy Object (GPO).

You need to migrate the GPO to Intune.

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

Assign the policy.

Create a compliance policy.

Set a scope tag to the policy.

Import an ADMX file.

Create a configuration profile.

Configure the Administrative Templates settings.

Assign the profile.

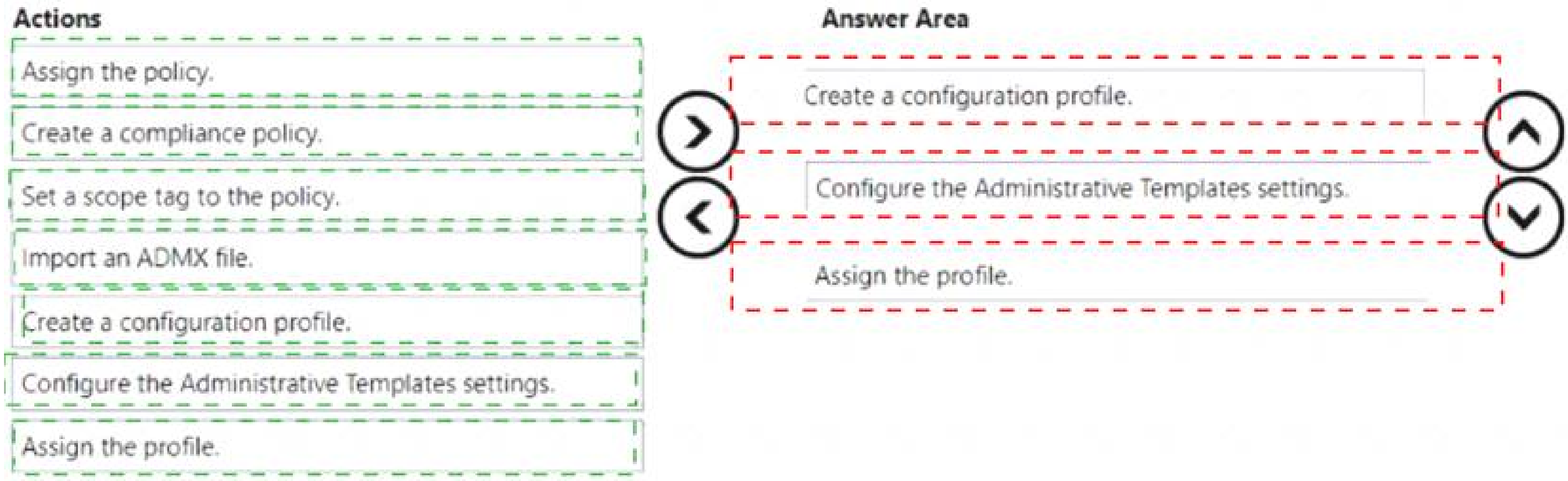
Answer Area

A. Mastered

B. Not Mastered

Answer: A

Explanation:



Actions

Assign the policy.

Create a compliance policy.

Set a scope tag to the policy.

Import an ADMX file.

Create a configuration profile.

Configure the Administrative Templates settings.

Assign the profile.

Answer Area

Create a configuration profile.

Configure the Administrative Templates settings.

Assign the profile.

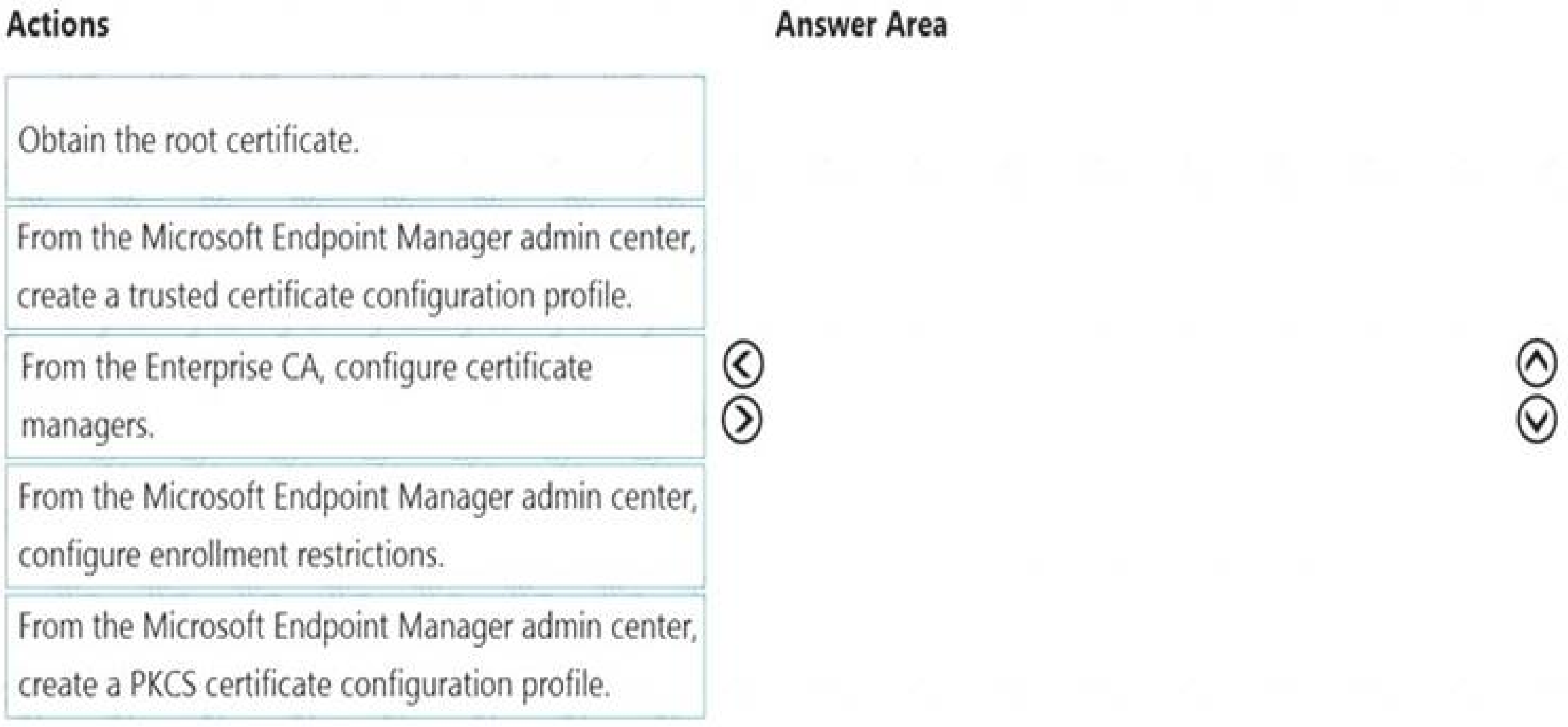
NEW QUESTION 9

- (Exam Topic 4)

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

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

Which three actions should you perform in sequence? To answer, move the appropriate actions from the list of actions to the answer area and arrange them in the correct order.



Actions

Obtain the root certificate.

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

From the Enterprise CA, configure certificate managers.

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

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

Answer Area

A. Mastered

B. Not Mastered

Answer: A

Explanation:
Graphical user interface, text, application, email Description automatically generated
Reference:
https://docs.microsoft.com/en-us/mem/intune/protect/certificates-pfx-configure

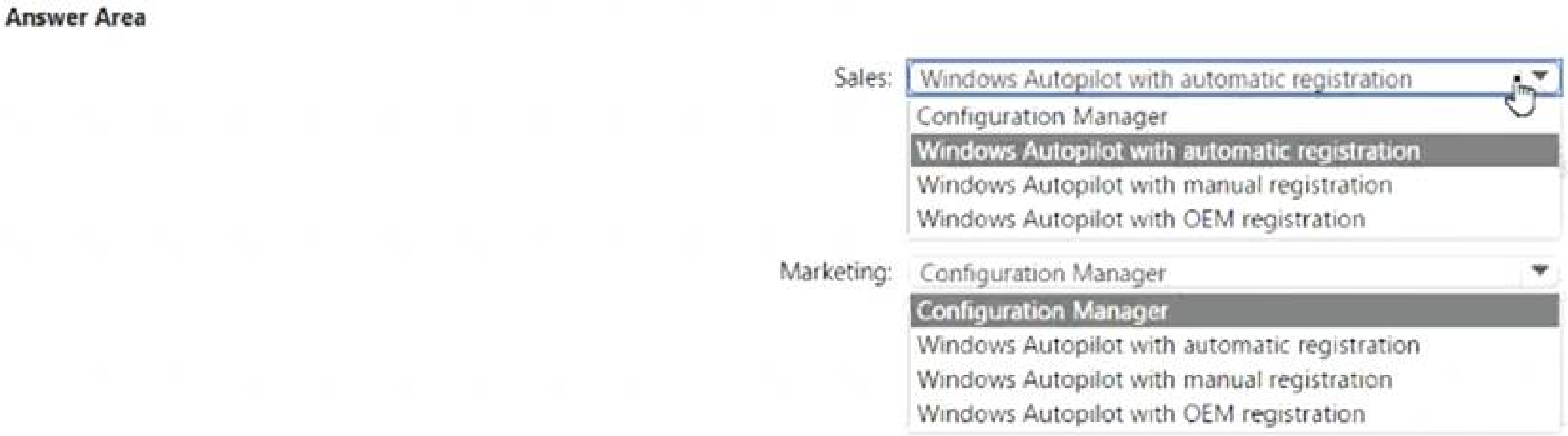
NEW QUESTION 10
- (Exam Topic 4)
You have a Windows 10 device named Device! that is joined to Active Directory and enrolled in Microsoft Intune.
Device1 is managed by using Group Policy and Intune.
You need to ensure that the Intune settings override the Group Policy settings. What should you configure?

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 10
- (Exam Topic 4)
Your network contains an on-premises Active Directory Domain Services {AD DS) domain that syncs with an Azure AD tenant by using Azure AD Connect.
You use Microsoft Intune and Configuration Manager to manage devices.
You need to recommend a deployment plan for new Windows 11 devices. The solution must meet the following requirements:
• Devices for the marketing department must be joined to the AD DS domain only. The IT department will install complex applications on the devices at build time, before giving the devices to the marketing department users.
• Devices for The sales department must be Azure AD joined. The devices will be shipped directly from the manufacturer to The homes of the sales department users.
• Administrative effort must be minimized.
Which deployment method should you recommend for each department? To answer, select the appropriate options in the answer area. NOTE: Each correct selection is worth one point.


Answer Area

Sales: Windows Autopilot with automatic registration

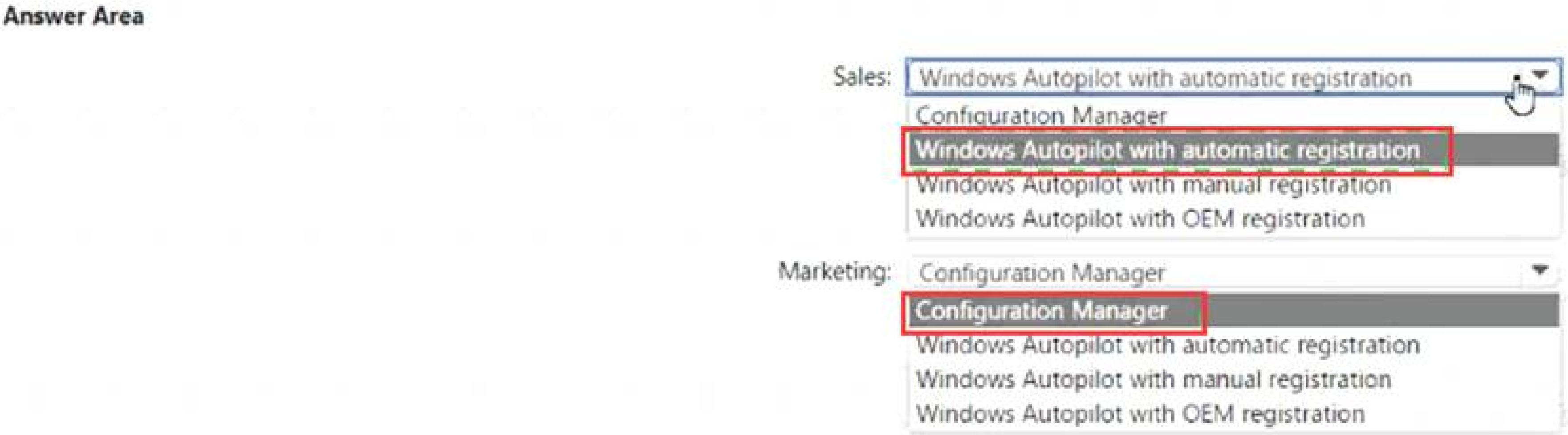
Marketing: Configuration Manager

Configuration Manager
Windows Autopilot with automatic registration
Windows Autopilot with manual registration
Windows Autopilot with OEM registration
Configuration Manager
Windows Autopilot with automatic registration
Windows Autopilot with manual registration
Windows Autopilot with OEM registration

A. Mastered
B. Not Mastered

Answer: A

Explanation:

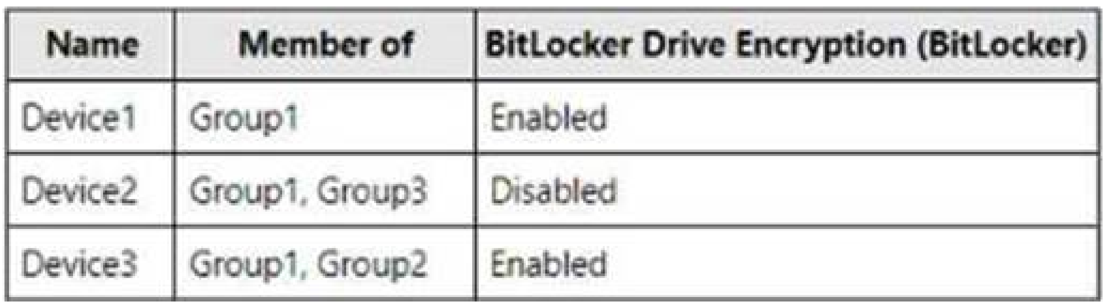

Answer Area

Sales: Windows Autopilot with automatic registration

Marketing: Configuration Manager

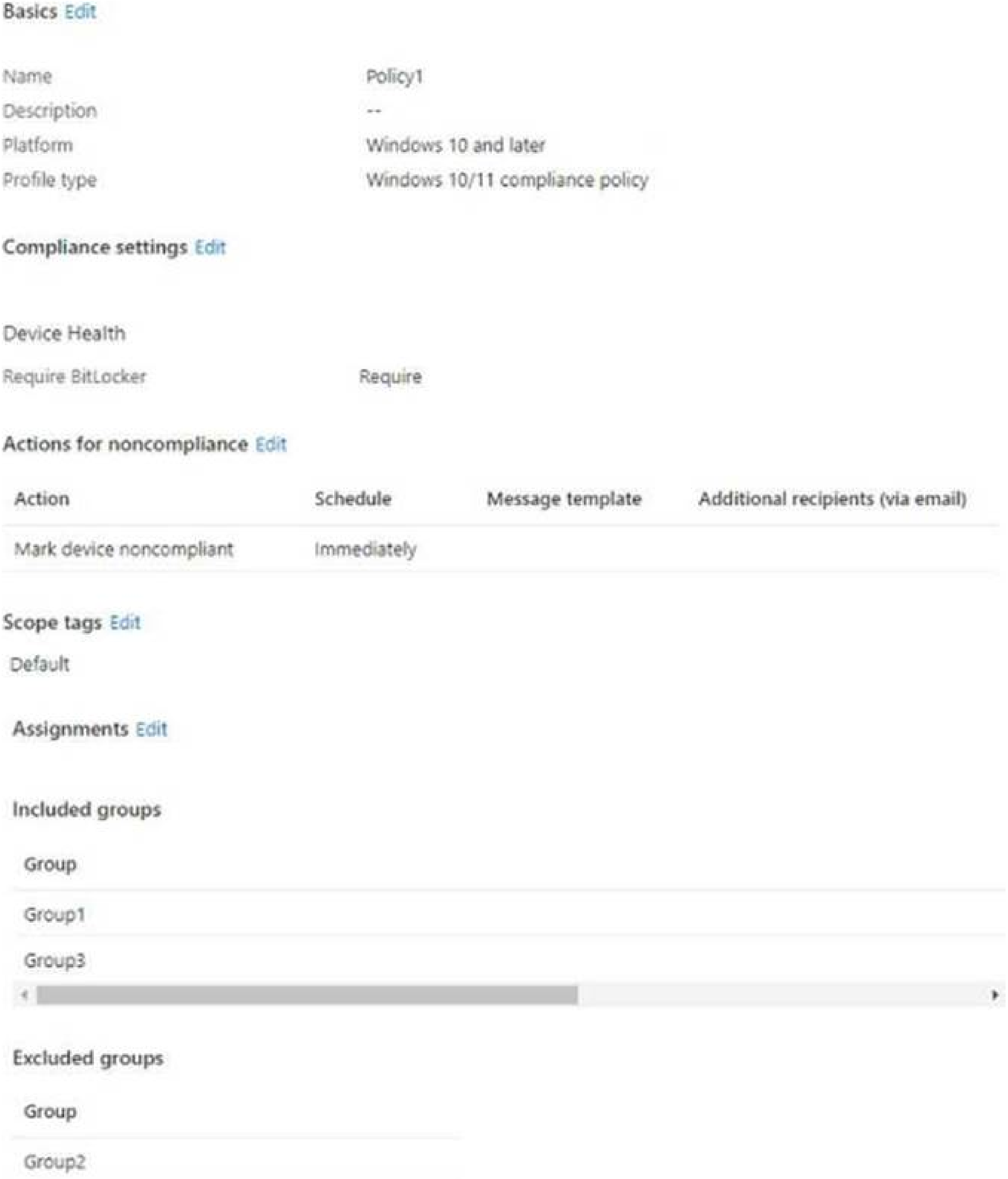
Configuration Manager
Windows Autopilot with automatic registration
Windows Autopilot with manual registration
Windows Autopilot with OEM registration
Configuration Manager
Windows Autopilot with automatic registration
Windows Autopilot with manual registration
Windows Autopilot with OEM registration

NEW QUESTION 15
- (Exam Topic 4)
You have a Microsoft 365 E5 subscription that uses Microsoft Intune. You have the Windows 11 devices shown in the following table.



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

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



Basics Edit

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

Compliance settings Edit

Device Health

Require BitLocker	Require

Actions for noncompliance Edit

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

Scope tags Edit

Default

Assignments Edit

Included groups

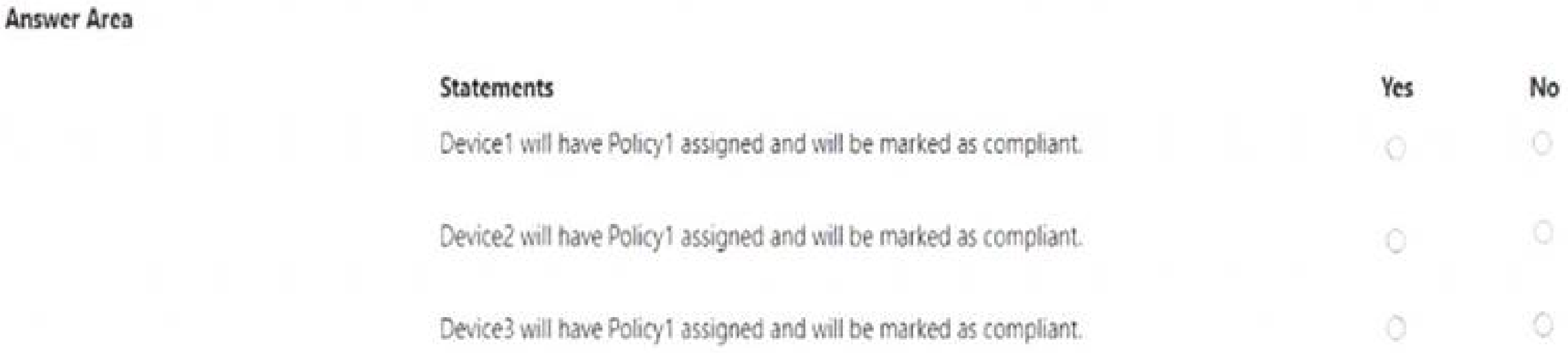
Group
Group1
Group3

Excluded groups

Group
Group2

For each of the following statements, select Yes if the statement is true. Otherwise, select No.

NOTE: Each correct selection is worth one point.



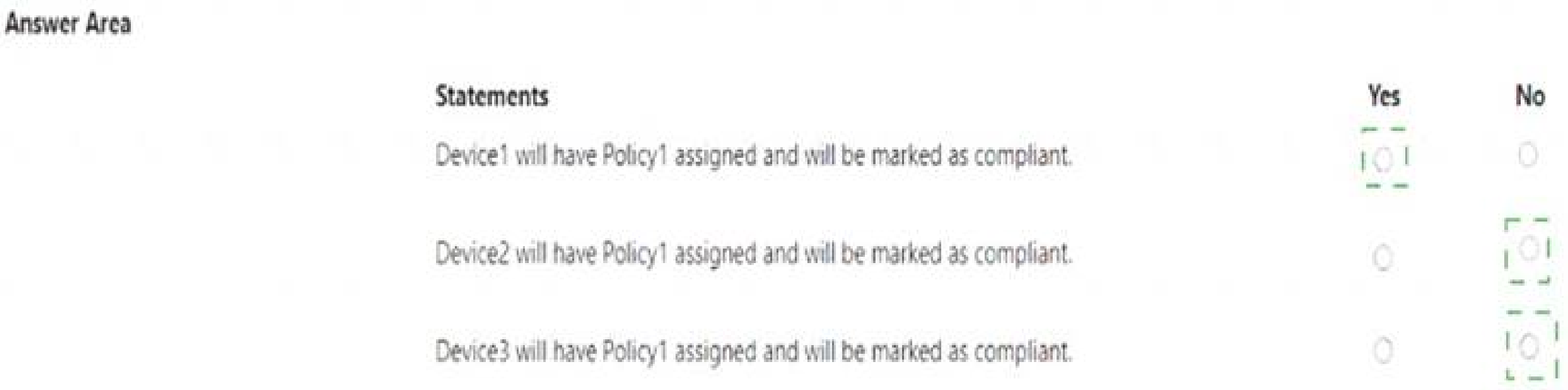
Answer Area

Statements	Yes	No
Device1 will have Policy1 assigned and will be marked as compliant.	○	○
Device2 will have Policy1 assigned and will be marked as compliant.	○	○
Device3 will have Policy1 assigned and will be marked as compliant.	○	○

A. Mastered
B. Not Mastered

Answer: A

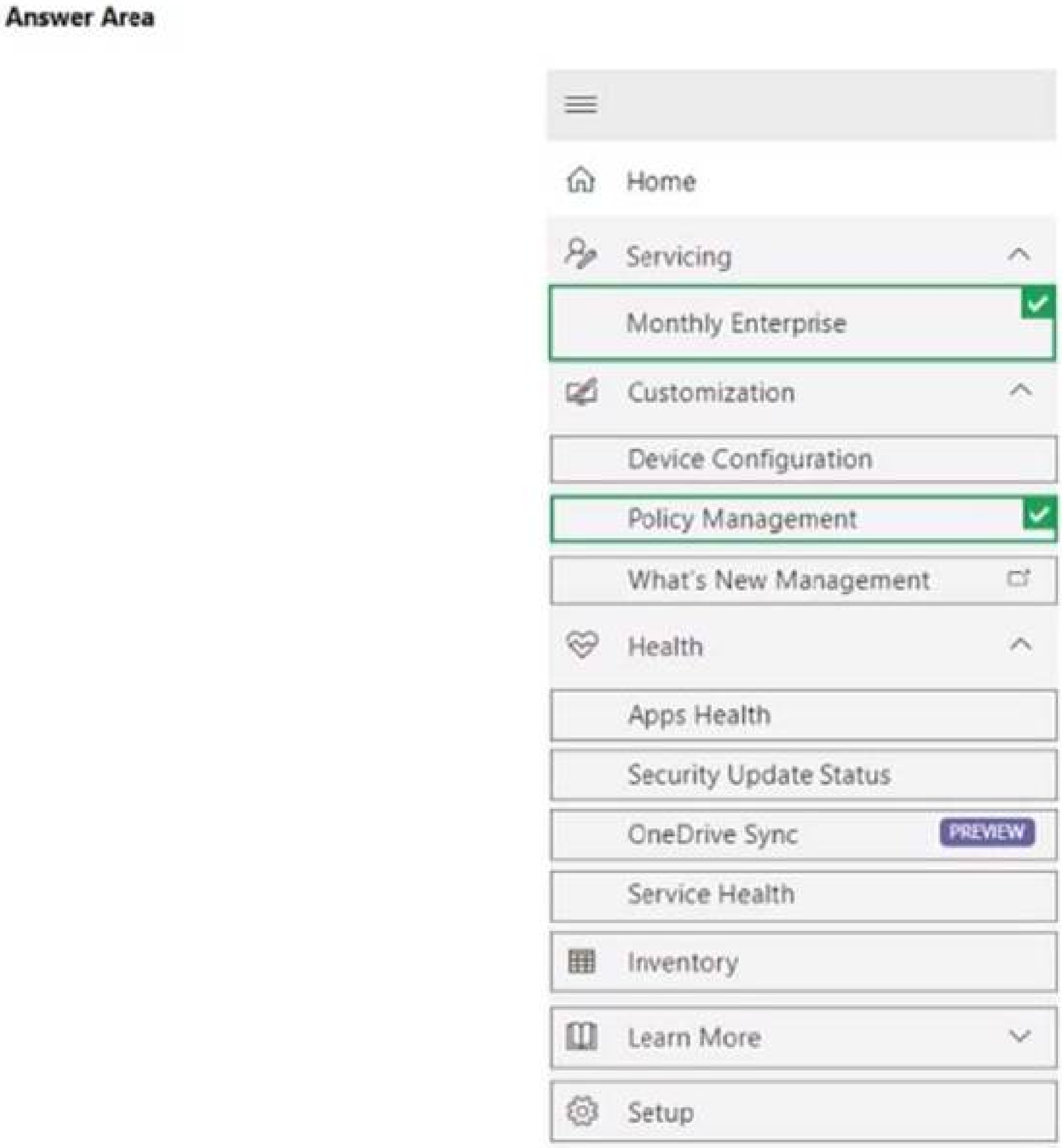
Explanation:



Answer Area

Statements	Yes	No
Device1 will have Policy1 assigned and will be marked as compliant.	[✓ ○]	○
Device2 will have Policy1 assigned and will be marked as compliant.	○	[✓ ○]
Device3 will have Policy1 assigned and will be marked as compliant.	○	[✓ ○]

NEW QUESTION 20
- (Exam Topic 4)
You have a Microsoft 365 subscription.
All users have Microsoft 365 apps deployed.
You need to configure Microsoft 365 apps to meet the following requirements:
• Enable the automatic installation of WebView2 Runtime.
• Prevent users from submitting feedback.
Which two settings should you configure in the Microsoft 365 Apps admin center? To answer, select the appropriate settings in the answer area.
NOTE: Each correct selection is worth one point.



