Microsoft.MD-102.vApr-2024.by.QuiangLee.141q

Number: MD-102
Passing Score: 800
Time Limit: 120
File Version: 12.0

Exam Code: MD-102

Exam Name: Endpoint Administrator

Case 01 - Contoso

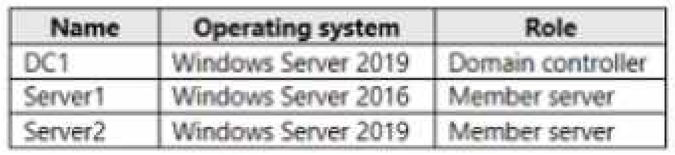
Overview

Contoso, Ltd. is a consulting company that has a main office in Montreal and branch offices in Seattle and New York.

Contoso has a Microsoft 365 E5 subscription.

Network Environment

The network contains an on-premises Active domain named Contoso.com. The domain contains theservers shown in the following table.



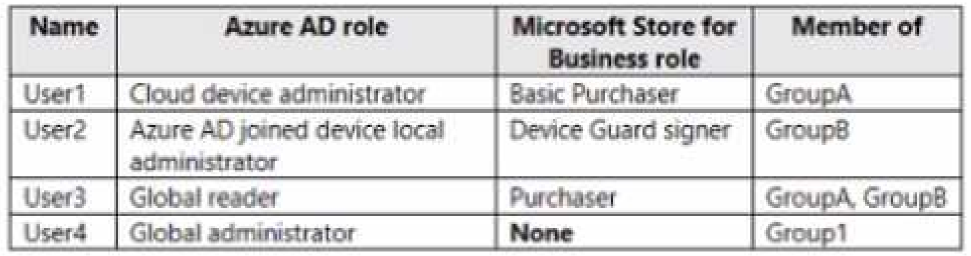
Name	Operating system	Role
DC1	Windows Server 2019	Domain controller
Server1	Windows Server 2016	Member server
Server2	Windows Server 2019	Member server

Contoso has a hybrid Azure Active Directory (Azure AD) tenant named Contoso.com.

Contoso has a Microsoft Store for Business instance.

Users and Groups

The Contoso.com tenant contains the users shown in the following table.



Name	Azure AD role	Microsoft Store for Business role	Member of
User1	Cloud device administrator	Basic Purchaser	GroupA
User2	Azure AD joined device local administrator	Device Guard signer	GroupB
User3	Global reader	Purchaser	GroupA, GroupB
User4	Global administrator	**None**	Group1

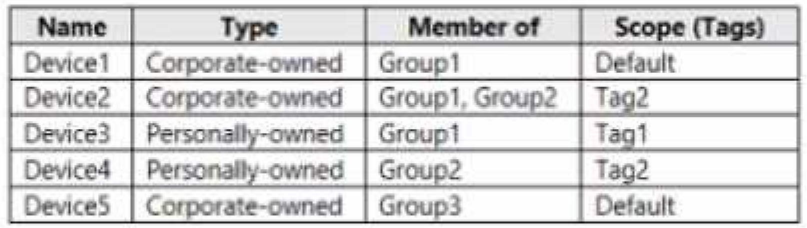
All users are assigned a Microsoft Office 365 license and an Enterprise Mobility + Security E3 lic

Enterprise State Roaming is enabled for Group1 and GroupA.

Group and Group have a Membership type of Assign

Devices

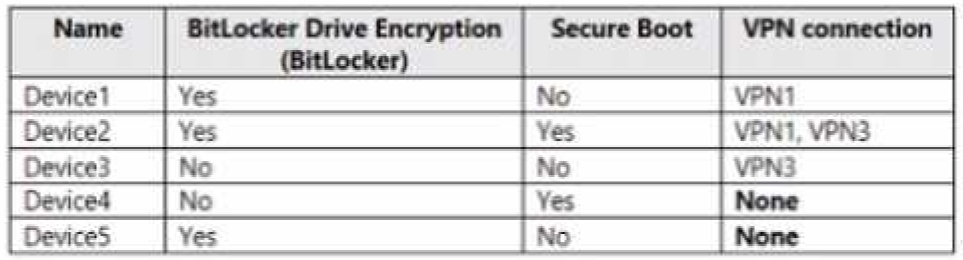
Contoso has the Windows 10 devices shown in the following table.



Name	Type	Member of	Scope (Tags)
Device1	Corporate-owned	Group1	Default
Device2	Corporate-owned	Group1, Group2	Tag2
Device3	Personally-owned	Group1	Tag1
Device4	Personally-owned	Group2	Tag2
Device5	Corporate-owned	Group3	Default

The Windows 10 devices are joined to Azure AD and enrolled in Microsoft intune.

The Windows 10 devices are configured as shown in the following table.



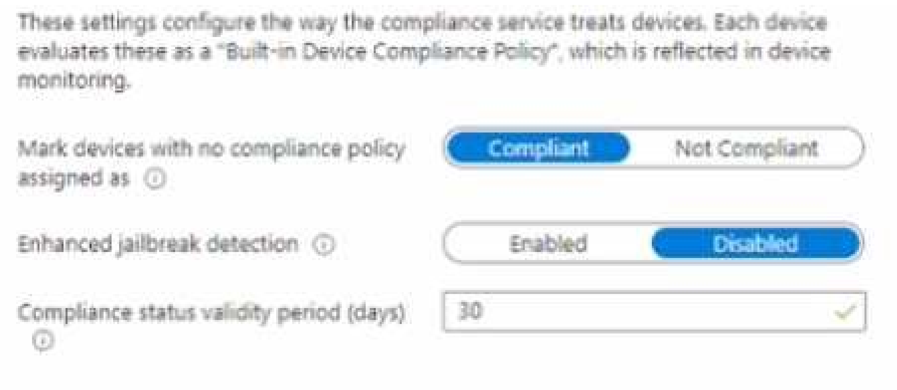
Name	BitLocker Drive Encryption (BitLocker)	Secure Boot	VPN connection
Device1	Yes	No	VPN1
Device2	Yes	Yes	VPN1, VPN3
Device3	No	No	VPN3
Device4	No	Yes	**None**
Device5	Yes	No	**None**

All the Azure AD joined devices have an executable file named C:\AppA.exe and a folder D:\Folder 1.

Microsoft Endpoint Manager Configuration

Microsoft Endpoint Manager has the compliance policies shown in the following table.

The Compliance policy settings are 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 ✓

The Automatic Enrolment settings have the following configurations:

• MDM user scope GroupA

• MAM user scope: GroupB

You have an Endpoint protection configuration profile that has the following Controlled folder access settings:

• Name: Protection1

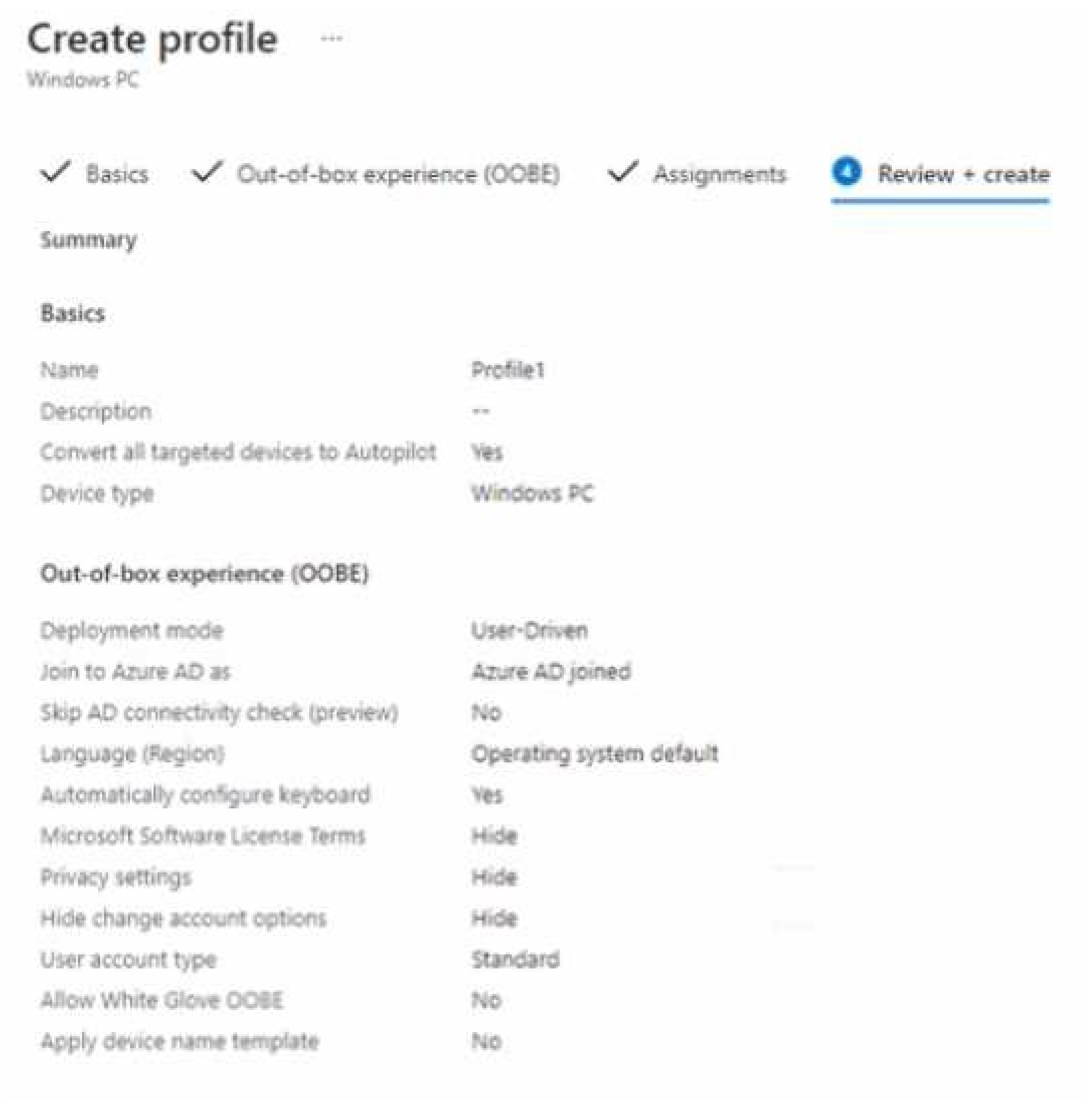
• Folder protection: Enable

• List of apps that have access to protected folders: CV\AppA.exe

• List of additional folders that need to be protected: D:\Folderi1

• Assignments

Windows Autopilot Configuration



Create profile ...

Windows PC

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

Summary

Basics

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

Out-of-box experience (OOBE)

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

Currently, there are no devices deployed by using Window Autopilot

The Intune connector tor Active Directory is installed on Server 1.

Planned Changes

Contoso plans to implement the following changes:

- Purchase a new Windows 10 device named Device6 and enroll the device in Intune.
- New computers will be deployed by using Windows Autopilot and will be hybrid Azure AO joined.
- Deploy a network boundary configuration profile that will have the following settings:
- Name Boundary 1
- Network boundary 192.168.1.0/24
- Scope tags: Tag 1
- Assignments;
- included groups: Group 1. Group2
- Deploy two VPN configuration profiles named Connection1 and Connection that will have the following settings:
- Name: Connection 1
- Connection name: VPNI

- Connection type: L2TP
- Assignments:
- Included groups: Group1. Group2, GroupA
- Excluded groups: —
- Name: Connection
- Connection name: VPN2
- Connection type: IKEv2 i Assignments:
- included groups: GroupA
- Excluded groups: GroupB
- Purchase an app named App1 that is available in Microsoft Store for Business and to assign the app

to all the users.

Technical Requirements

Contoso must meet the following technical requirements:

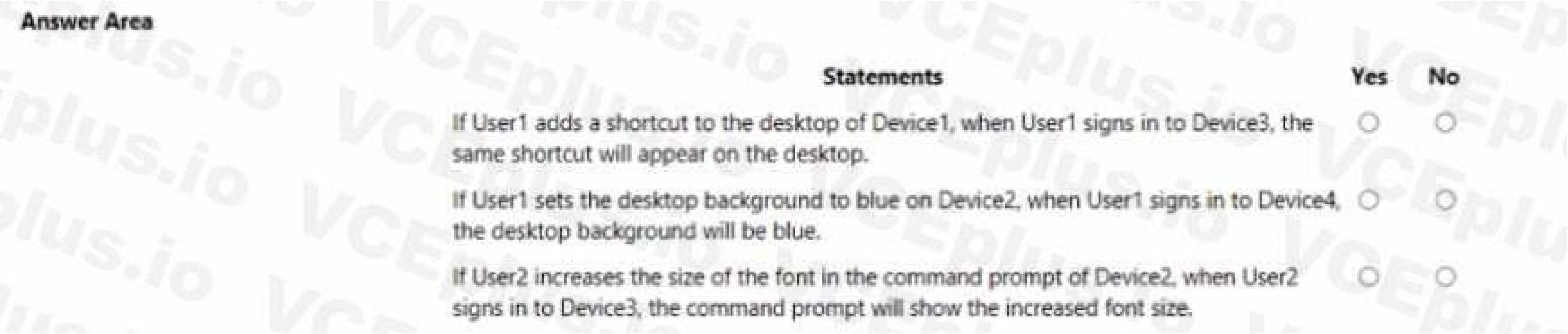
- Users in GroupA must be able to deploy new computers.
- Administrative effort must be minimized.

QUESTION 1

HOTSPOT

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

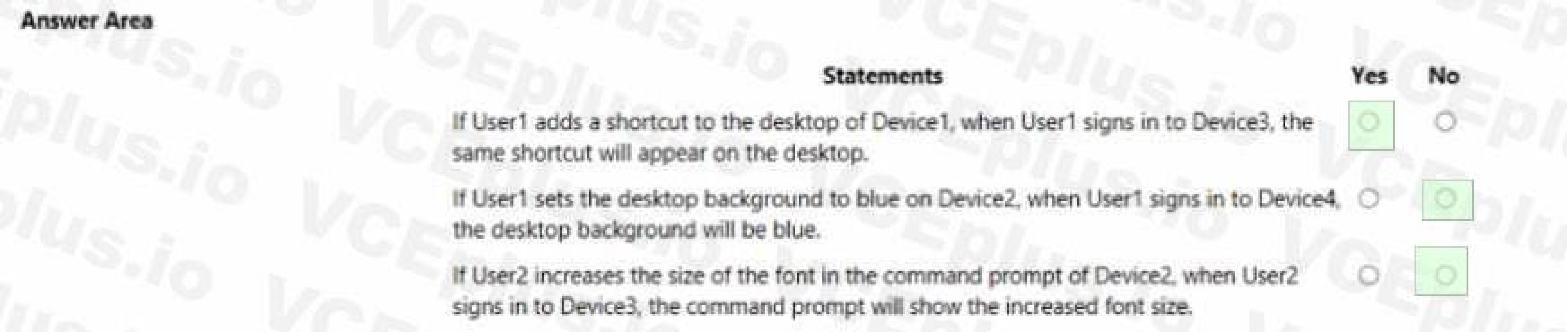
Hot Area:



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.	○	○

Answer Area:



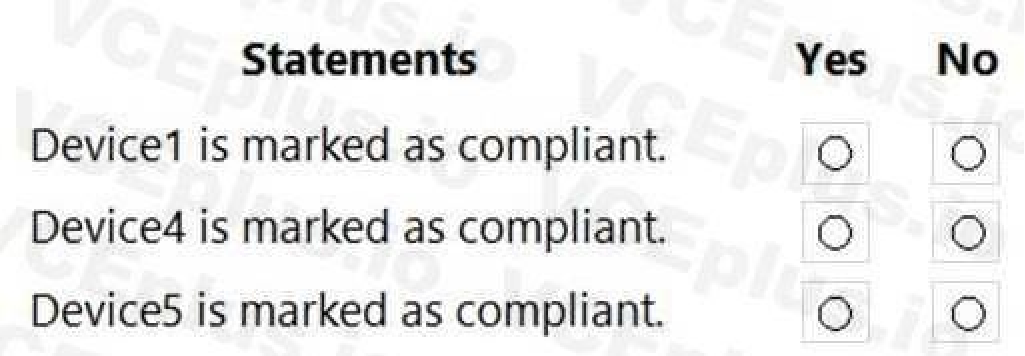
Answer Area

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.	○	[✓ ○]

Section:
Explanation:

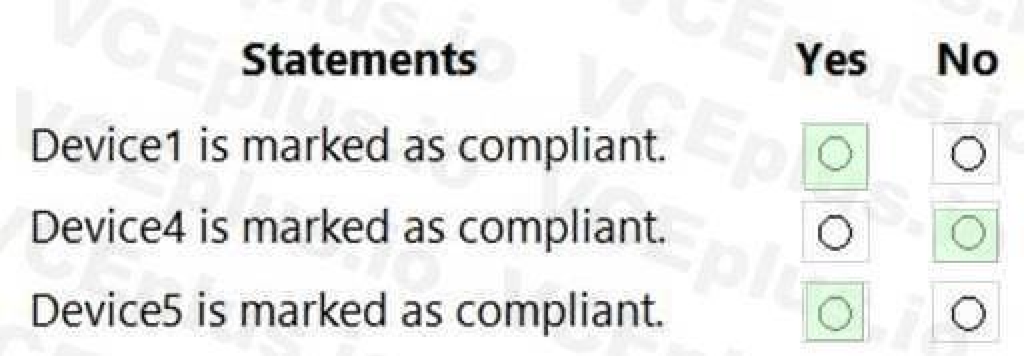
QUESTION 2
HOTSPOT
For each of the following statements, select Yes if the statement is true. Otherwise, select No.
NOTE: Each correct selection is worth one point.

Hot Area:



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

Answer Area:



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

Section:
Explanation:

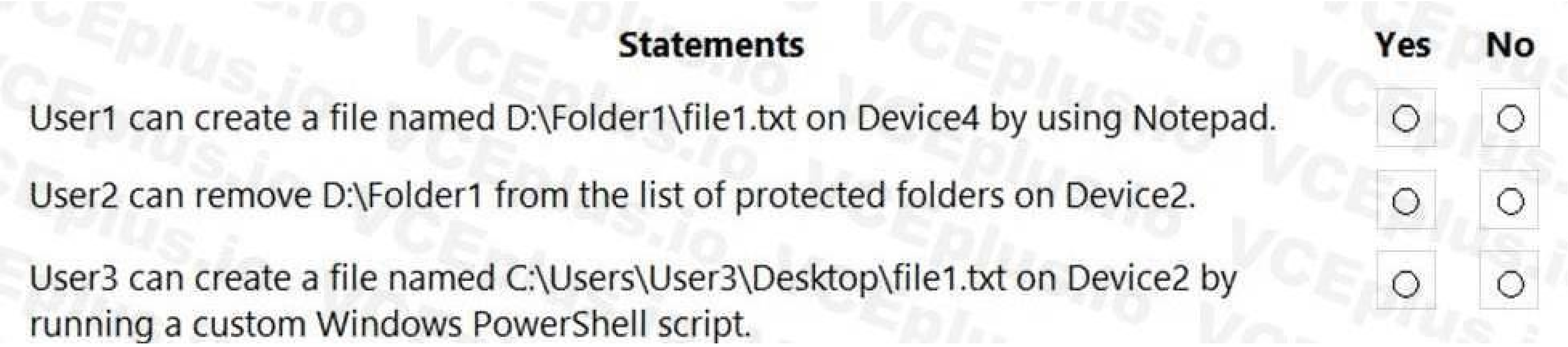
QUESTION 3
Which user can enroll Device6 in Intune?

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

Correct Answer: C
Section:

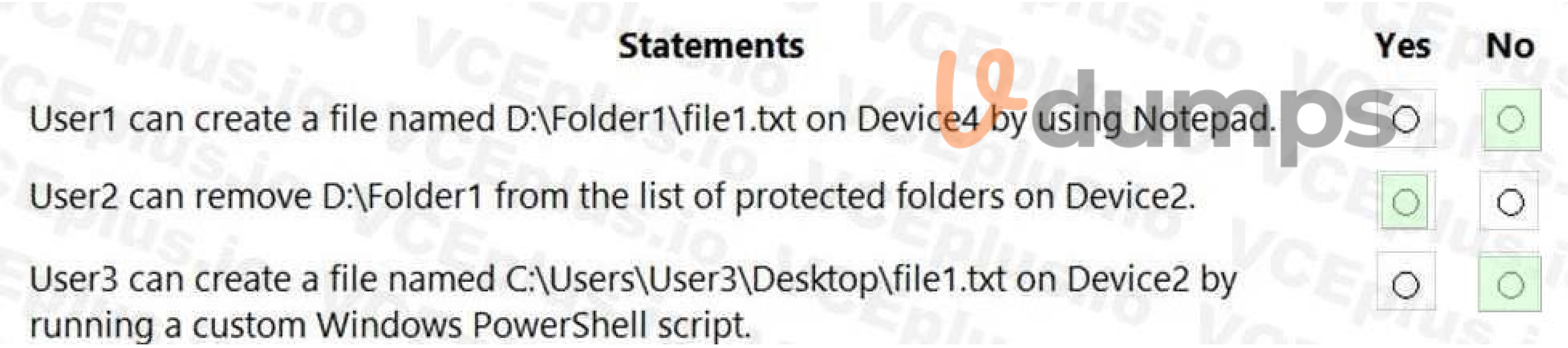
QUESTION 4
HOTSPOT
For each of the following statements, select Yes if the statement is true. Otherwise, select No.
NOTE: Each correct selection is worth one point.

Hot Area:



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.	○	○

Answer Area:



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.	○	[✓ ○]

Section:
Explanation:

QUESTION 5
You implement Boundary1 based on the planned changes.
Which devices have a network boundary of 192.168.1.0/24 applied?

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

Correct Answer: D
Section:
Explanation:
Reference:

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

QUESTION 6

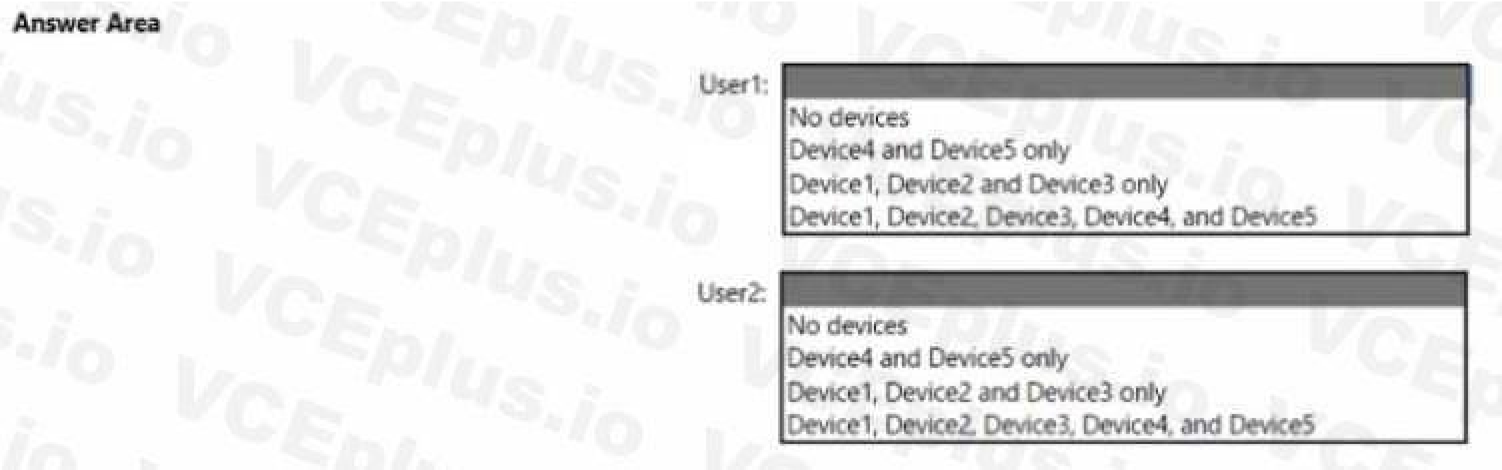
HOTSPOT

User1 and User2 plan to use Sync your settings.

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

NOTE: Each correct selection is worth one point.

Hot Area:

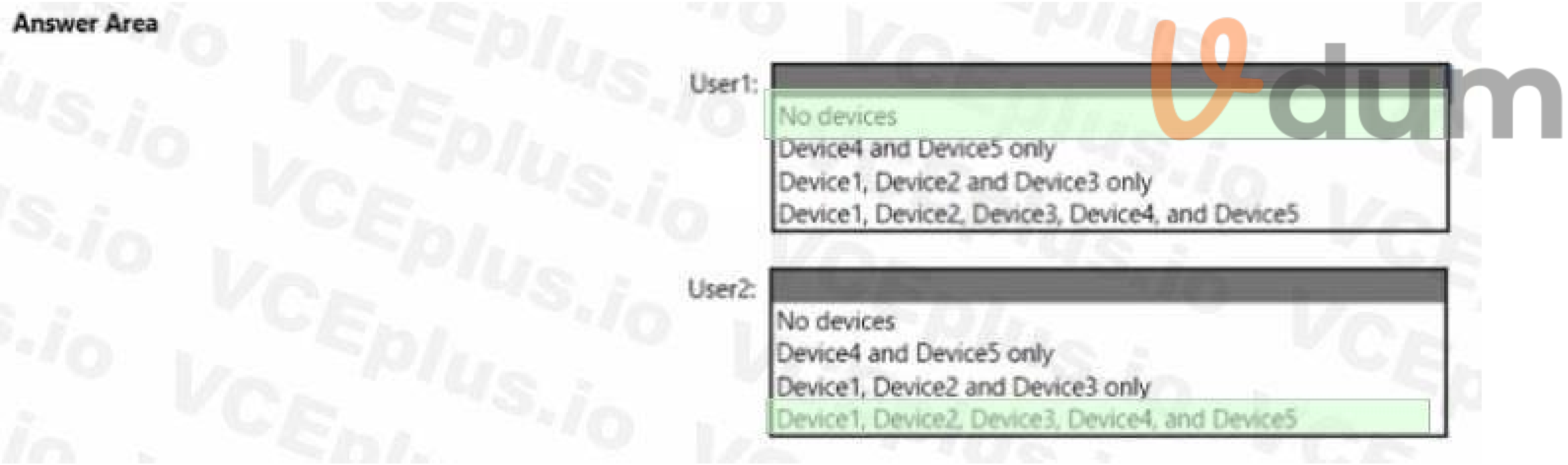


Answer Area

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

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

Answer Area:



Answer Area

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

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

Section:

Explanation:

Reference:

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

QUESTION 7

You need to ensure that computer objects can be created as part of the Windows Autopilot deployment. The solution must meet the technical requirements.

To what should you grant the right to create the computer objects?