Answer Area

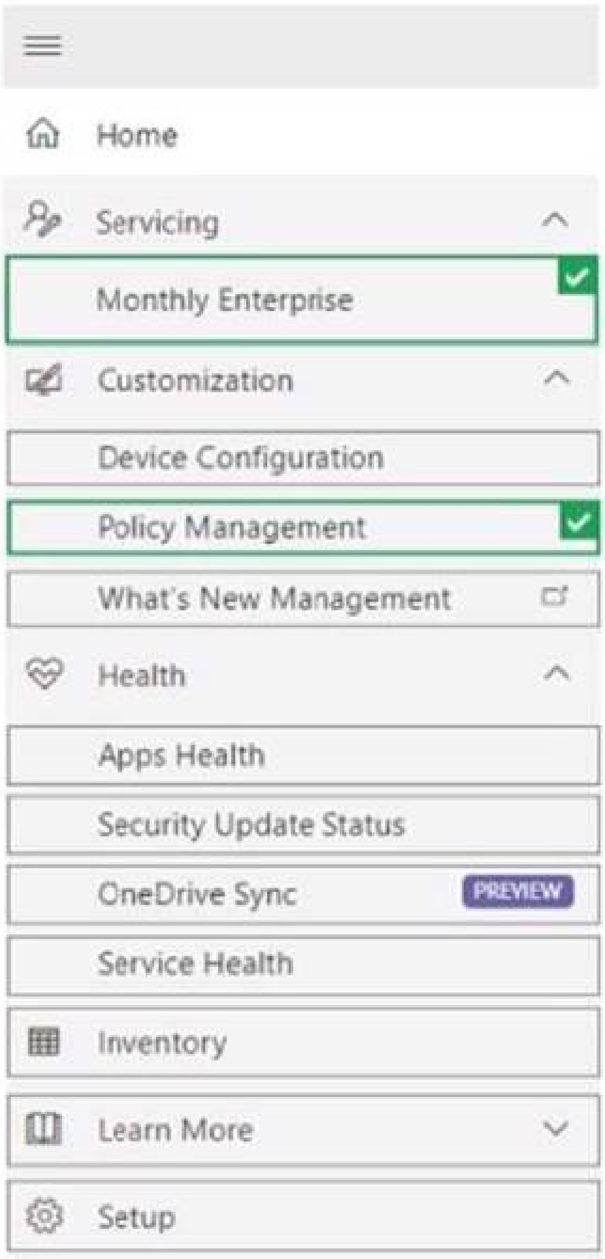
- Home
- Servicing
  - Monthly Enterprise ✓
- Customization
  - Device Configuration
  - Policy Management ✓
  - What's New Management
- Health
  - Apps Health
  - Security Update Status
  - OneDrive Sync PREVIEW
  - Service Health
- Inventory
- Learn More
- Setup

A. Mastered
B. Not Mastered

Answer: A

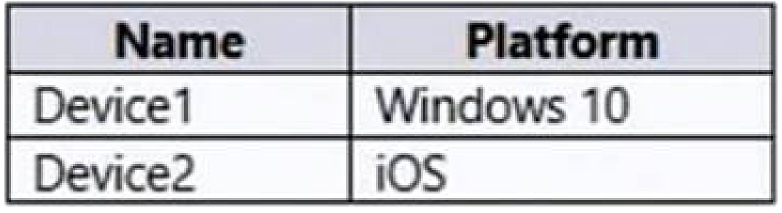
Explanation:

Answer Area



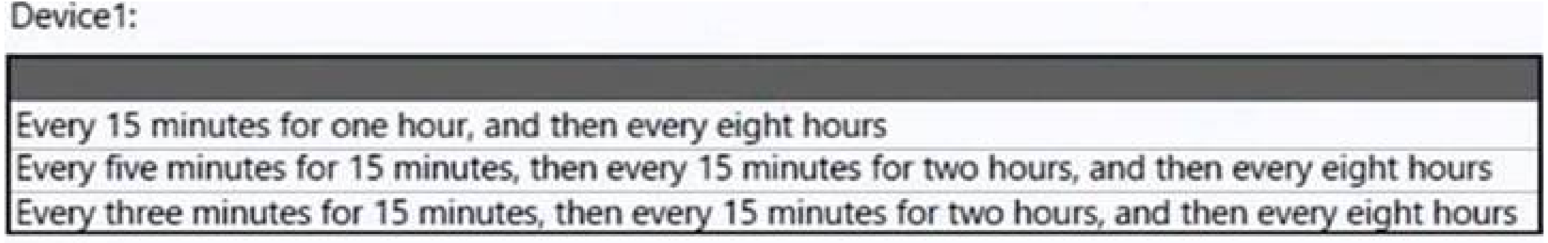
- Home
- Servicing
  - Monthly Enterprise ✓
- Customization
  - Device Configuration
  - Policy Management ✓
  - What's New Management
- Health
  - Apps Health
  - Security Update Status
  - OneDrive Sync PREVIEW
  - Service Health
- Inventory
- Learn More
- Setup

NEW QUESTION 21
- (Exam Topic 4)
You have a Microsoft 365 subscription that contains the devices shown in the following table.



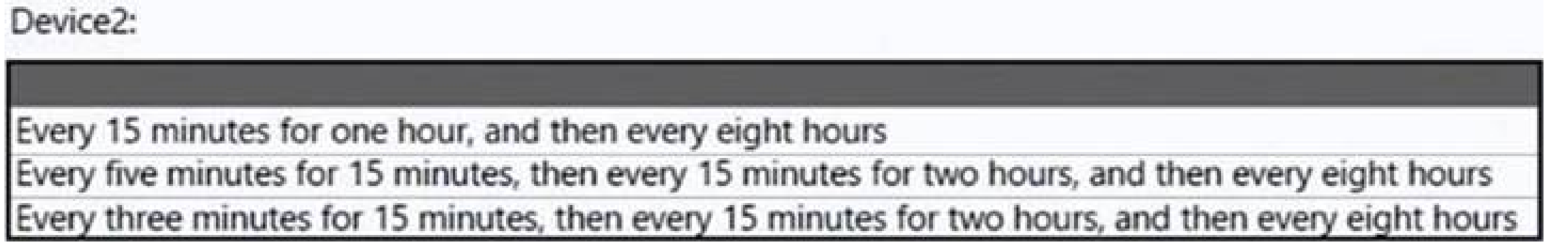
Name	Platform
Device1	Windows 10
Device2	iOS

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



Device1:

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



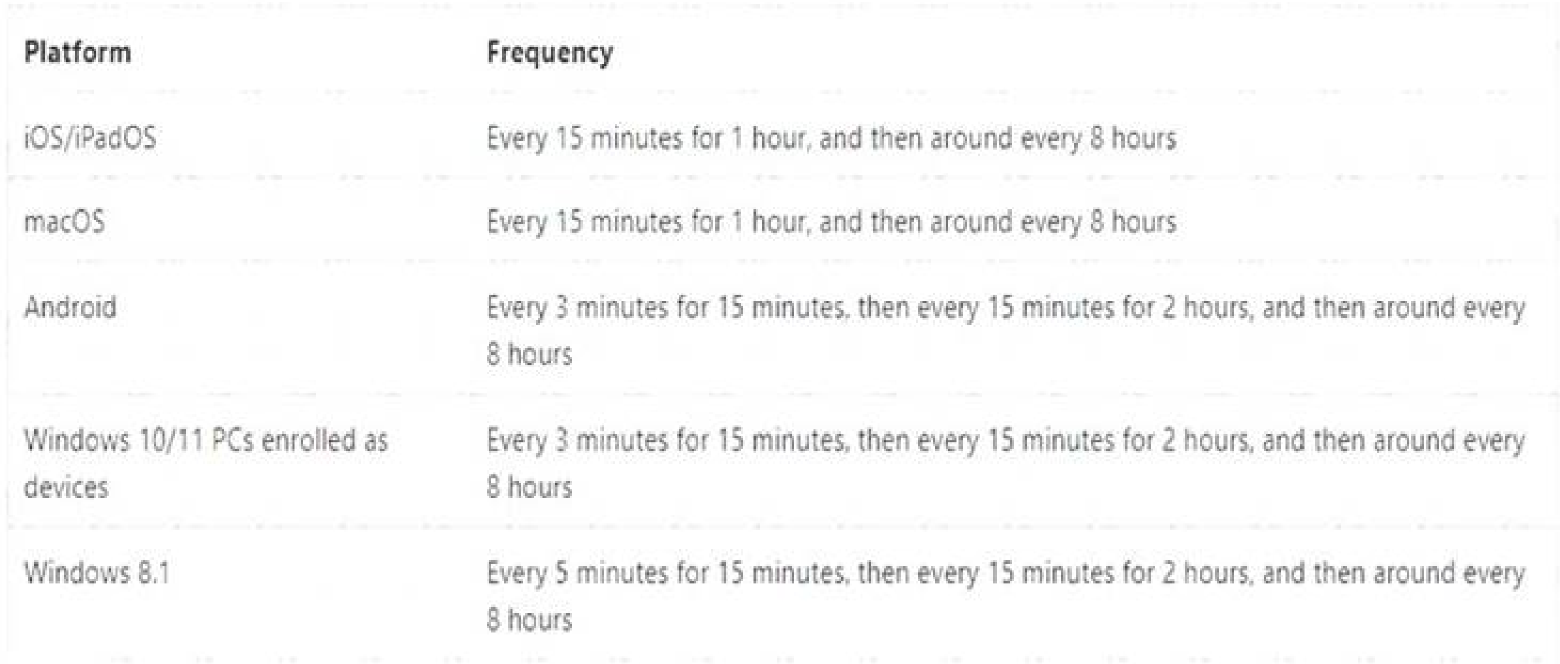
Device2:

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

A. Mastered
B. Not Mastered

Answer: A

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



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

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

NEW QUESTION 25
- (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

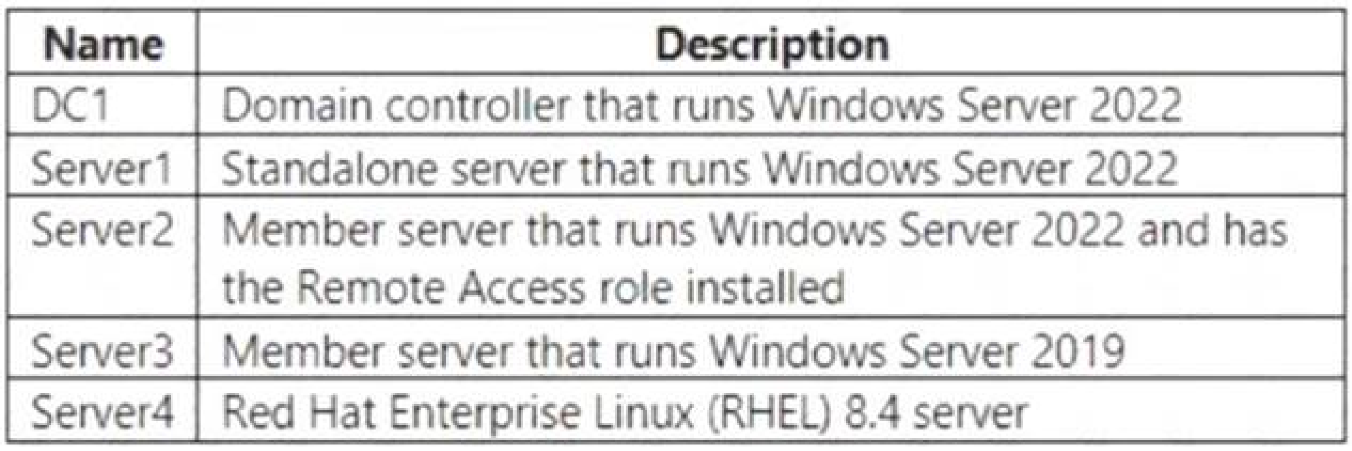
Explanation:
To ensure that Profile1 applies to Device1 only, you need to modify the Applicability Rules in Profile1. You can use applicability rules to filter which devices receive a profile based on criteria such as device model, manufacturer, or operating system version. You can create an applicability 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 30
- (Exam Topic 4)
You have a Microsoft 365 subscription. All devices run Windows 10.
You need to prevent users from enrolling the devices in the Windows Insider Program.
What two configurations should you perform from the Microsoft Intune admin center? Each correct answer is a complete solution.
NOTE: Each correct selection is worth one point.

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

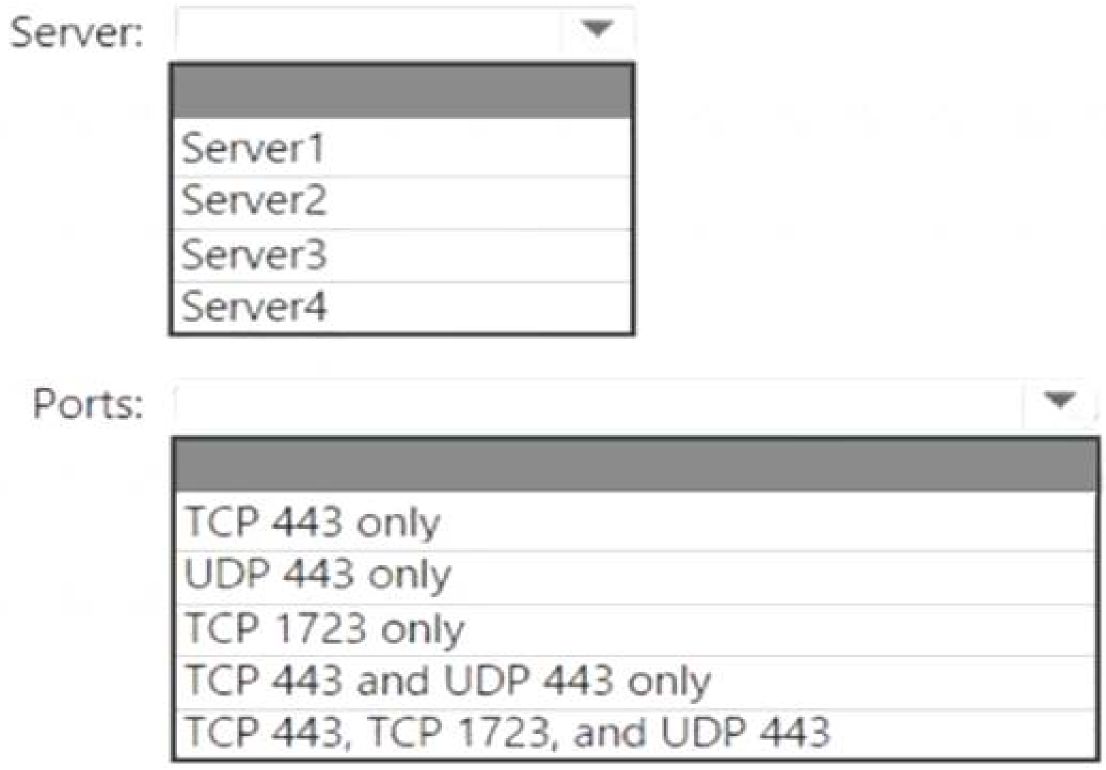
Answer: AE

NEW QUESTION 31
- (Exam Topic 4)
You have the on-premises servers shown in the following table.



Name	Description
DC1	Domain controller that runs Windows Server 2022
Server1	Standalone server that runs Windows Server 2022
Server2	Member server that runs Windows Server 2022 and has the Remote Access role installed
Server3	Member server that runs Windows Server 2019
Server4	Red Hat Enterprise Linux (RHEL) 8.4 server

You have a Microsoft 365 E5 subscription that contains Android and iOS devices. All the devices are managed by using Microsoft Intune.
You need to implement Microsoft Tunnel for Intune. The solution must minimize the number of open firewall ports.
To which server can you deploy a Tunnel Gateway server, and which inbound ports should be allowed on the server to support Microsoft Tunnel connections? To answer, select the appropriate options in the answer area.
NOTE: Each correct selection is worth one point.



Server:
- Server1
- Server2
- Server3
- Server4

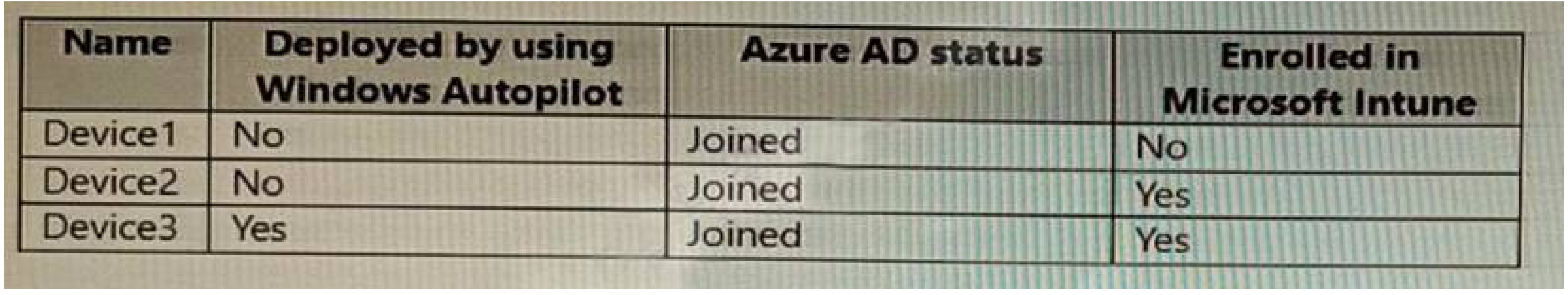
Ports:
- TCP 443 only
- UDP 443 only
- TCP 1723 only
- TCP 443 and UDP 443 only
- TCP 443, TCP 1723, and UDP 443

A. Mastered
B. Not Mastered

Answer: A

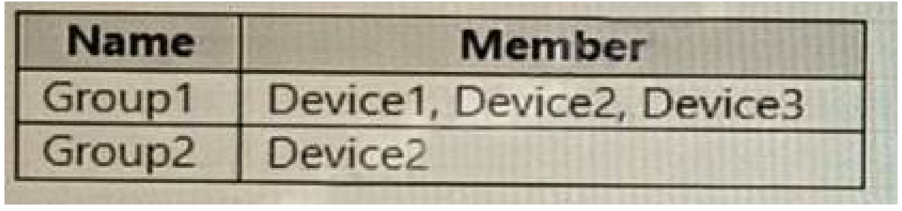
Explanation:
Box 1: Server4
Microsoft Tunnel is a VPN gateway solution for Microsoft Intune that runs in a container on Linux and allows access to on-premises resources from iOS/iPadOS and Android Enterprise devices using modern authentication and Conditional Access.
Box 2: TCP 443 and UDP 443 only
Some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

NEW QUESTION 33
- (Exam Topic 4)
You have an Azure AD tenant named contoso.com that contains the devices shown in the following table.



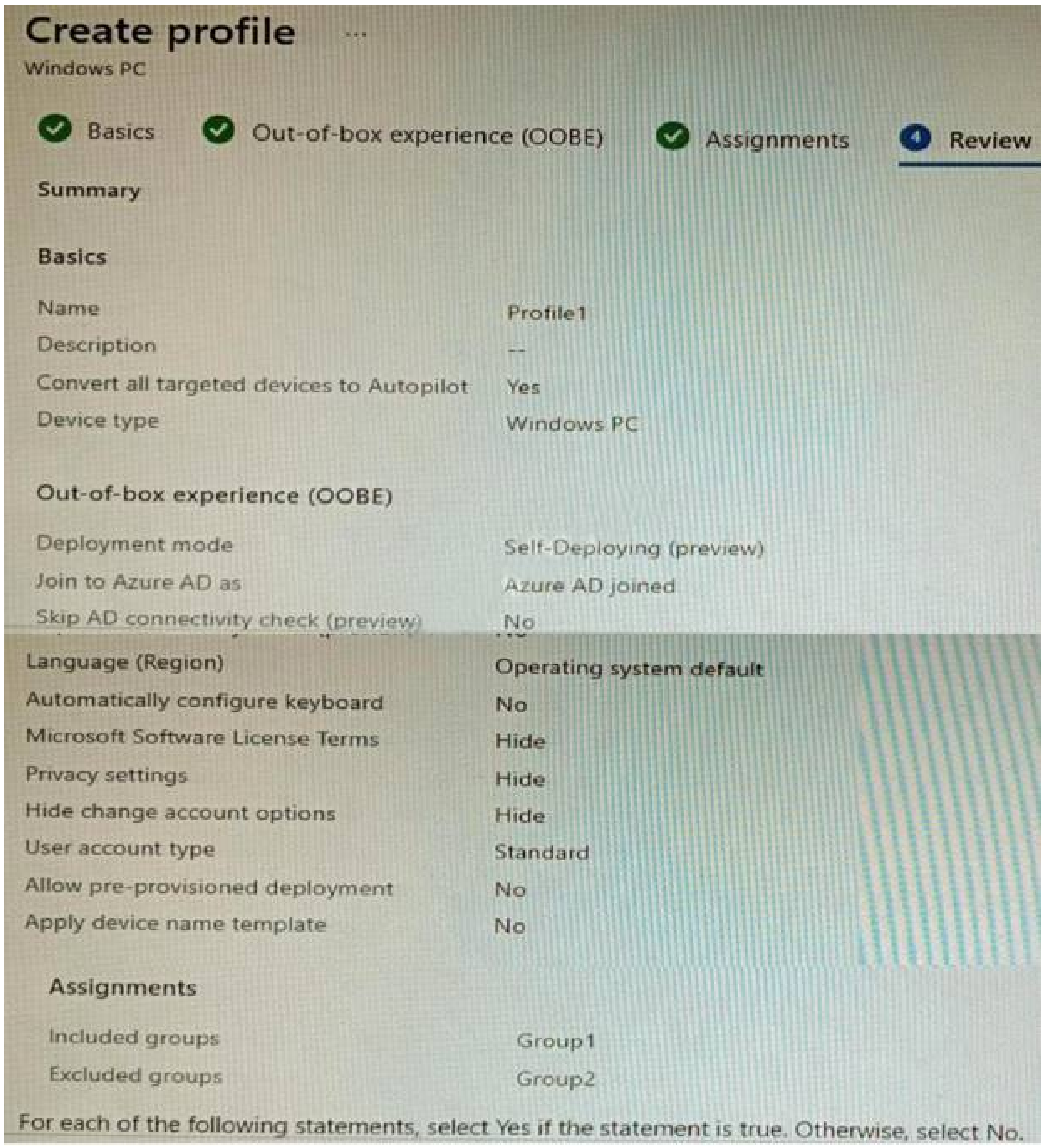
Name	Deployed by using Windows Autopilot	Azure AD status	Enrolled in Microsoft Intune
Device1	No	Joined	No
Device2	No	Joined	Yes
Device3	Yes	Joined	Yes

The tenant contains the Azure AD groups shown in the following table.



Name	Member
Group1	Device1, Device2, Device3
Group2	Device2

You add an Autopilot deployment profile as shown in the following exhibit.



Create profile ...

Windows PC

✓ Basics ✓ Out-of-box experience (OOBE) ✓ Assignments 4 Review

Summary

Basics

Name	Profile1
Description	--
Convert all targeted devices to Autopilot	Yes
Device type	Windows PC

Out-of-box experience (OOBE)

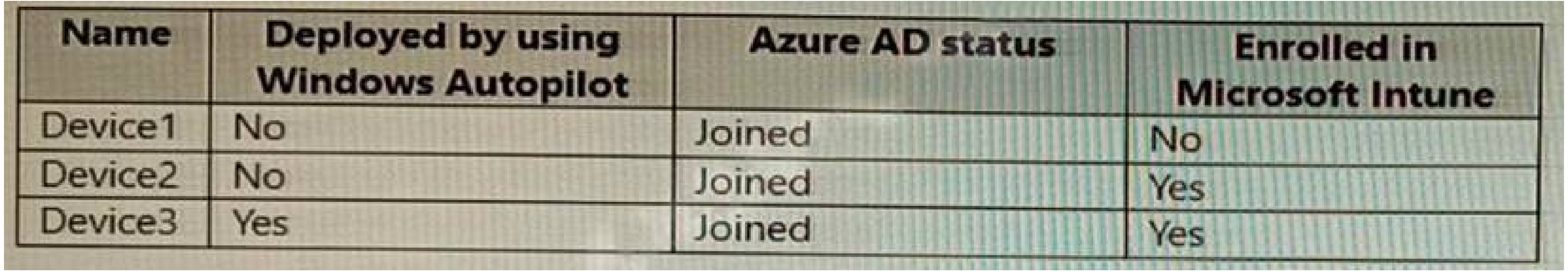
Deployment mode	Self-Deploying (preview)
Join to Azure AD as	Azure AD joined
Skip AD connectivity check (preview)	No
Language (Region)	Operating system default
Automatically configure keyboard	No
Microsoft Software License Terms	Hide
Privacy settings	Hide
Hide change account options	Hide
User account type	Standard
Allow pre-provisioned deployment	No
Apply device name template	No

Assignments

Included groups	Group1
Excluded groups	Group2

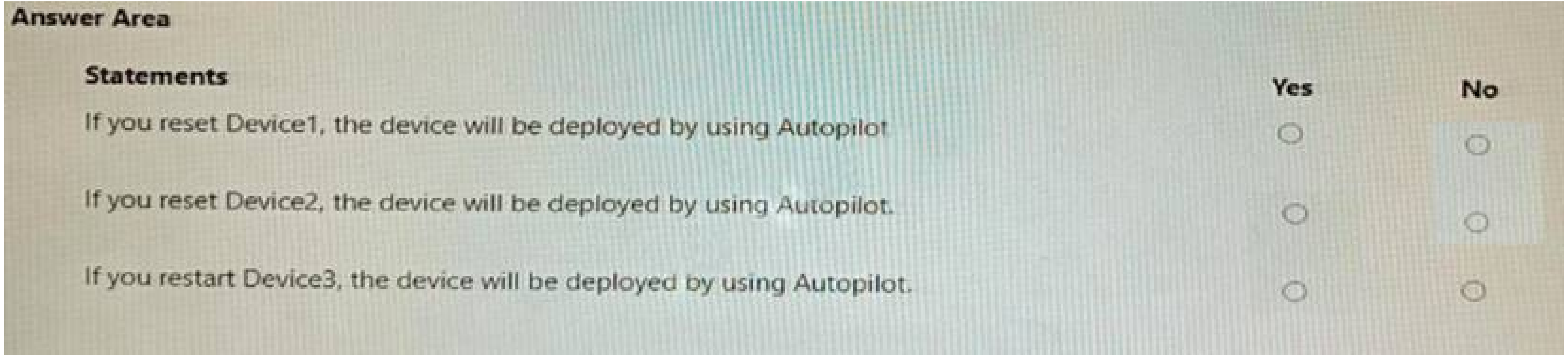
For each of the following statements, select Yes if the statement is true. Otherwise, select No.

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



Name	Deployed by using Windows Autopilot	Azure AD status	Enrolled in Microsoft Intune
Device1	No	Joined	No
Device2	No	Joined	Yes
Device3	Yes	Joined	Yes

The tenant contains the Azure AD groups shown in the following table.



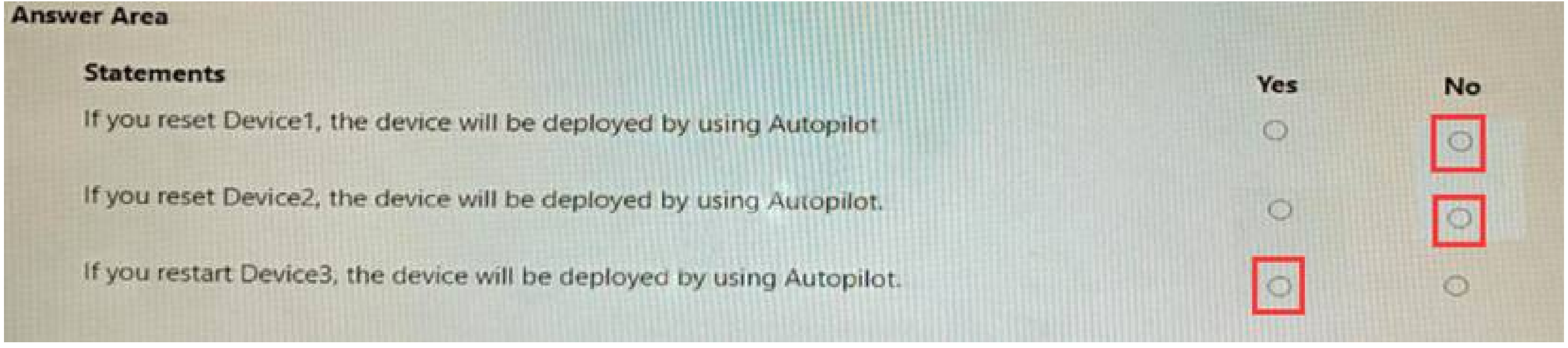
Answer Area

Statements	Yes	No
If you reset Device1, the device will be deployed by using Autopilot	○	○
If you reset Device2, the device will be deployed by using Autopilot.	○	○
If you restart Device3, the device will be deployed by using Autopilot.	○	○

A. Mastered
B. Not Mastered

Answer: A

Explanation:



Answer Area

Statements	Yes	No
If you reset Device1, the device will be deployed by using Autopilot	○	[✓ ○]
If you reset Device2, the device will be deployed by using Autopilot.	○	[✓ ○]
If you restart Device3, the device will be deployed by using Autopilot.	[✓ ○]	○

NEW QUESTION 35
- (Exam Topic 4)
You are creating a device configuration profile in Microsoft Intu You need to configure specific OMA-URI settings in the profile. Which profile type template should you use?

A. Device restrictions (Windows 10 Team)
B. Identity protection
C. Custom
D. Device restrictions

Answer: C

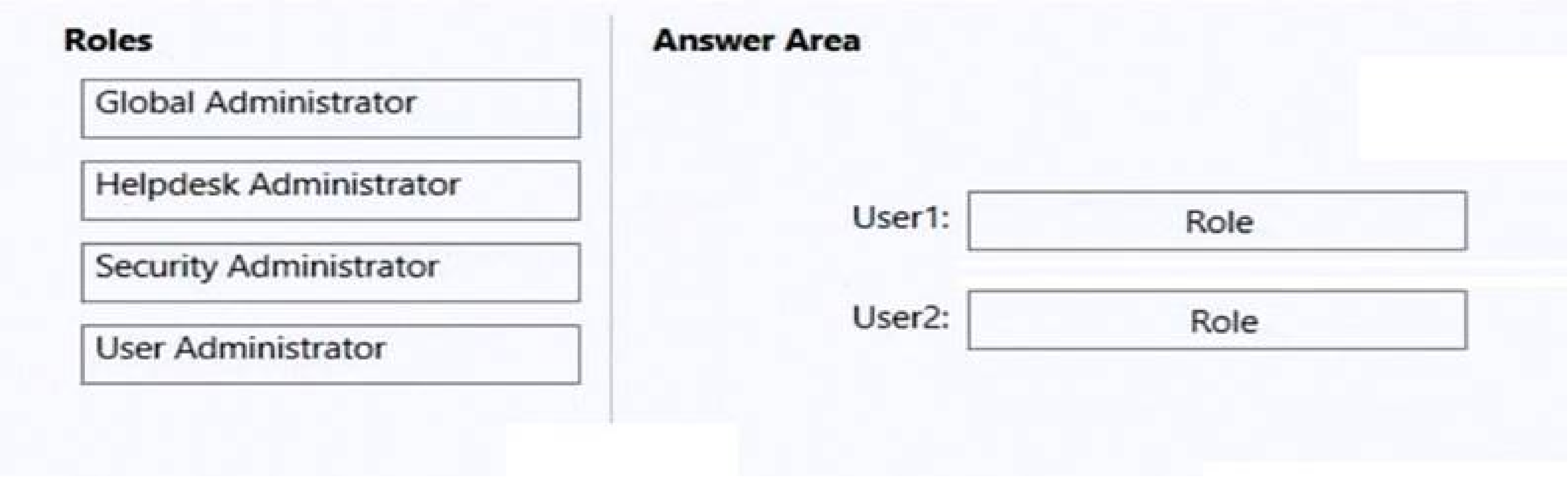
NEW QUESTION 38
- (Exam Topic 4)
You have a Microsoft 365 E5 subscription that contains 1,000 Windows 11 devices. All the devices are enrolled in Microsoft Intune.
You plan to integrate Intune with Microsoft Defender for Endpoint.
You need to establish a service-to-service connection between Intune and 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 40
- (Exam Topic 4)
You have a Microsoft 365 subscription that contains two users named User1 and User2. You need to ensure that the users can perform the following tasks:
• User1 must be able to create groups and manage users.
• User2 must be able to reset passwords for no administrative users. The solution must use the principle of least privilege.
Which role should you assign to each user? To answer, drag the appropriate roles to the correct users. Each role 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.



Roles

Global Administrator
Helpdesk Administrator
Security Administrator
User Administrator

Answer Area

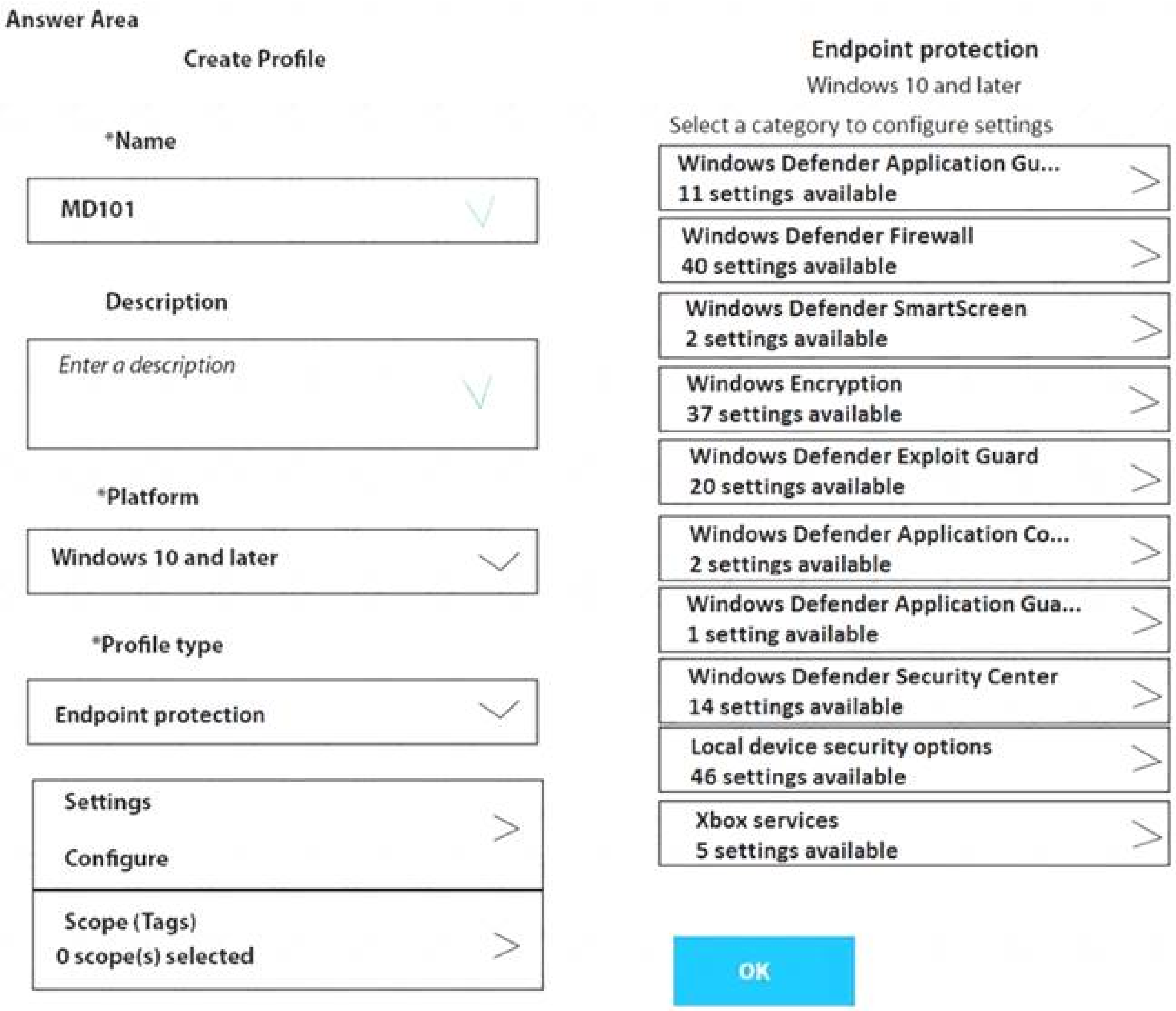
User1: Role
User2: Role

A. Mastered
B. Not Mastered

Answer: A

Explanation:
Microsoft 365 or Office 365 subscription comes with a set of admin roles that you can assign to users in your organization using the Microsoft 365 admin center. Each admin role maps to common business functions and gives people in your organization permissions to do specific tasks in the admin centers1.
To ensure that User1 can create groups and manage users, you should assign the User Administrator role to User1. This role allows User1 to create and manage all aspects of users and groups, including resetting passwords for non-administrative users1.
To ensure that User2 can reset passwords for non-administrative users, you should assign the Helpdesk Administrator role to User2. This role allows User2 to reset passwords, manage service requests, and monito service health for non-administrative users1.

NEW QUESTION 45
- (Exam Topic 4)
You have 200 computers that run Windows 10. The computers are joined to Microsoft Azure Active Directory (Azure AD) and enrolled in Microsoft Intune.
You need to configure an Intune device configuration profile to meet the following requirements:
➢ Prevent Microsoft Office applications from launching child processes.
➢ Block users from transferring files over FTP.
Which two settings should you configure in Endpoint protection? To answer, select the appropriate settings in the answer area.
NOTE: Each correct selection is worth one point.



Answer Area

Create Profile

*Name

MD101

Description

Enter a description

*Platform

Windows 10 and later

*Profile type

Endpoint protection

Settings
Configure

Scope (Tags)
0 scope(s) selected

Endpoint protection
Windows 10 and later

Select a category to configure settings

Windows Defender Application Gu...
11 settings available

Windows Defender Firewall
40 settings available

Windows Defender SmartScreen
2 settings available

Windows Encryption
37 settings available

Windows Defender Exploit Guard
20 settings available

Windows Defender Application Co...
2 settings available

Windows Defender Application Gua...
1 setting available

Windows Defender Security Center
14 settings available

Local device security options
46 settings available

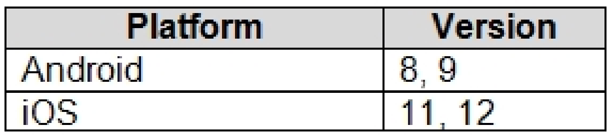
Xbox services
5 settings available

A. Mastered
B. Not Mastered

Answer: A

Explanation:
A screenshot of a computer Description automatically generated
References:
https://docs.microsoft.com/en-us/intune/endpoint-protection-windows-10

NEW QUESTION 47
- (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.

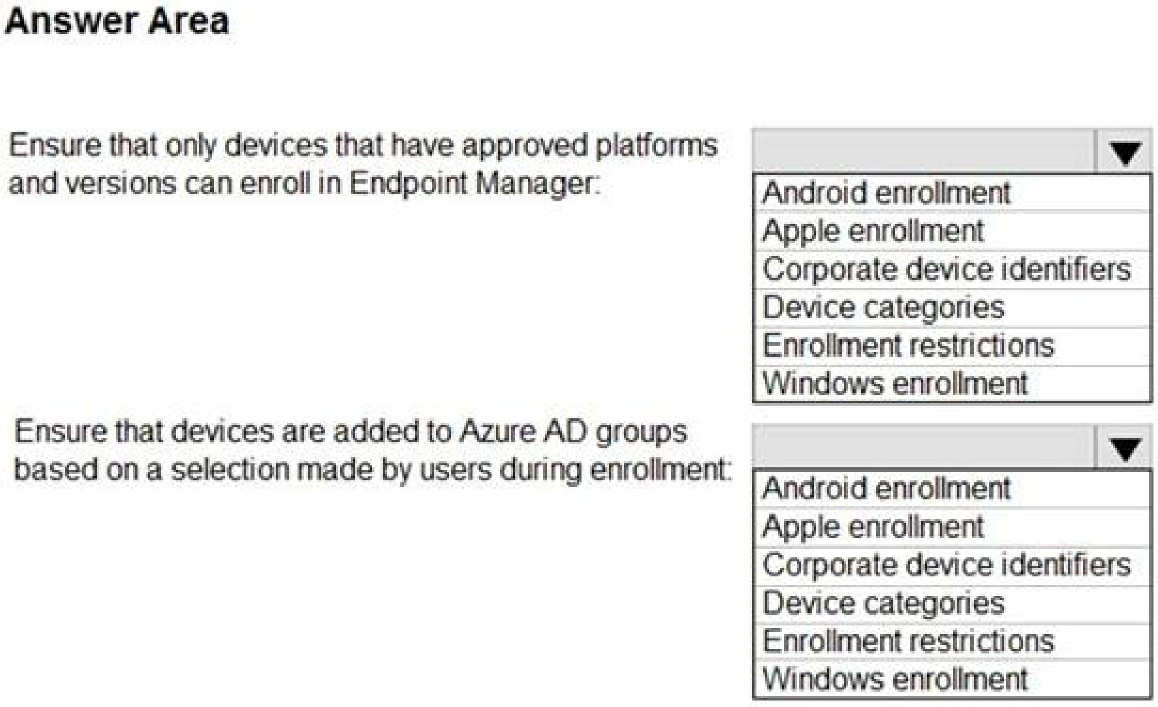


Platform	Version
Android	8, 9
iOS	11, 12

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

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

Answer: CE

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

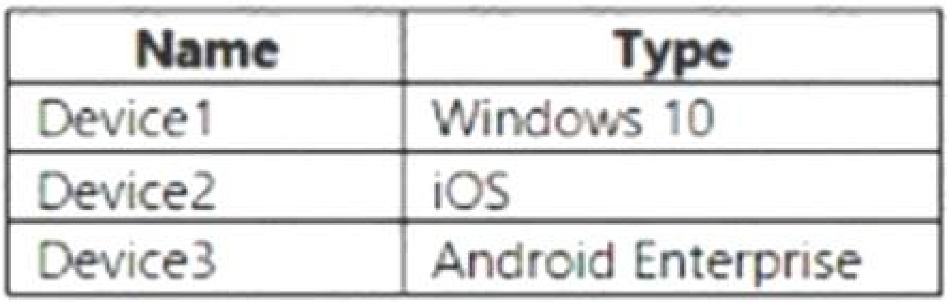
- Enroll the devices in Microsoft Intune by using Apple Business Manager. Apple Business Manager is a service that allows you to enroll and manage iOS/iPadOS devices in bulk. You can use Apple Business Manager to assign devices to Microsoft Intune and enroll them as supervised devices. Supervised devices are devices that have more management features and restrictions than unsupervised devices. You can also use Apple Business Manager to create device groups and assign roles and permissions12.
- Create a device configuration profile. A device configuration profile is a policy that you can create and assign in Microsoft Intune to configure settings on your devices. You can use a device configuration profile to manage software updates for iOS/iPadOS supervised devices. You can choose to deploy the latest update or an older update, specify a schedule for the update installation, and delay the visibility of software updates on the devices34.

The other options are not correct for this scenario because:

- Enrolling the devices in Microsoft Intune by using the Intune Company Portal is not suitable for unmanaged devices. The Intune Company Portal is an app that users can download and install on their personal or corporate-owned devices to enroll them in Microsoft Intune. However, this method requires user interaction and consent, and does not enroll the devices as supervised devices5.
- Creating a compliance policy is not necessary for this scenario. A compliance policy is a policy that you can create and assign in Microsoft Intune to evaluate and enforce compliance settings on your devices. You can use a compliance policy to check if the devices meet certain requirements, such as minimum OS version, encryption, or password settings. However, a compliance policy does not deploy or manage software updates on the devices6.
- Creating an iOS app provisioning profile is not relevant for this scenario. An iOS app provisioning profile is a file that contains information about the app and its distribution method. You can use an iOS app provisioning profile to deploy custom or line-of-business apps to your iOS/iPadOS devices by using Microsoft Intune. However, an iOS app provisioning profile does not affect the software updates on the devices7.

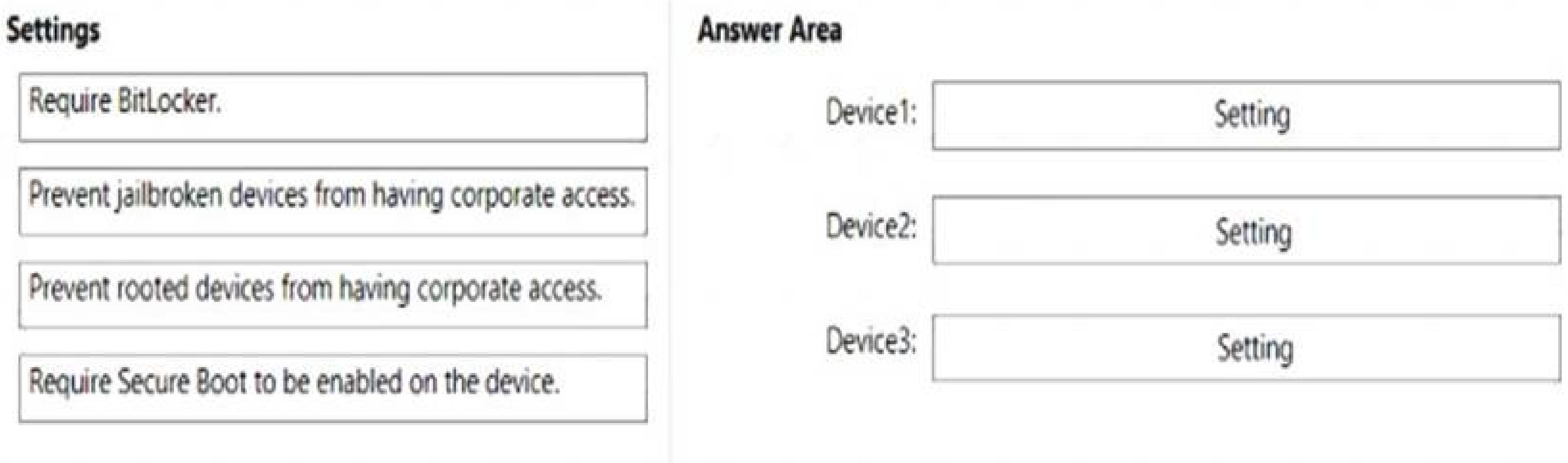
References: What is Apple Business Manager?, Enroll iOS/iPadOS devices in Intune, Manage iOS/iPadOS software update policies in Intune, Software updates planning guide and scenarios for supervised iOS/iPadOS devices in Microsoft Intune, Enroll your personal device in Intune, Device compliance policies in Microsoft Intune, Add an iOS app provisioning profile with Microsoft Intune

NEW QUESTION 56
- (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

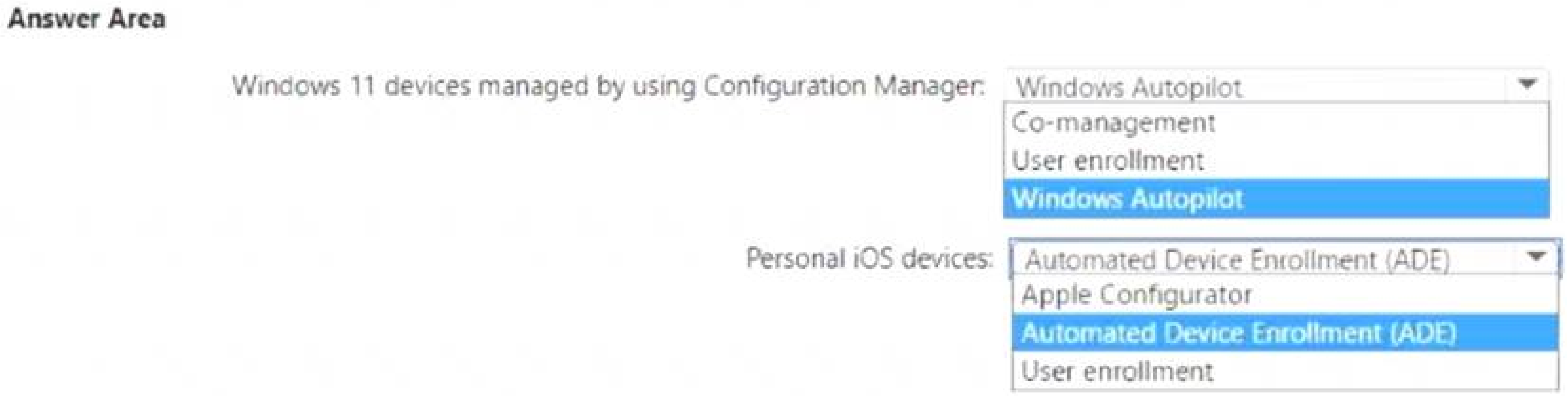
Explanation:
Box 1:
Device Compliance settings for Windows 10/11 in Intune
There are the different compliance settings you can configure on Windows devices in Intune. As part of your mobile device management (MDM) solution, use these settings to require BitLocker, set a minimum and maximum operating 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 58
- (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 61
- (Exam Topic 4)
You have a Microsoft 365 subscription.
You plan to enable Microsoft Intune enrollment for the following types of devices:
• Existing Windows 11 devices managed by using Configuration Manager
• Personal iOS devices
The solution must minimize user disruption.
Which enrollment method should you use for each device type? To answer, select the appropriate options in the answer area.
NOTE: Each correct selection is worth one point.