A. Server2

B. Server1

C. GroupA

D. DC1

Correct Answer: C
Section:
Explanation:

QUESTION 8

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

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

Correct Answer: C
Section:
Explanation:
Scenario: Windows Autopilot Configuration
Assignments
Included groups: Group1
Excluded groups: Group2
Device1 is member of Group1.
Device2 is member of Group1 and member of Group2.
Device3 is member of Group1.
Group1 and Group2 have a Membership type of Assigned.
Exclusion takes precedence over inclusion in the following same group type scenarios.
Reference: https://learn.microsoft.com/en-us/mem/intune/apps/apps-inc-exl-assignments

Case 02 - Azure DevOps

This is a case study. Case studies are not timed separately. You can use as much exam time as you would like to complete each case. However, there may be additional case studies and sections on this exam. You must manage your time to ensure that you are able to complete all questions included on this exam in the time provided.

To answer the questions included in a case study, you will need to reference information that is provided in the case study. Case studies might contain exhibits and other resources that provide more information about the scenario that is described in the case study. Each question is independent of the other questions in this case study.

At the end of this case study, a review screen will appear. This screen allows you to review your answers and to make changes before you move to the next section of the exam. After you begin a new section, you cannot return to this section.

To start the case study

To display the first question in this case study, click the Next button. Use the buttons in the left pane to explore the content of the case study before you answer the questions. Clicking these buttons displays information such as business requirements, existing environment, and problem statements.

When you are ready to answer a question, click the Question button to return to the question.

Existing Environment

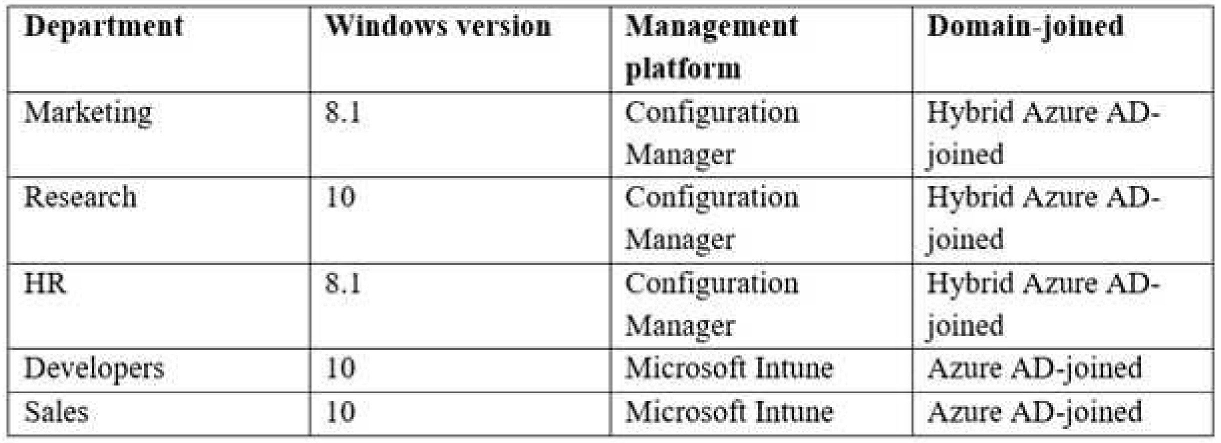
Current Business Model

The Los Angeles office has 500 developers. The developers work flexible hours ranging from 11:00 to 22:00. Litware has a Microsoft System Center 2012 R2 Configuration Manager deployment. During discovery, the company discovers a process where users are emailing bank account information of its customers to internal and external recipients.

Current Environment

The network contains an Active Directory domain that is synced to Microsoft Azure Active Directory (Azure AD). The functional level of the forest and the domain is Windows Server 2012 R2. All domain controllers run Windows Server 2012 R2.

Litware has the computers shown in the following table.



Department	Windows version	Management platform	Domain-joined
Marketing	8.1	Configuration Manager	Hybrid Azure AD-joined
Research	10	Configuration Manager	Hybrid Azure AD-joined
HR	8.1	Configuration Manager	Hybrid Azure AD-joined
Developers	10	Microsoft Intune	Azure AD-joined
Sales	10	Microsoft Intune	Azure AD-joined

The development department uses projects in Azure DevOps to build applications.

Most of the employees in the sales department are contractors. Each contractor is assigned a computer that runs Windows 10. At the end of each contract, the computer is assigned to different contractor. Currently, the computers are re-provisioned manually by the IT department.

Problem Statements

Litware identifies the following issues on the network:

Employees in the Los Angeles office report slow Internet performance when updates are downloading. The employees also report that the updates frequently consume considerable resources when they are installed. The Update settings are configured as shown in the Updates exhibit. (Click the Updates button.)

Management suspects that the source code for the proprietary applications in Azure DevOps in being shared externally.

Re-provisioning the sales department computers is too time consuming.

Requirements

Business Goals

Litware plans to transition to co-management for all the company-owned Windows 10 computers.

Whenever possible, Litware wants to minimize hardware and software costs.

Device Management Requirements

Litware identifies the following device management requirements:

Prevent the sales department employees from forwarding email that contains bank account information.

Ensure that Microsoft Edge Favorites are accessible from all computers to which the developers sign in.

Prevent employees in the research department from copying patented information from trusted applications to untrusted applications.

Technical Requirements

Litware identifies the following technical requirements for the planned deployment:

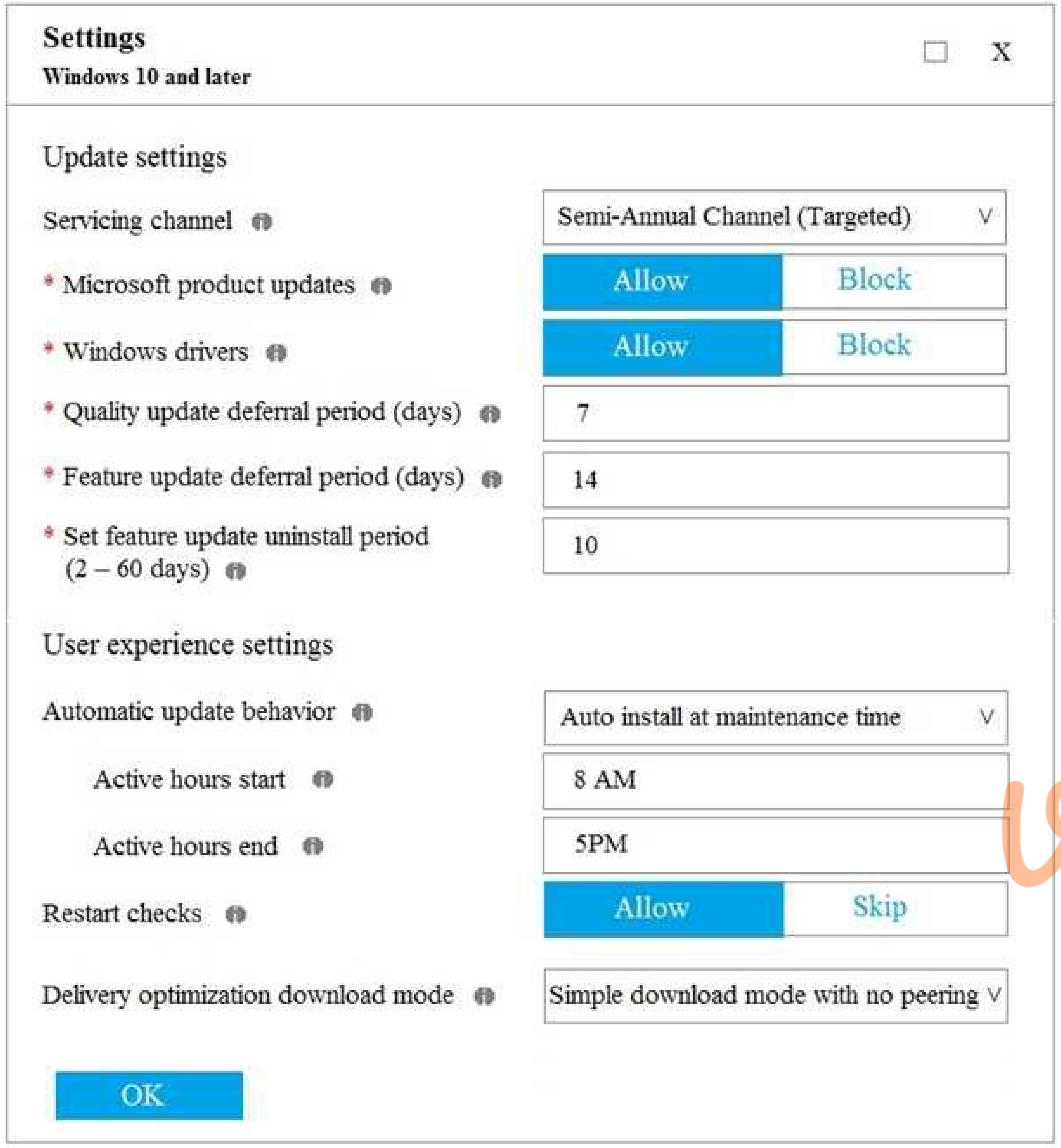
Re-provision the sales department computers by using Windows AutoPilot.

Ensure that the projects in Azure DevOps can be accessed from the corporate network only.

Ensure that users can sign in to the Azure AD-joined computers by using a PIN. The PIN must expire every 30 days.

Ensure that the company name and logo appears during the Out of Box Experience (OOBE) when using Windows AutoPilot.

Exhibits



Settings
Windows 10 and later

Update settings

Servicing channel: Semi-Annual Channel (Targeted)

* Microsoft product updates: [✓ Allow] Block

* Windows drivers: [✓ Allow] Block

* Quality update deferral period (days): 7

* Feature update deferral period (days): 14

* Set feature update uninstall period (2 – 60 days): 10

User experience settings

Automatic update behavior: Auto install at maintenance time

Active hours start: 8 AM

Active hours end: 5PM

Restart checks: [✓ Allow] Skip

Delivery optimization download mode: Simple download mode with no peering

QUESTION 1
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)

Correct Answer: B
Section:
Explanation:
Reference:

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

QUESTION 2
You need to meet the device management requirements for the developers.
What should you implement?

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

Correct Answer: B
Section:
Explanation:
Litware identifies the following device management requirements:
Ensure that Microsoft Edge Favorites are accessible from all computers to which the developers sign in.
Enterprise State Roaming allows for the synchronization of Microsoft Edge browser setting, including favorites and reading list, across devices.
Reference:
https://docs.microsoft.com/en-us/azure/active-directory/devices/enterprise-state-roamingwindows-settings-reference

QUESTION 3
You need to capture the required information for the sales department computers to meet the technical requirements.
Which Windows PowerShell command should you run first?

A. Install-Module WindowsAutoPilotIntune
B. Install-Script Get-WindowsAutoPilotInfo
C. Import-AutoPilotCSV
D. Get-WindowsAutoPilotInfo

Correct Answer: B
Section:
Explanation:
Reference:
https://docs.microsoft.com/en-us/windows/deployment/windows-autopilot/existing-devices "This topic describes how to convert Windows 7 or Windows 8.1 domain-joined computers to Windows 10 devices joined to either Azure Active Directory or Active Directory (Hybrid Azure AD
Join) by using Windows Autopilot"

QUESTION 4
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

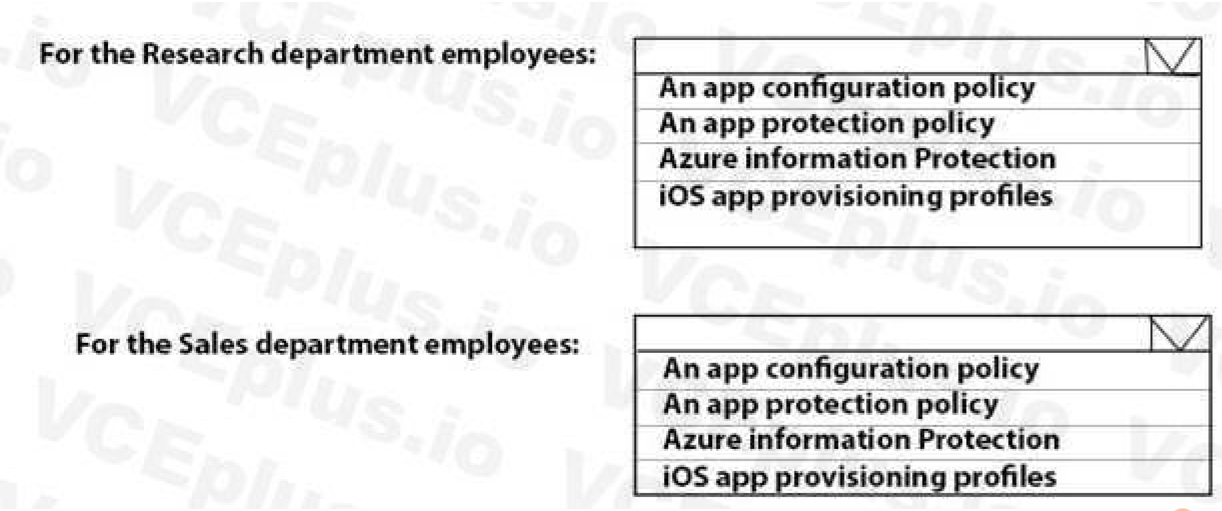
Correct Answer: C
Section:
Explanation:

Reference:
https://docs.microsoft.com/en-us/azure/devops/organizations/accounts/manage-conditionalaccess?view=azure-devops

QUESTION 5

HOTSPOT
You need to recommend a solution to meet the device management requirements.
What should you include in the recommendation? To answer, select the appropriate options in the answer area.
NOTE: Each correct selection is worth one point.

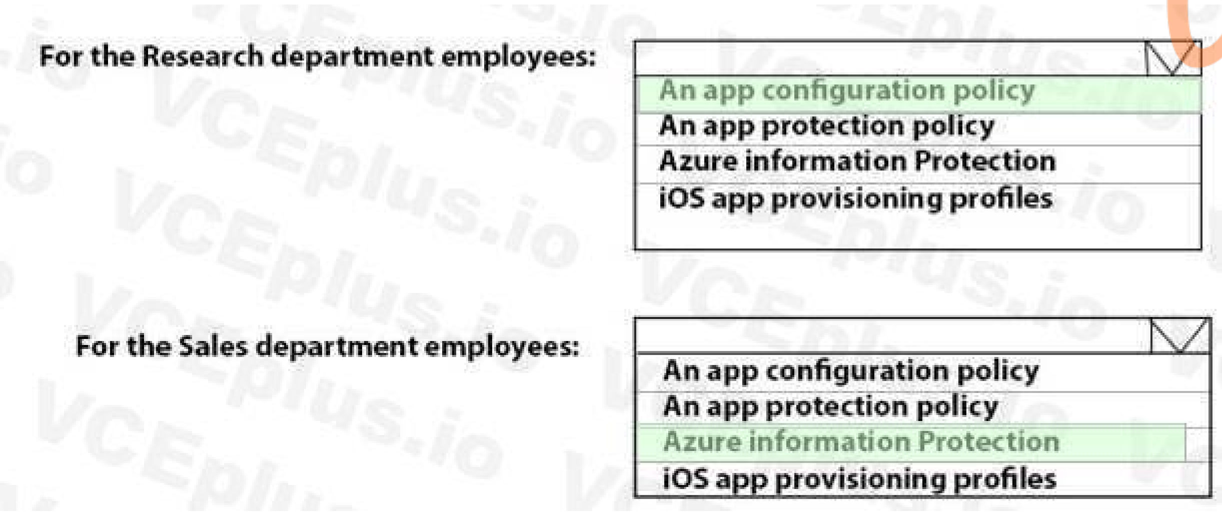
Hot Area:



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

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

Answer Area:



For the Research department employees:
- [✓ An app configuration policy]
- An app protection policy
- Azure information Protection
- iOS app provisioning profiles

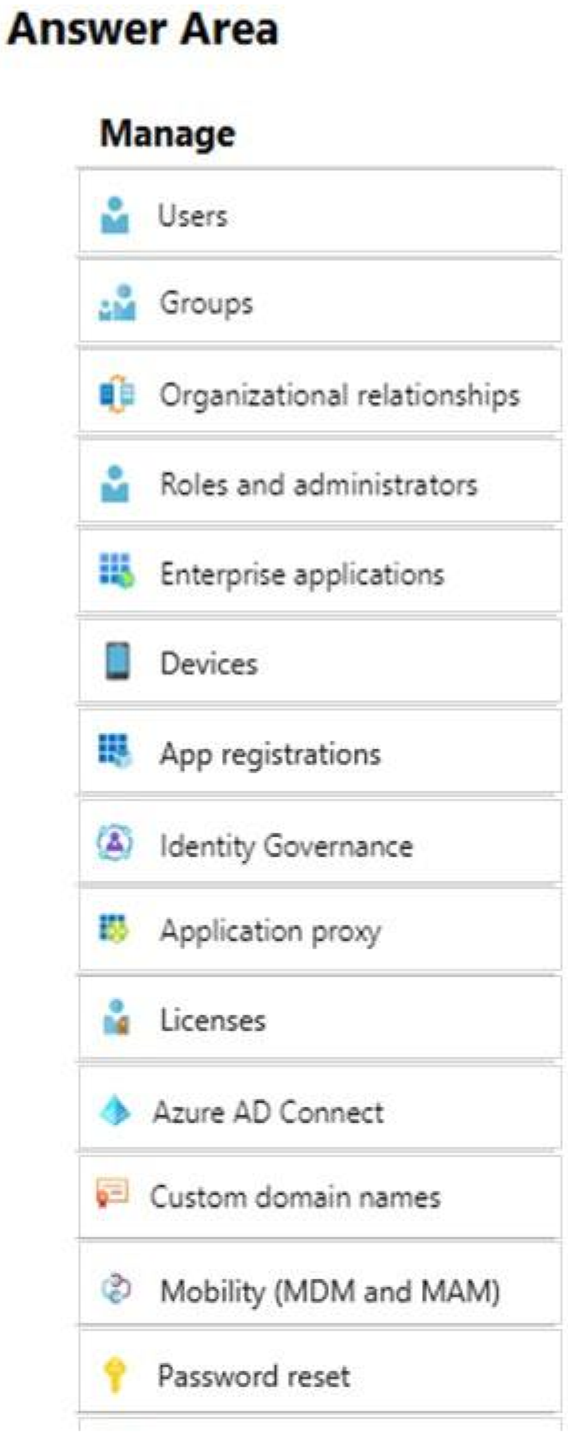
For the Sales department employees:
- An app configuration policy
- An app protection policy
- [✓ Azure information Protection]
- iOS app provisioning profiles

Section:
Explanation:
Reference:
https://github.com/MicrosoftDocs/IntuneDocs/blob/master/intune/app-protection-policy.md
https://docs.microsoft.com/en-us/azure/information-protection/configure-usage-rights#do-notforward-option-for-emails

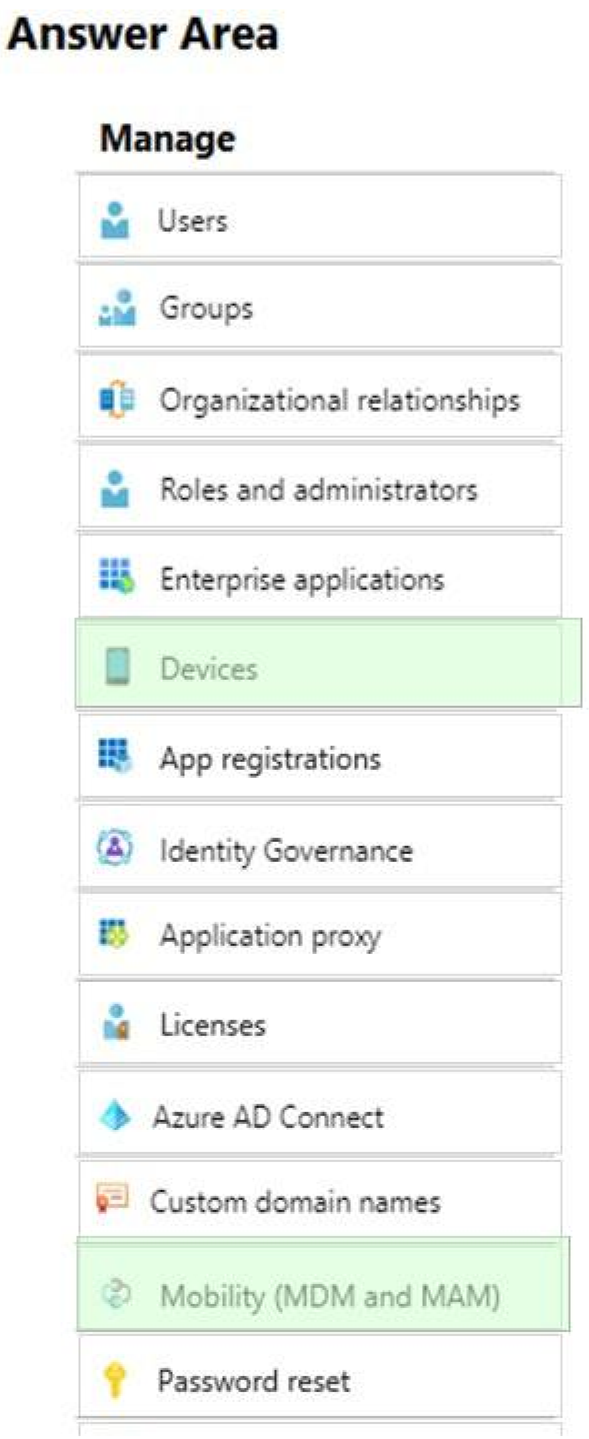
QUESTION 6

HOTSPOT
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.

Hot Area:



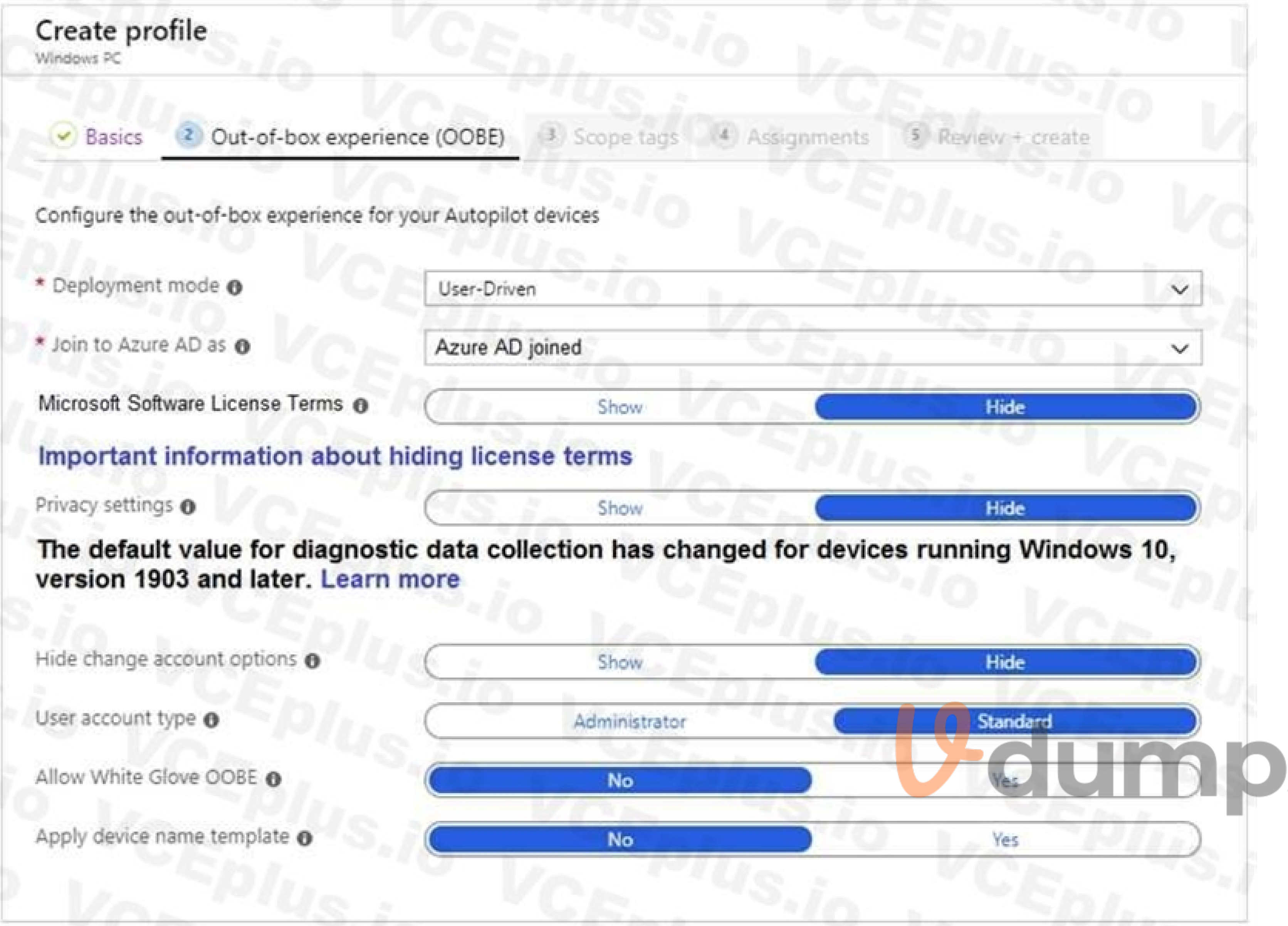
Answer Area:



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

Exam C

QUESTION 1
HOTSPOT
You have a Microsoft Intune subscription.
You are creating a Windows Autopilot deployment profile named Profile1 as shown in the following exhibit.



Create profile

Windows PC

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

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

* Deployment mode: User-Driven

* Join to Azure AD as: Azure AD joined

Microsoft Software License Terms: Show [✓ Hide]

Important information about hiding license terms

Privacy settings: Show [✓ Hide]

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

Hide change account options: Show [✓ Hide]

User account type: Administrator [✓ Standard]

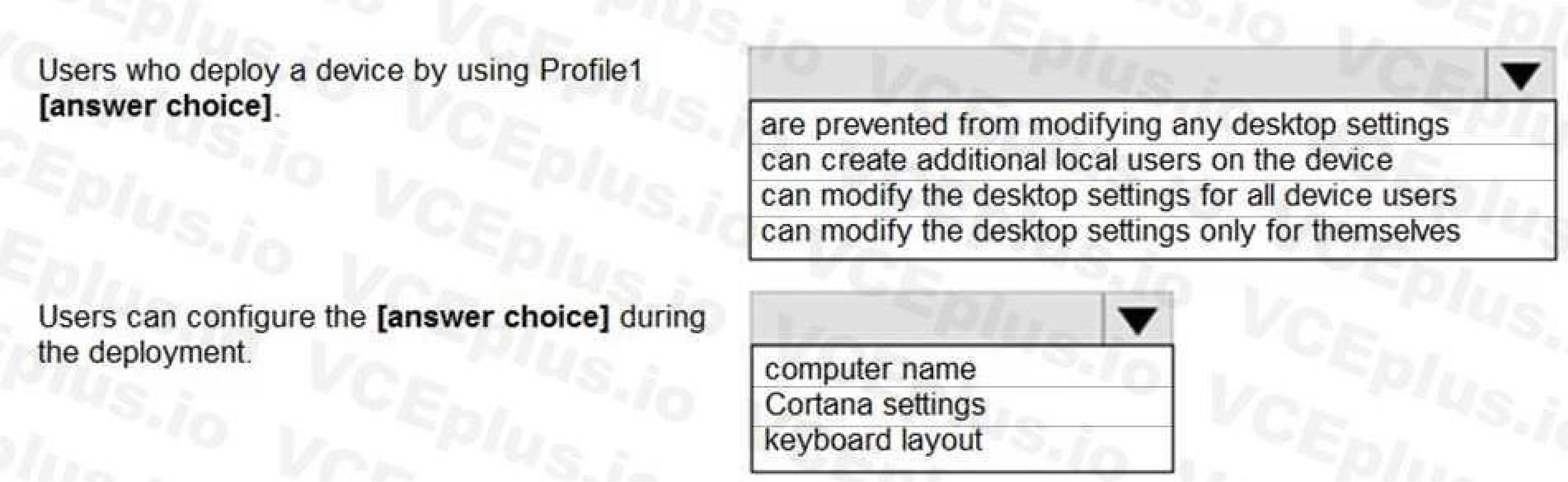
Allow White Glove OOBE: [✓ No] Yes

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.