Answer Area

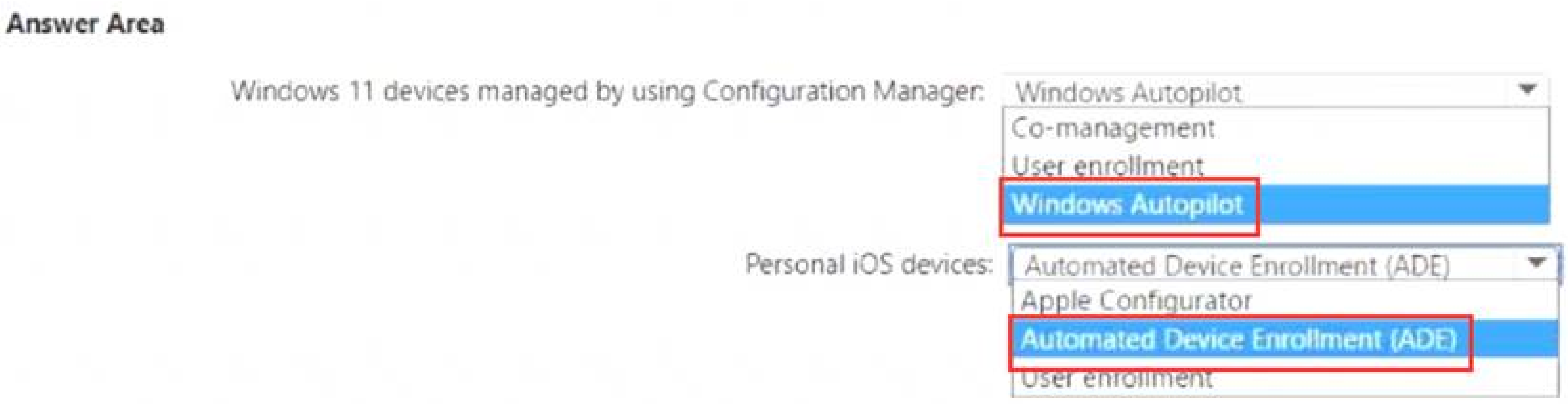
Windows 11 devices managed by using Configuration Manager: Windows Autopilot

Personal iOS devices: Automated Device Enrollment (ADE)

A. Mastered
B. Not Mastered

Answer: A

Explanation:



Answer Area

Windows 11 devices managed by using Configuration Manager: Windows Autopilot

Personal iOS devices: Automated Device Enrollment (ADE)

NEW QUESTION 63
- (Exam Topic 4)
You have a Microsoft 365 subscription that uses Microsoft Intune Suite. You use Microsoft Intune to manage devices.
You use Windows Autopilot to deploy Windows 11 to devices.
A support engineer reports that when a deployment fails, they cannot collect deployment logs from failed device.
You need to ensure that when a deployment fails, the deployment logs can be collected.
What should you configure?

A. the automatic enrollment settings
B. the Windows Autopilot deployment profile
C. the enrollment status page (ESP) profile
D. the device configuration profile

Answer: B

NEW QUESTION 65
- (Exam Topic 4)
Your company uses Microsoft Intune to manage devices.
You need to ensure that only Android devices that use Android work profiles can enroll in intune. Which two configurations should you perform in the device enrollment restrictions? Each correct answer
presents part of the solution.
NOTE Each correct selection is worth one point.

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

Answer: AB

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

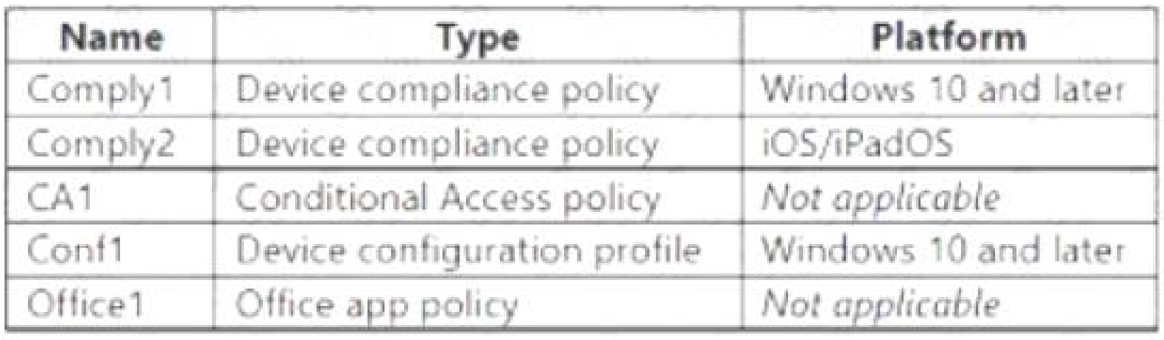
NEW QUESTION 70
- (Exam Topic 4)
You have a Microsoft 365 subscription that uses Microsoft Intune Suite. You use Microsoft Intune to manage devices.
You plan to deploy two apps named App1 and App2 to all Windows devices. App1 must be installed before App2.
From the Intune admin center, you create and 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 75
- (Exam Topic 4)
You have a Microsoft Intune deployment that contains the resources shown in the following table.



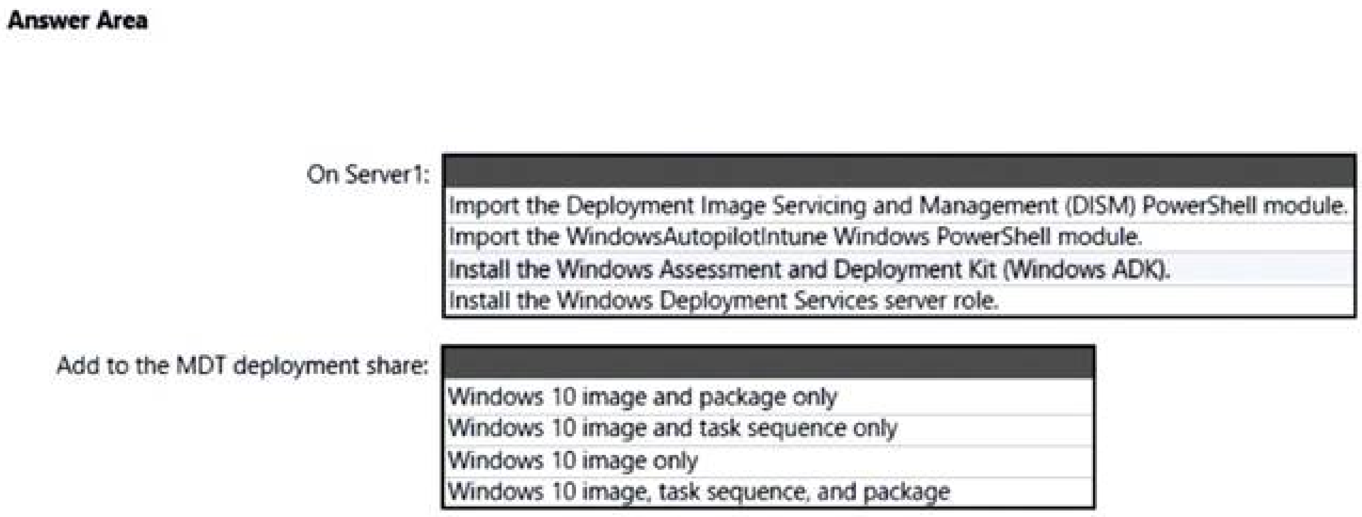
Name	Type	Platform
Comply1	Device compliance policy	Windows 10 and later
Comply2	Device compliance policy	iOS/iPadOS
CA1	Conditional Access policy	*Not applicable*
Conf1	Device configuration profile	Windows 10 and later
Office1	Office app policy	*Not applicable*

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

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

Answer: B

NEW QUESTION 76
- (Exam Topic 4)
You have a server named Server1 and computers that run Windows 8.1. Server1 has the Microsoft Deployment Toolkit (MDT) installed.
You plan to upgrade the Windows 8.1 computers to Windows 10 by using the MDT deployment wizard. You need to create a deployment share on Server1.
What should you do on Server1, and what are the minimum components you should add to the MDT deployment share? To answer, select the appropriate options in the answer area.
NOTE: Each correct selection is worth one point.



Answer Area

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

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

A. Mastered
B. Not Mastered

Answer: A

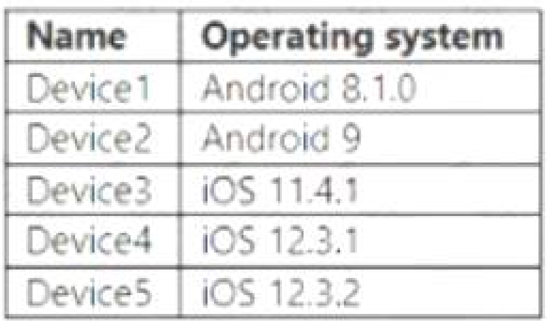
Explanation:
Box 1: Install the Windows Deployment Services role. Install and initialize Windows Deployment Services (WDS) On the server:
Open an elevated Windows PowerShell prompt and enter the following command: Install-WindowsFeature -Name WDS -IncludeManagementTools WDSUTIL /Verbose /Progress /Initialize-Server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

NEW QUESTION 77
- (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 82
- (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

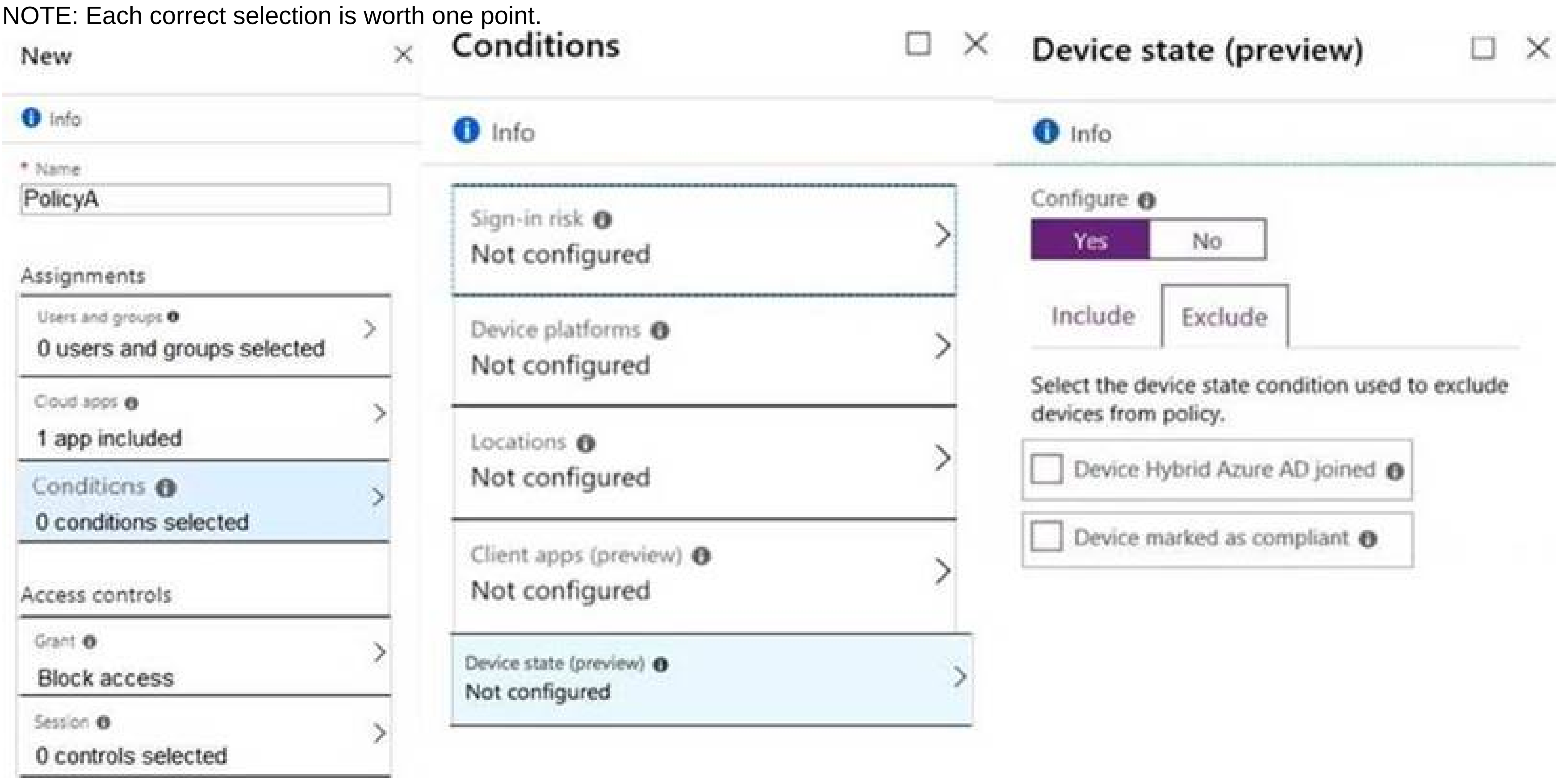
An app named App1 is installed on each device.
What is the minimum number of app configuration policies required to manage Appl ?

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 86
- (Exam Topic 3)
You need a new conditional access policy that has an assignment for Office 365 Exchange Online. You need to configure the policy to meet the technical requirements for Group4.
Which two settings should you configure in the policy? To answer, select the appropriate settings in the answer area.
NOTE: Each correct selection is worth one point.



New

Info

* Name
PolicyA

Assignments

Users and groups
0 users and groups selected

Cloud apps
1 app included

Conditions
0 conditions selected

Access controls

Grant
Block access

Session
0 controls selected

Conditions

Info

Sign-in risk
Not configured

Device platforms
Not configured

Locations
Not configured

Client apps (preview)
Not configured

Device state (preview)
Not configured

Device state (preview)

Info

Configure
Yes | No

Include | Exclude

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

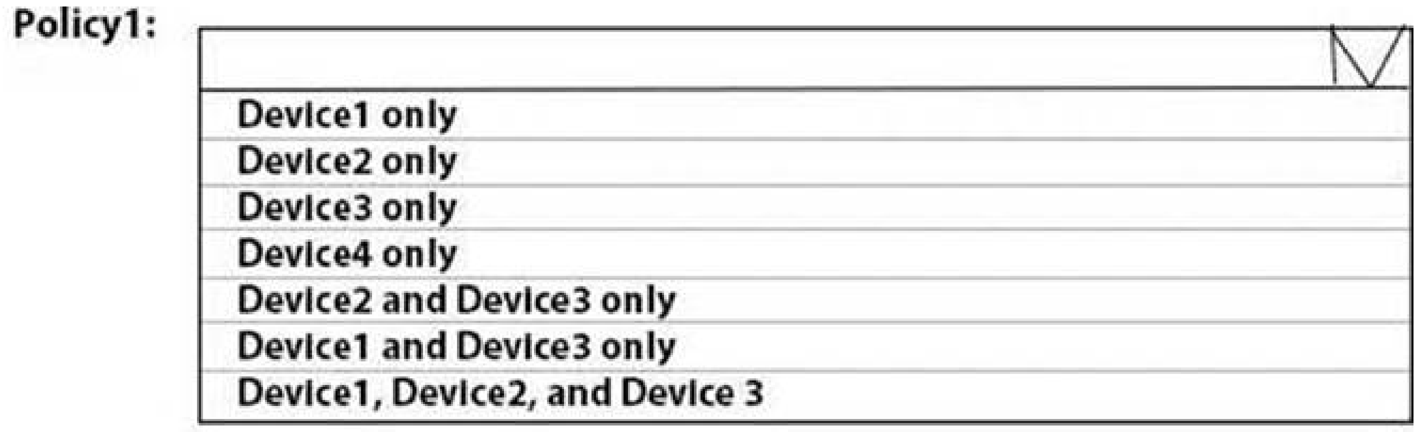
□ Device Hybrid Azure AD joined
□ Device marked as compliant

A. Mastered
B. Not Mastered

Answer: A

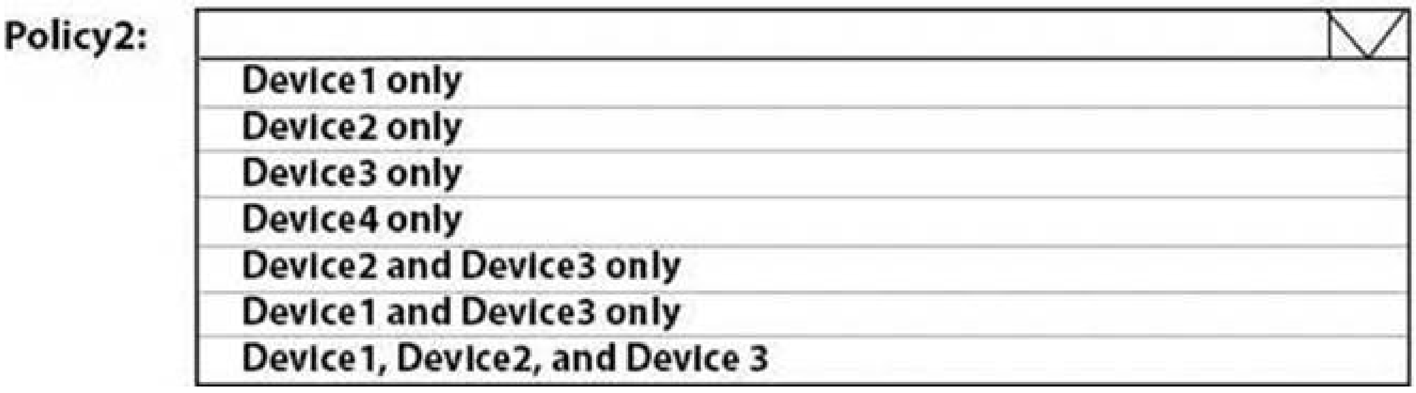
Explanation:
The policy needs to be applied to Group4 so we need to configure Users and Groups. The Access controls are set to Block access
A screenshot of a computer Description automatically generated
We therefore need to exclude compliant devices. From the scenario:
➢ Ensure that the users in a group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

NEW QUESTION 90
- (Exam Topic 3)
To which devices do Policy1 and Policy2 apply? To answer, select the appropriate options in the answer area. NOTE: Each correct selection is worth one point.



Policy1:

- Device1 only
- Device2 only
- Device3 only
- Device4 only
- Device2 and Device3 only
- Device1 and Device3 only
- Device1, Device2, and Device 3



Policy2:

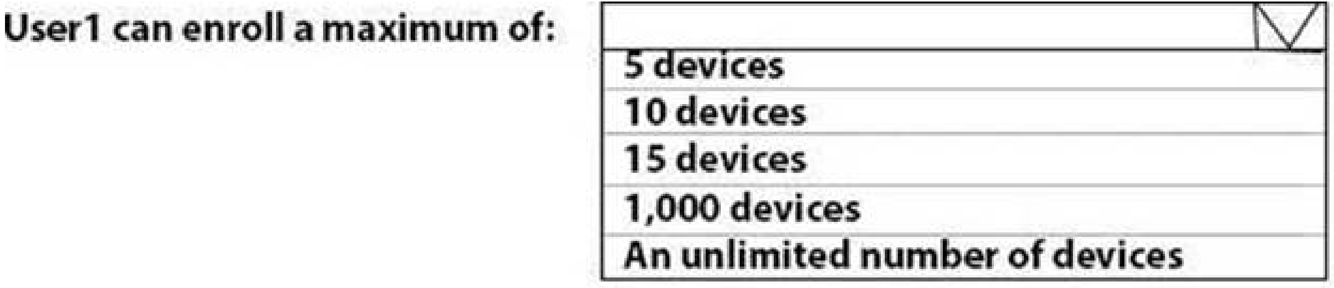
- Device1 only
- Device2 only
- Device3 only
- Device4 only
- Device2 and Device3 only
- Device1 and Device3 only
- Device1, Device2, and Device 3

A. Mastered
B. Not Mastered

Answer: A

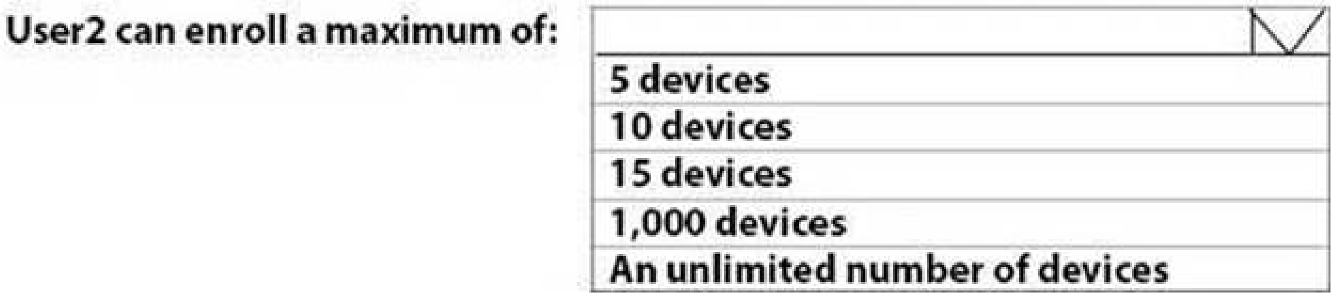
Explanation:
Reference:
https://docs.microsoft.com/en-us/intune/device-profile-assign

NEW QUESTION 92
- (Exam Topic 3)
What is the maximum number of devices that User1 and User2 can enroll in Intune? To answer, select the appropriate options in the answer area.
NOTE: Each correct selection is worth one point.



User1 can enroll a maximum of:

- 5 devices
- 10 devices
- 15 devices
- 1,000 devices
- An unlimited number of devices



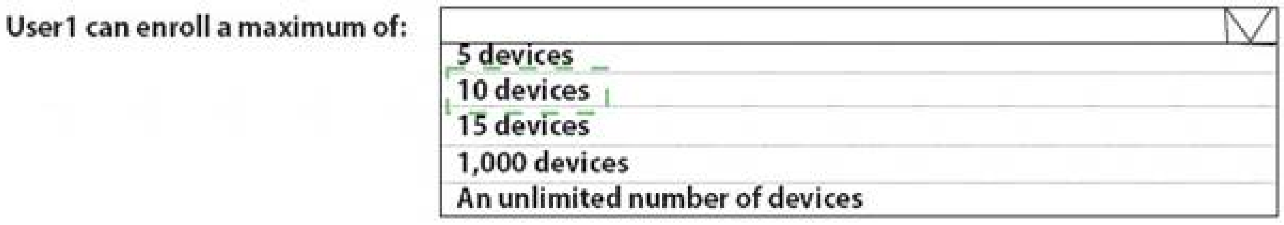
User2 can enroll a maximum of:

- 5 devices
- 10 devices
- 15 devices
- 1,000 devices
- An unlimited number of devices

A. Mastered
B. Not Mastered

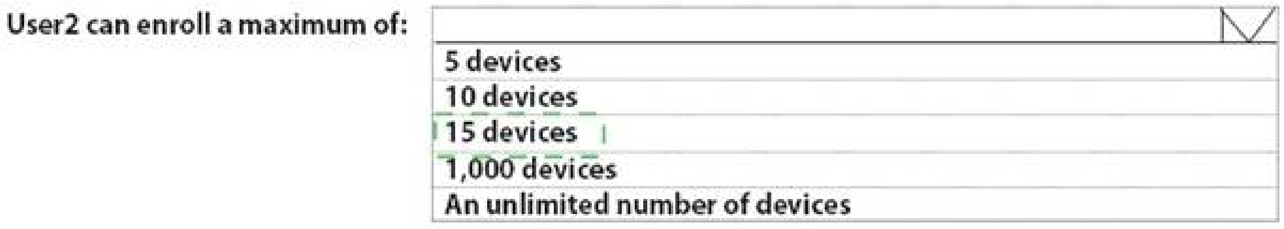
Answer: A

Explanation:



User1 can enroll a maximum of:

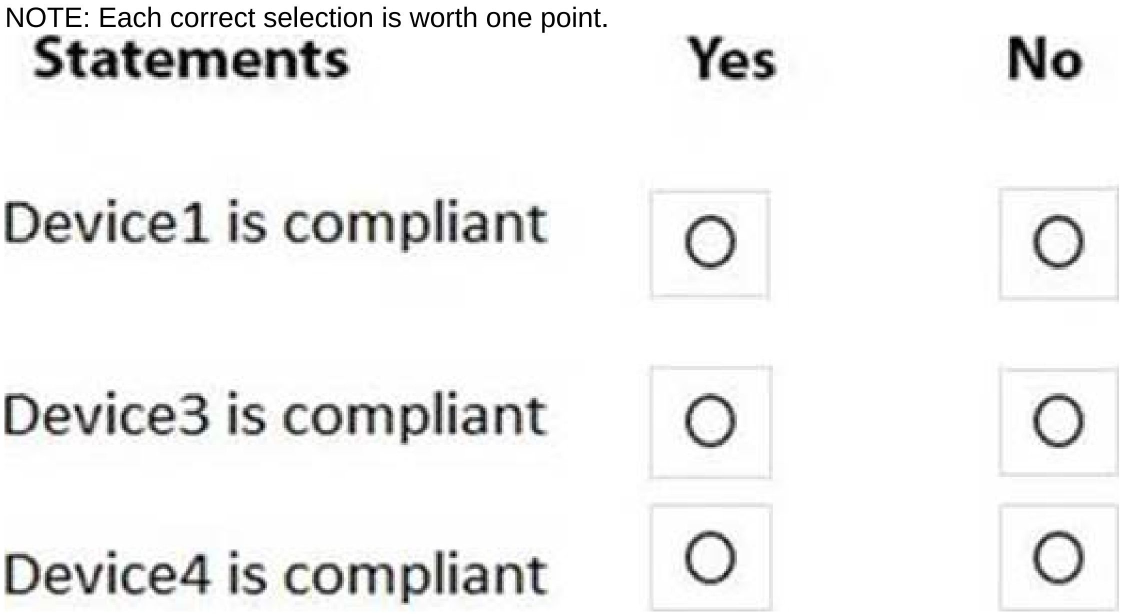
- 5 devices
- [✓ 10 devices]
- 15 devices
- 1,000 devices
- An unlimited number of devices



User2 can enroll a maximum of:

- 5 devices
- 10 devices
- [✓ 15 devices]
- 1,000 devices
- An unlimited number of devices

NEW QUESTION 96
- (Exam Topic 3)
You are evaluating which devices are compliant.
For each of the following statements, select Yes if the statement is true. Otherwise, select No.
NOTE: Each correct selection is worth one point.

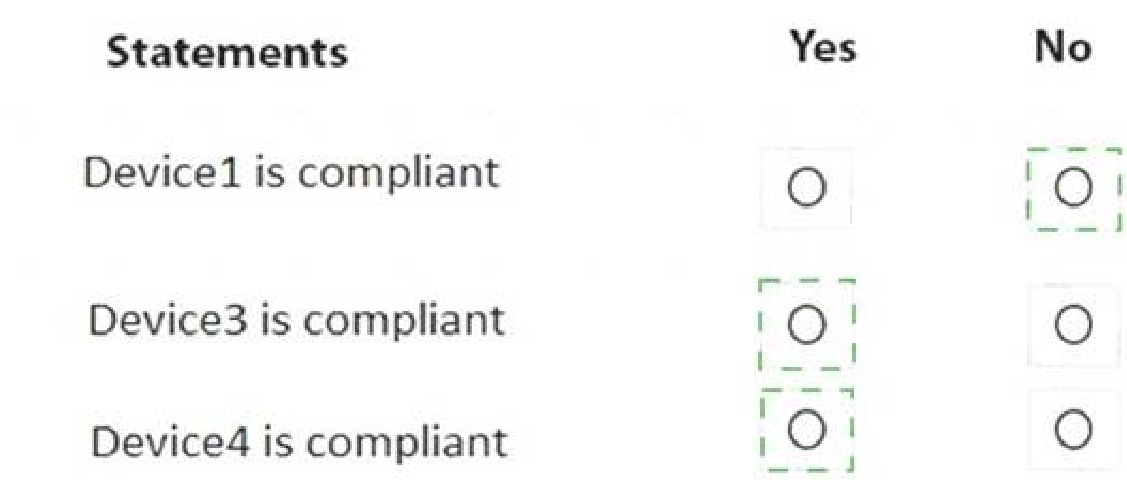


Statements	Yes	No
Device1 is compliant	○	○
Device3 is compliant	○	○
Device4 is compliant	○	○

A. Mastered
B. Not Mastered

Answer: A

Explanation:



Statements	Yes	No
Device1 is compliant	○	[✓ ○]
Device3 is compliant	[✓ ○]	○
Device4 is compliant	[✓ ○]	○

NEW QUESTION 97
- (Exam Topic 3)
You need to meet the technical requirements for the IT department. What should you do first?

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

Answer: C

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

NEW QUESTION 98
- (Exam Topic 3)
You need to meet the technical requirements for the iOS devices. Which object should you create in Intune?

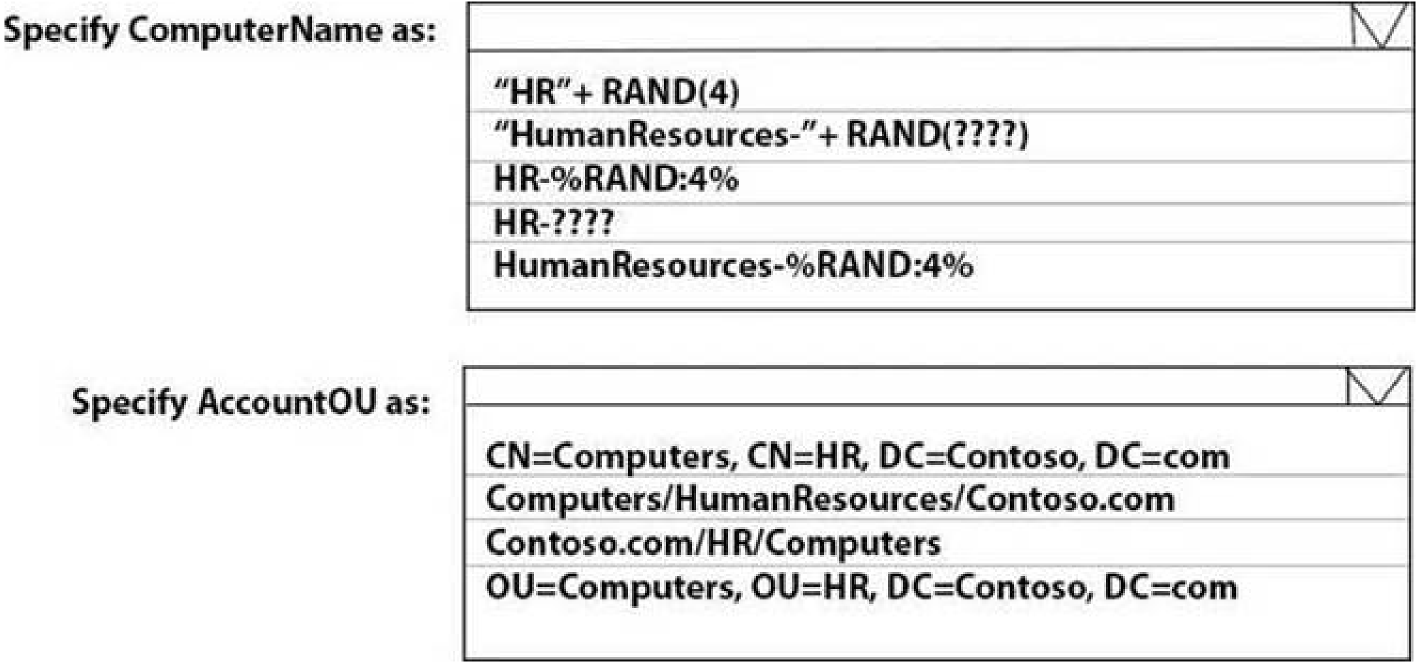
A. A compliance policy
B. An app protection policy
C. A Deployment profile
D. A device configuration profile

Answer: D

Explanation:
References:
https://docs.microsoft.com/en-us/intune/device-restrictions-configure https://docs.microsoft.com/en-us/intune/device-restrictions-ios

NEW QUESTION 100
- (Exam Topic 3)

You need to meet the technical requirements for the new HR department computers.
How should you configure the provisioning package? To answer, select the appropriate options in the answer area.
NOTE: Each correct selection is worth one point.



Specify ComputerName as:

- “HR”+ RAND(4)
- “HumanResources-”+ RAND(????)
- HR-%RAND:4%
- HR-????
- HumanResources-%RAND:4%

Specify AccountOU as:

- CN=Computers, CN=HR, DC=Contoso, DC=com
- Computers/HumanResources/Contoso.com
- Contoso.com/HR/Computers
- OU=Computers, OU=HR, DC=Contoso, DC=com

A. Mastered
B. Not Mastered

Answer: A

Explanation:
Reference:
https://docs.microsoft.com/en-us/windows/configuration/wcd/wcd-accounts

NEW QUESTION 101
- (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

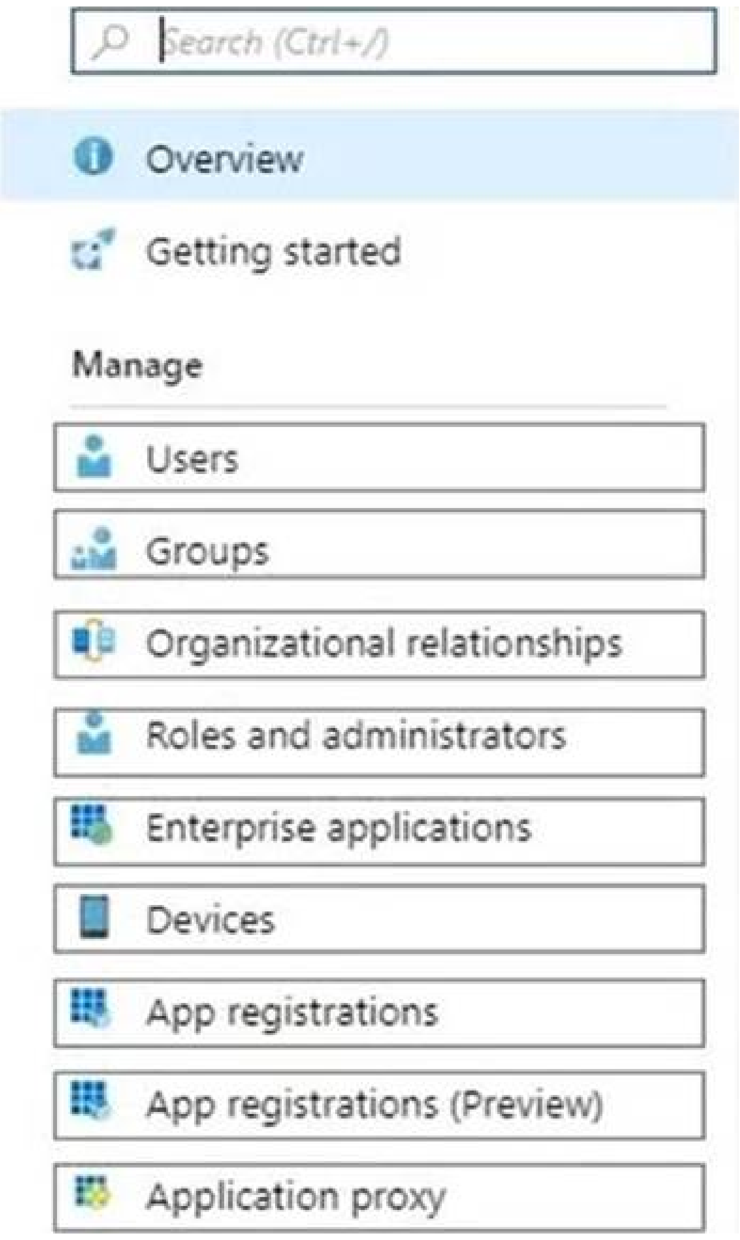
NEW QUESTION 105
- (Exam Topic 2)
What should you upgrade before you can configure the environment to support co-management?

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

Answer: B

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

NEW QUESTION 110
- (Exam Topic 2)
You need to meet the technical requirements for Windows AutoPilot.
Which two settings should you configure from the Azure Active Directory blade? To answer, select the appropriate settings in the answer area.
NOTE: Each correct selection is worth one point.



A. Mastered
B. Not Mastered

Answer: A

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

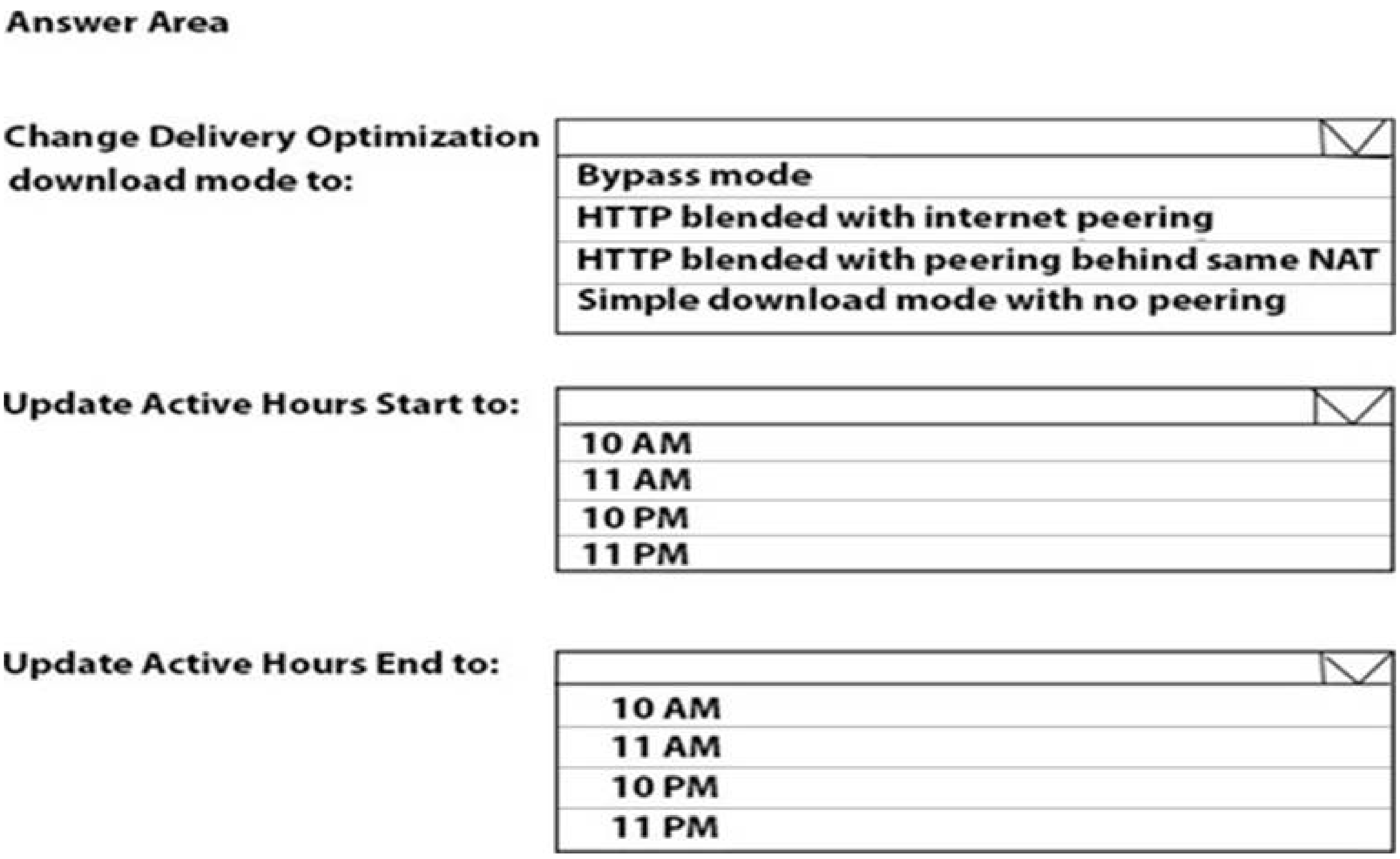
NEW QUESTION 114
- (Exam Topic 2)
What should you use to meet the technical requirements for Azure DevOps?

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 116
- (Exam Topic 2)
You need to resolve the performance issues in the Los Angeles office.
How should you configure the update settings? To answer, select the appropriate options in the answer area. NOTE: Each correct selection is worth one point.



Answer Area

Change Delivery Optimization download mode to:
- Bypass mode
- HTTP blended with internet peering
- HTTP blended with peering behind same NAT
- Simple download mode with no peering

Update Active Hours Start to:
- 10 AM
- 11 AM
- 10 PM
- 11 PM

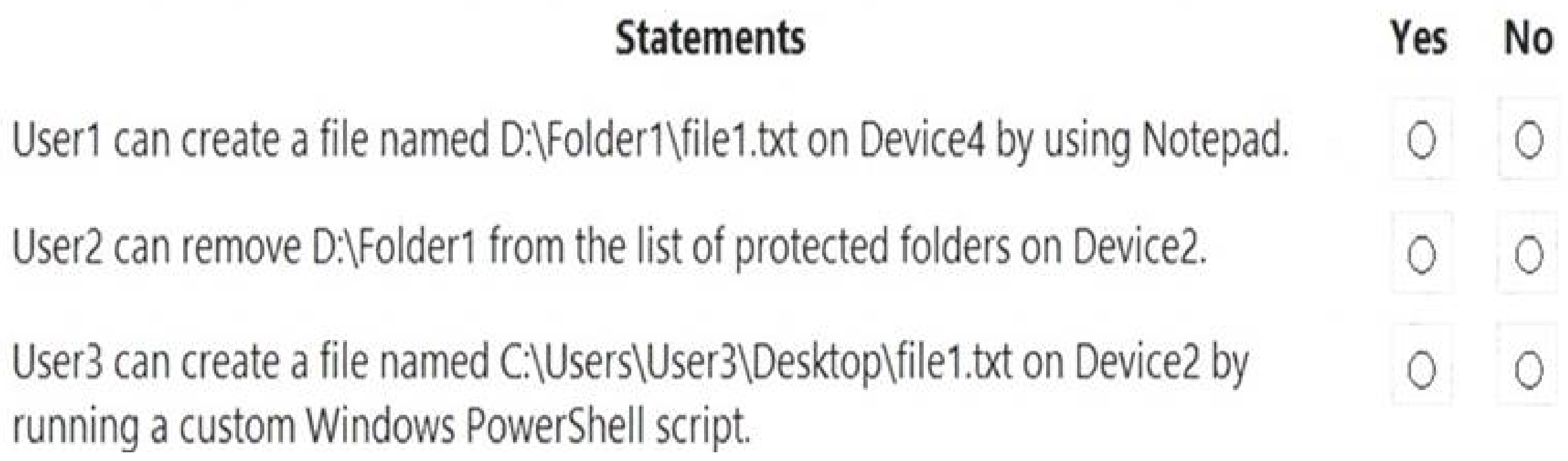
Update Active Hours End to:
- 10 AM
- 11 AM
- 10 PM
- 11 PM

A. Mastered
B. Not Mastered

Answer: A

Explanation:
A screenshot of a computer Description automatically generated with low confidence
Reference:
https://docs.microsoft.com/en-us/windows/deployment/update/waas-delivery-optimization https://2pintsoftware.com/delivery-optimization-dl-mode/

NEW QUESTION 120
- (Exam Topic 1)
For each of the following statements, select Yes if the statement is true. Otherwise, select No.
NOTE: Each correct selection is worth one point.



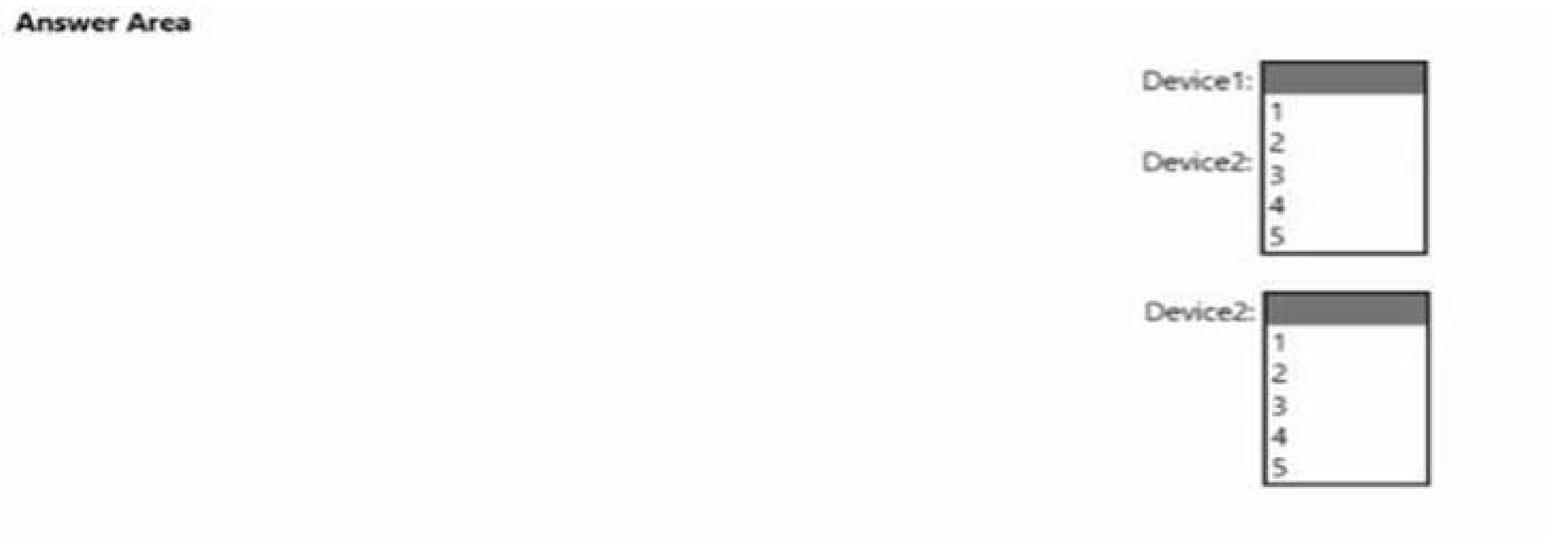
Statements	Yes	No
User1 can create a file named D:\Folder1\file1.txt on Device4 by using Notepad.	○	○
User2 can remove D:\Folder1 from the list of protected folders on Device2.	○	○
User3 can create a file named C:\Users\User3\Desktop\file1.txt on Device2 by running a custom Windows PowerShell script.	○	○

A. Mastered
B. Not Mastered

Answer: A

Explanation:
A screenshot of a computer Description automatically generated with medium confidence

NEW QUESTION 124
- (Exam Topic 1)
You implement the planned changes for Connection1 and Connection2
How many VPN connections will there be for User1 when the user signs in to Device 1 and Devke2? To answer select the appropriate options in the answer area.
NOTE; Each correct selection is worth one point.



Answer Area

Device1: 1 2 3 4 5

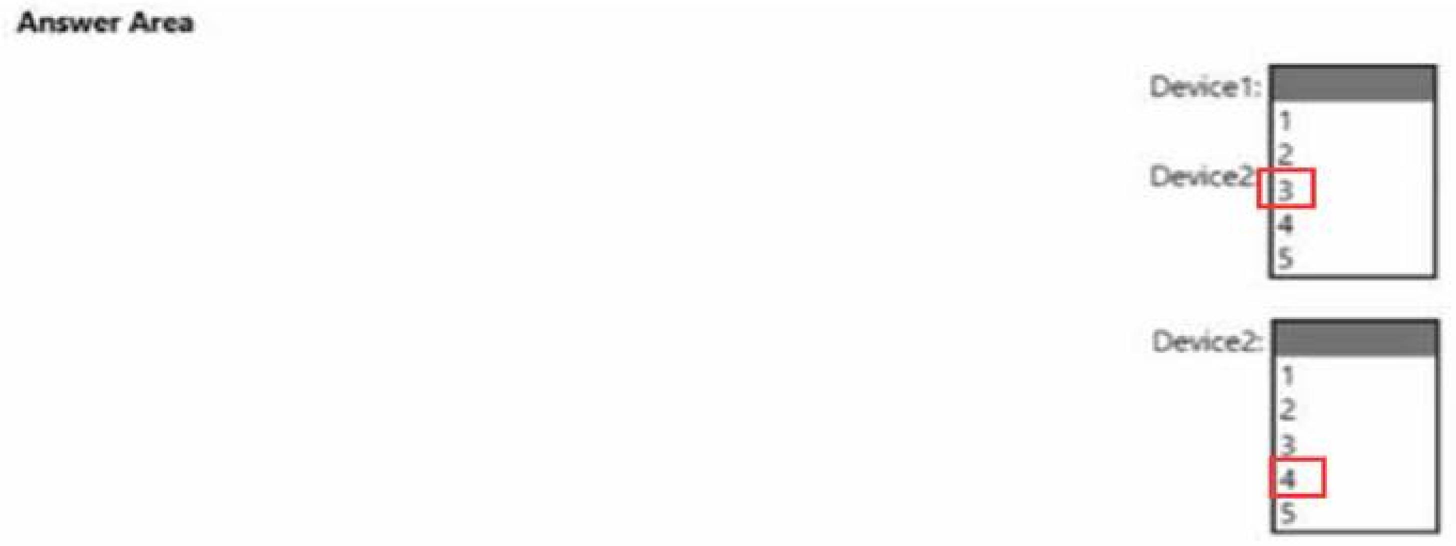
Device2: 1 2 3 4 5

Device2: 1 2 3 4 5

A. Mastered
B. Not Mastered

Answer: A

Explanation:

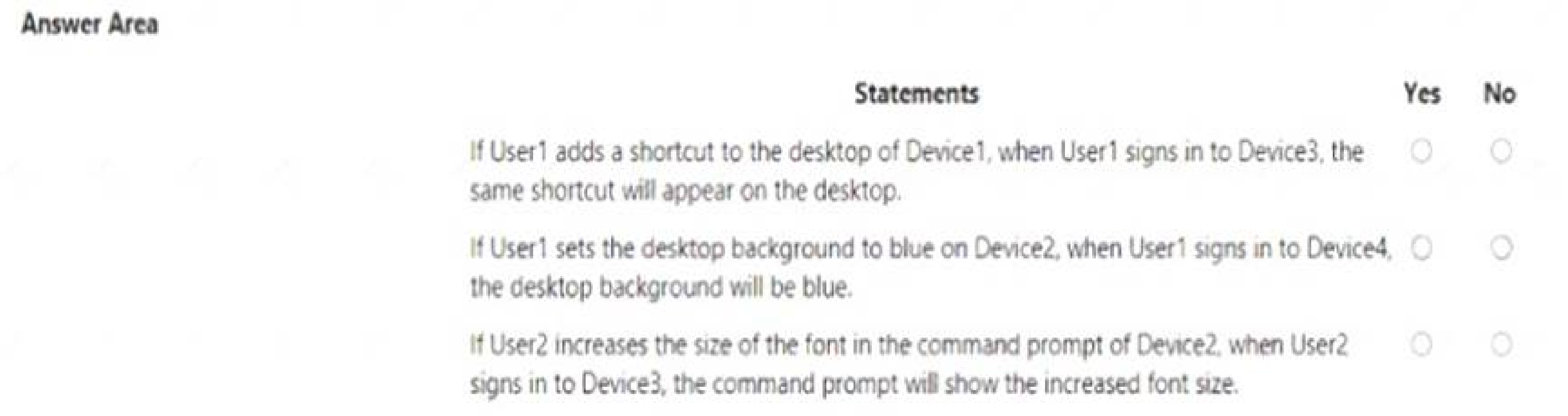


Answer Area

Device1: 1 2 [✓ 3] 4 5

Device2: 1 2 3 [✓ 4] 5

NEW QUESTION 126
- (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 129
- (Exam Topic 4)
You have a Microsoft 365 E5 subscription that contains 100 iOS devices enrolled in Microsoft Intune. You need to ensure that notifications of iOS updates are deferred for 30 days after the updates are released. What should you create?

A. a device configuration profile based on the Device features template
B. a device configuration profile based on the Device restrictions template
C. an update policy for iOS/iPadOS
D. an iOS app provisioning profile

Answer: C

Explanation:
Manage iOS/iPadOS software update policies in Intune, delay visibility of software updates.
When you use update policies for iOS, you might have need to delay visibility of an iOS software update. Reasons to delay visibility include:
Prevent users from updating the OS manually
To deploy an older update while preventing users from installing a more recent one
To delay visibility, deploy a device restriction template that configures the following settings: Defer software updates = Yes
This doesn't affect any scheduled updates. It represents days before software updates are visible to end users after release.
Delay default visibility of software updates = 1 to 90 90 days is the maximum delay that Apple supports.
Reference: https://docs.microsoft.com/en-us/mem/intune/protect/software-updates-ios

NEW QUESTION 130
- (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 131
- (Exam Topic 4)
You have a Microsoft 365 E5 subscription. The subscription contains 25 computers that run Windows 11 and are enrolled in Microsoft Intune. You need to onboard the devices to Microsoft Defender for Endpoint. What should you create in the Microsoft Intune admin center?