Hot Area:



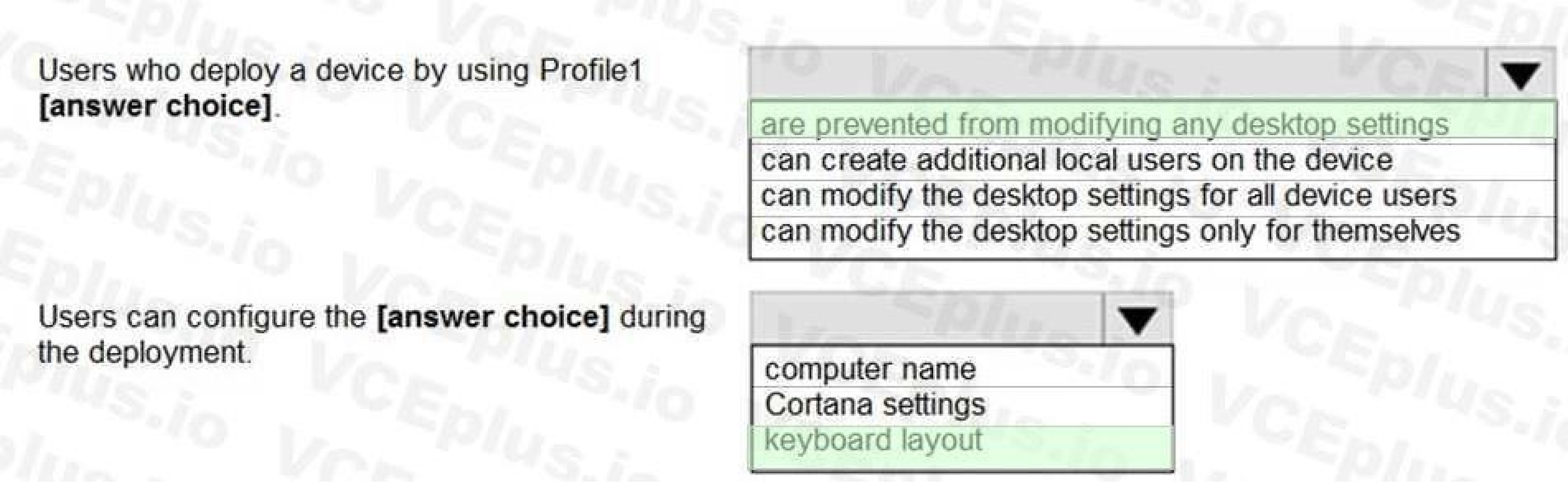
Users who deploy a device by using Profile1 **[answer choice]**.

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

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

- computer name
- Cortana settings
- keyboard layout

Answer Area:



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

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

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

- computer name
- Cortana settings
- keyboard layout

Section:
Explanation:

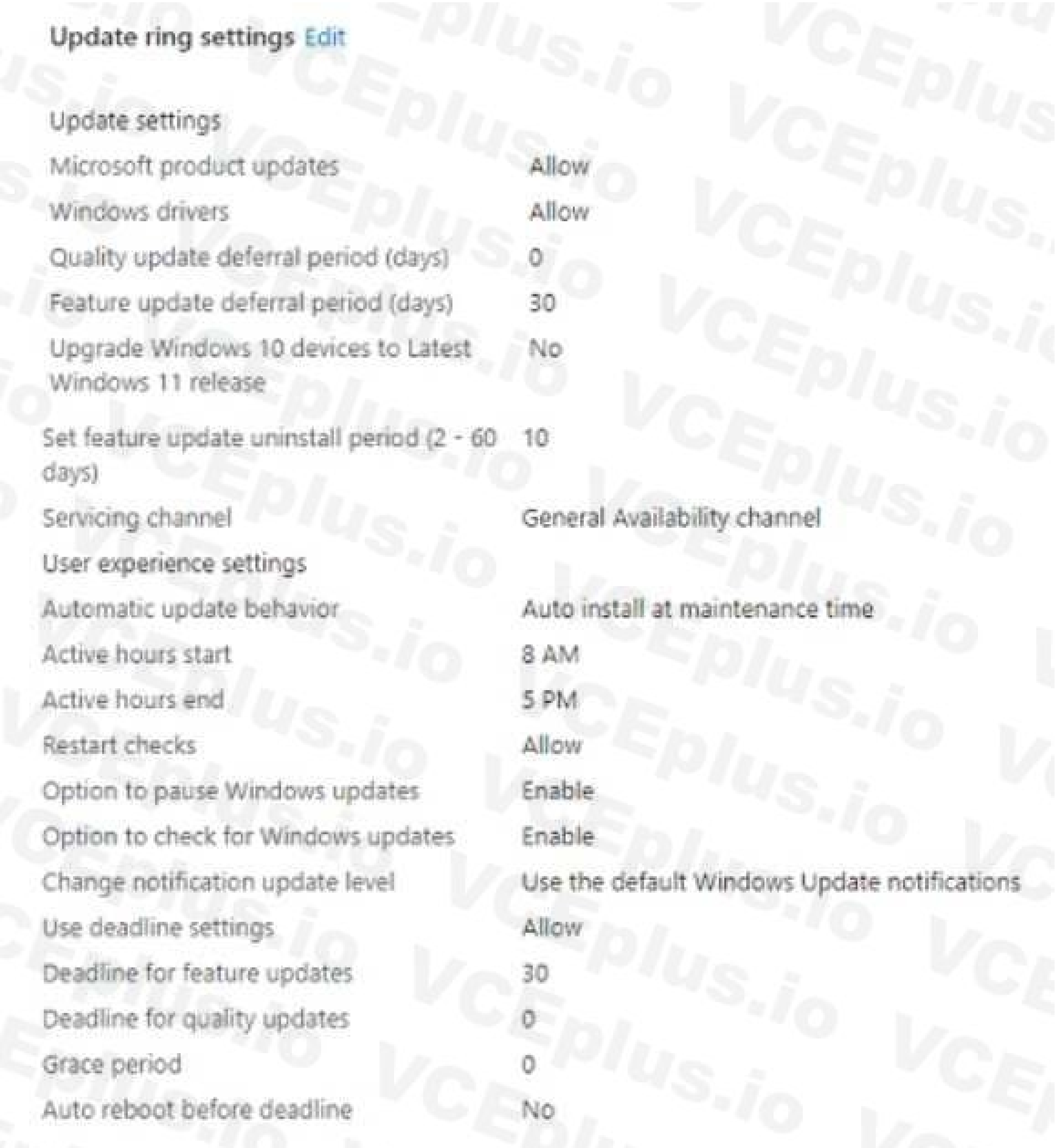
QUESTION 2
Your network contains an Active Directory domain. The domain contains a computer named Computer1 that runs Windows 8.1.
Computer1 has apps that are compatible with Windows 10.
You need to perform a Windows 10 in-place upgrade on Computer1.
Solution: You copy the Windows 10 installation media to a network share. You start Computer1 from Windows PE (WinPE), and then you run setup.exe from the network share.
Does this meet the goal?

A. Yes

B. No

Correct Answer: B
Section:
Explanation:

QUESTION 3
HOTSPOT
You have a Microsoft 365 E5 subscription.
You create a new update rings policy named Policy1 as shown in the following exhibit.



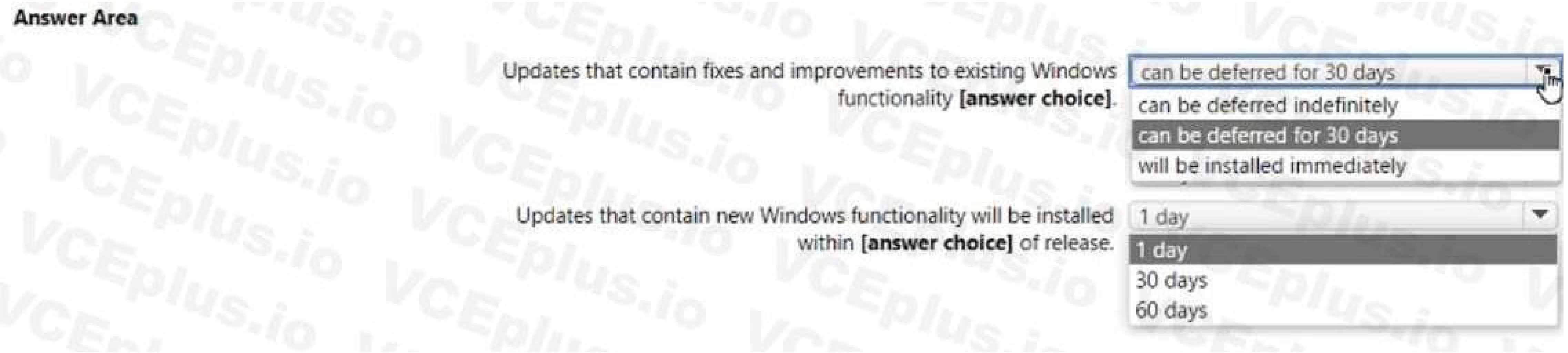
Update ring settings Edit

Update settings	
Microsoft product updates	Allow
Windows drivers	Allow
Quality update deferral period (days)	0
Feature update deferral period (days)	30
Upgrade Windows 10 devices to Latest Windows 11 release	No
Set feature update uninstall period (2 - 60 days)	10
Servicing channel	General Availability channel
User experience settings	
Automatic update behavior	Auto install at maintenance time
Active hours start	8 AM
Active hours end	5 PM
Restart checks	Allow
Option to pause Windows updates	Enable
Option to check for Windows updates	Enable
Change notification update level	Use the default Windows Update notifications
Use deadline settings	Allow
Deadline for feature updates	30
Deadline for quality updates	0
Grace period	0
Auto reboot before deadline	No

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

Answer:

Hot Area:



Answer Area

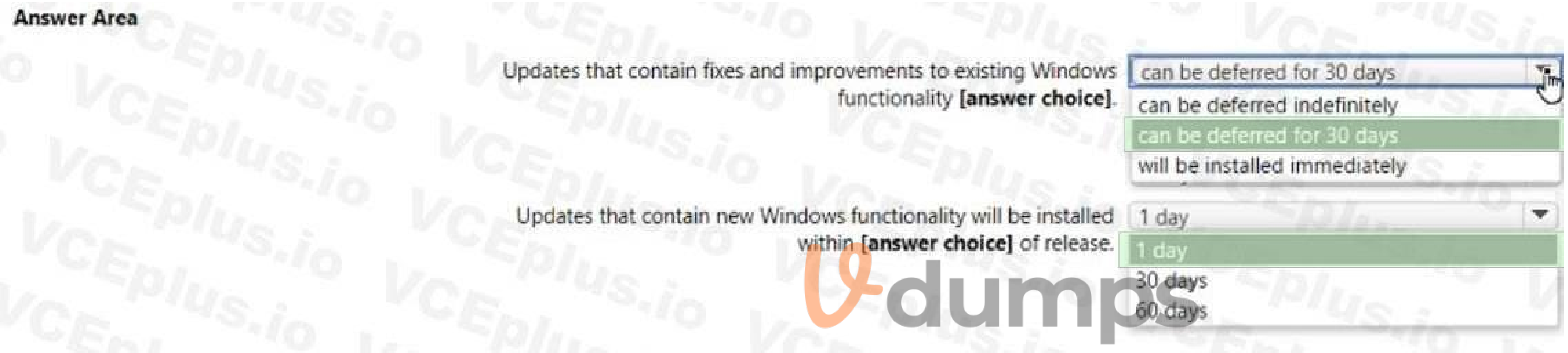
Updates that contain fixes and improvements to existing Windows functionality **[answer choice]**.

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

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

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

Answer Area:



Answer Area

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

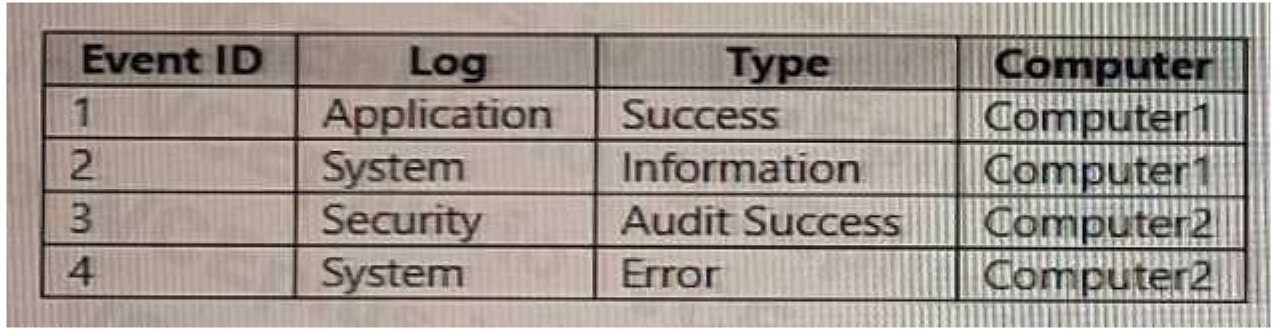
- can be deferred for 30 days
- can be deferred indefinitely
- [✓ can be deferred for 30 days]
- will be installed immediately

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

- 1 day
- [✓ 1 day]
- 30 days
- 60 days

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

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



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

Which events are collected in the Log Analytics workspace?

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

Correct Answer: E
Section:
Explanation:
All events from Windows event logs are collected in the Log Analytics workspace, regardless of the event level or source. Therefore, events 1, 2, 3, and 4 are all collected in the workspace. Reference: https://docs.microsoft.com/en-us/azure/azure-monitor/agents/data-sources-windows-events

QUESTION 5
You have a Microsoft 365 E5 subscription that contains 10 Android Enterprise devices. Each device has a corporate-owned work profile and is enrolled in Microsoft Intune.
You need to configure the devices to run a single app in kiosk mode.
Which Configuration settings should you modify in the device restrictions profile?

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

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

QUESTION 6
You have a Microsoft 365 E5 subscription that contains 500 macOS devices enrolled in Microsoft Intune.
You need to ensure that you can apply Microsoft Defender for Endpoint antivirus policies to the macOS devices. The solution must minimize administrative effort.
What should you do?

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

Correct Answer: C
Section:
Explanation:
To apply Microsoft Defender for Endpoint antivirus policies to the macOS devices, you need to install Defender for Endpoint on the devices. You can use Intune to deploy a script that installs Defender for Endpoint on macOS devices. After installation, you can use Intune to create and assign antivirus policies to the devices. Reference: https://docs.microsoft.com/en-us/windows/security/threatprotection/ microsoft-defender-atp/mac-install-with-intune

QUESTION 7

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.

Correct Answer: C, E
Section:
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. Reference: https://docs.microsoft.com/enus/ mem/intune/protect/endpoint-protection-windows-10

QUESTION 8

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

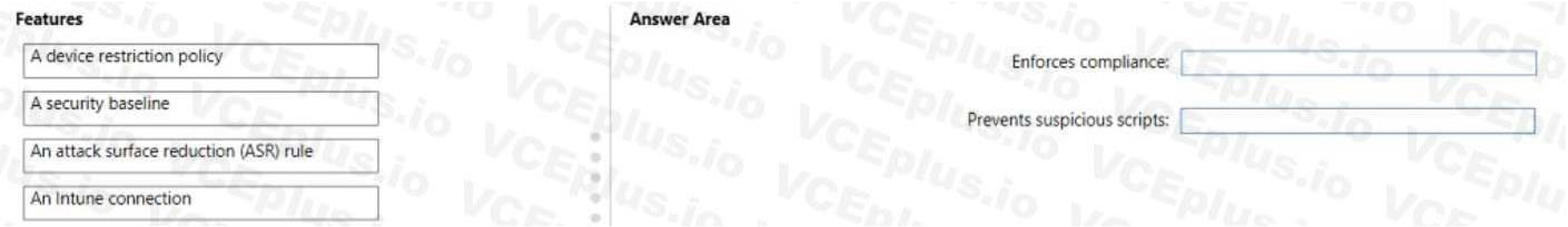
Correct Answer: D
Section:
Explanation:
To ensure that Profile1 applies to Device1 only, you need to modify the Applicability Rules in Profile1.
You can use applicability rules to filter which devices receive a profile based on criteria such as device model, manufacturer, or operating system version.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

QUESTION 9

DRAG DROP
You have a Microsoft 365 subscription that includes Microsoft Intune.
You need to implement a Microsoft Defender for Endpoint solution that meets the following requirements:
- Enforces compliance for Defender for Endpoint by using Conditional Access
- Prevents suspicious scripts from running on devices

What should you configure? To answer, drag the appropriate features to the correct requirements.
Each feature may be used once, more than once, or not at all. You may need to drag the split bar between panes or scroll to view content.
NOTE: Each correct selection is worth one point.

Select and Place:



Features

A device restriction policy

A security baseline

An attack surface reduction (ASR) rule

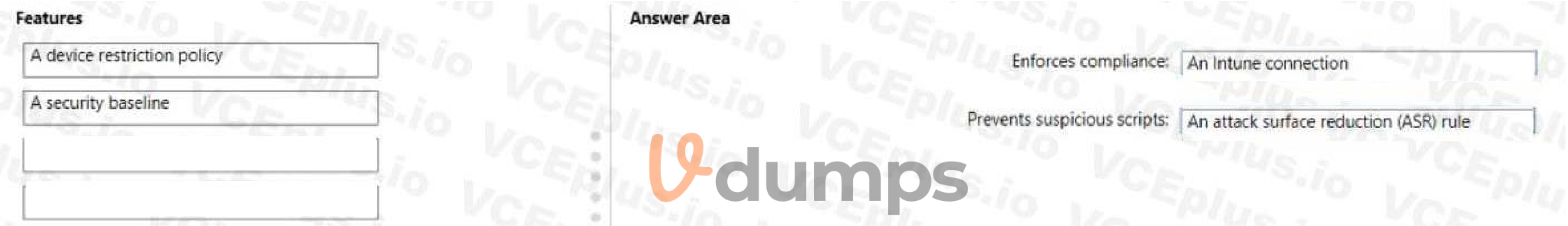
An Intune connection

Answer Area

Enforces compliance:

Prevents suspicious scripts:

Correct Answer:



Features

A device restriction policy

A security baseline

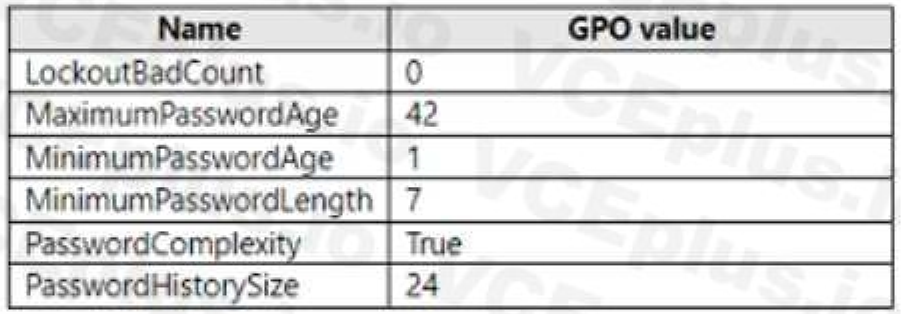
Answer Area

Enforces compliance: An Intune connection

Prevents suspicious scripts: An attack surface reduction (ASR) rule

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

QUESTION 10
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

Correct Answer: A
Section:
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. Reference: https://docs.microsoft.com/enus/ mem/intune/configuration/administrative-templates-windows

QUESTION 11
You have 100 computers that run Windows 10 and connect to an Azure Log Analytics workspace.
Which three types of data can you collect from the computers by using Log Analytics? Each correct answer a complete solution.
NOTE: Each correct selection is worth one point.

A. error events from the System log
B. failure events from the Security log
C. third-party application logs stored as text files
D. the list of processes and their execution times
E. the average processor utilization

Correct Answer: A, C, E
Section:
Explanation:
You can collect error events from the System log, third-party application logs stored as text files, and the average processor utilization from the computers by using Log Analytics. These are some of the types of data that you can collect by using data sources such as Windows event logs, custom logs, and performance counters. You cannot collect failure events from the Security log or the list of processes and their execution times by using Log Analytics. Reference:
https://docs.microsoft.com/en-us/azure/azure-monitor/agents/data-sources-overview

QUESTION 12
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

Correct Answer: C
Section:
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. Reference:

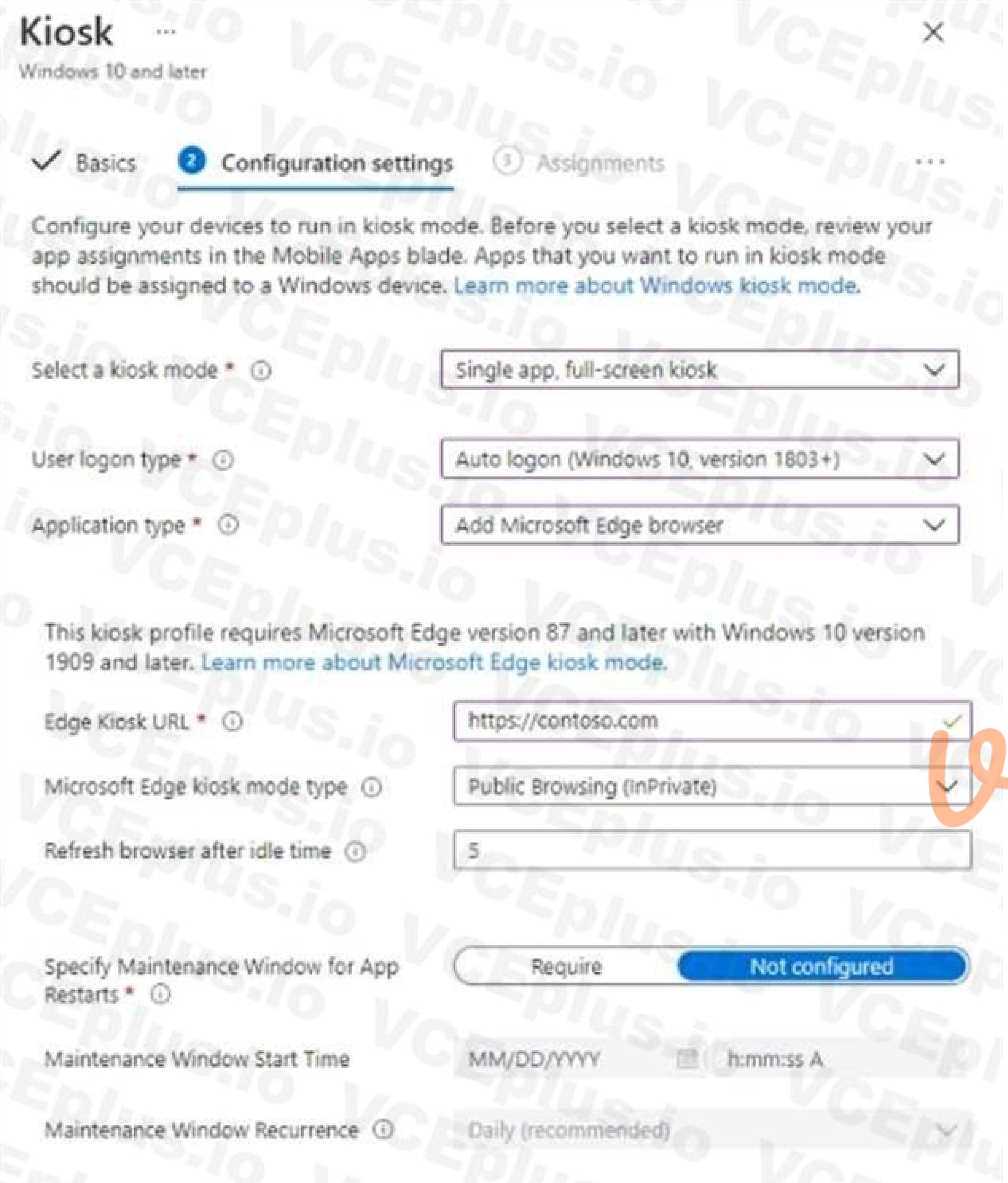
https://docs.microsoft.com/en-us/mem/intune/protect/edr-windows

QUESTION 13
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.

Correct Answer: A, B
Section:
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. Reference: https://docs.microsoft.com/en-us/mem/intune/enrollment/enrollmentrestrictions-set

QUESTION 14
HOTSPOT
You have the device configuration profile shown in the following exhibit.



Kiosk

Windows 10 and later

✓ Basics ② Configuration settings ③ Assignments

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

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

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

Application type *: Add Microsoft Edge browser

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

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

Microsoft Edge kiosk mode type: Public Browsing (InPrivate)

Refresh browser after idle time: 5

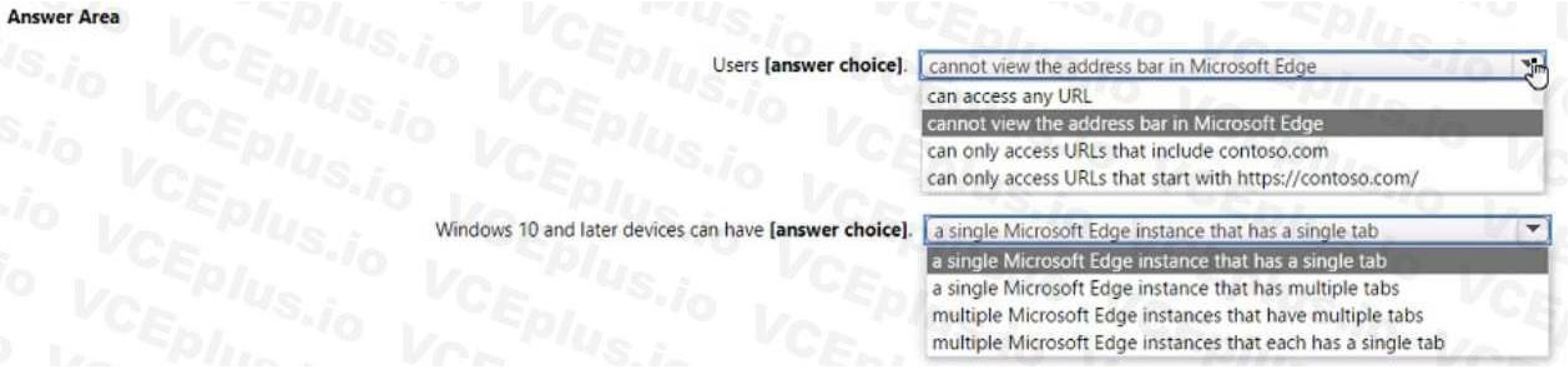
Specify Maintenance Window for App Restarts *: Require | Not configured

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

Maintenance Window Recurrence: Daily (recommended)

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

Hot Area:



Answer Area

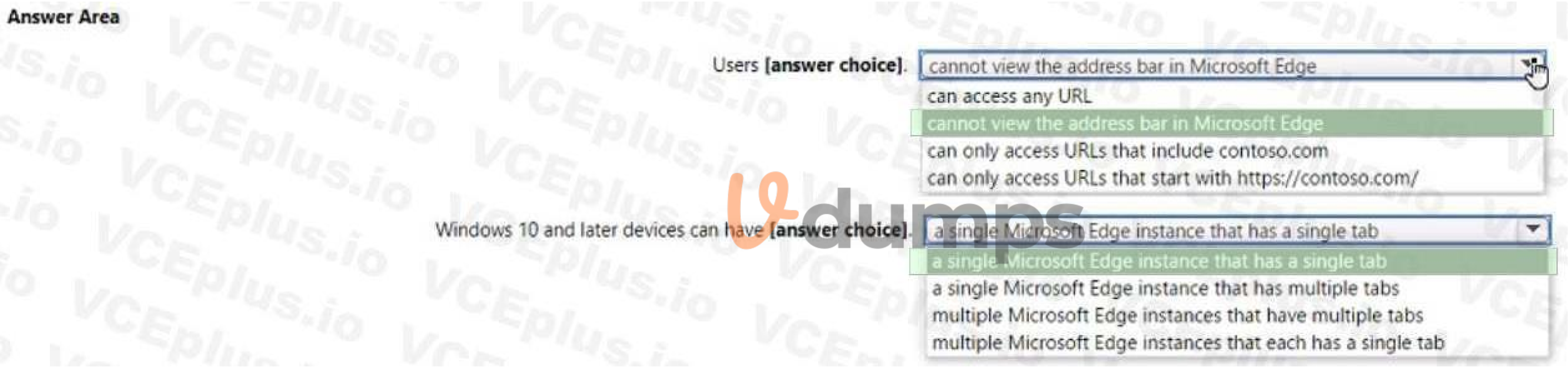
Users [answer choice]. cannot view the address bar in Microsoft Edge

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

Windows 10 and later devices can have [answer choice]. a single Microsoft Edge instance that has a single tab

- a single Microsoft Edge instance that has a single tab
- a single Microsoft Edge instance that has multiple tabs
- multiple Microsoft Edge instances that have multiple tabs
- multiple Microsoft Edge instances that each has a single tab

Answer Area:



Answer Area

Users [answer choice]. cannot view the address bar in Microsoft Edge

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

Windows 10 and later devices can have [answer choice]. a single Microsoft Edge instance that has a single tab

- a single Microsoft Edge instance that has a single tab
- a single Microsoft Edge instance that has multiple tabs
- multiple Microsoft Edge instances that have multiple tabs
- multiple Microsoft Edge instances that each has a single tab

Section:

Explanation:

Users can only access URLs that start with https://contoso.com/

Windows 10 and later devices can have multiple Microsoft Edge instances that each has a single tab he device configuration profile shown in the exhibit is a kiosk browser profile that configures Microsoft Edge to run in kiosk mode. The profile has the following settings:

Kiosk mode: Enabled

Kiosk type: Multi-app

Allowed URLs: https://contoso.com/*

Address bar: Disabled

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

QUESTION 15

HOTSPOT

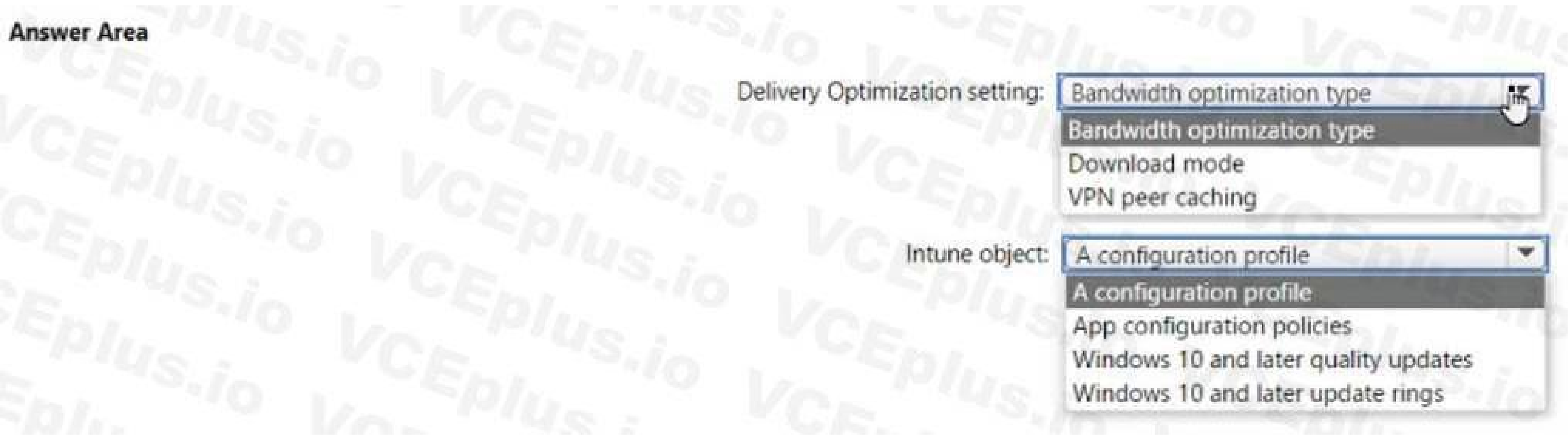
You have 100 Windows 10 devices enrolled in Microsoft Intune.

You need to configure the devices to retrieve Windows updates from the internet and from other computers on a local network.

Which Delivery Optimization setting should you configure, and which type of Intune object should you create? To answer, select the appropriate options in the answer area.

NOTE: Each correct selection is worth one point.

Hot Area:



Answer Area

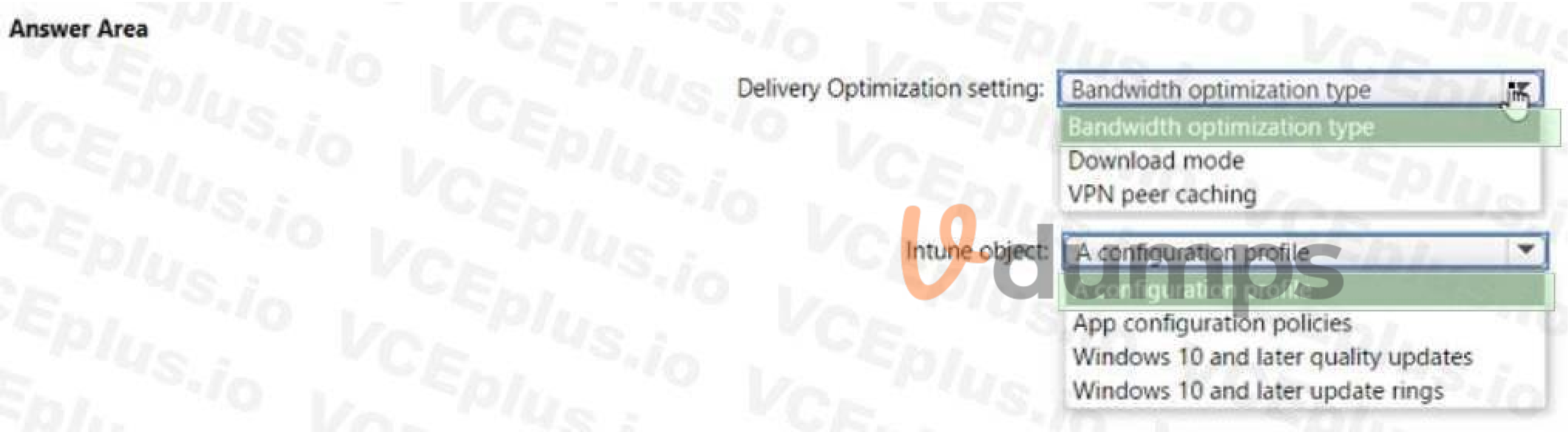
Delivery Optimization setting: Bandwidth optimization type

- Bandwidth optimization type
- Download mode
- VPN peer caching

Intune object: A configuration profile

- A configuration profile
- App configuration policies
- Windows 10 and later quality updates
- Windows 10 and later update rings

Answer Area:



Answer Area

Delivery Optimization setting: Bandwidth optimization type

- Bandwidth optimization type
- Download mode
- VPN peer caching

Intune object: A configuration profile

- A configuration profile
- App configuration policies
- Windows 10 and later quality updates
- Windows 10 and later update rings

Section:

Explanation:

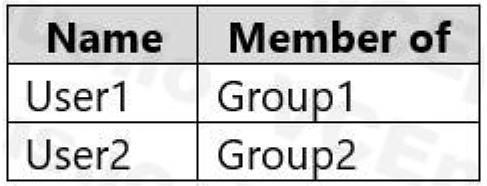
Delivery Optimization setting: B. Download mode Intune object: A configuration profile

To configure the devices to retrieve Windows updates from the internet and from other computers on a local network, you need to configure the Download mode setting in a Delivery Optimization device configuration profile. This setting specifies how the devices use Delivery Optimization to download updates. You can choose from several options, such as HTTP only, LAN only, or Group. For example, you can set the Download mode to Group and specify a group ID for the devices to share updates among themselves and with other devices that have the same group ID. You can also set the Download mode to Internet to allow the devices to download updates from Microsoft or other devices on the internet that use Delivery Optimization. Reference: https://docs.microsoft.com/enus/ mem/intune/configuration/delivery-optimization-windows

QUESTION 16

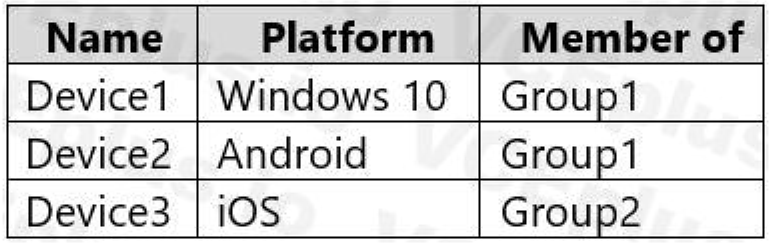
HOTSPOT

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



Name	Member of
User1	Group1
User2	Group2

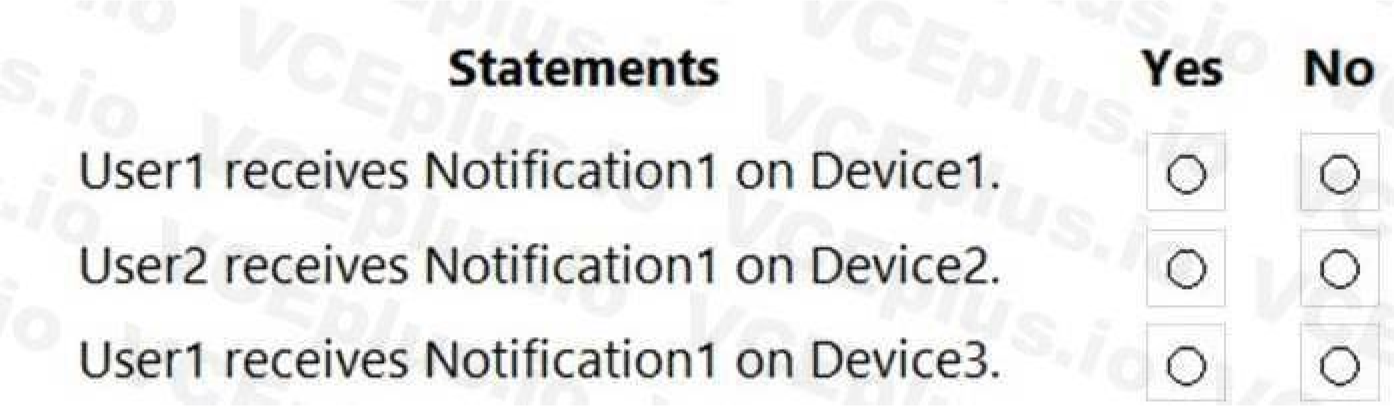
You have devices enrolled in Microsoft Intune as shown in the following table.



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

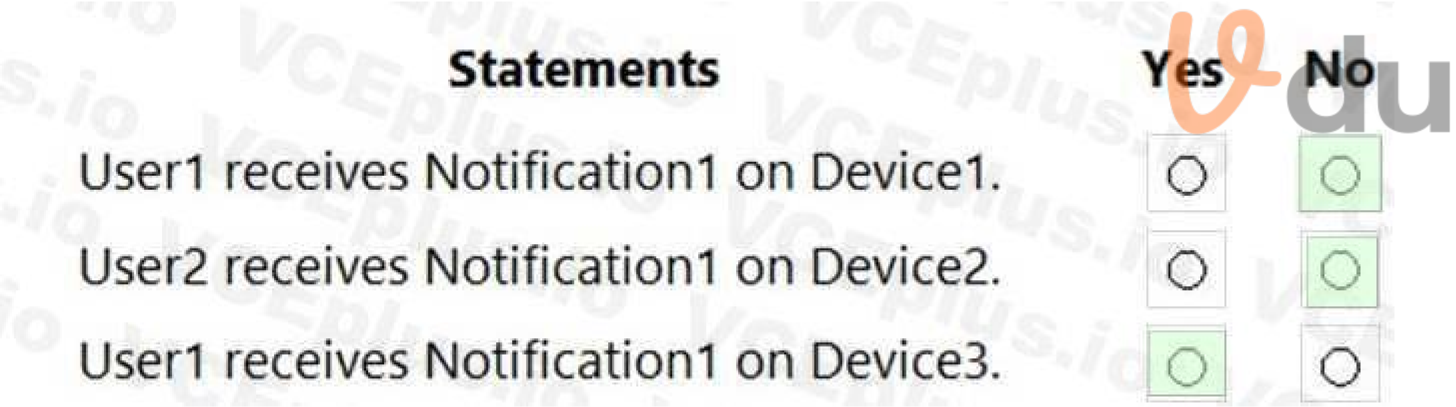
From Intune, you create and send a custom notification named Notification1 to Group1.
For each of the following statements, select Yes if the statement is true. Otherwise, select No.
NOTE: Each correct selection is worth one point.

Hot Area:



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

Answer Area:



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

Section:
Explanation:
Reference:
https://docs.microsoft.com/en-us/mem/intune/remote-actions/custom-notifications

QUESTION 17
You use Microsoft Intune and Intune Data Warehouse.
You need to create a device inventory report that includes the data stored in the data warehouse.
What should you use to create the report?

A. the Azure portal app
B. Endpoint analytics
C. the Company Portal app
D. Microsoft Power BI

Correct Answer: D

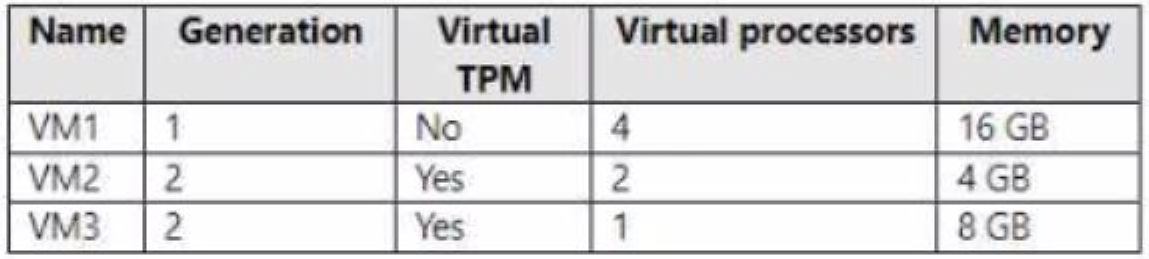
Section:
Explanation:
You can use the Power BI Compliance app to load interactive, dynamically generated reports for your Intune tenant. Additionally, you can load your tenant data in Power BI using the OData link. Intune provides connection settings to your tenant so that you can view the following sample reports and charts related to:
Devices
Enrollment
App protection policy
Compliance policy
Device configuration profiles
Software updates
Device inventory logs
Note: Load the data in Power BI using the OData link
With a client authenticated to Azure AD, the OData URL connects to the RESTful endpoint in the Data Warehouse API that exposes the data model to your reporting client. Follow these instructions to use Power BI Desktop to connect and create your own reports.
Sign in to the Microsoft Endpoint Manager admin center.
Select Reports > Intune Data warehouse > Data warehouse.
Retrieve the custom feed URL from the reporting blade, for example:
https://fef.{yourtenant}.manage.microsoft.com/ReportingService/DataWarehouseFEService/dates?api-version=v1.0
Open Power BI Desktop.
Choose File > Get Data. Select OData feed.
Choose Basic.
Type or paste the OData URL into the URL box.
Select OK.
If you have not authenticated to Azure AD for your tenant from the Power BI desktop client, type your credentials. To gain access to your data, you must authorize with Azure Active Directory (Azure AD) using OAuth 2.0.
Select Organizational account.
Type your username and password.
Select Sign In.
Select Connect.
Select Load.
Reference: https://docs.microsoft.com/en-us/mem/intune/developer/reports-proc-get-a-linkpowerbi

QUESTION 18
You have a Microsoft 365 subscription that uses Microsoft Intune.
You need to ensure that you can deploy apps to Android Enterprise devices.
What should you do first?

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

Correct Answer: D
Section:

QUESTION 19
You have a Hyper-V host. The host contains virtual machines that run Windows 10 as shown in following table.



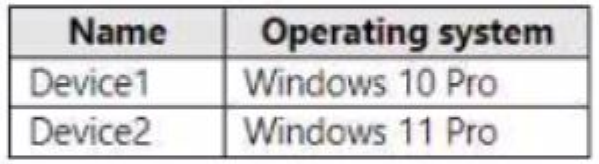
Name	Generation	Virtual TPM	Virtual processors	Memory
VM1	1	No	4	16 GB
VM2	2	Yes	2	4 GB
VM3	2	Yes	1	8 GB

Which virtual machines can be upgraded to Windows 11?

A. VM1 only
B. VM2 only
C. VM2 and VM3 only
D. VM1.VM2. andVM3

Correct Answer: C
Section:
Explanation:
Windows 11 has certain hardware requirements that must be met in order to upgrade from Windows 10. Some of these requirements are as follows:
A processor with at least1 GHzclock speed and2 cores.
A system firmware that supportsUEFIandSecure Boot.
ATrusted Platform Module (TPM)version2.0or higher.
At least4 GBof system memory (RAM).
At least64 GBof storage space.
In this scenario, the virtual machines that run Windows 10 have the following specifications:
VM1 is a generation 1 virtual machine with no virtual TPM, 4 virtual processors, and 16 GB of memory.
VM2 is a generation 2 virtual machine with a virtual TPM, 2 virtual processors, and 4 GB of memory.
VM3 is a generation 2 virtual machine with a virtual TPM, 1 virtual processor, and 8 GB of memory.
VM1 cannot be upgraded to Windows 11 because it does not have a virtual TPM and it is not a generation 2 virtual machine. Generation 1 virtual machines do not support UEFI and Secure Boot, which are required for Windows 11. VM2 and VM3 can be upgraded to Windows 11 because they have a virtual TPM and they are generation 2 virtual machines. They also meet the minimum requirements for processor speed, cores, memory, and storage space.

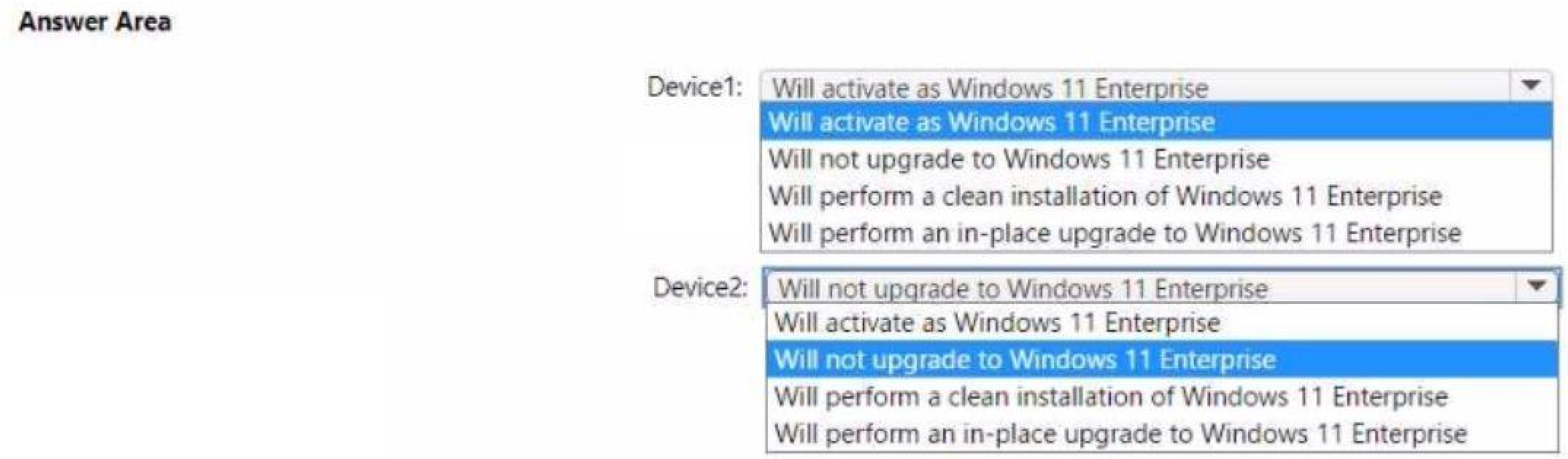
QUESTION 20
HOTSPOT
Your network contains an on-premises Active Directory domain named contoso.com that syncs to Azure AD. A user named User! uses the domain-joined devices shown in the following table.



Name	Operating system
Device1	Windows 10 Pro
Device2	Windows 11 Pro

In the Microsoft Entra admin center, you assign a Windows 11 Enterprise E5 license to User1.
You need to identify what will occur when User1 next signs in to the devices.
What should you identify for each device? To answer, select the appropriate options in the answer area.
NOTE: Each correct selection is worth one point.

Hot Area:



Answer Area

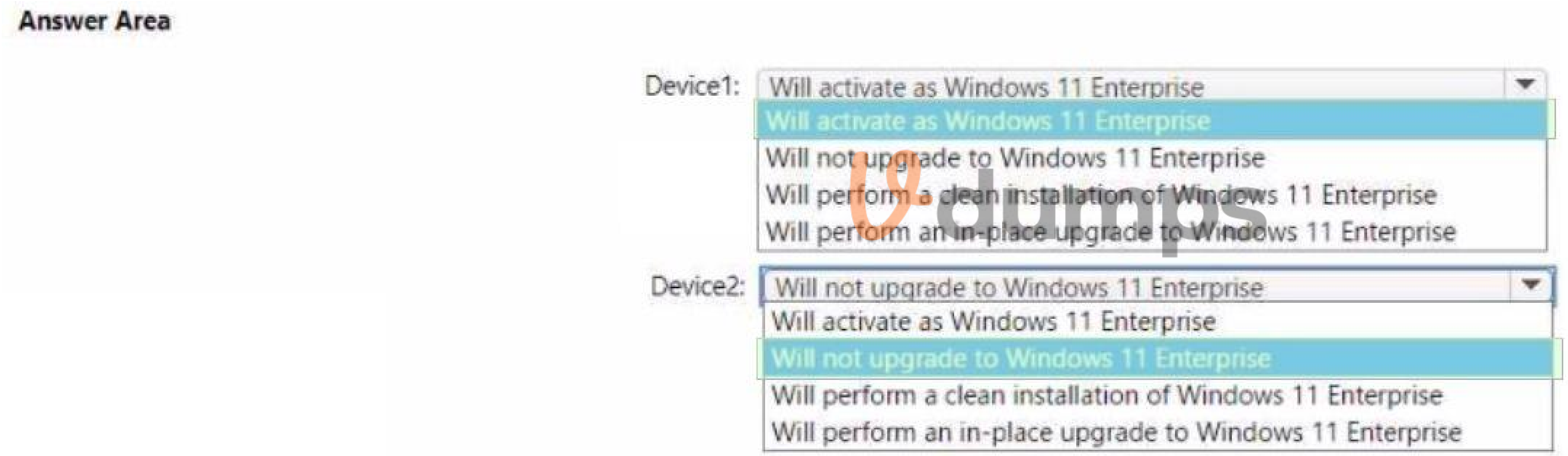
Device1: Will activate as Windows 11 Enterprise

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

Device2: Will not upgrade to Windows 11 Enterprise

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

Answer Area:



Answer Area

Device1: Will activate as Windows 11 Enterprise

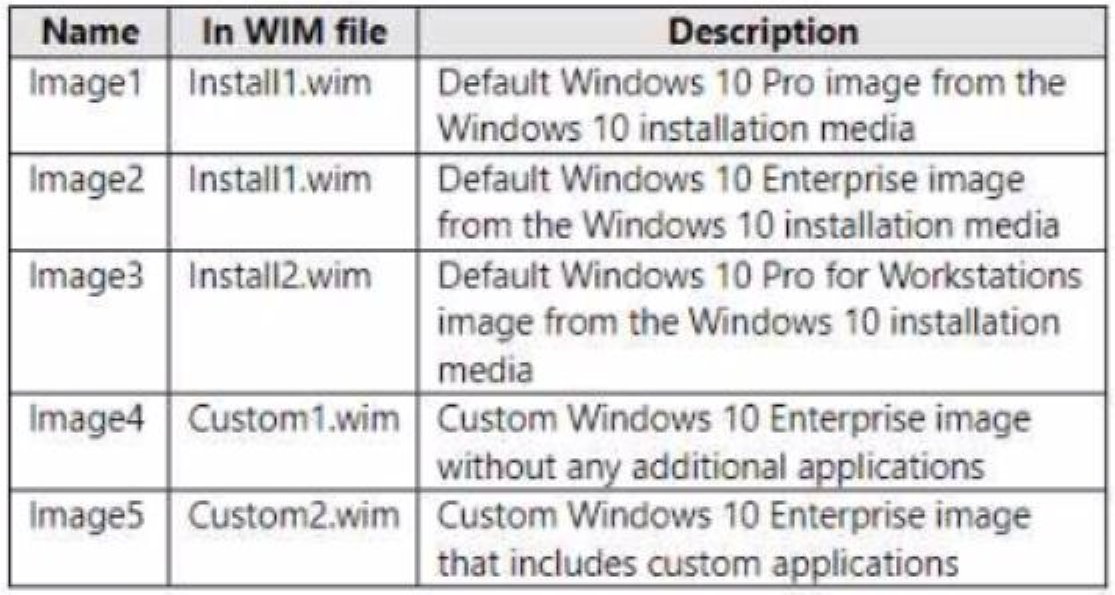
- Will activate as Windows 11 Enterprise
- Will not upgrade to Windows 11 Enterprise
- Will perform a clean installation of Windows 11 Enterprise
- Will perform an in-place upgrade to Windows 11 Enterprise

Device2: Will not upgrade to Windows 11 Enterprise

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

Section:
Explanation:

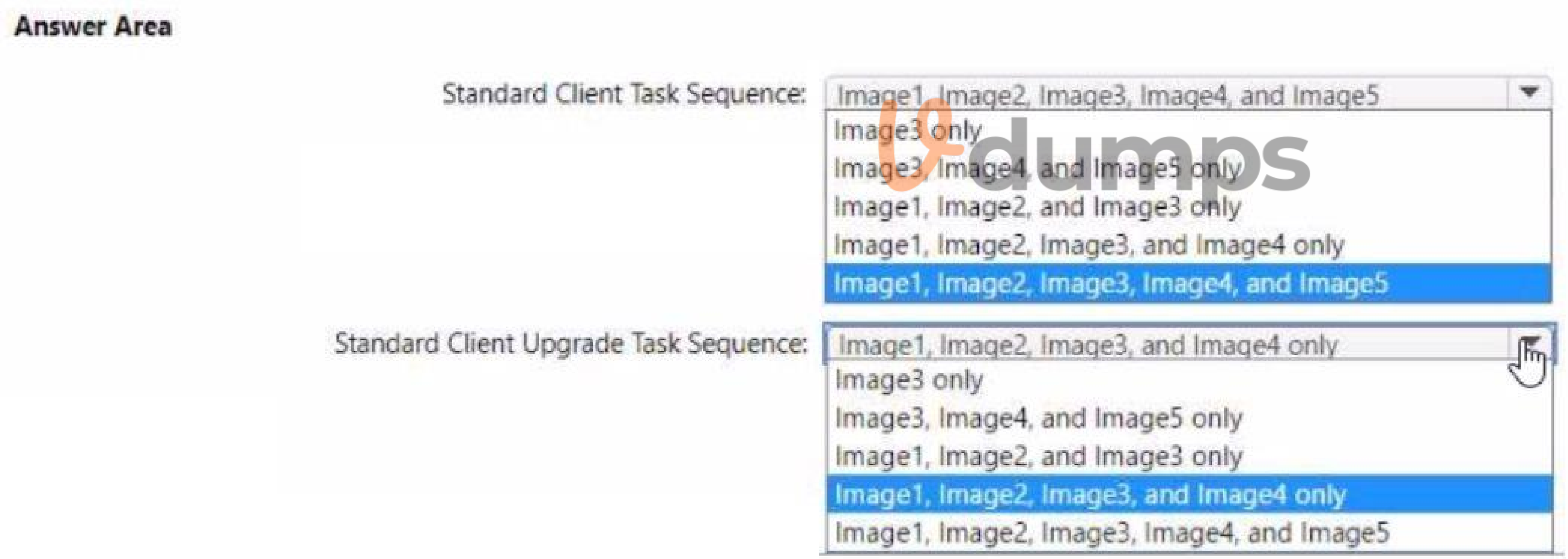
QUESTION 21
HOTSPOT
You have a Microsoft Deployment Toolkit (MDT) deployment share named Share 1. You add Windows 10 images to Share! as shown in the following table.