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

Answer: C

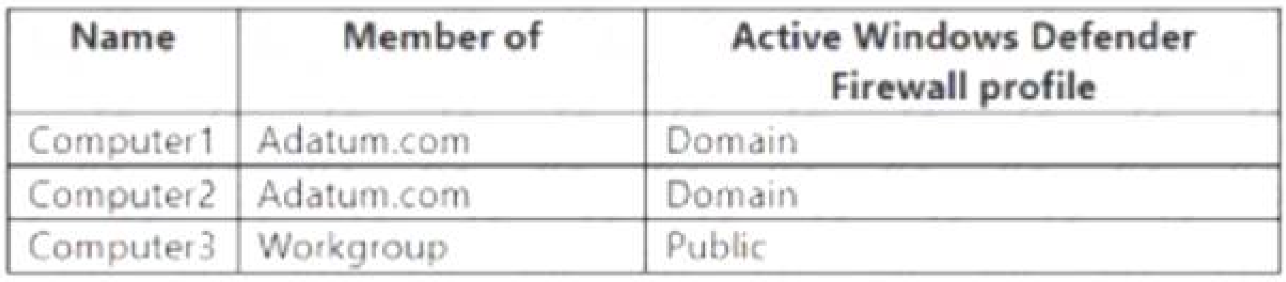
Explanation:
To onboard the devices to Microsoft Defender for Endpoint, you need to create an endpoint detection and response (EDR) policy in the Microsoft Intune admin center. This policy enables EDR capabilities on devices that are enrolled in Intune and allows you to configure various settings for EDR functionality. You can then assign the policy to groups of users or devices. References:
https://docs.microsoft.com/en-us/mem/intune/protect/edr-windows

NEW QUESTION 132
- (Exam Topic 4)
You have two computers named Computer1 and Computed that run Windows 10. Computed has Remote Desktop enabled.
From Computer1, you connect to Computer2 by using Remote Desktop Connection.
You need to ensure that you can access the local drives on Computer1 from within the Remote Desktop session.
What should you do?

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

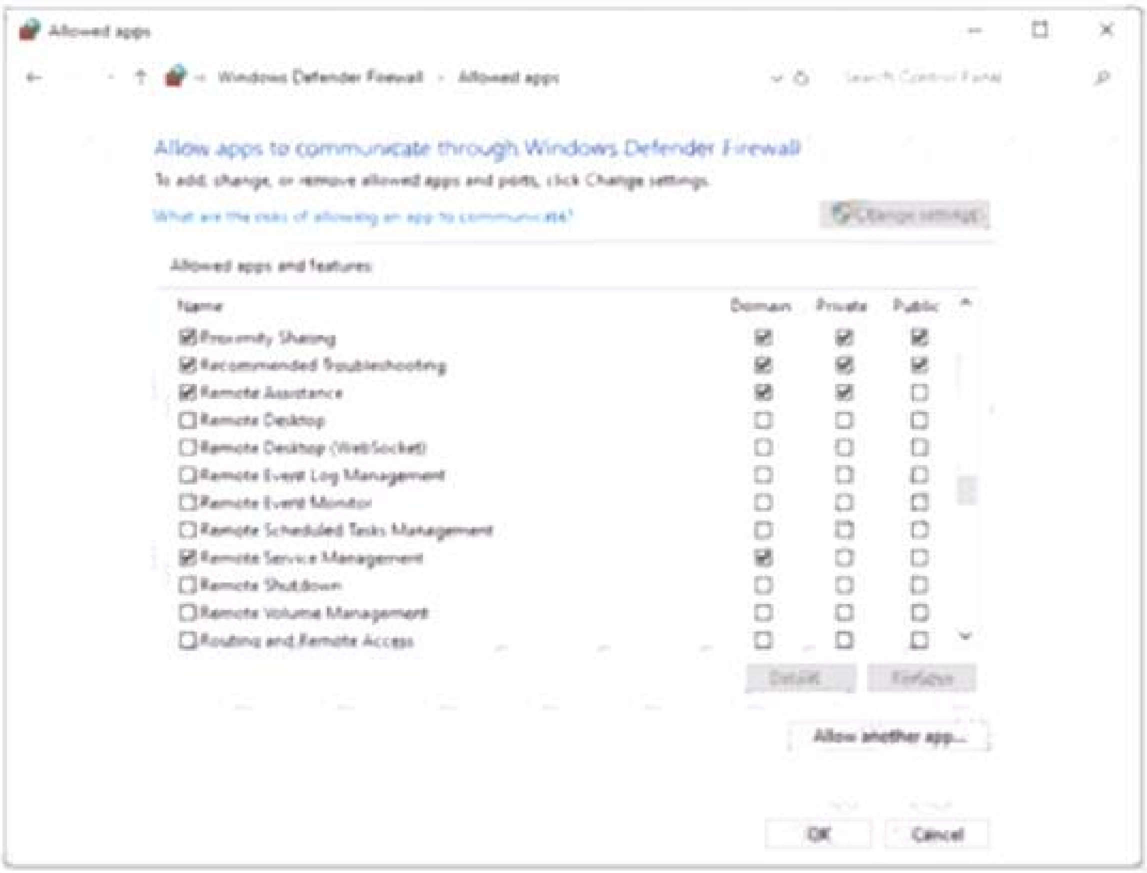
Answer: D

NEW QUESTION 133
- (Exam Topic 4)
Your network contains an Active Directory domain named adatum.com, a workgroup, and computers that run Windows 10. The computers are configured as shown in the following table.



Name	Member of	Active Windows Defender Firewall profile
Computer1	Adatum.com	Domain
Computer2	Adatum.com	Domain
Computer3	Workgroup	Public

The local Administrator accounts on Computed, Computed, and Computed have the same user name and password.
On Computed. Windows Defender Firewall is configured as shown in the following exhibit.



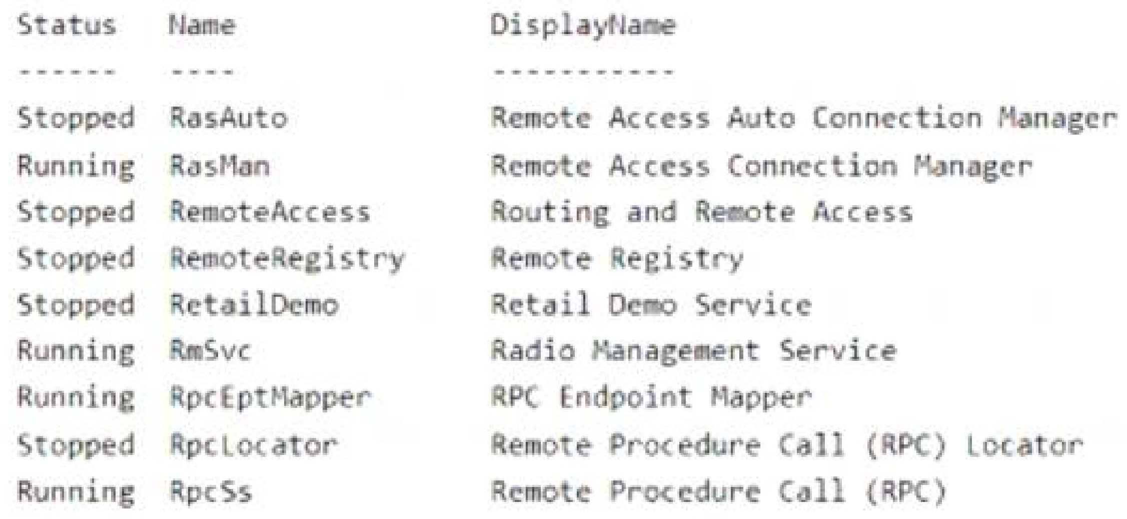
Allow apps to communicate through Windows Defender Firewall

To add, change, or remove allowed apps and ports, click Change settings.

What are the risks of allowing an app to communicate?

Allowed apps and features:

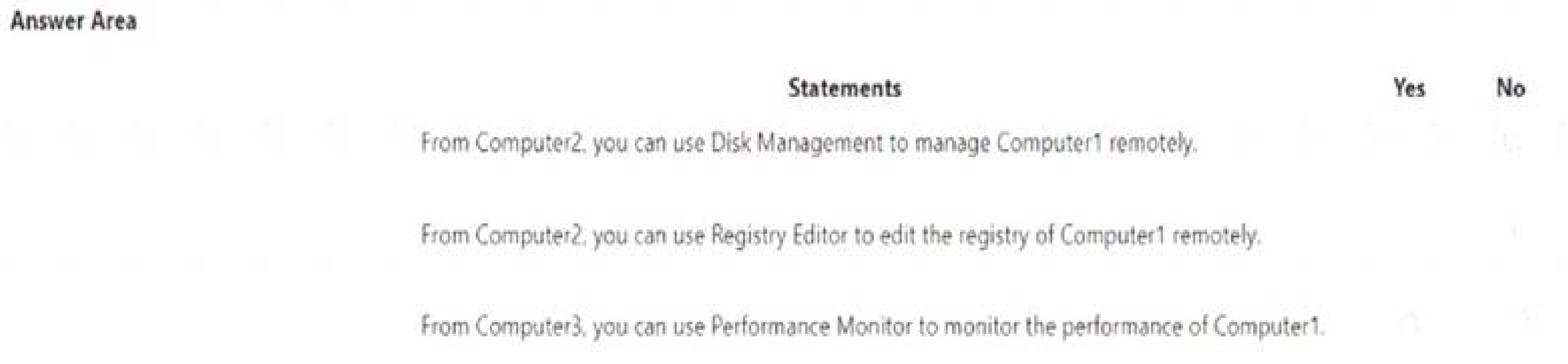
Name	Domain	Private	Public
☑ Proximity Sharing	☑	☑	☑
☑ Recommended Troubleshooting	☑	☑	☑
☑ Remote Assistance	☑	☑	□
□ Remote Desktop	□	□	□
□ Remote Desktop (WebSocket)	□	□	□
□ Remote Event Log Management	□	□	□
□ Remote Event Monitor	□	□	□
□ Remote Scheduled Tasks Management	□	□	□
☑ Remote Service Management	☑	□	□
□ Remote Shutdown	□	□	□
□ Remote Volume Management	□	□	□
□ Routing and Remote Access	□	□	□



```
Status   Name              DisplayName
------   ----              -----------
Stopped  RasAuto           Remote Access Auto Connection Manager
Running  RasMan            Remote Access Connection Manager
Stopped  RemoteAccess      Routing and Remote Access
Stopped  RemoteRegistry    Remote Registry
Stopped  RetailDemo        Retail Demo Service
Running  RmSvc             Radio Management Service
Running  RpcEptMapper      RPC Endpoint Mapper
Stopped  RpcLocator        Remote Procedure Call (RPC) Locator
Running  RpcSs             Remote Procedure Call (RPC)
```

For each of the following statements, select Yes if the statement is true. Otherwise, select No.

NOTE: Each correct selection is worth one point.



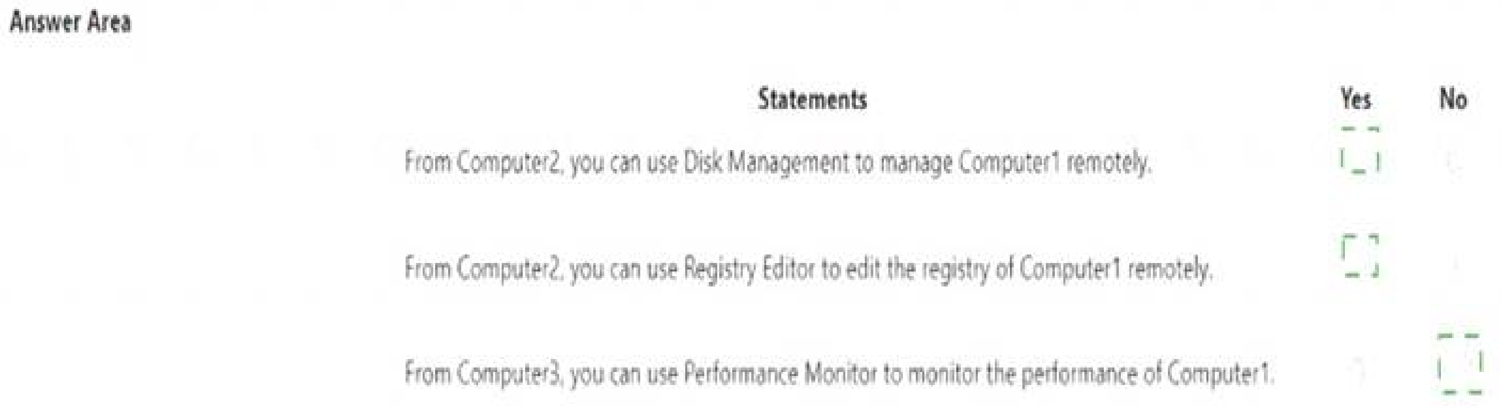
Answer Area

Statements	Yes	No
From Computer2, you can use Disk Management to manage Computer1 remotely.		
From Computer2, you can use Registry Editor to edit the registry of Computer1 remotely.		
From Computer3, you can use Performance Monitor to monitor the performance of Computer1.		

A. Mastered
B. Not Mastered

Answer: A

Explanation:



Answer Area

Statements	Yes	No
From Computer2, you can use Disk Management to manage Computer1 remotely.	✓	
From Computer2, you can use Registry Editor to edit the registry of Computer1 remotely.	✓	
From Computer3, you can use Performance Monitor to monitor the performance of Computer1.		✓

NEW QUESTION 134
- (Exam Topic 4)
You have a Microsoft 365 E5 subscription that contains 150 hybrid Azure AD joined Windows devices. All the devices are enrolled in Microsoft Intune. You need to configure Delivery Optimization on the devices to meet the following requirements:
• Allow downloads from the internet and from other computers on the local network.
• Limit the percentage of used bandwidth to 50. What should you use?

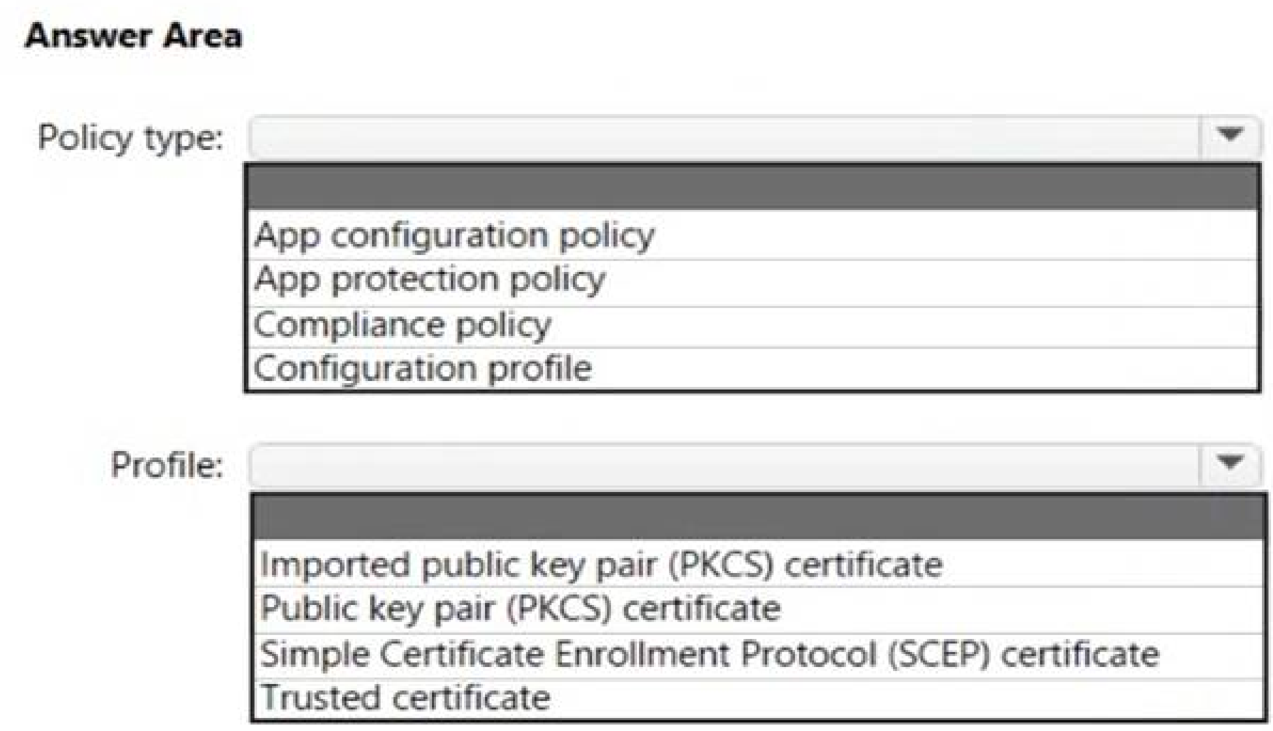
A. a configuration profile
B. a Windows Update for Business Group Policy setting
C. a Microsoft Peer-to-Peer Networking Services Group Policy setting
D. an Update ring for Windows 10 and later profile

Answer: A

Explanation:
A configuration profile is the correct answer because it allows you to configure Delivery Optimization settings for Windows devices in Intune. You can specify the download mode, bandwidth limit, caching options, and more. A configuration profile is a template that contains one or more settings that you can apply to groups of devices. References:

- Windows 10 Delivery Optimization settings for Intune - Microsoft Intune | Microsoft Learn
- Delivery Optimization settings in Microsoft Intune

NEW QUESTION 138
- (Exam Topic 4)
You have a Microsoft 365 tenant and an internal certification authority (CA).
You need to use Microsoft Intune to deploy the root CA certificate to managed devices.
Which type of Intune policy and profile should you use? To answer, select the appropriate options in the answer area.
NOTE: Each correct selection is worth one point.



Answer Area

Policy type:
- App configuration policy
- App protection policy
- Compliance policy
- Configuration profile

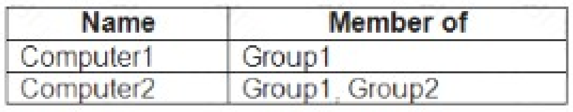
Profile:
- Imported public key pair (PKCS) certificate
- Public key pair (PKCS) certificate
- Simple Certificate Enrollment Protocol (SCEP) certificate
- Trusted certificate

A. Mastered
B. Not Mastered

Answer: A

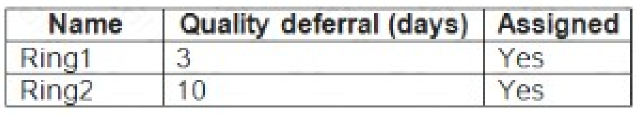
Explanation:
Box 1: Configuration profile Create a trusted certificate profile. Box 2: Trusted certificate
When using Intune to provision devices with certificates to access your corporate resources and network, use a trusted certificate profile to deploy the trusted root certificate to those devices. Trusted root certificates establish a trust from the device to your root or intermediate (issuing) CA from which the other certificates are issued.
Reference: https://docs.microsoft.com/en-us/mem/intune/protect/certificates-trusted-root

NEW QUESTION 143
- (Exam Topic 4)
You have two computers that run Windows 10. The computers are enrolled in Microsoft Intune as shown in the following table.



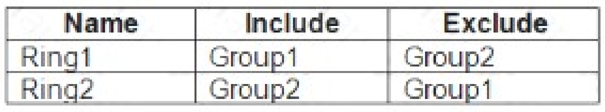
Name	Member of
Computer1	Group1
Computer2	Group1, Group2

Windows 10 update rings are defined in Intune as shown in the following table.



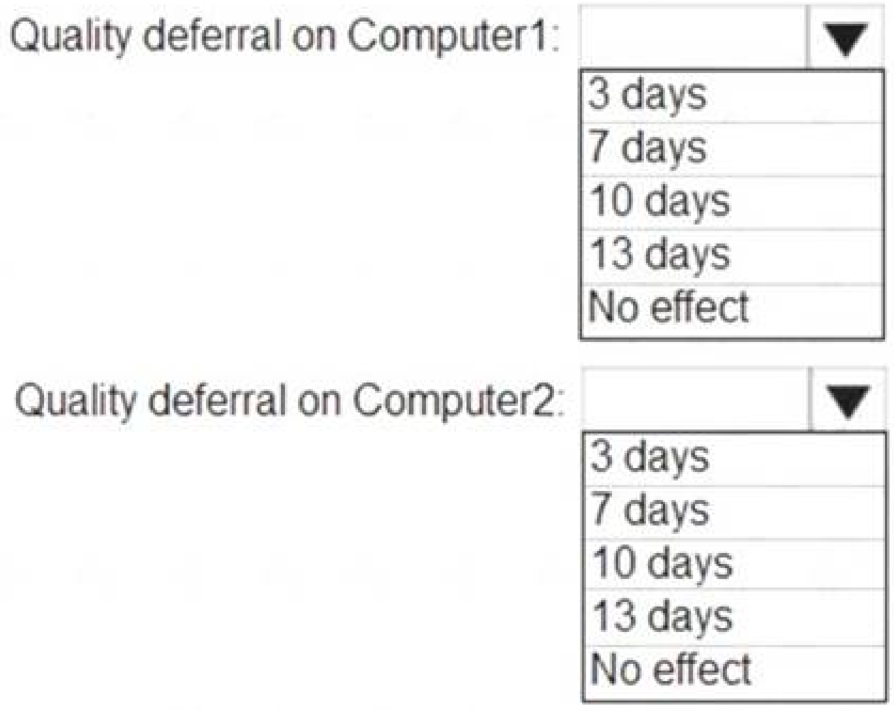
Name	Quality deferral (days)	Assigned
Ring1	3	Yes
Ring2	10	Yes

You assign the update rings as shown in the following table.



Name	Include	Exclude
Ring1	Group1	Group2
Ring2	Group2	Group1

What is the effect of the configurations on Computer1 and Computer2? To answer, select the appropriate options in the answer area.
NOTE: Each correct selection is worth one point.



Quality deferral on Computer1:
- 3 days
- 7 days
- 10 days
- 13 days
- No effect

Quality deferral on Computer2:
- 3 days
- 7 days
- 10 days
- 13 days
- No effect

A. Mastered
B. Not Mastered

Answer: A

Explanation:
A screenshot of a computer Description automatically generated
Computer1 and Computer2 are members of Group1. Ring1 is applied to Group1.
Note: The term "Exclude" is misleading. It means that the ring is not applied to that group, rather than that group being blocked.
References:
https://docs.microsoft.com/en-us/windows/deployment/update/waas-wufb-intune https://allthingscloud.blog/configure-windows-update-business-using-microsoft-intune/

NEW QUESTION 148
- (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

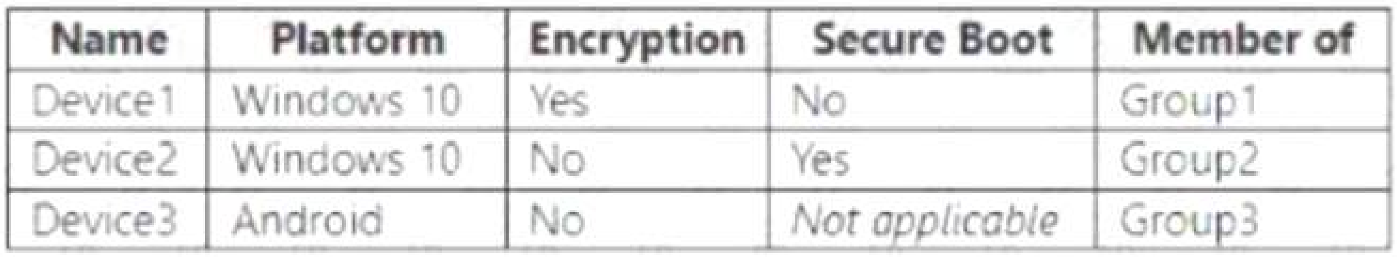
Answer: B

NEW QUESTION 150
- (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

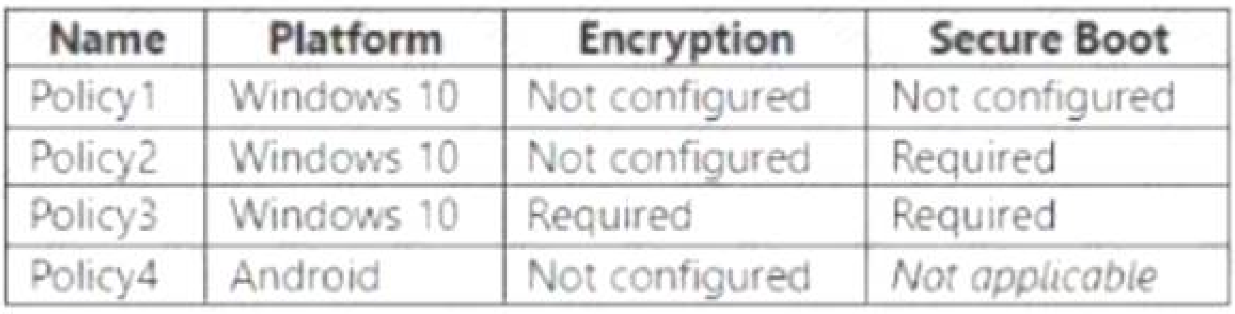
Answer: B

NEW QUESTION 152
- (Exam Topic 4)
You have devices enrolled in Microsoft Intune as shown in the following table.