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

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

Hot Area:



Answer Area

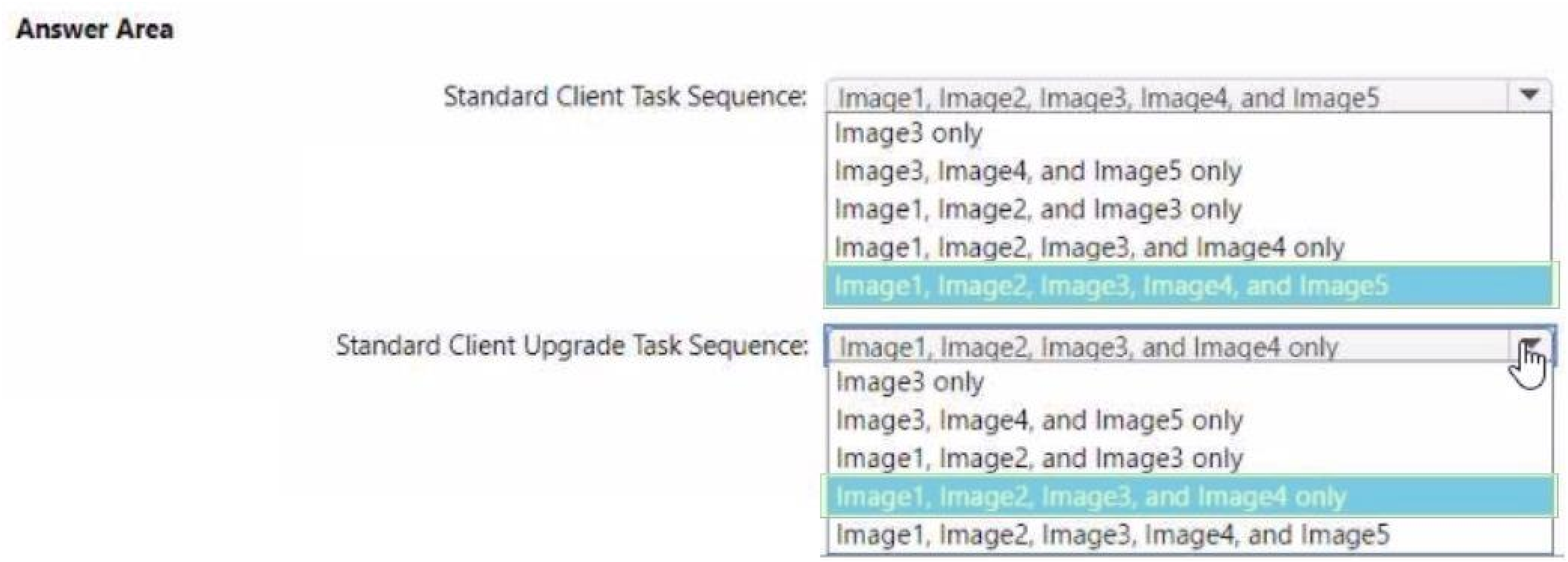
Standard Client Task Sequence: Image1, Image2, Image3, Image4, and Image5

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

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

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

Answer Area:



Answer Area

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

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

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

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

Section:
Explanation:

QUESTION 22
You have a Microsoft 365 E5 subscription and 25 Apple iPads.
You need to enroll the iPads in Microsoft Intune by using the Apple Configurator enrollment method.
What should you do first?

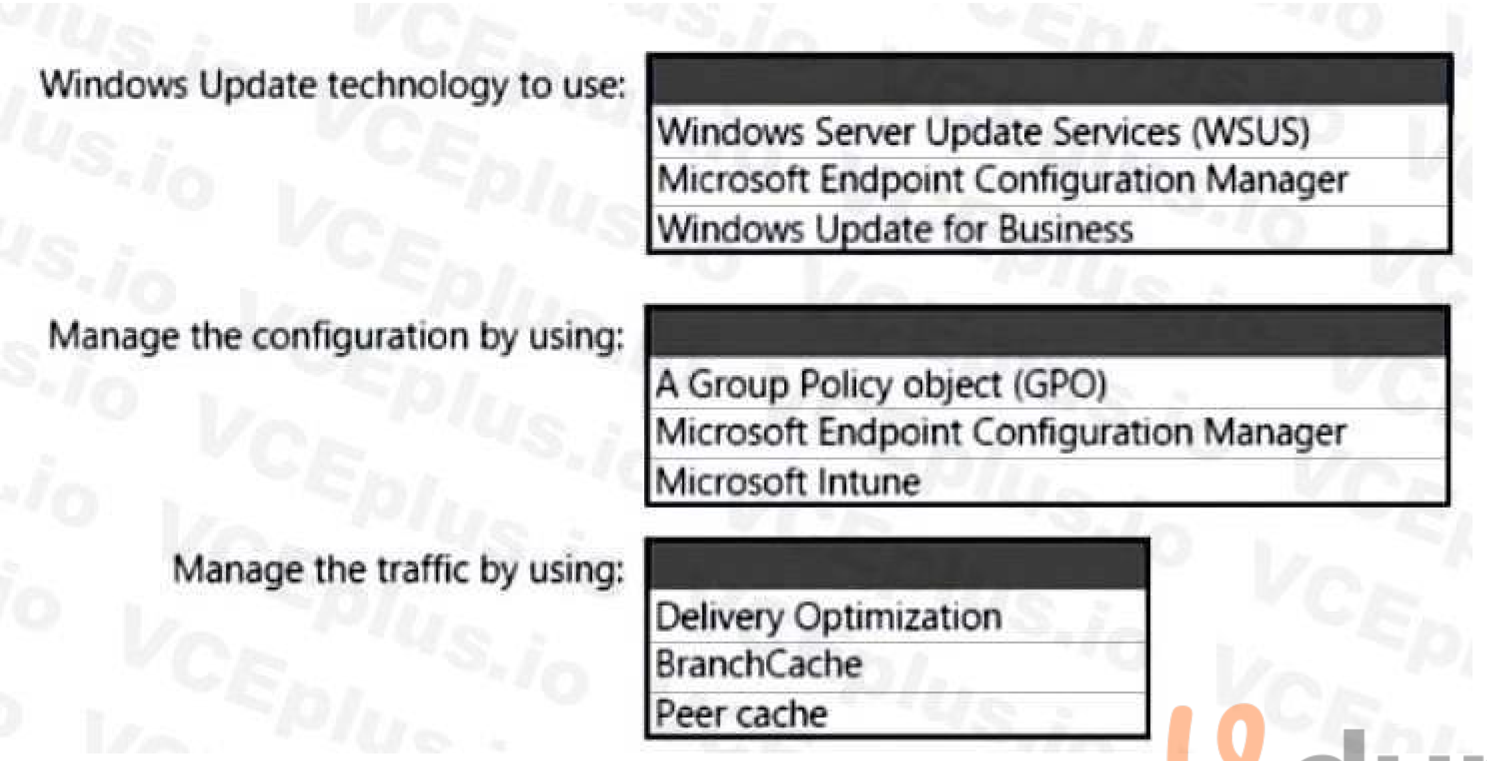
A. Upload a file that has the device identifiers for each iPad.
B. Modify the enrollment restrictions.
C. Configure an Apple MDM push certificate.
D. Add your user account as a device enrollment manager (DEM).

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

QUESTION 23
HOTSPOT
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.

Hot Area:

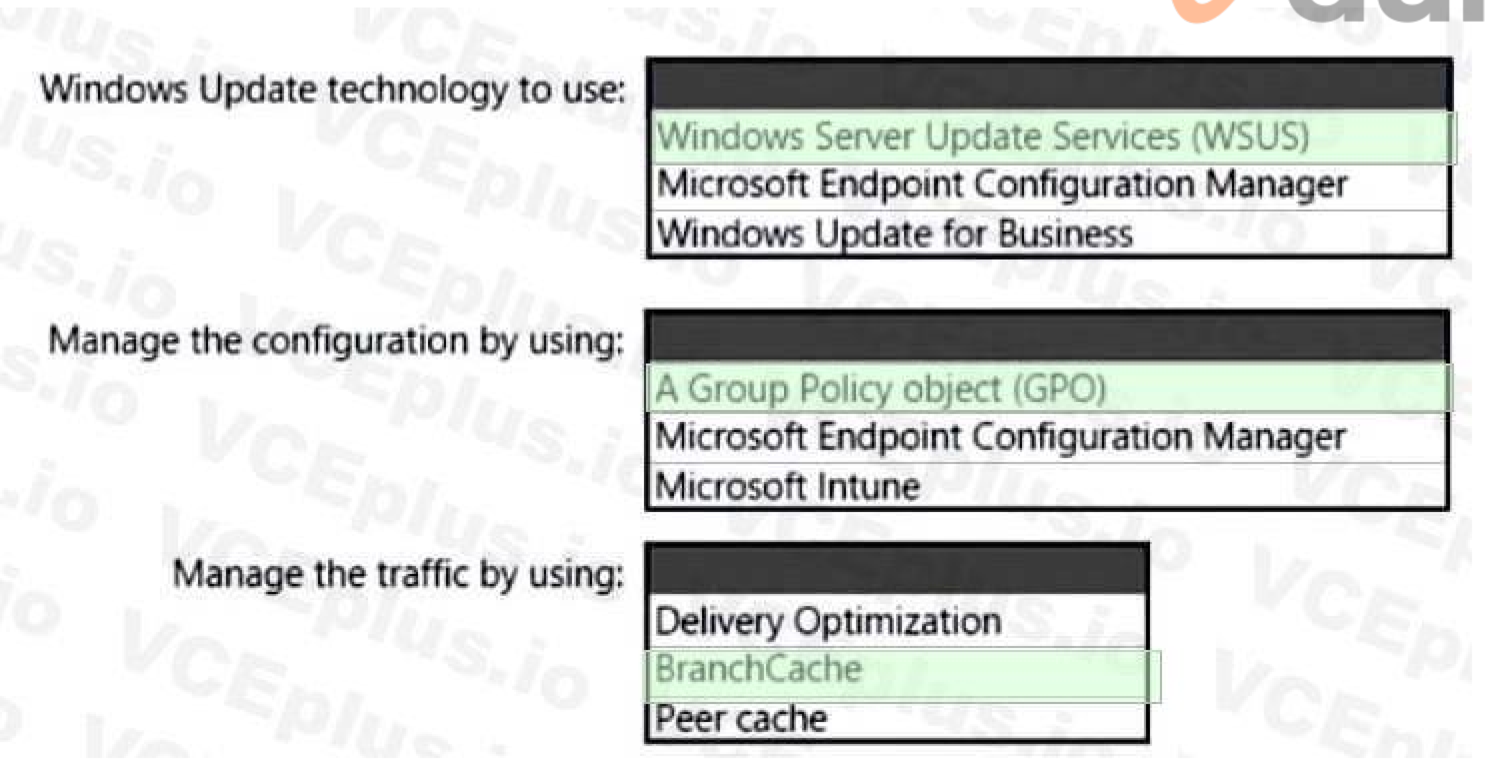


Windows Update technology to use:
- Windows Server Update Services (WSUS)
- Microsoft Endpoint Configuration Manager
- Windows Update for Business

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

Answer Area:



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

Section:
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

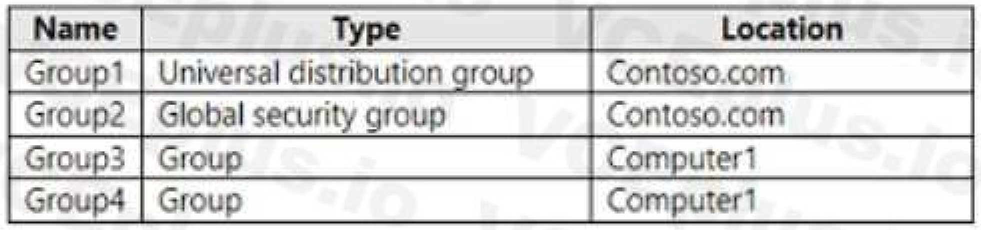
through Microsoft Update to computers on your network.
Windows Server Update Services is a built-in server role that includes the following enhancements:
Can be added and removed by using the Server Manager
Includes Windows PowerShell cmdlets to manage the most important administrative tasks in WSUS
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-updateservices/deploy/4-configure-group-policy-settings-for-automatic-updates

QUESTION 24
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

Correct Answer: C
Section:
Explanation:

QUESTION 25
Your network contains an Active Directory domain named contoso.com. The domain contains a computer named Computer1 that runs Windows 10. You have the groups shown in the following table.



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

Which groups can you add to Group4?

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

Correct Answer: C
Section:

QUESTION 26

DRAG DROP

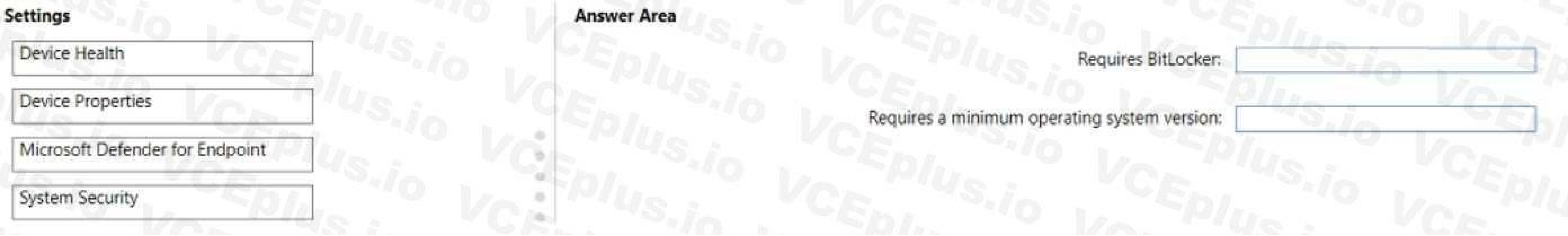
You have a Microsoft 365 subscription. The subscription contains computers that run Windows 11 and are enrolled in Microsoft Intune. You need to create a compliance policy that meets the following requirements:

- 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,

Select and Place:



Settings

Device Health

Device Properties

Microsoft Defender for Endpoint

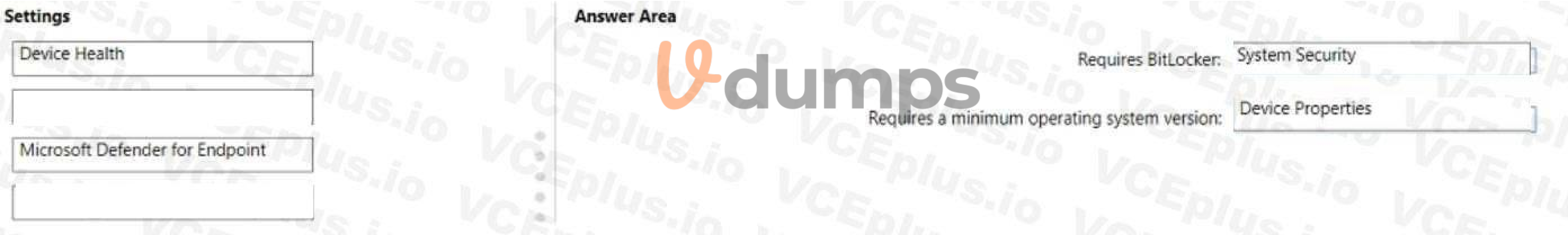
System Security

Answer Area

Requires BitLocker:

Requires a minimum operating system version:

Correct Answer:



Settings

Device Health

Microsoft Defender for Endpoint

Answer Area

Requires BitLocker: System Security

Requires a minimum operating system version: Device Properties

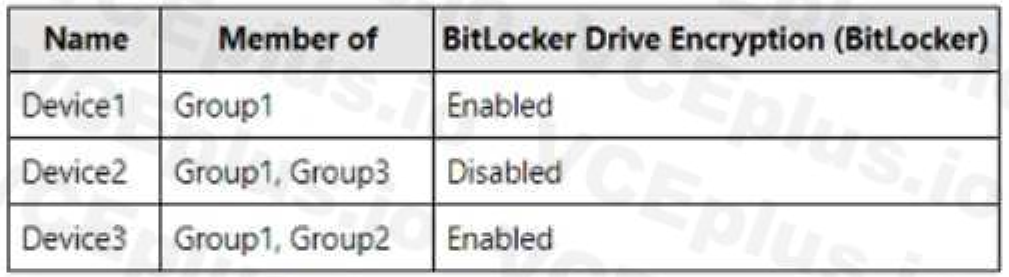
Section:

Explanation:

QUESTION 27

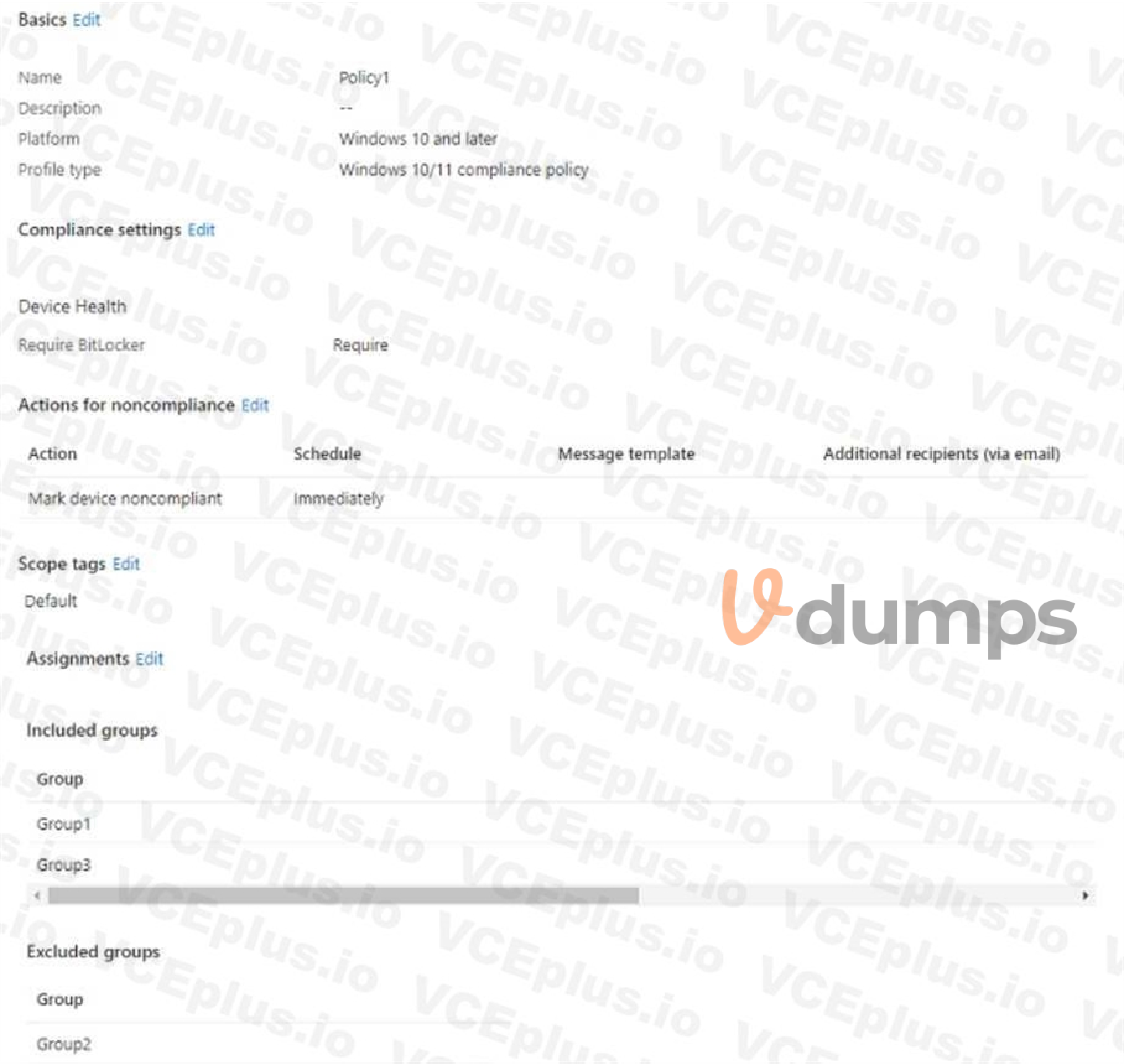
HOTSPOT

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

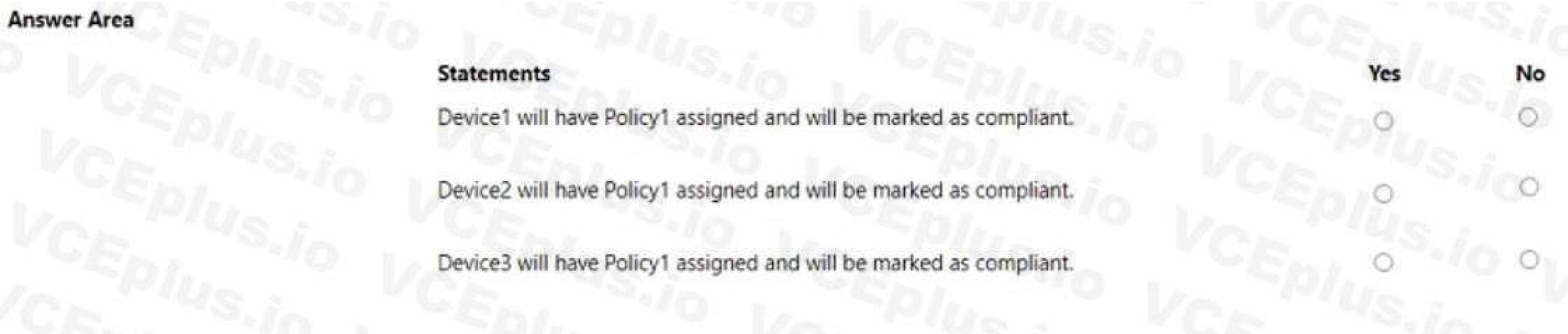
Group
Group1
Group3

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.

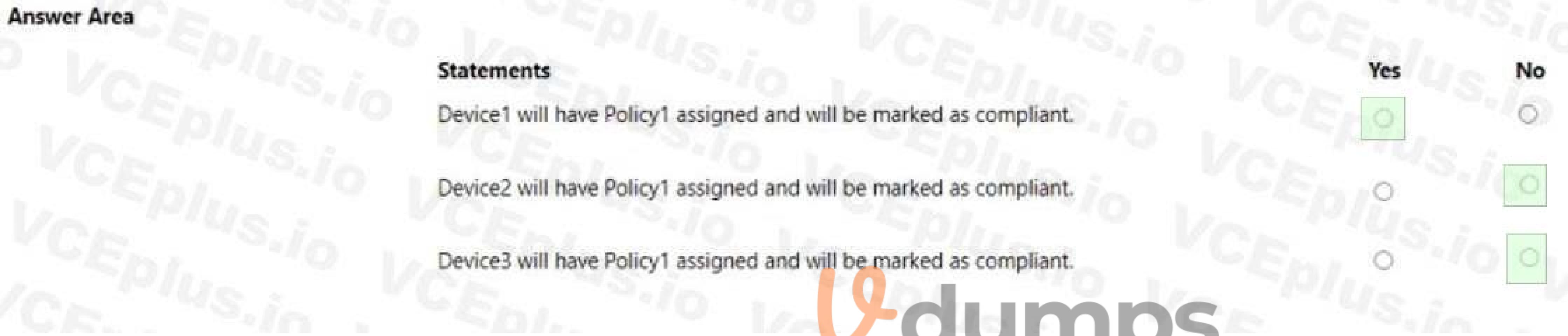
Hot Area:



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.	○	○

Answer Area:



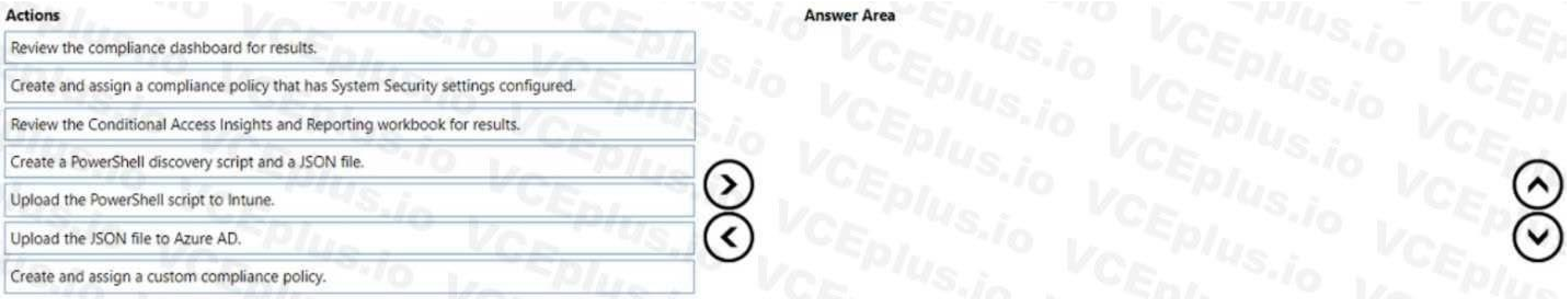
Answer Area

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.	○	[✓ ○]

Section:
Explanation:

QUESTION 28
DRAG DROP
You have a Microsoft 365 subscription that contains 1,000 Windows 11 devices enrolled in Microsoft Intune.
You plan to create and monitor the results of a compliance policy used to validate the BIOS version of the devices.
Which four 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.

Select and Place:



Actions

Review the compliance dashboard for results.

Create and assign a compliance policy that has System Security settings configured.

Review the Conditional Access Insights and Reporting workbook for results.

Create a PowerShell discovery script and a JSON file.

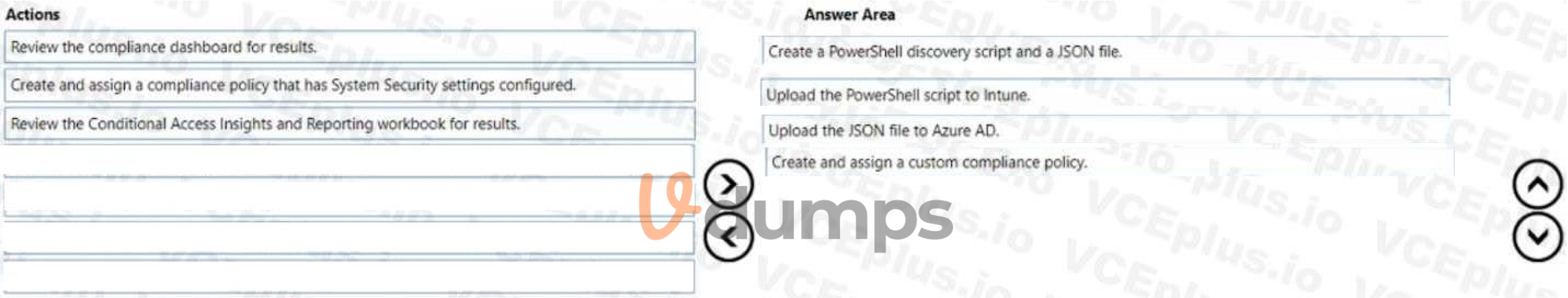
Upload the PowerShell script to Intune.

Upload the JSON file to Azure AD.

Create and assign a custom compliance policy.

Answer Area

Correct Answer:



Actions

Review the compliance dashboard for results.

Create and assign a compliance policy that has System Security settings configured.

Review the Conditional Access Insights and Reporting workbook for results.

Answer Area

Create a PowerShell discovery script and a JSON file.

Upload the PowerShell script to Intune.

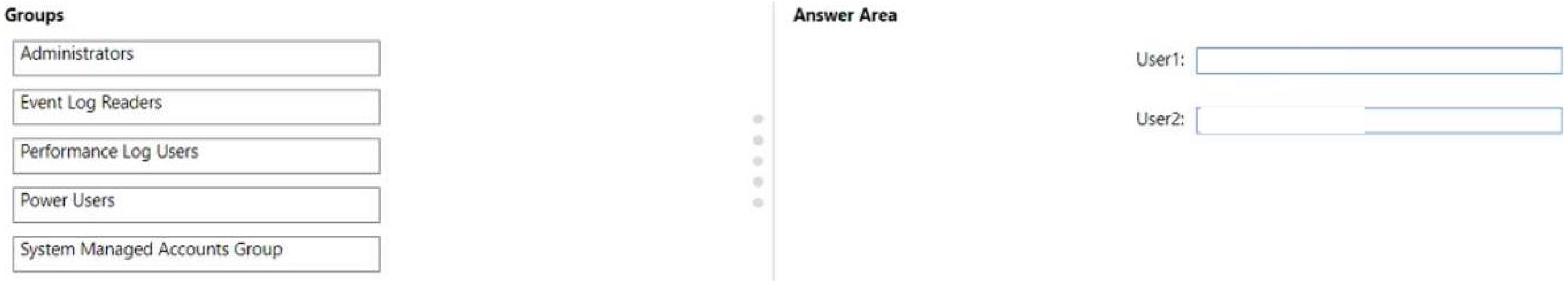
Upload the JSON file to Azure AD.

Create and assign a custom compliance policy.

Section:
Explanation:

QUESTION 29
DRAG DROP
You have a computer that runs Windows 10 and contains two local users named User! and User2.
You need to ensure that the users can perform the following anions:
• User 1 must be able to adjust the date and time.
• User2 must be able to clear Windows logs.
The solution must use the principle of least privilege.
To which group should you add each user? To answer, drag the appropriate groups to the correct users. Each group may be used once, more than once, or not at all. You may need to drag the split bar between panes or scroll to view content.
NOTE: Each correct selection is worth one point.

Select and Place:



Groups

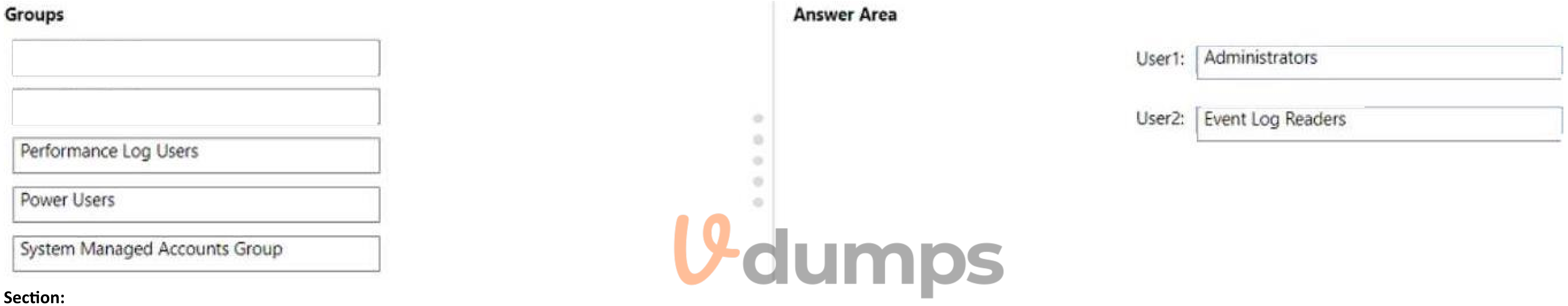
- Administrators
- Event Log Readers
- Performance Log Users
- Power Users
- System Managed Accounts Group

Answer Area

User1:

User2:

Correct Answer:



Groups

- Performance Log Users
- Power Users
- System Managed Accounts Group

Answer Area

User1: Administrators

User2: Event Log Readers

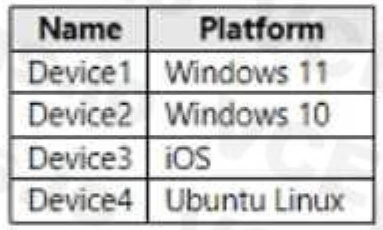
Section:

Explanation:

QUESTION 30

HOTSPOT

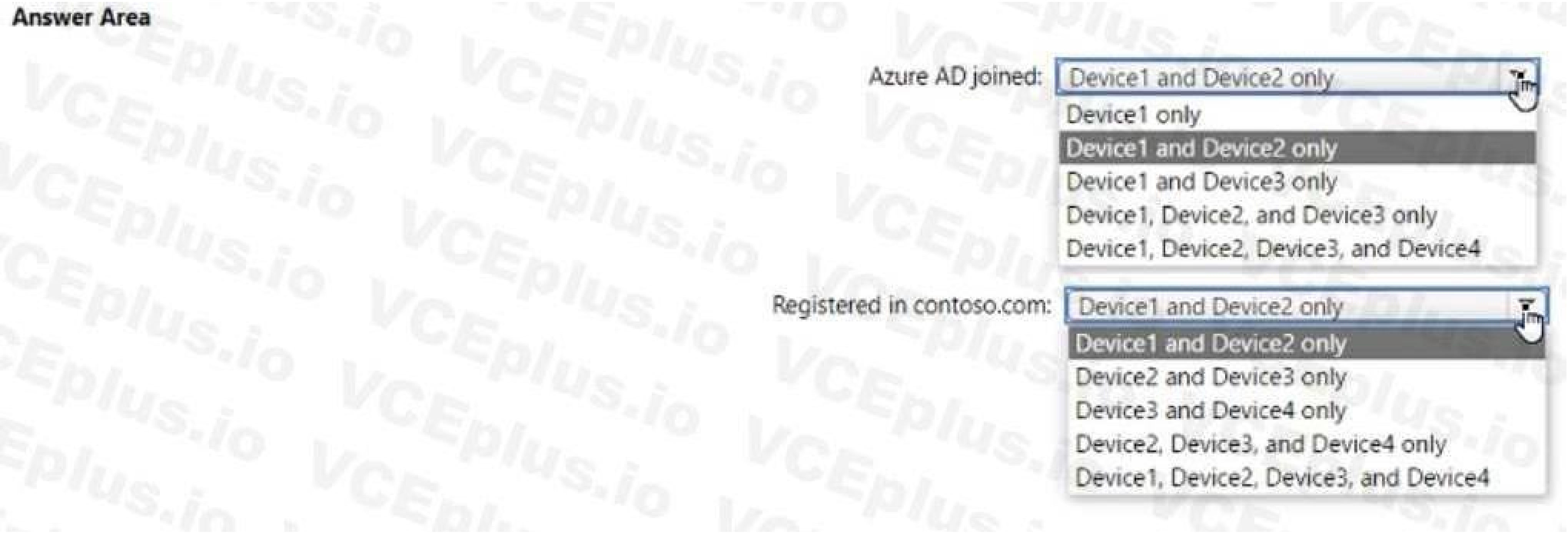
You have an Azure AD tenant named contoso.com. You have the devices shown in the following table.



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

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

Hot Area:



Answer Area

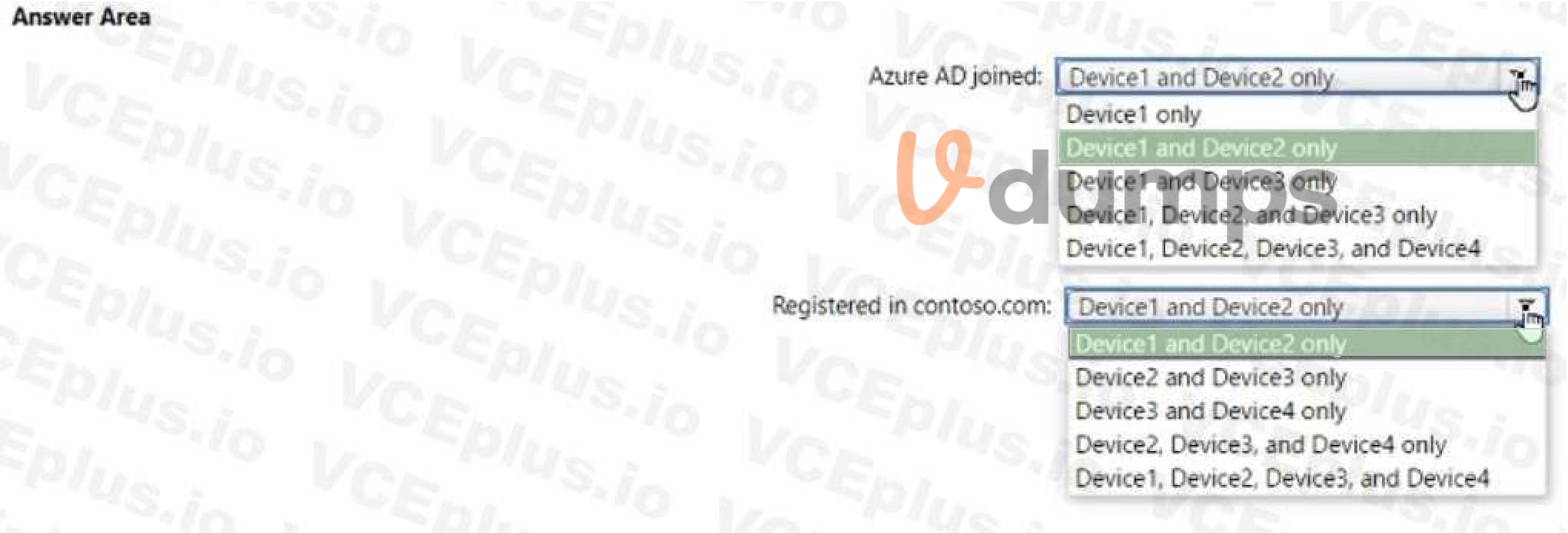
Azure AD joined: Device1 and Device2 only

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

Registered in contoso.com: Device1 and Device2 only

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

Answer Area:



Answer Area

Azure AD joined: Device1 and Device2 only

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

Registered in contoso.com: Device1 and Device2 only

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

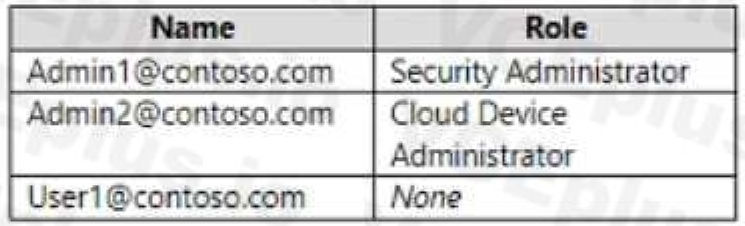
Section:

Explanation:

QUESTION 31

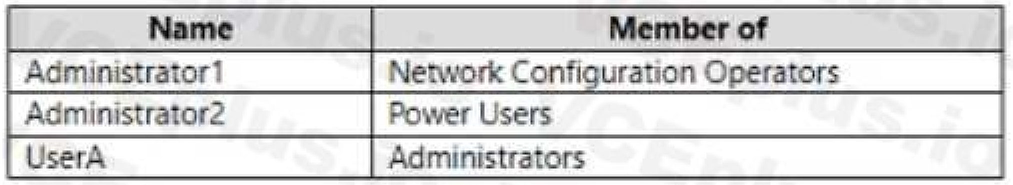
HOTSPOT

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



Name	Role
Admin1@contoso.com	Security Administrator
Admin2@contoso.com	Cloud Device Administrator
User1@contoso.com	*None*

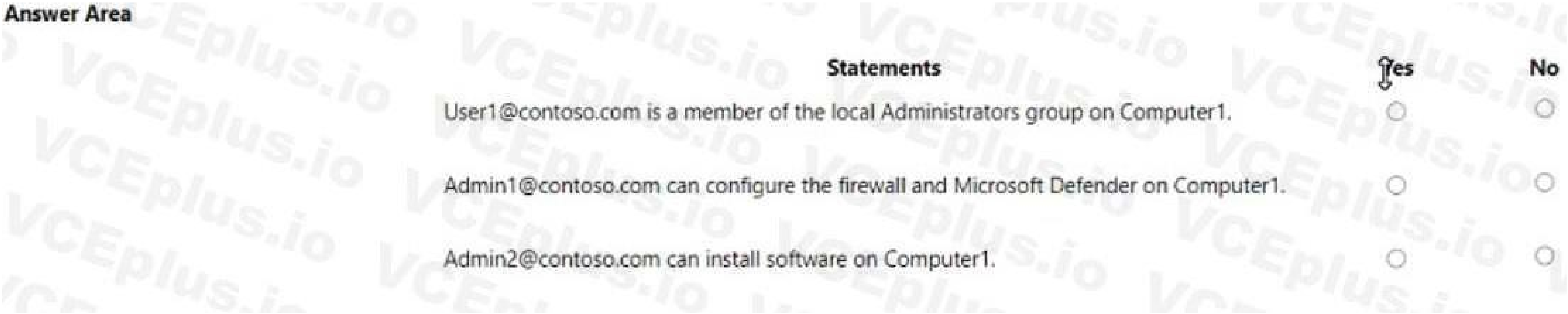
You have a computer named Computer1 that runs Windows 10. Computer1 is in a workgroup and has the local users shown in the following table.



Name	Member of
Administrator1	Network Configuration Operators
Administrator2	Power Users
UserA	Administrators

UserA joins Computer1 to Azure AD by using user1@contoso.com.
For each of the following statements, select Yes if the statement is true. Otherwise, select No.
NOTE: Each correct selection is worth one point.

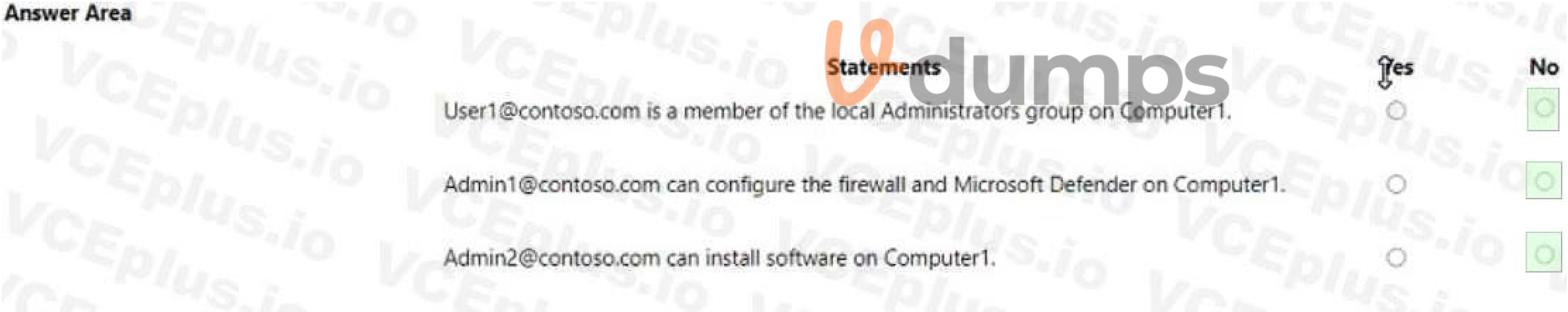
Hot Area:



Answer Area

Statements	Yes	No
User1@contoso.com is a member of the local Administrators group on Computer1.	○	○
Admin1@contoso.com can configure the firewall and Microsoft Defender on Computer1.	○	○
Admin2@contoso.com can install software on Computer1.	○	○

Answer Area:



Answer Area

Statements	Yes	No
User1@contoso.com is a member of the local Administrators group on Computer1.	○	[✓ ○]
Admin1@contoso.com can configure the firewall and Microsoft Defender on Computer1.	○	[✓ ○]
Admin2@contoso.com can install software on Computer1.	○	[✓ ○]

Section:
Explanation:

QUESTION 32
Your network contains an Active Directory domain. The domain contains a user named Admin1. All computers run Windows 10.
You enable Windows PowerShell remoting on the computers.
You need to ensure that Admin1 can establish remote PowerShell connections to the computers. The solution must use the principle of least privilege.
To which group should you add Admin1?

A. Access Control Assistance Operators
B. Remote Desktop Users
C. Power Users
D. Remote Management Users

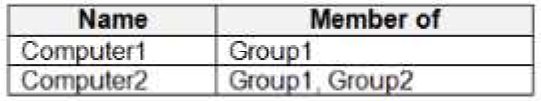
Correct Answer: B

Section:

QUESTION 33

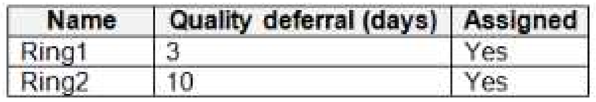
HOTSPOT

You have two computers that run Windows 10. The computers are enrolled in Microsoft Intune as shown in the following table.



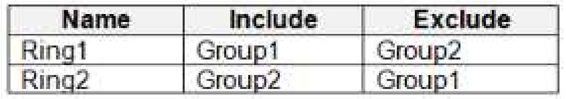
Name	Member of
Computer1	Group1
Computer2	Group1, Group2

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.

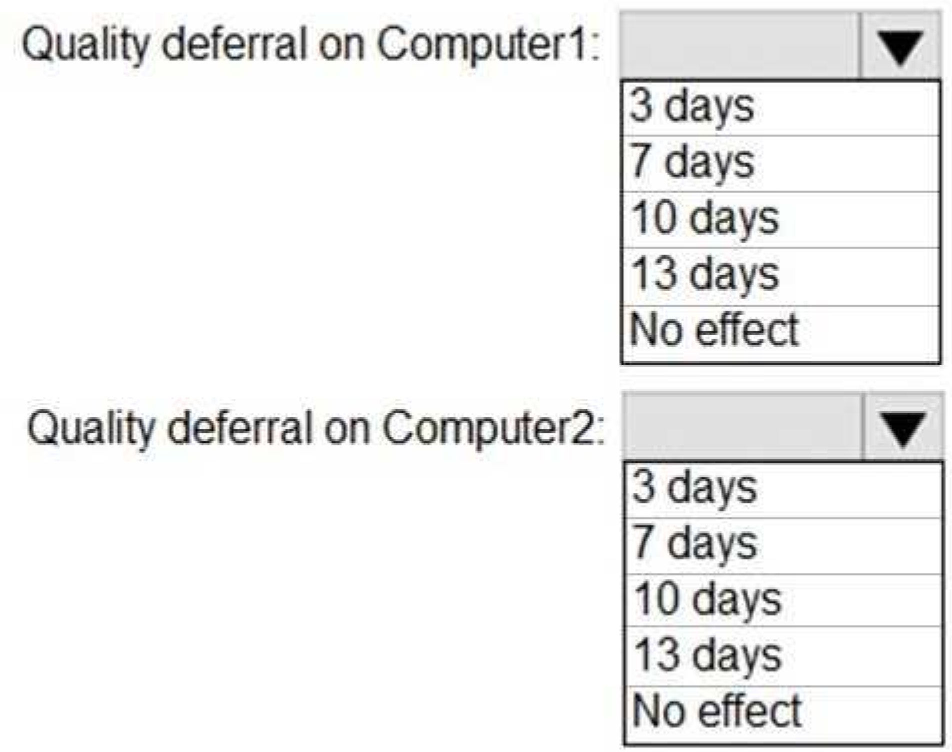


Name	Include	Exclude
Ring1	Group1	Group2
Ring2	Group2	Group1

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.