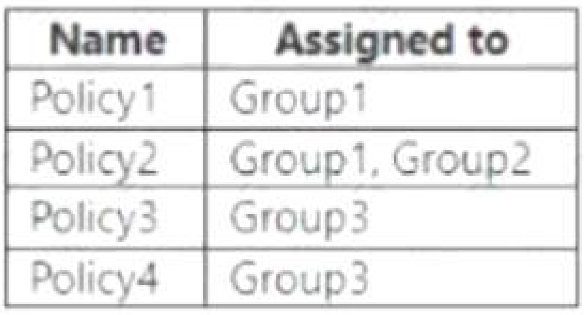
Name	Platform	Encryption	Secure Boot	Member of
Device1	Windows 10	Yes	No	Group1
Device2	Windows 10	No	Yes	Group2
Device3	Android	No	*Not applicable*	Group3

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



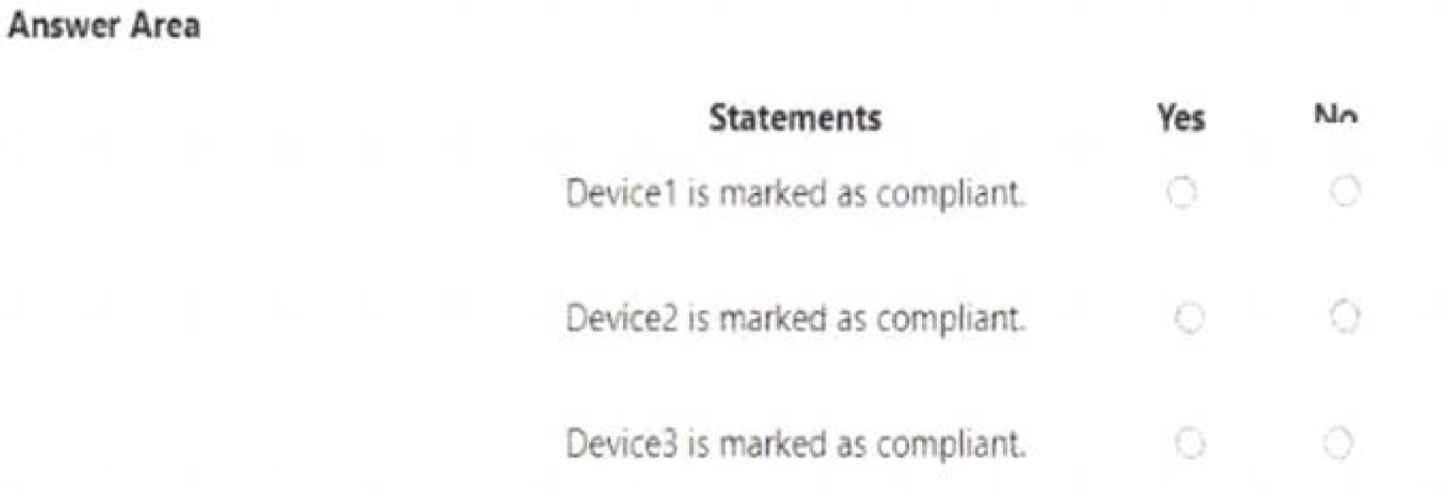
Name	Platform	Encryption	Secure Boot
Policy1	Windows 10	Not configured	Not configured
Policy2	Windows 10	Not configured	Required
Policy3	Windows 10	Required	Required
Policy4	Android	Not configured	*Not applicable*

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



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

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



Answer Area

Statements	Yes	No
Device1 is marked as compliant.	○	○
Device2 is marked as compliant.	○	○
Device3 is marked as compliant.	○	○

A. Mastered
B. Not Mastered

Answer: A

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

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

NEW QUESTION 156
- (Exam Topic 4)
You have the Microsoft Deployment Toolkit (MDT) installed. You install and customize Windows 11 on a reference computer
You need to capture an image of the reference computer and ensure that the image can be deployed to multiple computers.
Which command should you run before you capture the image?

A. dism
B. wpeinit
C. sysprep
D. bcdedit

Answer: C

Explanation:
To capture an image of a reference computer and make it ready for deployment to multiple computers, you need to run the sysprep command with the /generalize option. This option removes all unique system information from the Windows installation, such as the computer name, security identifier (SID), and driver cache. The other commands are not used for this purpose. References: Sysprep (Generalize) a Windows installation

NEW QUESTION 157

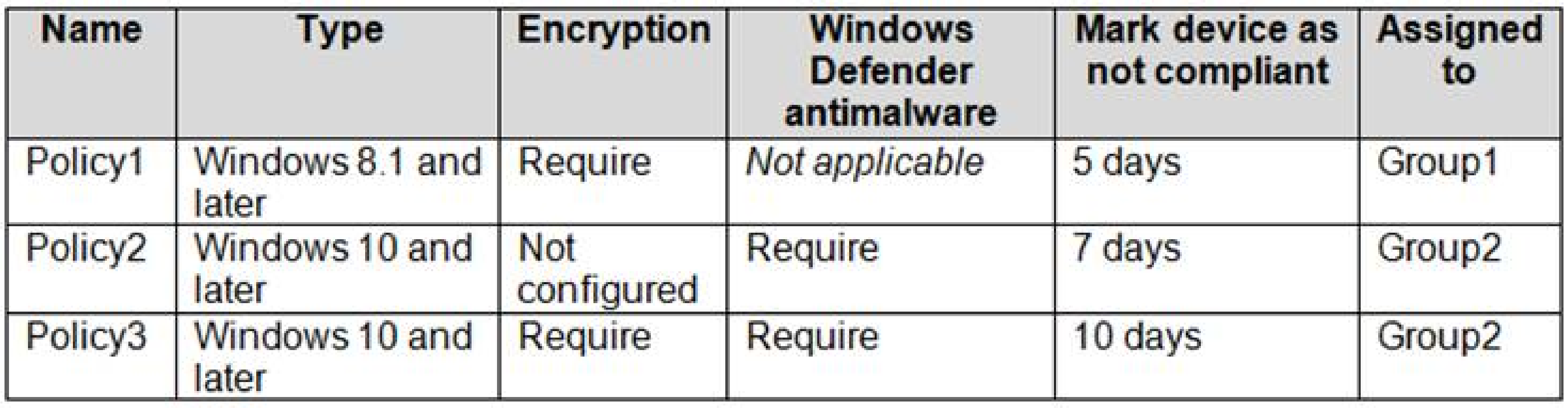
- (Exam Topic 4)
You have an Azure AD tenant and 100 Windows 10 devices that are Azure AD joined and managed by using Microsoft Intune.
You need to configure Microsoft Defender Firewall and Microsoft Defender Antivirus on the devices. The solution must minimize administrative effort.
Which two actions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

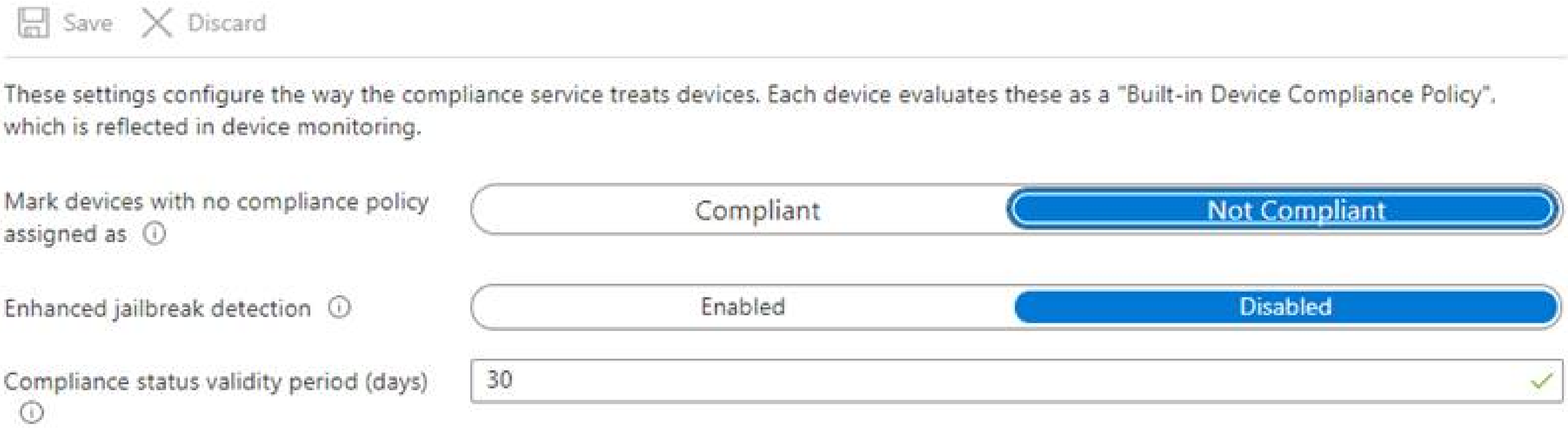
Explanation:
To configure Microsoft Defender Firewall and Microsoft Defender Antivirus on Azure AD joined devices that are managed by Intune, you need to create a device configuration profile and configure the Endpoint protection settings. You can use this profile to configure various settings for firewall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

NEW QUESTION 158
- (Exam Topic 4)
In Microsoft Intune, you have the device compliance policies shown in the following table.



Name	Type	Encryption	Windows Defender antimalware	Mark device as not compliant	Assigned to
Policy1	Windows 8.1 and later	Require	*Not applicable*	5 days	Group1
Policy2	Windows 10 and later	Not configured	Require	7 days	Group2
Policy3	Windows 10 and later	Require	Require	10 days	Group2

The Intune compliance policy settings are configured as shown in the following exhibit.



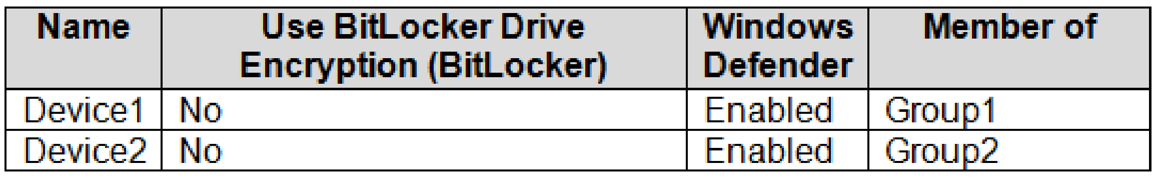
These settings configure the way the compliance service treats devices. Each device evaluates these as a "Built-in Device Compliance Policy", which is reflected in device monitoring.

Mark devices with no compliance policy assigned as: Compliant [✓ Not Compliant]

Enhanced jailbreak detection: Enabled [✓ Disabled]

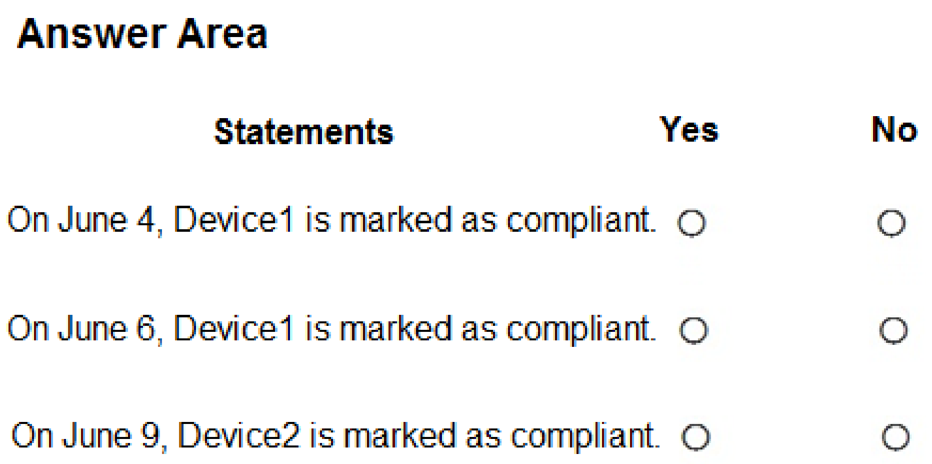
Compliance status validity period (days): 30

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



Name	Use BitLocker Drive Encryption (BitLocker)	Windows Defender	Member of
Device1	No	Enabled	Group1
Device2	No	Enabled	Group2

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



Answer Area

Statements	Yes	No
On June 4, Device1 is marked as compliant.	○	○
On June 6, Device1 is marked as compliant.	○	○
On June 9, Device2 is marked as compliant.	○	○

A. Mastered
B. Not Mastered

Answer: A

Explanation:
Device 1 is Windows 10 - and policy 1 is for Windows 8. Default compliance for devices without a policy is not compliant so first 2 questions are NO.
Then the third device has 2 policies, the first one is compliant and the second policy is not compliant but the device is not marked as non-compliant due to the fact

that mark device as non-compliant is set to 10 days. This means that the machine will be compliant until june 10th.
Source:
Mark device non-compliant: By default, this action is set for each compliance policy and has a schedule of zero (0) days, marking devices as noncompliant immediately.
When you change the default schedule, you provide a grace period in which a user can remediate issues or become compliant without being marked as non-compliant.
This action is supported on all platforms supported by Intune. https://docs.microsoft.com/en-us/mem/intune/protect/actions-for-noncompliance

NEW QUESTION 160
- (Exam Topic 4)
You have an Azure AD tenant named contoso.com.
You have a workgroup computer named Computer! that runs Windows 11. You need to add Computer1 to contoso.com.
What should you use?

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

Answer: A

NEW QUESTION 165
- (Exam Topic 4)
You have a Microsoft 365 subscription that uses Microsoft Intune Suite. You use Microsoft Intune to manage devices.
Auto-enrollment in Intune is configured.
You have 100 Windows 11 devices in a workgroup.
You need to connect the devices to the corporate wireless network and enroll 100 new Windows devices in Intune.
What should you use?

A. a provisioning package
B. a Group Policy Object (GPO)
C. mobile device management (MDM) automatic enrollment
D. a device configuration policy

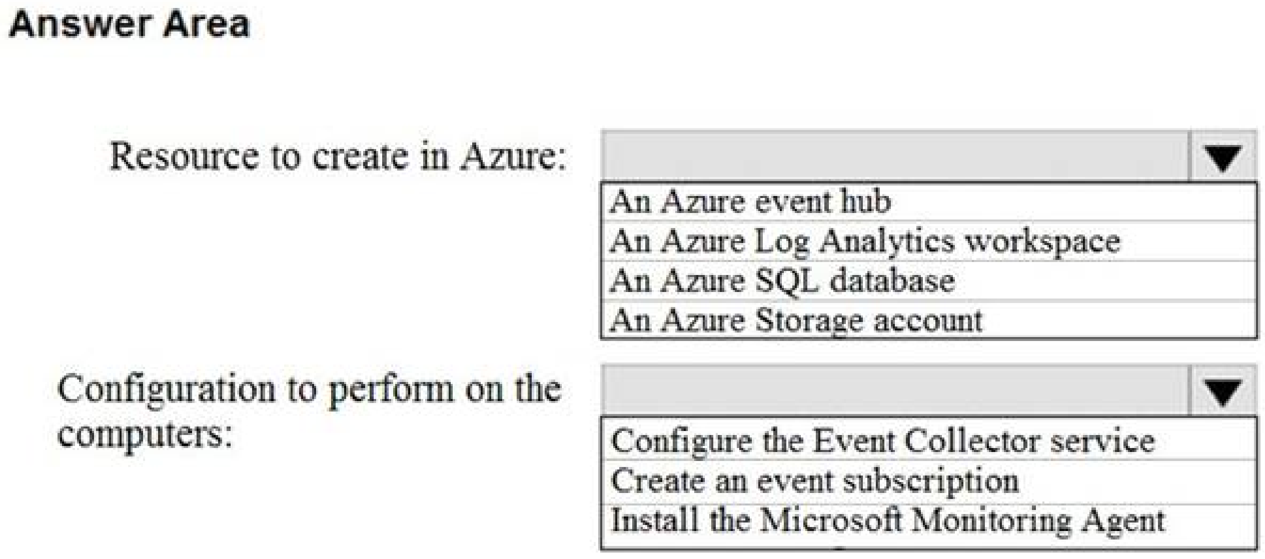
Answer: C

NEW QUESTION 167
- (Exam Topic 4)
You have a Microsoft 365 subscription that contains 1.000 Windows 11 devices enrolled in Microsoft Intune. You plan to use Intune to deploy an application named App1 that contains multiple installation files.
What should you do first?

A. Prepare the contents of App1 by using the Microsoft Win32 Content Prep Tool.
B. Create an Android application package (APK).
C. Upload the contents of App1 to Intune.
D. Install the Microsoft Deployment Toolkit (MDT).

Answer: A

NEW QUESTION 170
- (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

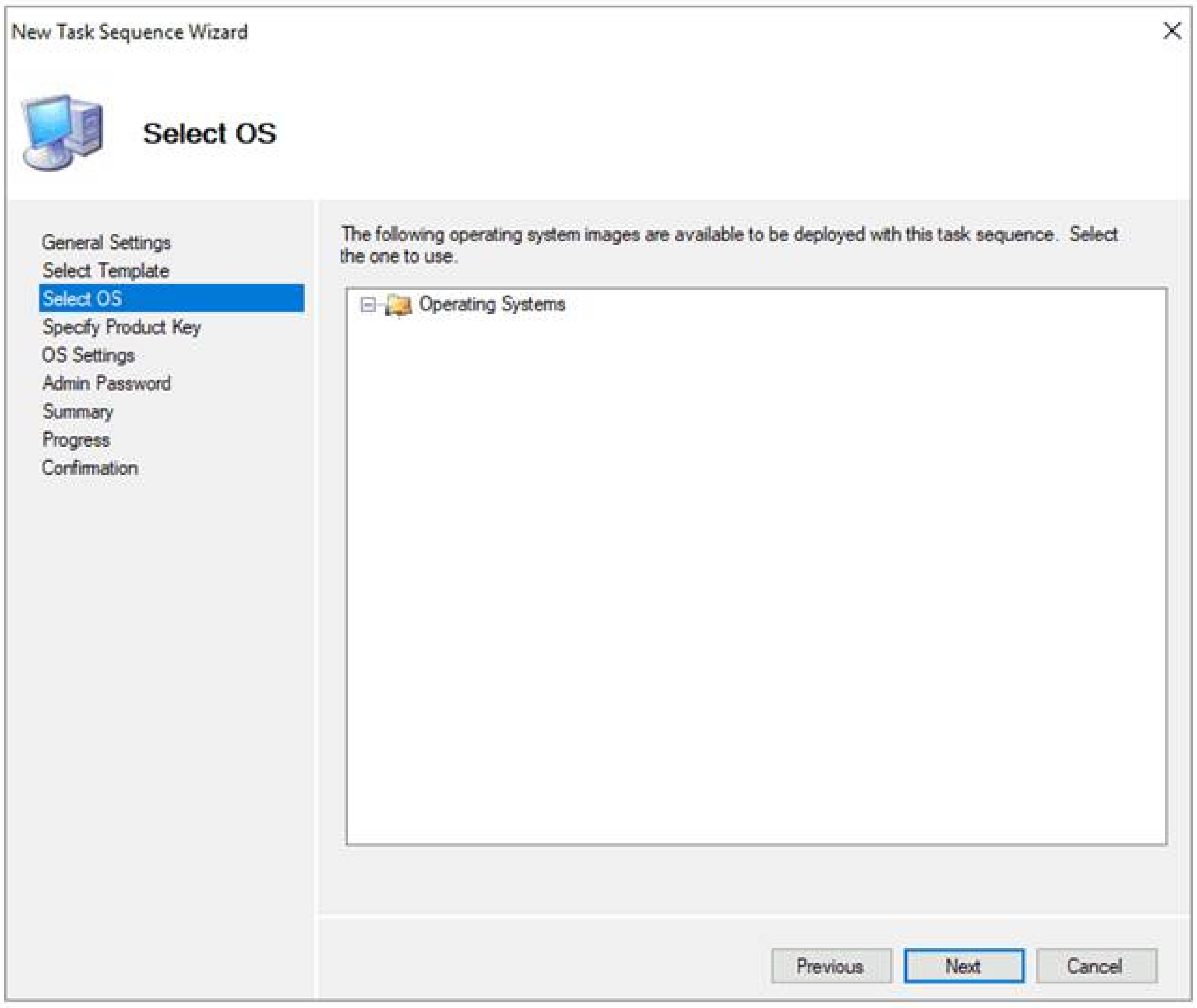
Configuration to perform on the computers:
- Configure the Event Collector service
- Create an event subscription
- Install the Microsoft Monitoring Agent

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 171
- (Exam Topic 4)
You have a Microsoft Deployment Toolkit (MDT) deployment share.
From the Deployment Workbench, you open the New Task Sequence Wizard and select the Standard Client Upgrade Task Sequence task sequence template.
You discover that there are no operating system images listed on the Select OS page as shown in the following exhibit.



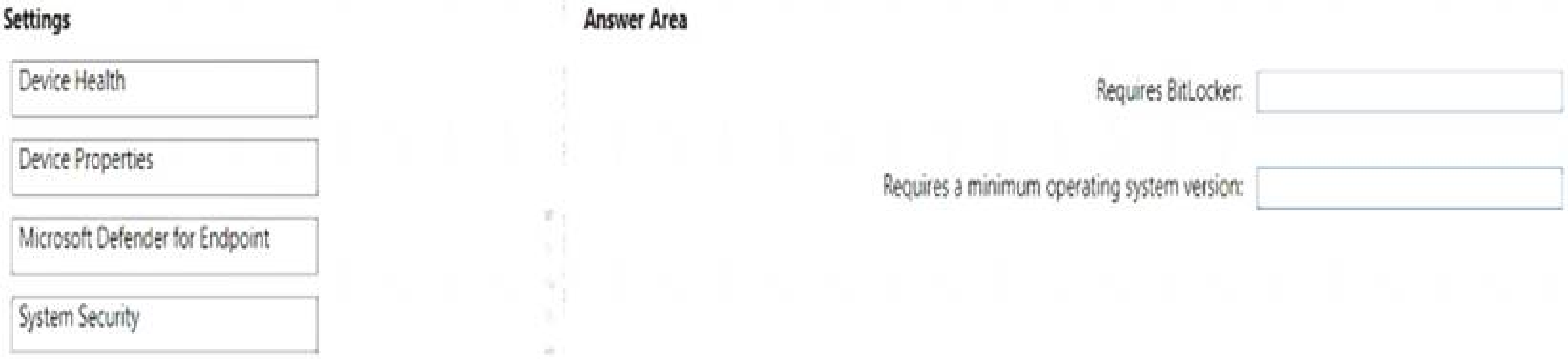
The following operating system images are available to be deployed with this task sequence. Select the one to use.

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

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

Answer: D

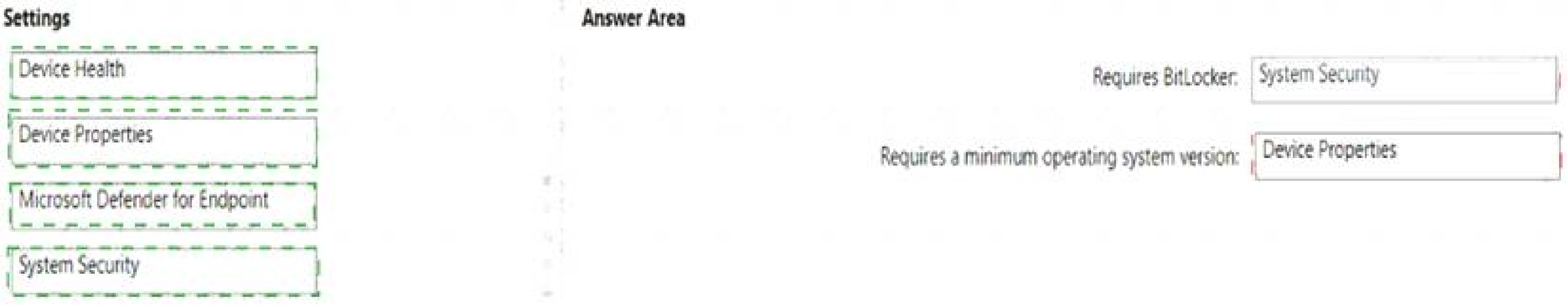
NEW QUESTION 173
- (Exam Topic 4)
You have a Microsoft 365 subscription. The subscription contains computers that run Windows 11 and are enrolled in Microsoft Intune. You need to create a compliance policy that meets the following requirements:
• Requires BitLocker Drive Encryption (BitLocker) on each device
• Requires a minimum operating system version
Which setting of the compliance policy should you configure for each requirement? To answer, drag the appropriate settings to the correct requirements. Each setting may be used once, more than once, or not at all. You may need to drag the split bar between panes or scroll to view content.
NOTE: Each correct selection is worth one point,



A. Mastered
B. Not Mastered

Answer: A

Explanation:



Settings

Device Health

Device Properties

Microsoft Defender for Endpoint

System Security

Answer Area

Requires BitLocker: System Security

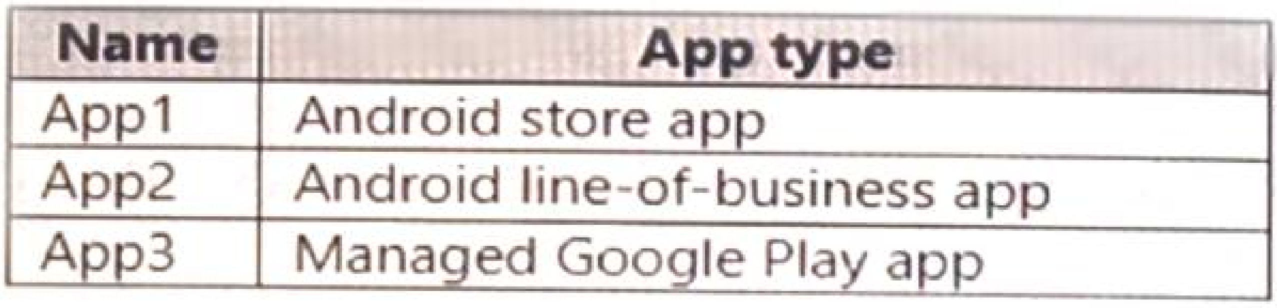
Requires a minimum operating system version: Device Properties

NEW QUESTION 175

- (Exam Topic 4)

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

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



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

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

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

Answer: D

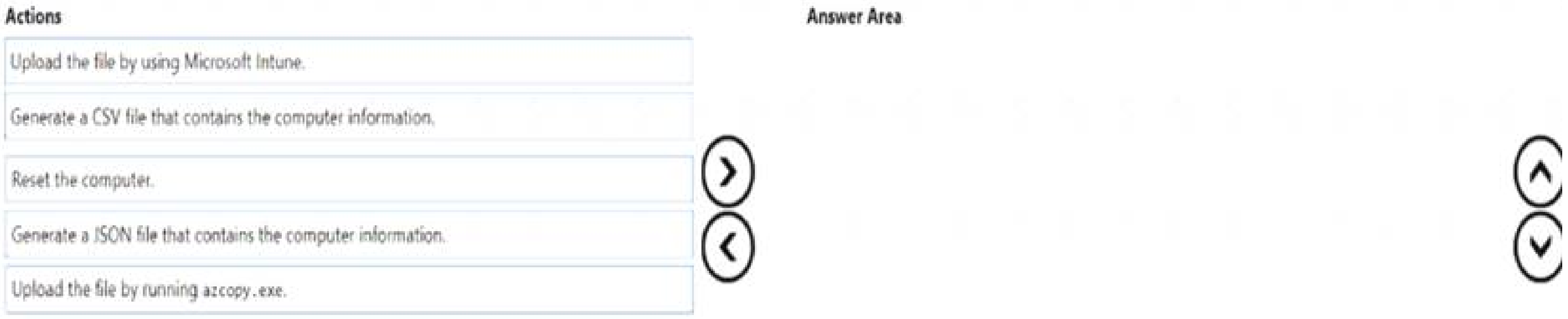
NEW QUESTION 180

- (Exam Topic 4)

Your company has a computer named Computer1 that runs Windows 10. Computed was used by a user who left the company.