Hot Area:



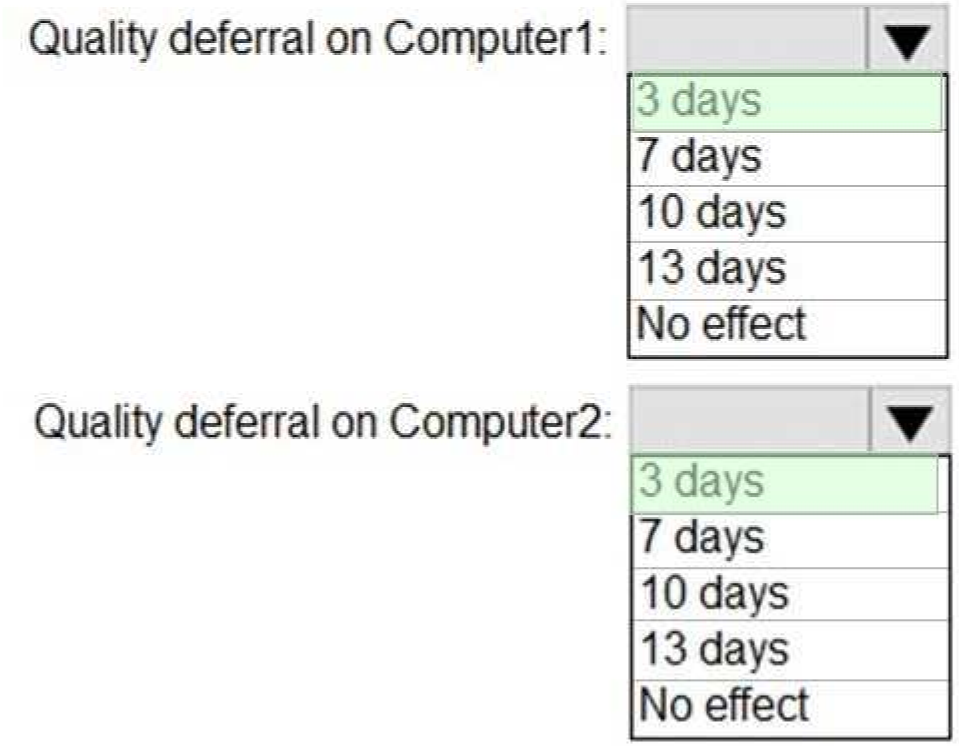
Quality deferral on Computer1: ▼

- 3 days
- 7 days
- 10 days
- 13 days
- No effect

Quality deferral on Computer2: ▼

- 3 days
- 7 days
- 10 days
- 13 days
- No effect

Answer Area:



Quality deferral on Computer1:

- [✓ 3 days]
- 7 days
- 10 days
- 13 days
- No effect

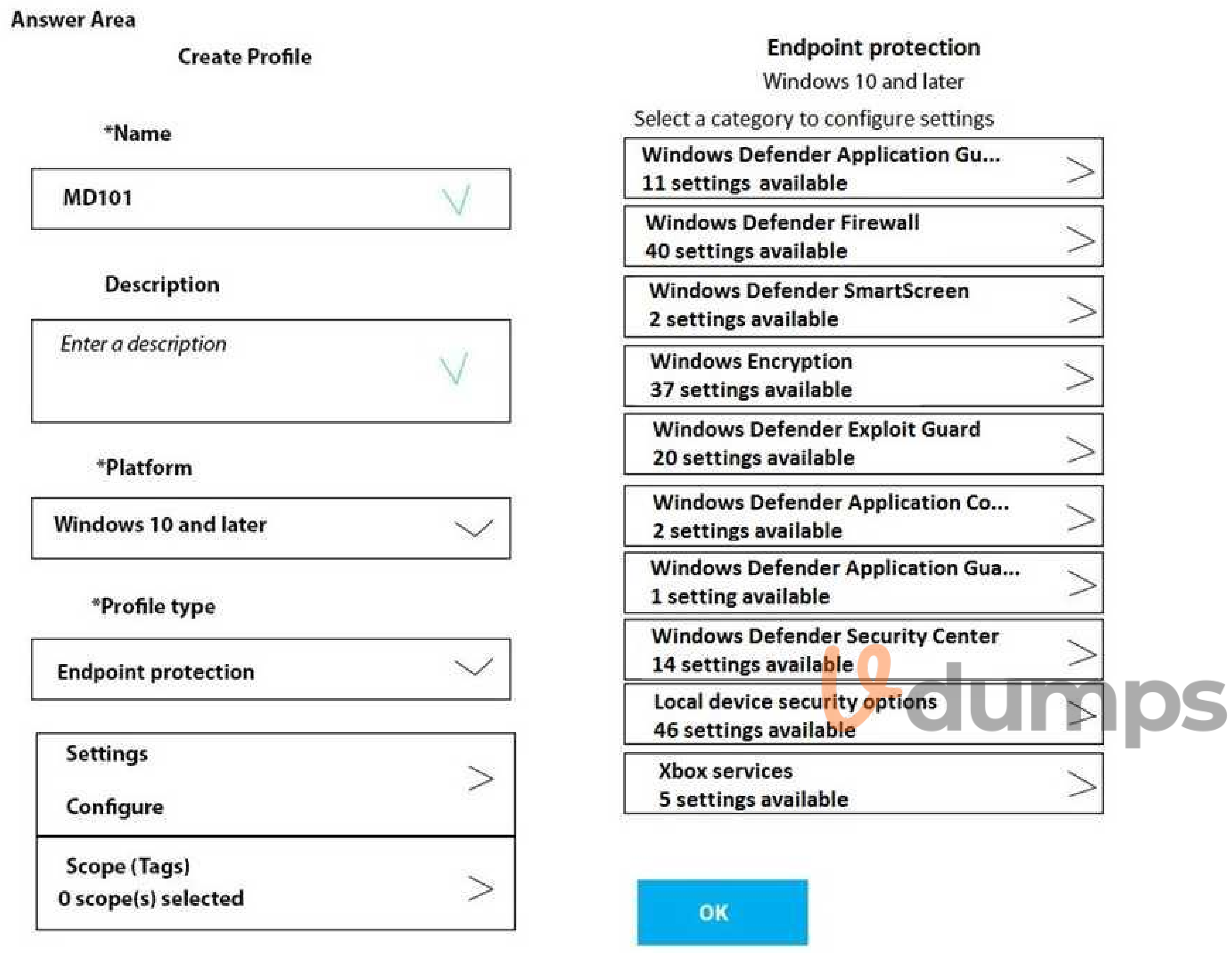
Quality deferral on Computer2:

- [✓ 3 days]
- 7 days
- 10 days
- 13 days
- No effect

Section:
Explanation:
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.
Reference:
https://docs.microsoft.com/en-us/windows/deployment/update/waas-wufb-intune
https://allthingscloud.blog/configure-windows-update-business-using-microsoft-intune/

QUESTION 34
HOTSPOT
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.

Hot Area:



Answer Area

Create Profile

*Name

MD101 ✓

Description

Enter a description ✓

*Platform

Windows 10 and later

*Profile type

Endpoint protection

Settings
Configure >

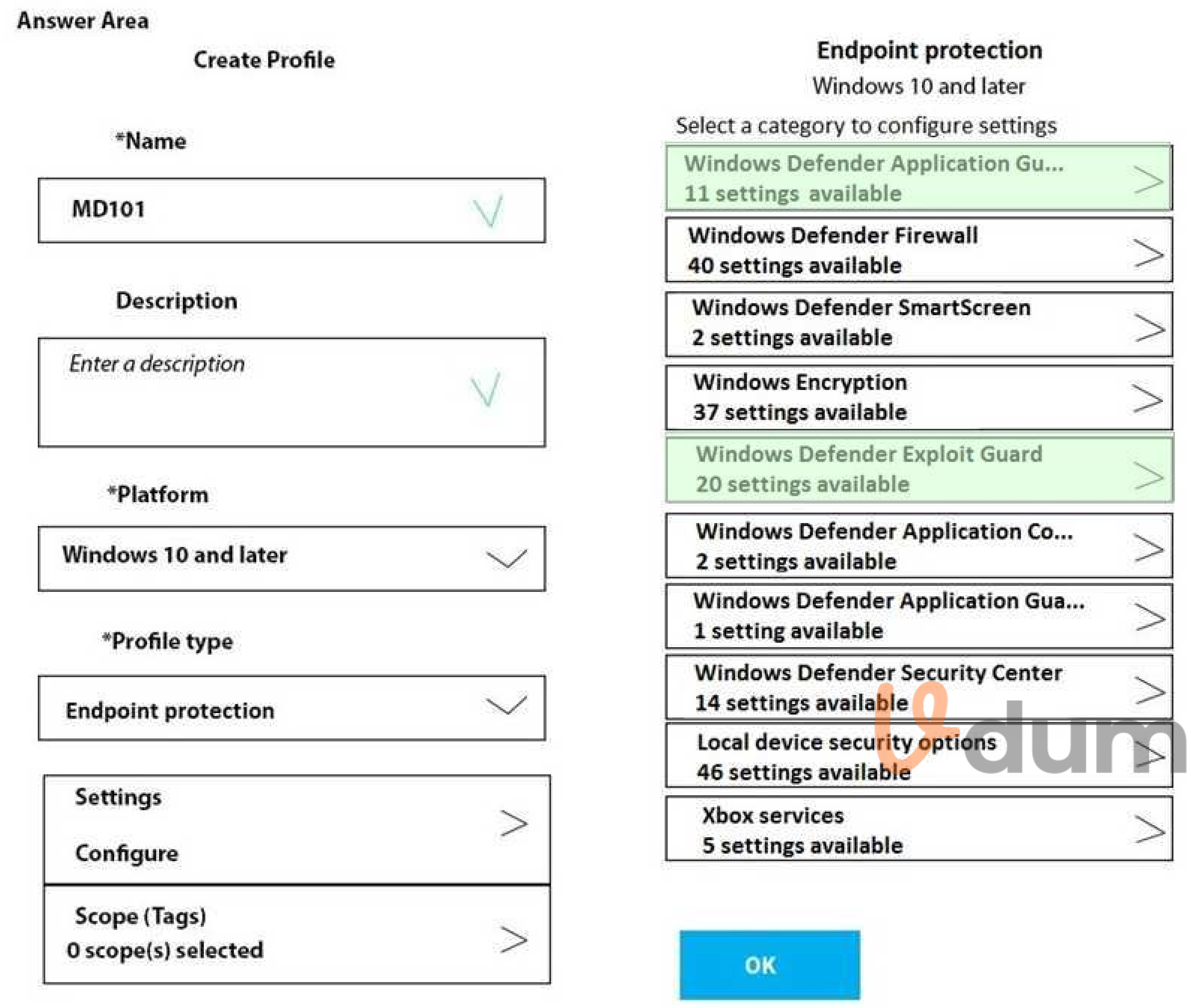
Scope (Tags)
0 scope(s) selected >

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 >

Answer Area:



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

Section:
Explanation:
Reference:
https://docs.microsoft.com/en-us/intune/endpoint-protection-windows-10

QUESTION 35
You have a Microsoft 365 tenant that contains the objects shown in the following table.
You are creating a compliance policy named Compliance1.
Which objects can you specify in Compliance1 as additional recipients of noncompliance notifications?

A. Group3 and Group4 only

B. Group3, Group4, and Admin1 only

C. Group1, Group2, and Group3 only

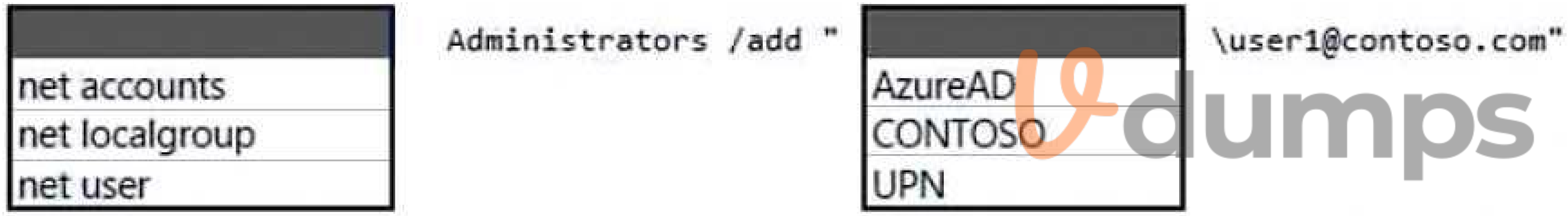
D. Group1, Group2, Group3, and Group4 only

E. Group1, Group2, Group3, Group4, and Admin1

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

QUESTION 36
HOTSPOT
You have an Azure Active Directory (Azure AD) tenant named contoso.com that contains a user named User1. User1 has a user principal name (UPN) of user1 @contoso.com.
You join a Windows 10 device named Client1 to contoso.com.
You need to add User1 to the local Administrators group of Client1.
How should you complete the command? To answer, select the appropriate options in the answer area.
NOTE: Each correct selection is worth one point.

Hot Area:



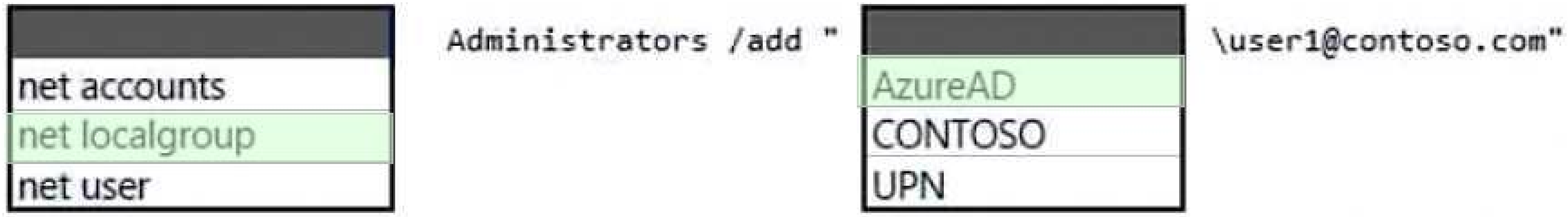
net accounts
net localgroup
net user

`Administrators /add "`

AzureAD
CONTOSO
UPN

`\user1@contoso.com"`

Answer Area:



net accounts
[✓ net localgroup]
net user

`Administrators /add "`

[✓ AzureAD]
CONTOSO
UPN

`\user1@contoso.com"`

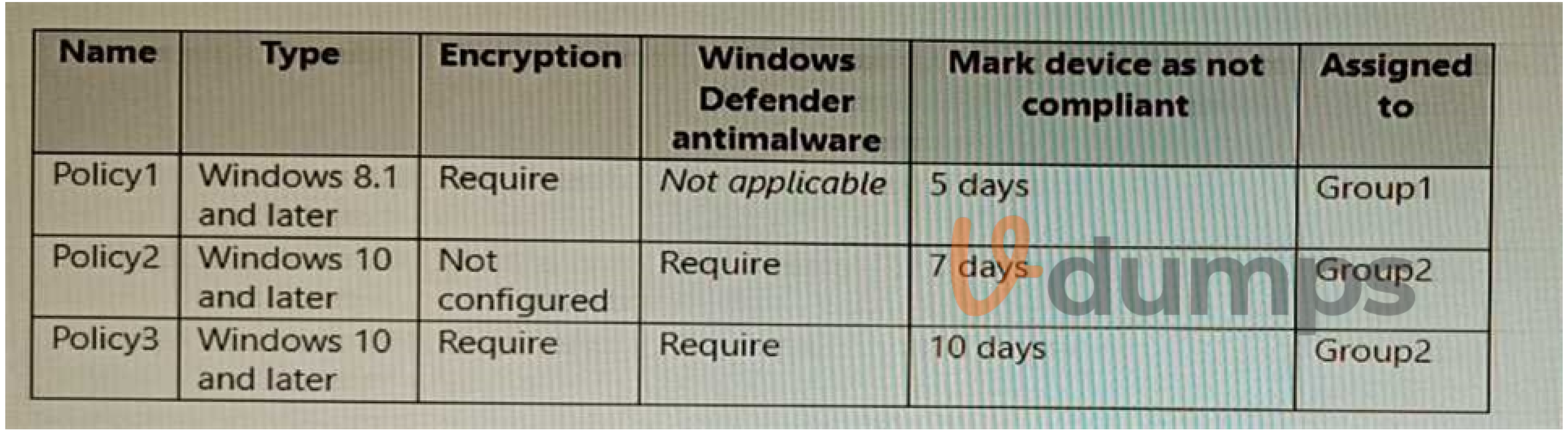
Section:
Explanation:

QUESTION 37
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

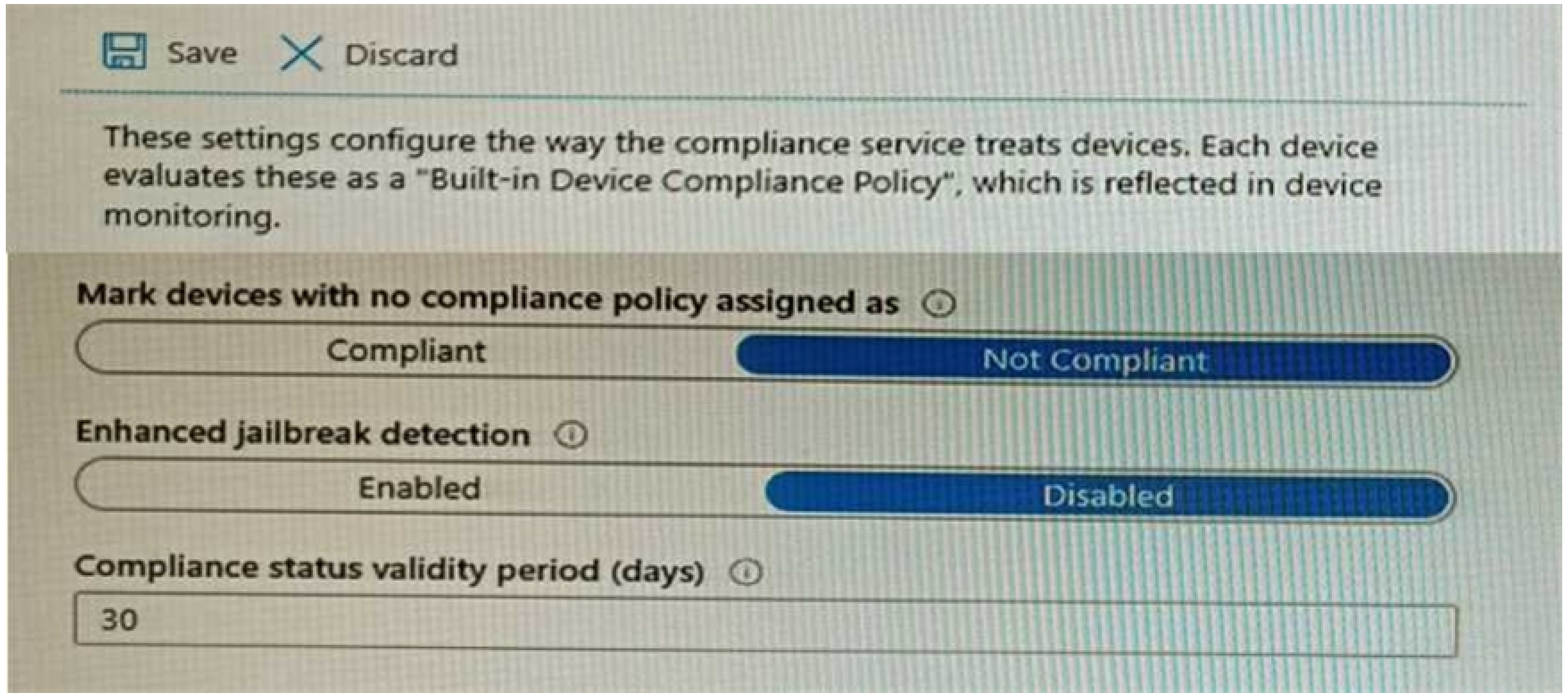
Correct Answer: B
Section:
Explanation:
To enable or disable security defaults in your directory, sign in to the Azure portal as a security administrator, Conditional Access administrator, or global administrator.
Note: Conditional Access Administrator
Users with this role have the ability to manage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

QUESTION 38
HOTSPOT
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.



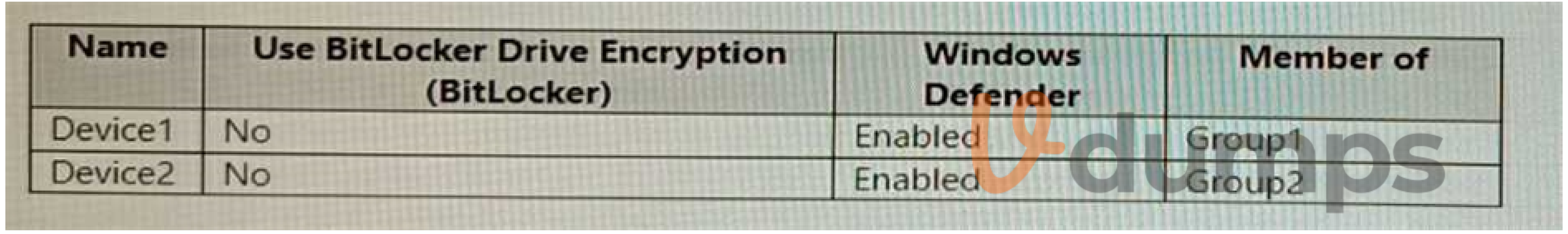
These settings configure the way the compliance service treats devices. Each device evaluates these as a "Built-in Device Compliance Policy", which is reflected in device monitoring.

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

Enhanced jailbreak detection
Enabled [✓ Disabled]

Compliance status validity period (days)
30

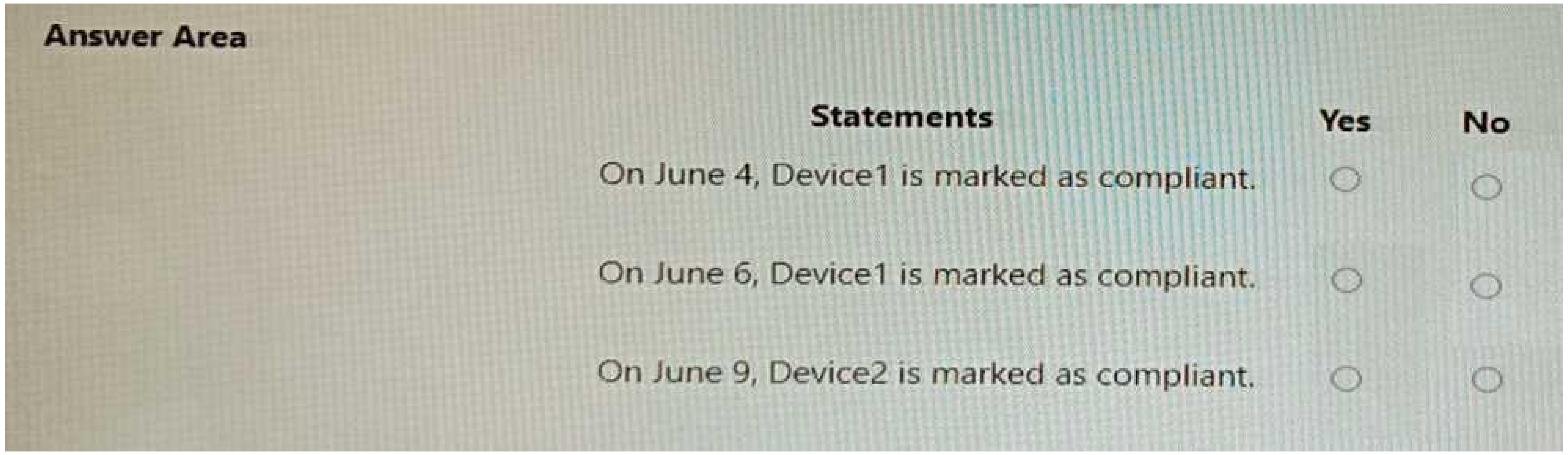
On June 1, you enroll Windows 10 devices in Intune as shown in the following table.



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.

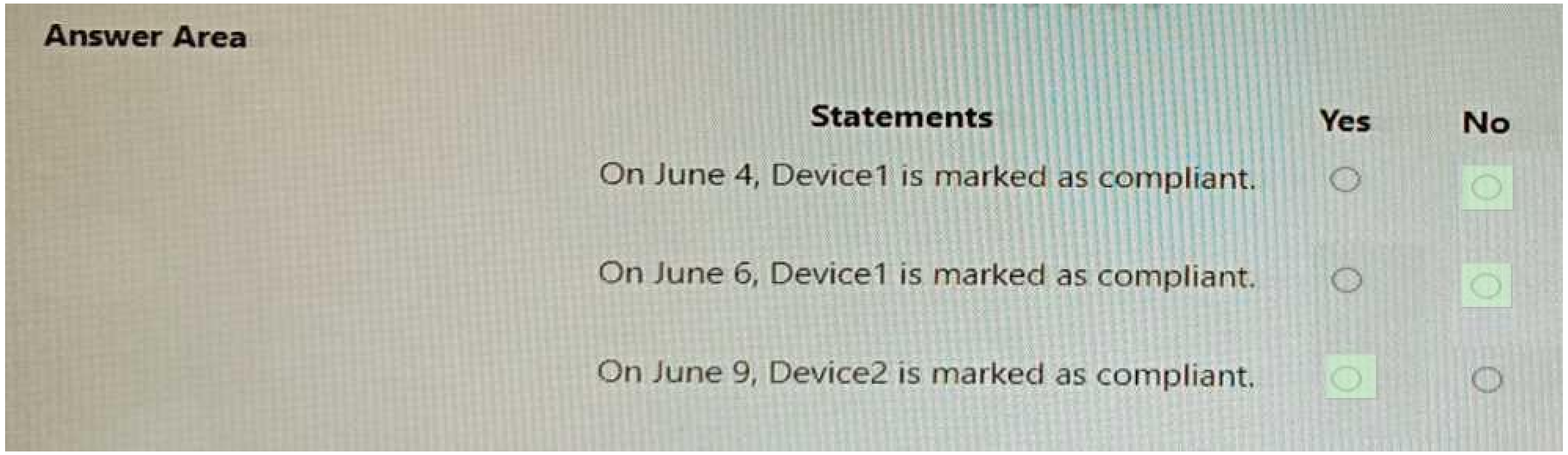
Hot Area:



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.	○	○

Answer Area:



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.	[✓ ○]	○

Section:
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

QUESTION 39
You have a Microsoft 365 subscription that contains a user named User1 and uses Microsoft Intune Suite.
You use Microsoft Intune to manage devices that run Windows 11.
User1 provides remote support for 75 devices in the marketing department.
You need to add User1 to the Remote Desktop Users group on each marketing department device.
What should you configure?

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

Correct Answer: D
Section:

QUESTION 40
You have a Microsoft 365 subscription that uses Microsoft Intune Suite.
You use Microsoft Intune to deploy and manage Windows devices.
You have 100 devices from users that left your company.
You need to repurpose the devices for new users by removing all the data and applications installed by the previous users. The solution must minimize administrative effort.
What should you do?

A. Deploy a new configuration profile to the devices.

B. Perform a Windows Autopilot reset on the devices.

C. Perform an in-place upgrade on the devices.

D. Perform a clean installation of Windows 11 on the devices.

Correct Answer: B
Section:

QUESTION 41

You have a Microsoft 365 subscription that uses Microsoft Intune Suite.
You use Microsoft Intune to manage Windows 11 devices.
You need to implement passwordless authentication that requires users to use number matching Which authentication method should you use?

A. Microsoft Authenticator

B. voice calls

C. FI002 security keys

D. text messages

Correct Answer: A
Section:

QUESTION 42

You use a Microsoft Intune subscription to manage iOS devices.
You configure a device compliance policy that blocks jailbroken iOS devices.
You need to enable Enhanced jailbreak detection.
What should you configure?

A. the Compliance policy settings

B. the device compliance policy

C. a network location

D. a configuration profile

Correct Answer: D
Section:

QUESTION 43

You have a Microsoft 365 subscription that uses Microsoft Intune.
You have five new Windows 11 Pro devices.
You need to prepare the devices for corporate use. The solution must meet the following requirements:
• Install Windows 11 Enterprise on each device.
• Install a Windows Installer (MSI) package named App1 on each device.
• Add a certificate named Certificate1 that is required by App1.
• Join each device to Azure AD.
Which three provisioning options can you use? Each correct answer presents a complete solution.
NOTE: Each correct selection is worth one point.

A. subscription activation

B. a custom Windows image

C. an in-place upgrade

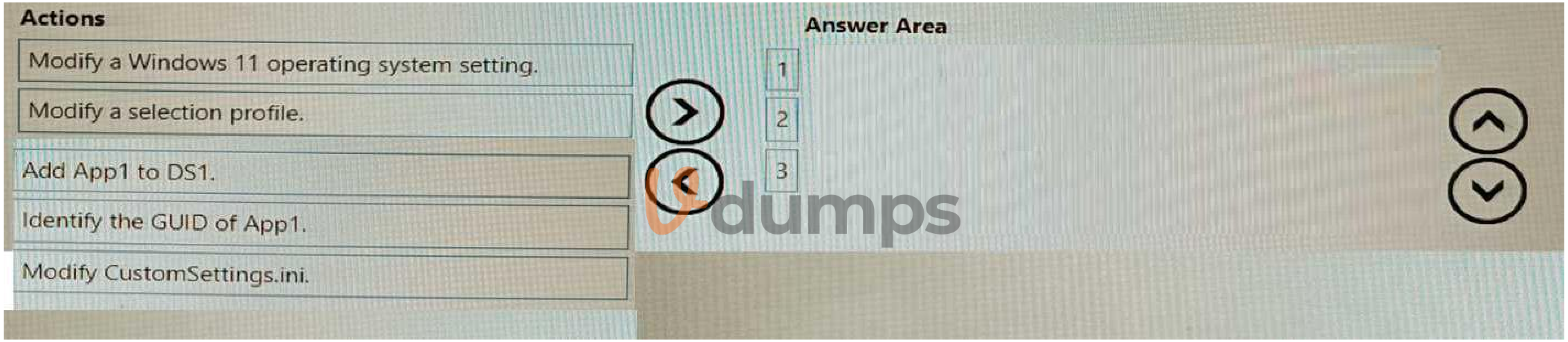
D. Windows Autopilot

E. provisioning packages

Correct Answer: B, D, E
Section:

QUESTION 44
DRAG DROP
You have a Microsoft Deployment Toolkit (MDT) deployment share named DS1.
You import a Windows 11 image to DS1.
You have an executable installer for an application named App1.
You need to ensure that App1 will be installed for all the task sequences that deploy the image.
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.