You plan to repurpose Computer1 and assign the computer to a new user. You need to redeploy Computer1 by using Windows Autopilot.

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

Upload the file by using Microsoft Intune.

Generate a CSV file that contains the computer information.

Reset the computer.

Generate a JSON file that contains the computer information.

Upload the file by running azcopy.exe.

Answer Area

A. Mastered
B. Not Mastered

Answer: A

Explanation:

To redeploy Computer1 by using Windows Autopilot, you need to perform the following three actions in sequence:

- Generate a JSON file that contains the computer information. This file specifies the Autopilot profile to be applied during the deployment. You can use the Get-AutopilotProfilesForExistingDevices PowerShell script to generate this file1.
- Reset the computer. You can use the Windows Automatic Redeployment feature to trigger a reset from the login screen by pressing Ctrl + R and providing an administrator account2. Alternatively, you can use the Windows Autopilot Reset feature to remotely reset the device from Intune1.
- Upload the file by running azcopy.exe. This step copies the JSON file to a blob storage account in Azure, where it can be accessed by the device during the deployment. You need to specify the storage account name, access key, and container name as parameters for azcopy.exe1.

NEW QUESTION 184

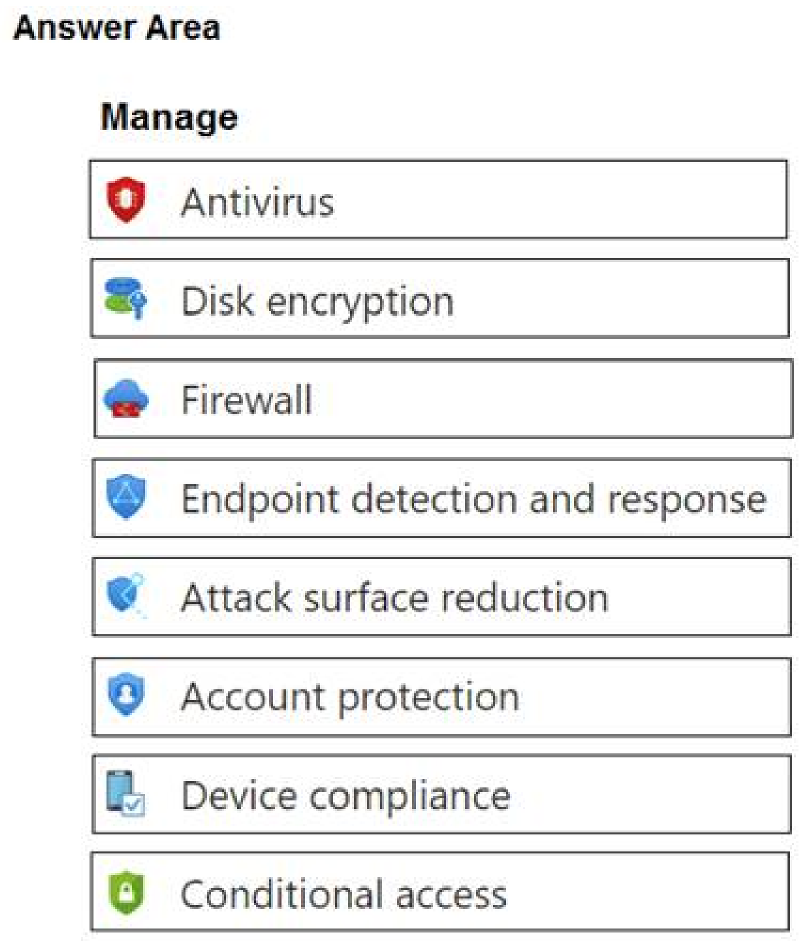
- (Exam Topic 4)

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

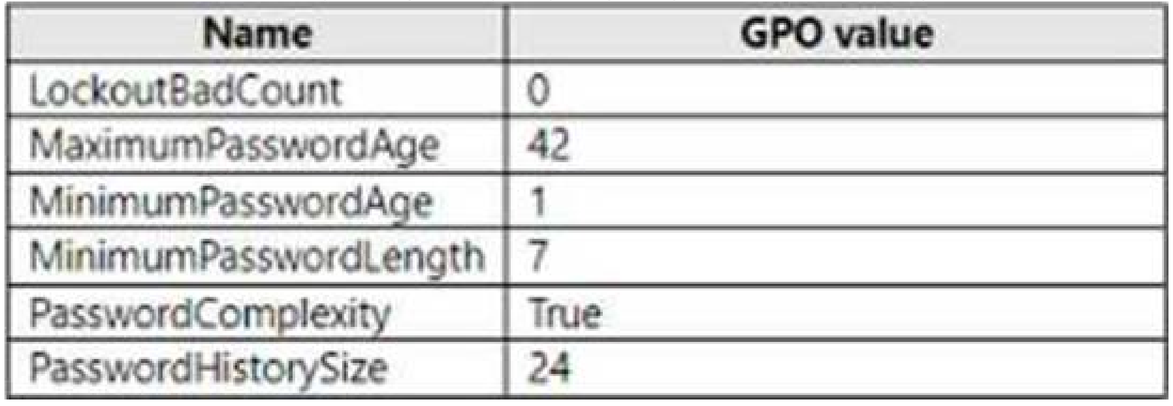
- Antivirus
- Disk encryption
- Firewall
- Endpoint detection and response
- Attack surface reduction
- Account protection
- Device compliance
- Conditional access

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 185
- (Exam Topic 4)
Your network contains an on-premises Active Directory domain and an Azure AD tenant.
The Default Domain Policy Group Policy Object (GPO) contains the settings shown in the following table.



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

Which device configuration profile type template should you use?

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

Answer: A

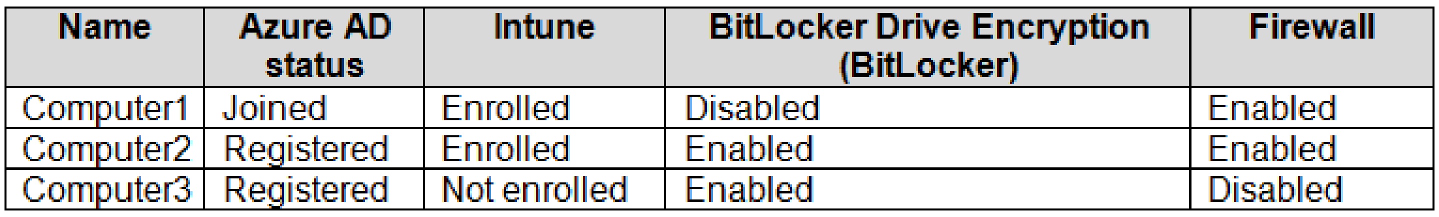
Explanation:
To configure the settings shown in the table, you need to use the Administrative Templates device configuration profile type template. This template allows you to configure hundreds of settings that are also available in Group Policy. You can use this template to configure settings such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

NEW QUESTION 186
- (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

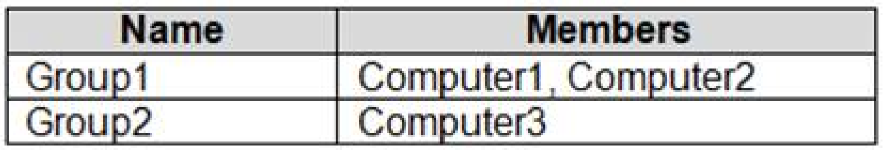
Answer: A

NEW QUESTION 189
- (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.



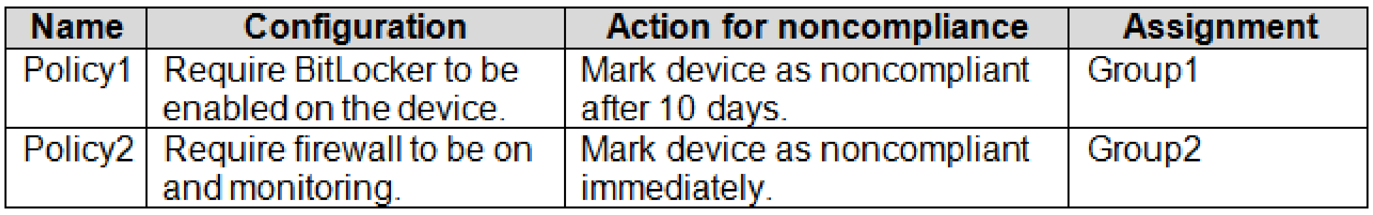
Name	Azure AD status	Intune	BitLocker Drive Encryption (BitLocker)	Firewall
Computer1	Joined	Enrolled	Disabled	Enabled
Computer2	Registered	Enrolled	Enabled	Enabled
Computer3	Registered	Not enrolled	Enabled	Disabled

You have the groups shown in the following table.



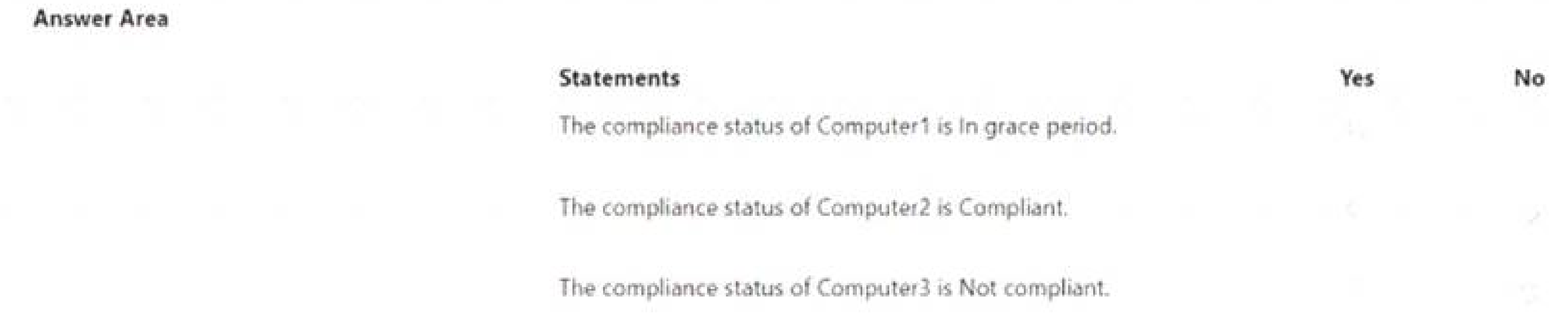
Name	Members
Group1	Computer1, Computer2
Group2	Computer3

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.



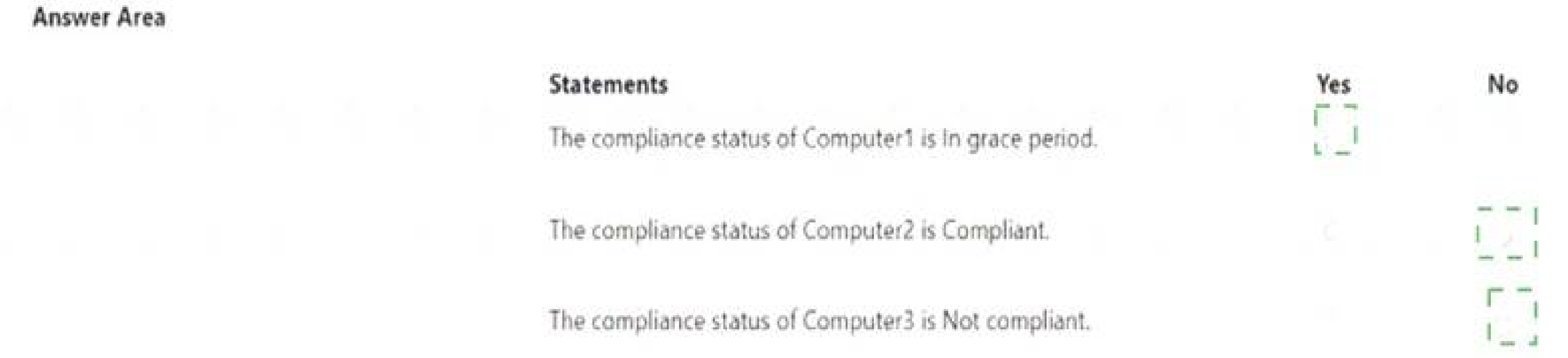
Answer Area

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

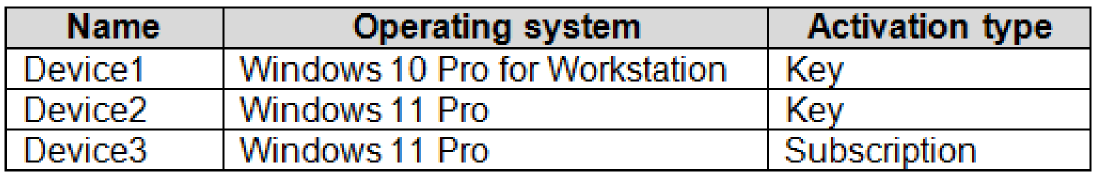
Explanation:



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 191
- (Exam Topic 4)
You have a Microsoft 365 subscription that uses Microsoft Intune Suite. You use Microsoft Intune to manage devices.
You have the devices shown in the following table.



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

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

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

Answer: A

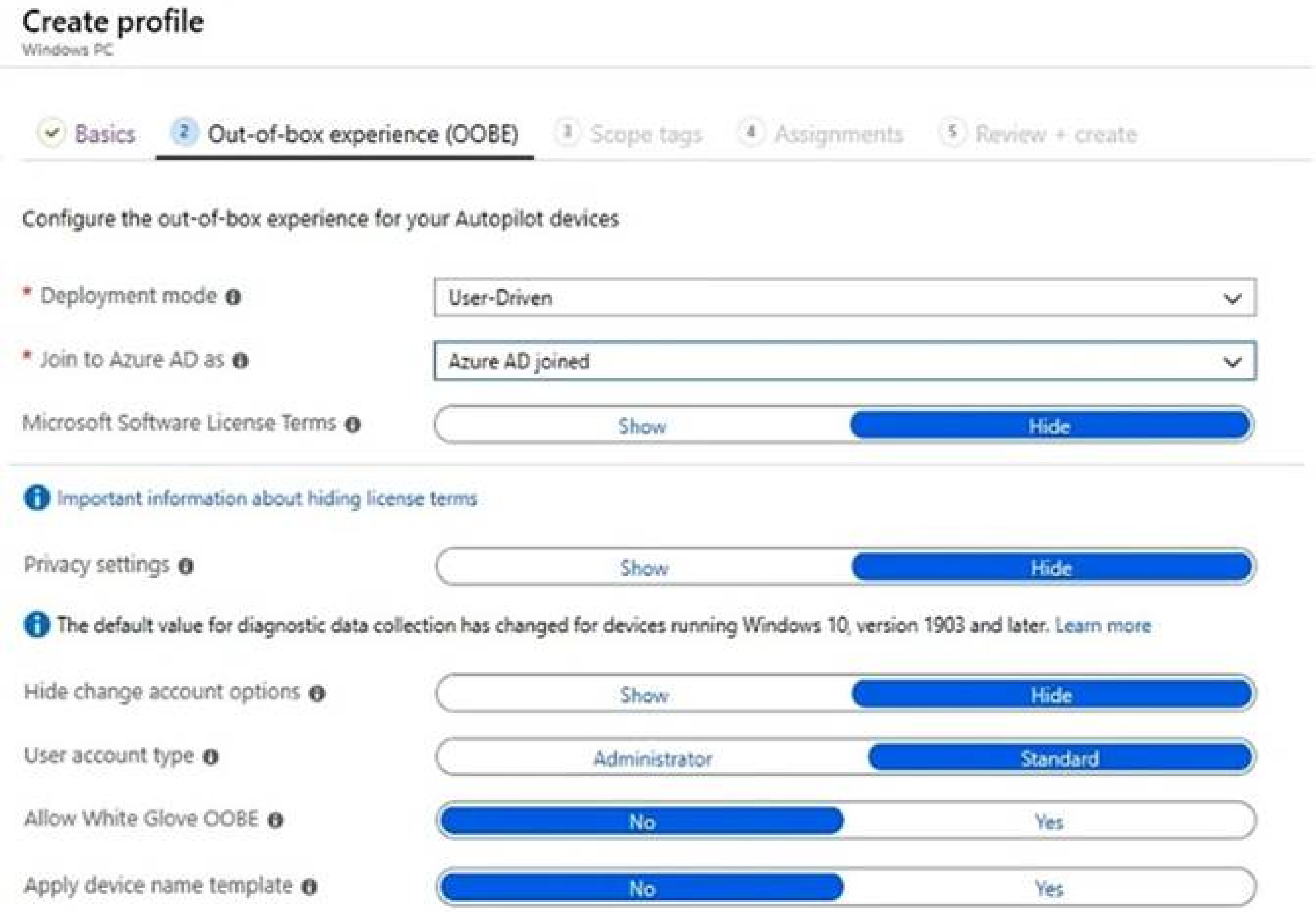
NEW QUESTION 195
- (Exam Topic 4)

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

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

Answer: B

NEW QUESTION 197
- (Exam Topic 4)
You have a hybrid Azure AD tenant.
You configure a Windows Autopilot deployment profile as shown in the following exhibit.



Create profile
Windows PC

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

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

* Deployment mode: User-Driven
* Join to Azure AD as: Azure AD joined
Microsoft Software License Terms: Show [✓ Hide]

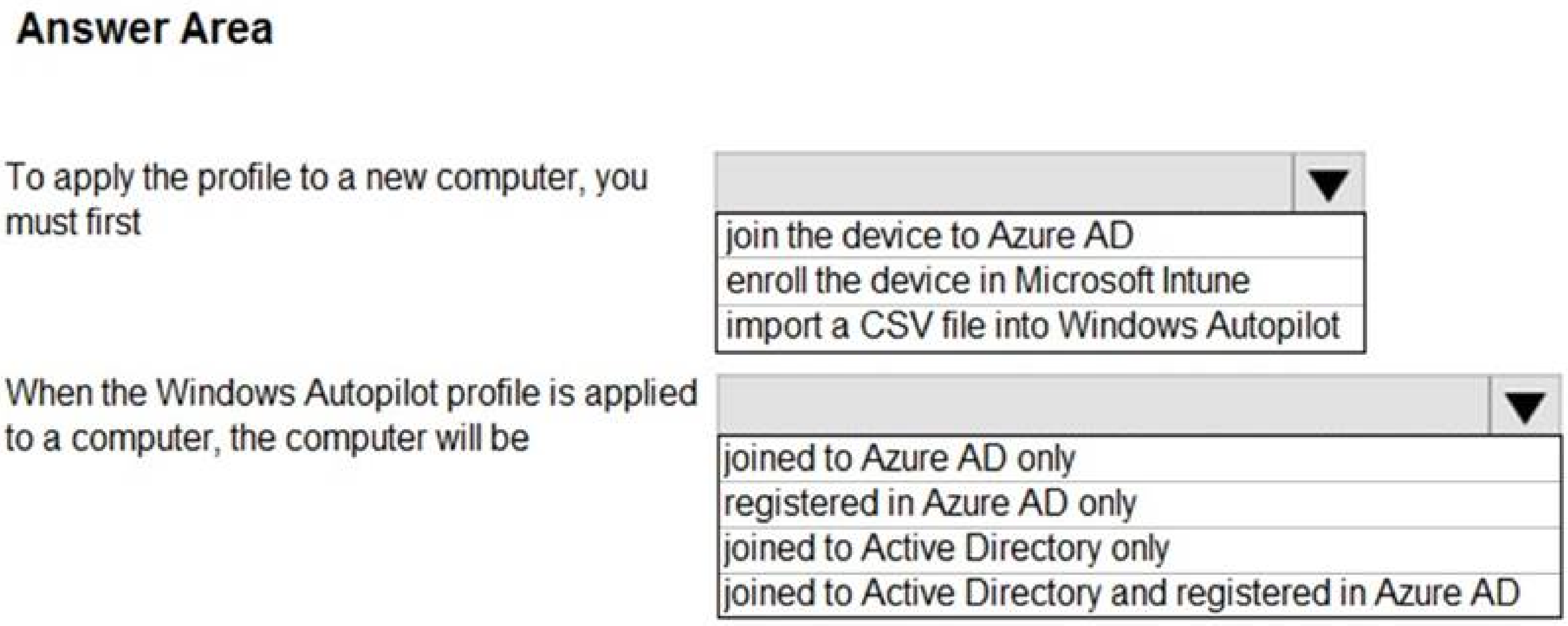
Important information about hiding license terms

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
Apply device name template: [✓ No] Yes

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



Answer Area

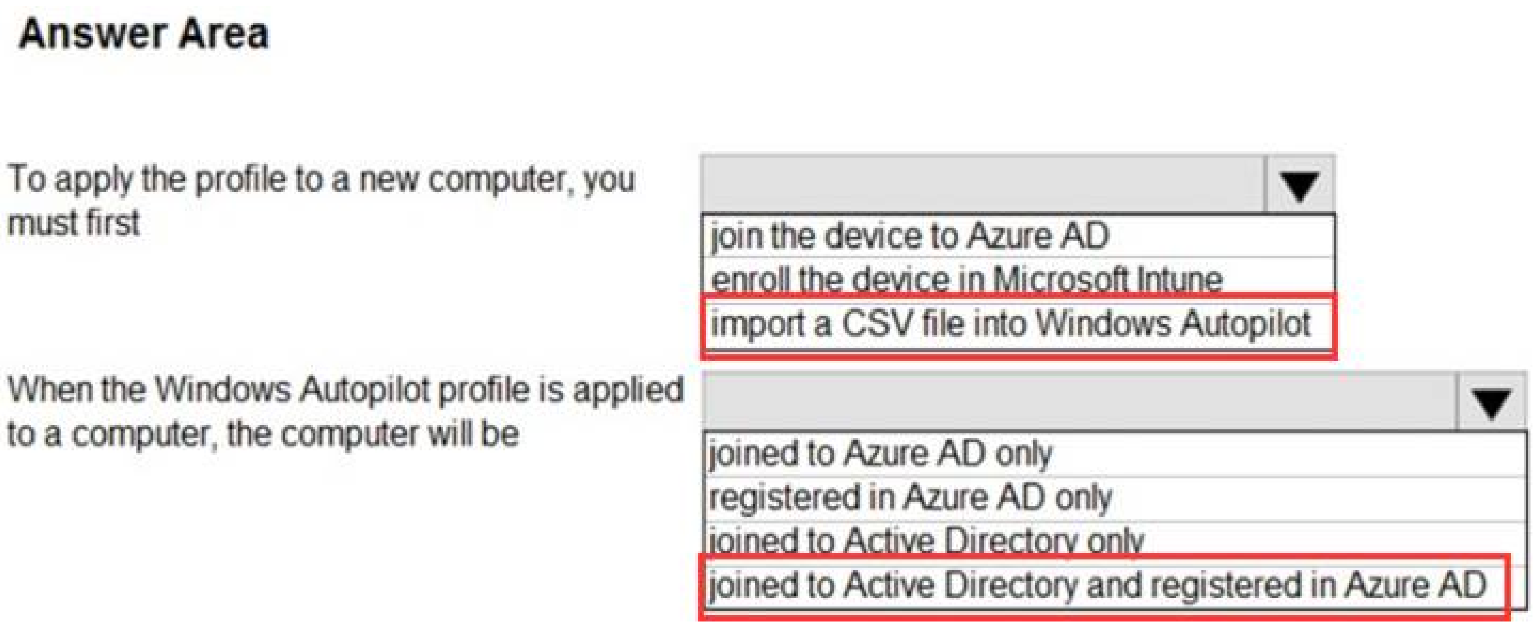
To apply the profile to a new computer, you must first
- join the device to Azure AD
- enroll the device in Microsoft Intune
- import a CSV file into Windows Autopilot

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

A. Mastered
B. Not Mastered

Answer: A

Explanation:



Answer Area

To apply the profile to a new computer, you must first

- join the device to Azure AD
- enroll the device in Microsoft Intune
- [✓ import a CSV file into Windows Autopilot]

When the Windows Autopilot profile is applied to a computer, the computer will be

- joined to Azure AD only
- registered in Azure AD only
- joined to Active Directory only
- [✓ joined to Active Directory and registered in Azure AD]

NEW QUESTION 199
- (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 200
- (Exam Topic 4)
You have a Microsoft 365 subscription.
You need provide a user the ability to disable Security defaults and principle of least privilege. Which role should you assign to the user?

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

Answer: B

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

NEW QUESTION 202
......