Select and Place:



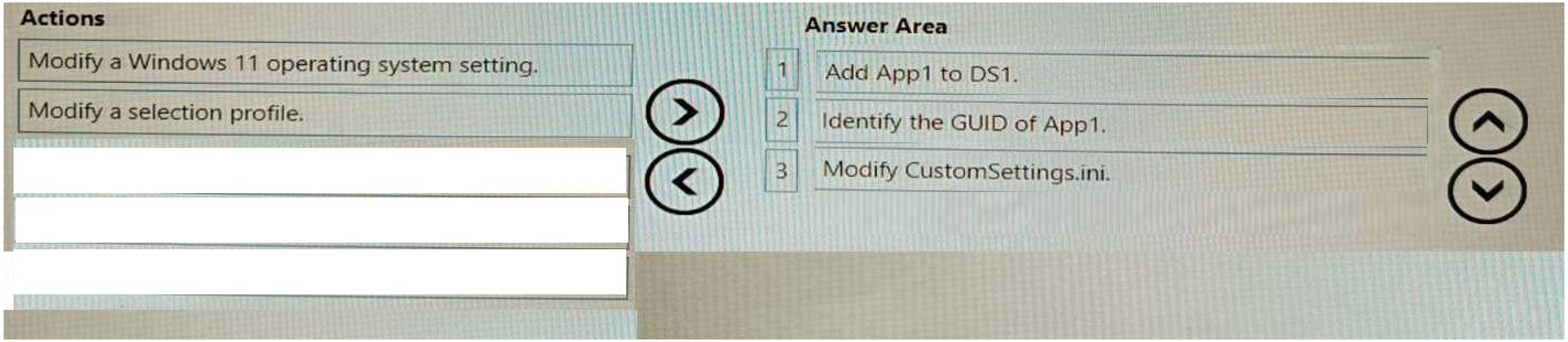
Actions

- Modify a Windows 11 operating system setting.
- Modify a selection profile.
- Add App1 to DS1.
- Identify the GUID of App1.
- Modify CustomSettings.ini.

Answer Area

1
2
3

Correct Answer:



Actions

- Modify a Windows 11 operating system setting.
- Modify a selection profile.

Answer Area

1 Add App1 to DS1.
2 Identify the GUID of App1.
3 Modify CustomSettings.ini.

Section:

Explanation:

MDT is a tool that allows you to automate the deployment of Windows operating systems and applications. To install an application for all the task sequences that deploy a Windows 11 image, you need to perform the following three actions in sequence:

Add App1 to DS1. You can use the Deployment Workbench to import the executable installer of App1 to a folder in your deployment share. This will create an application entry with a unique GUID that identifies App11.

Identify the GUID of App1. You can find the GUID of App1 by opening the application properties in the Deployment Workbench and looking at the Application GUID field1. You can copy the GUID to use it later.

Modify CustomSettings.ini. You can edit the CustomSettings.ini file in your deployment share to specify which applications to install for each task sequence. You can use the Applications property to list the GUIDs of the applications you want to install, separated by commas1. For example, if you want to install App1 and another application with GUID {1234-5678-90AB-CDEF}, you can use this line:

Applications={GUID of App1},{1234-5678-90AB-CDEF}

These are the three actions you need to perform to ensure that App1 will be installed for all the task sequences that deploy the Windows 11 image from DS1. I hope this helps you.

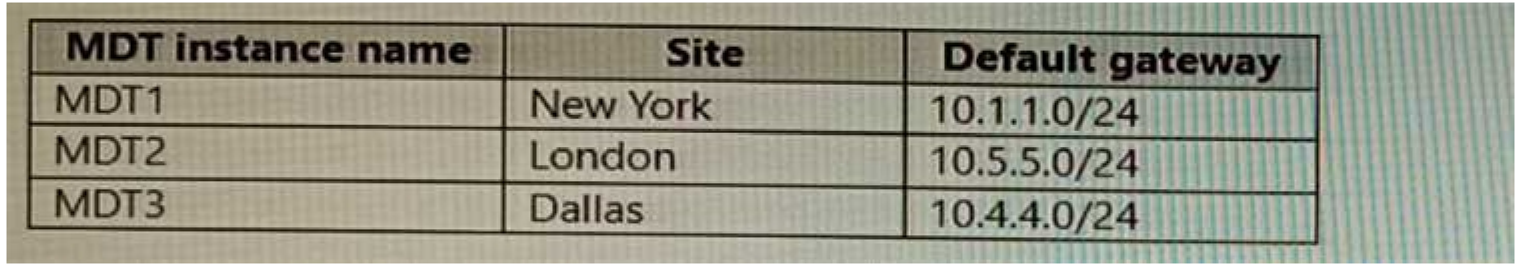
If you want to learn more about MDT and how to deploy applications with it, you can check out these resources:

Get started with the Microsoft Deployment Toolkit (MDT) (Windows 10) How to deploy applications with the Microsoft Deployment Toolkit

QUESTION 45

HOTSPOT

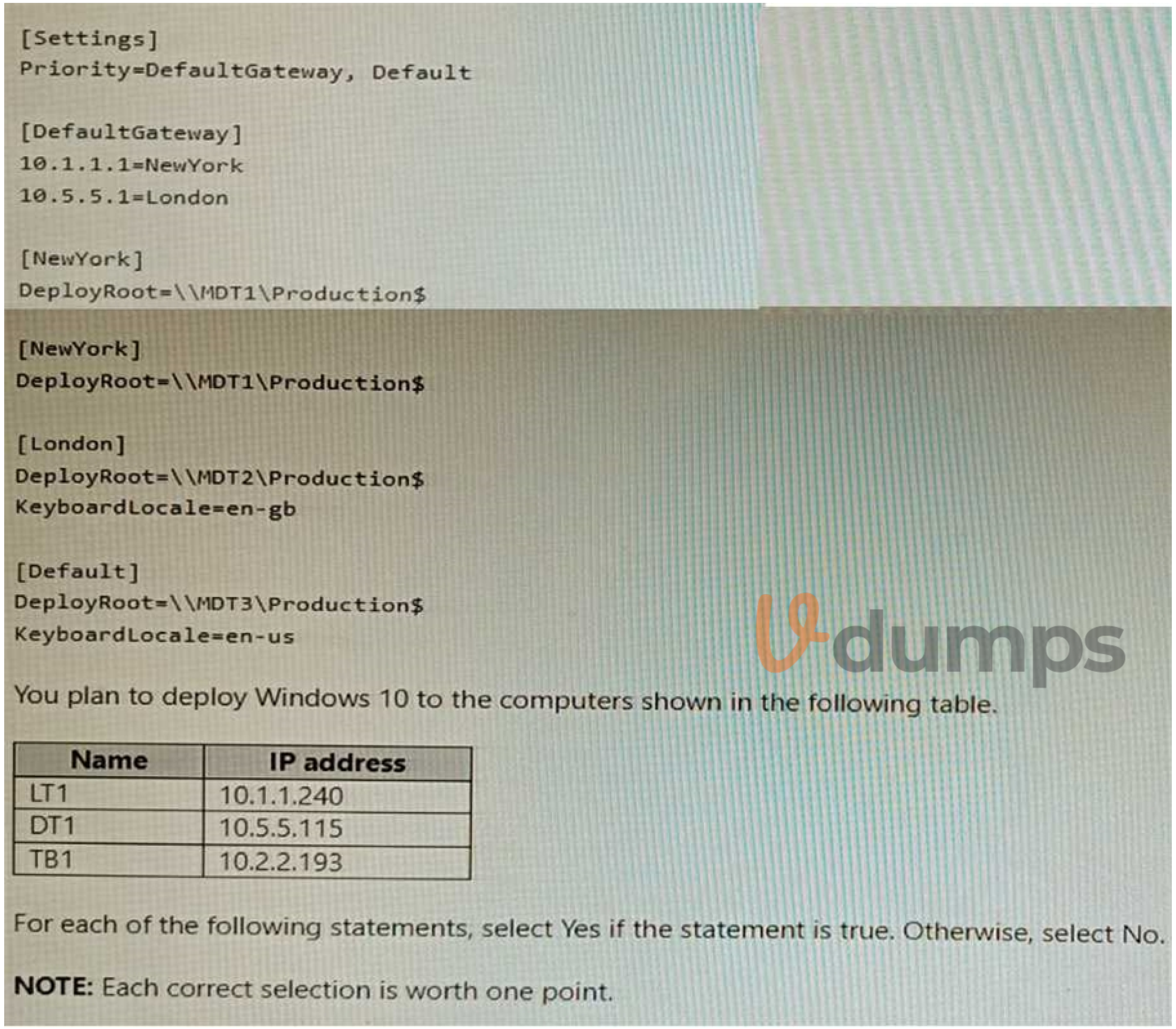
You have the Microsoft Deployment Toolkit (MDT) installed in three sites as shown in the following table.



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

You use Distributed File System (DFS) Replication to replicate images in a share named Production.

You configure the following settings in the Bootstrap.ini file.



```
[Settings]
Priority=DefaultGateway, Default

[DefaultGateway]
10.1.1.1=NewYork
10.5.5.1=London

[NewYork]
DeployRoot=\\MDT1\Production$
```

```
[NewYork]
DeployRoot=\\MDT1\Production$
```

```
[London]
DeployRoot=\\MDT2\Production$
KeyboardLocale=en-gb

[Default]
DeployRoot=\\MDT3\Production$
KeyboardLocale=en-us
```

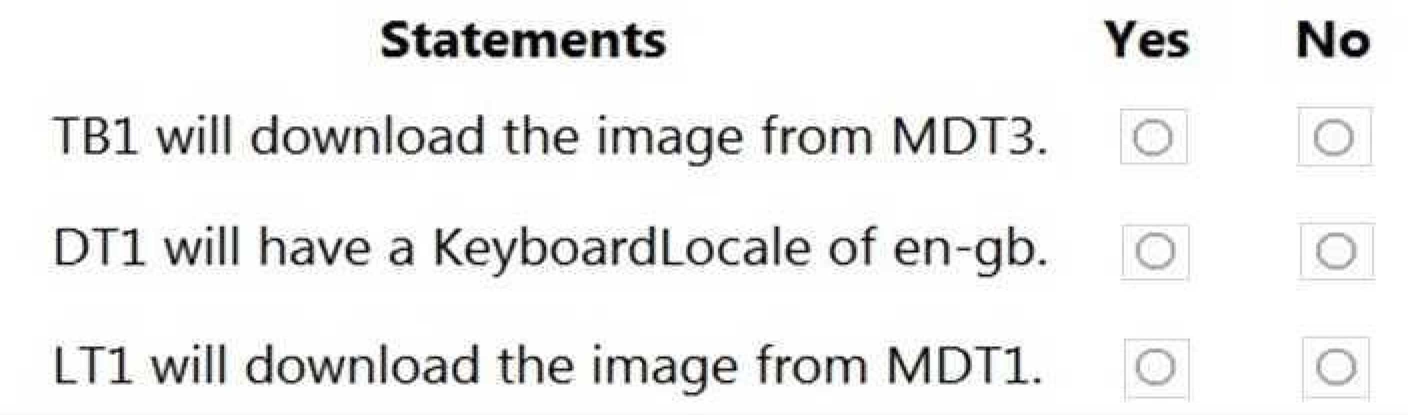
You plan to deploy Windows 10 to the computers shown in the following table.

Name	IP address
LT1	10.1.1.240
DT1	10.5.5.115
TB1	10.2.2.193

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

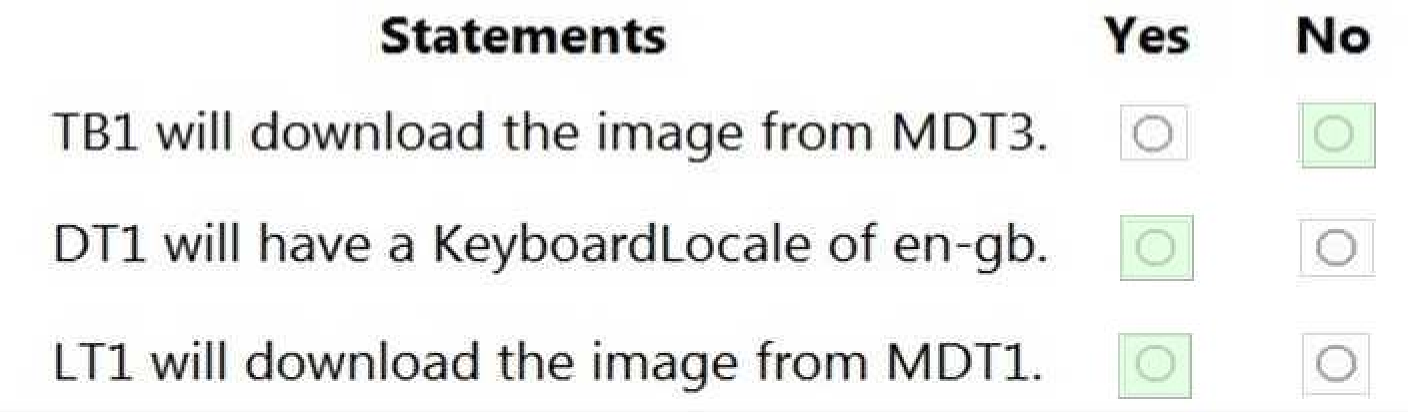
NOTE: Each correct selection is worth one point.

Hot Area:



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

Answer Area:

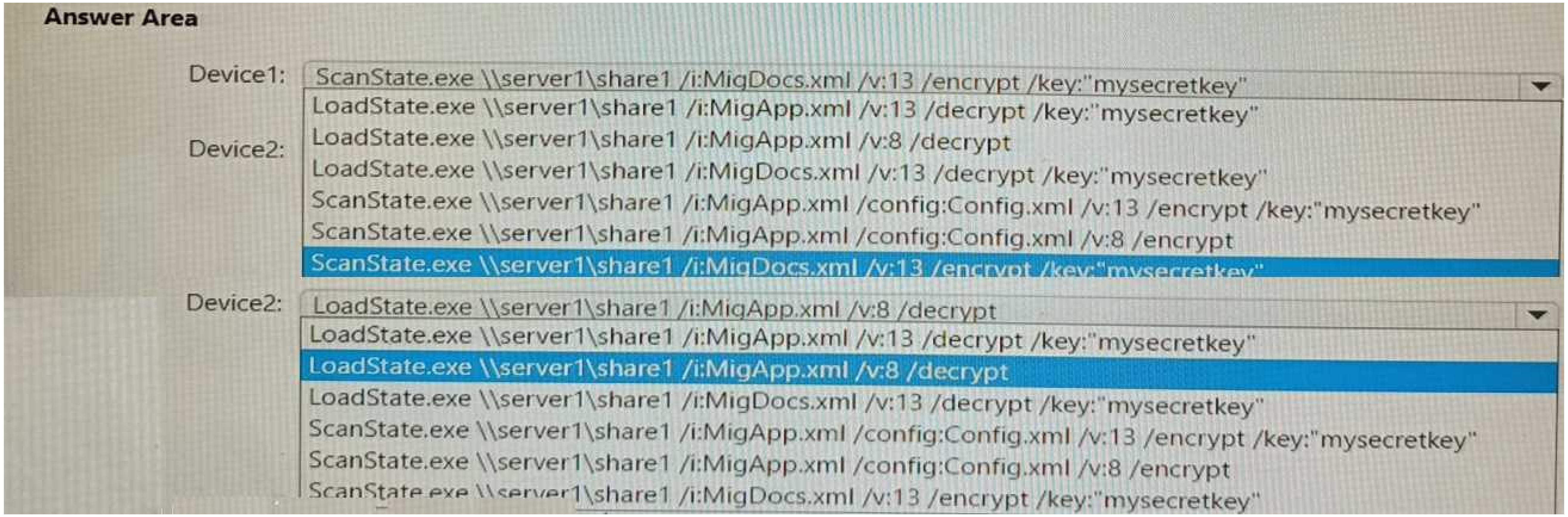


Statements	Yes	No
TB1 will download the image from MDT3.	○	●
DT1 will have a KeyboardLocale of en-gb.	●	○
LT1 will download the image from MDT1.	●	○

Section:
Explanation:

QUESTION 46
HOTSPOT
You have the devices shown in the following table.
You need to migrate app data from Device1 to Device2. The data must be encrypted and stored on Seryer1 during the migration.
Which command should you run on each device? To answer, select the appropriate options in the answer area.
NOTE: Each correct selection is worth one point.

Hot Area:



Answer Area

Device1: ScanState.exe \\server1\share1 /i:MigDocs.xml /v:13 /encrypt /key:"mysecretkey"

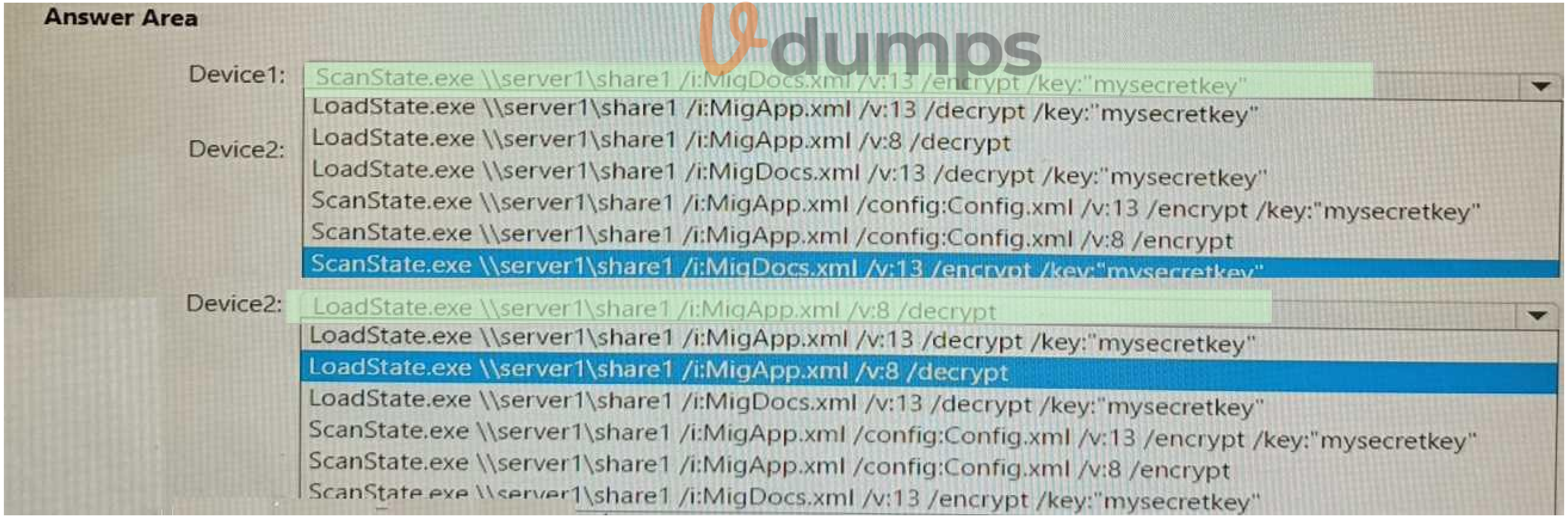
LoadState.exe \\server1\share1 /i:MigApp.xml /v:13 /decrypt /key:"mysecretkey"
LoadState.exe \\server1\share1 /i:MigApp.xml /v:8 /decrypt
LoadState.exe \\server1\share1 /i:MigDocs.xml /v:13 /decrypt /key:"mysecretkey"
ScanState.exe \\server1\share1 /i:MigApp.xml /config:Config.xml /v:13 /encrypt /key:"mysecretkey"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

Device2:

Device2: LoadState.exe \\server1\share1 /i:MigApp.xml /v:8 /decrypt

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

Answer Area:



Answer Area

Device1: ScanState.exe \\server1\share1 /i:MigDocs.xml /v:13 /encrypt /key:"mysecretkey"

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

Device2:

Device2: LoadState.exe \\server1\share1 /i:MigApp.xml /v:8 /decrypt

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

Section:
Explanation:

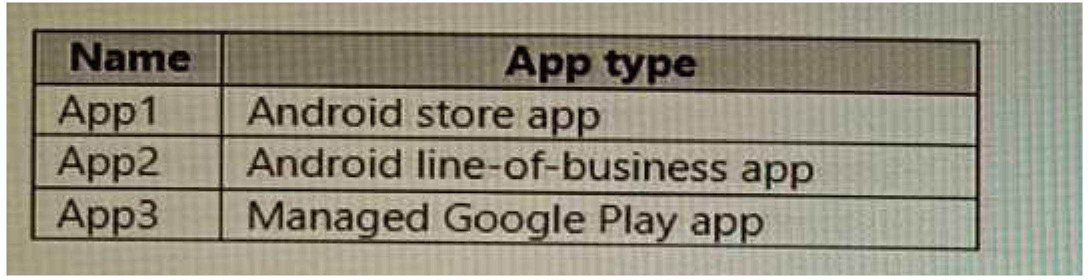
QUESTION 47

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

Correct Answer: B
Section:

QUESTION 48
You have an Azure AD tenant that contains the devices shown in the following table.
You purchase Windows 11 Enterprise E5 licenses.



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

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

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

Correct Answer: B
Section:

QUESTION 49
You have a Microsoft 365 E5 subscription that uses Microsoft Intune.
You add apps to Intune as shown in the following table.
You need to create an app configuration policy named Policy1 for the Android Enterprise platform.
Which apps can you manage by using Policyl1?

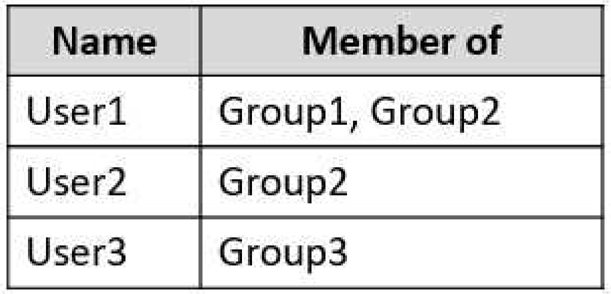
A. App2 only
B. App3 only
C. App1 and App3 only
D. App2 and App3 only
E. App1, App2, and App3

Correct Answer: D
Section:

QUESTION 50

HOTSPOT

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

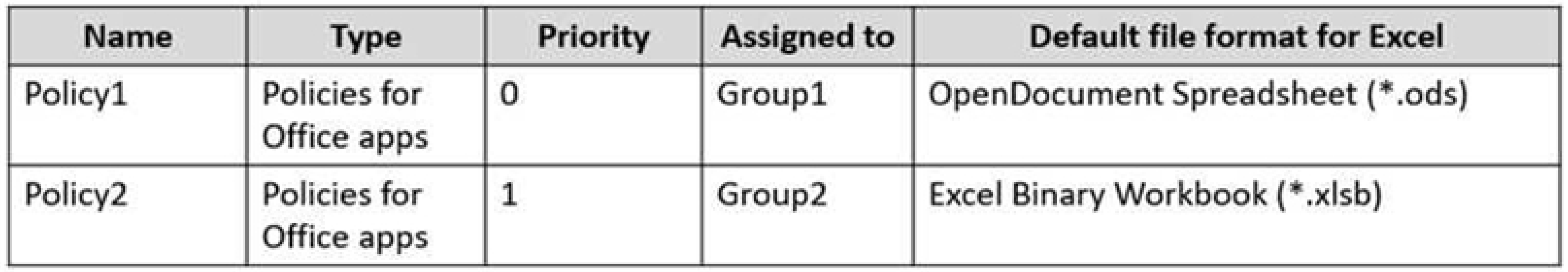


Name	Member of
User1	Group1, Group2
User2	Group2
User3	Group3

Group2 and Group3 are members of Group1.

All the users use Microsoft Excel.

From the Microsoft Endpoint Manager admin center, you create the policies shown in the following table.

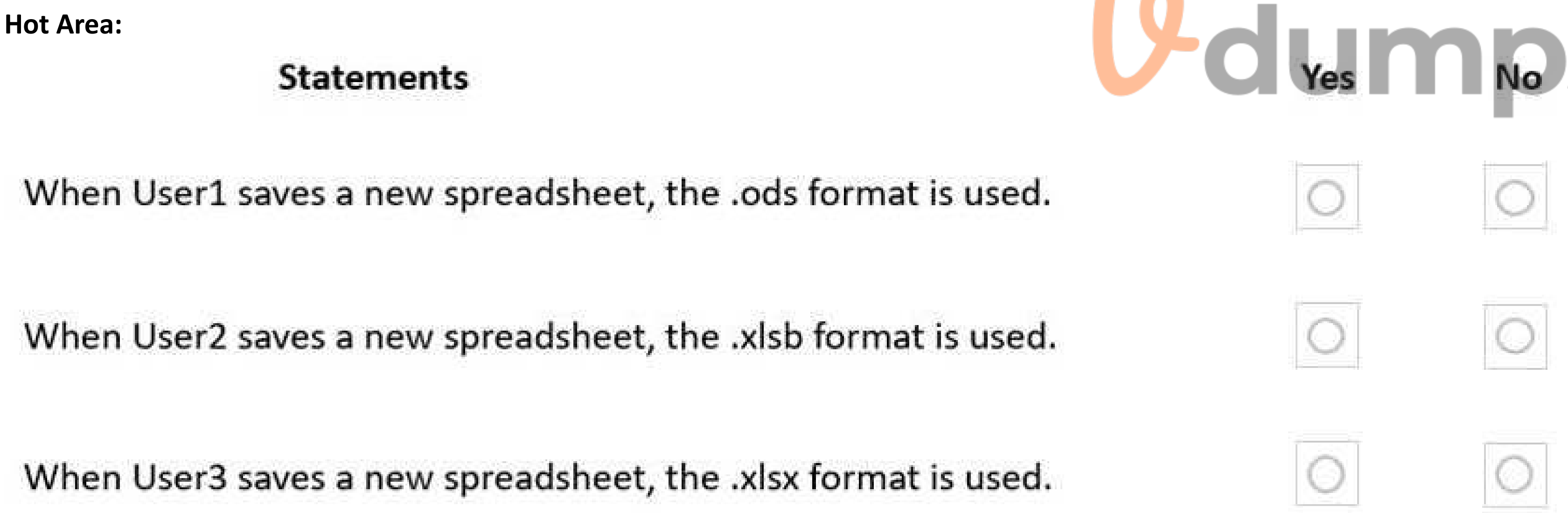


Name	Type	Priority	Assigned to	Default file format for Excel
Policy1	Policies for Office apps	0	Group1	OpenDocument Spreadsheet (*.ods)
Policy2	Policies for Office apps	1	Group2	Excel Binary Workbook (*.xlsb)

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

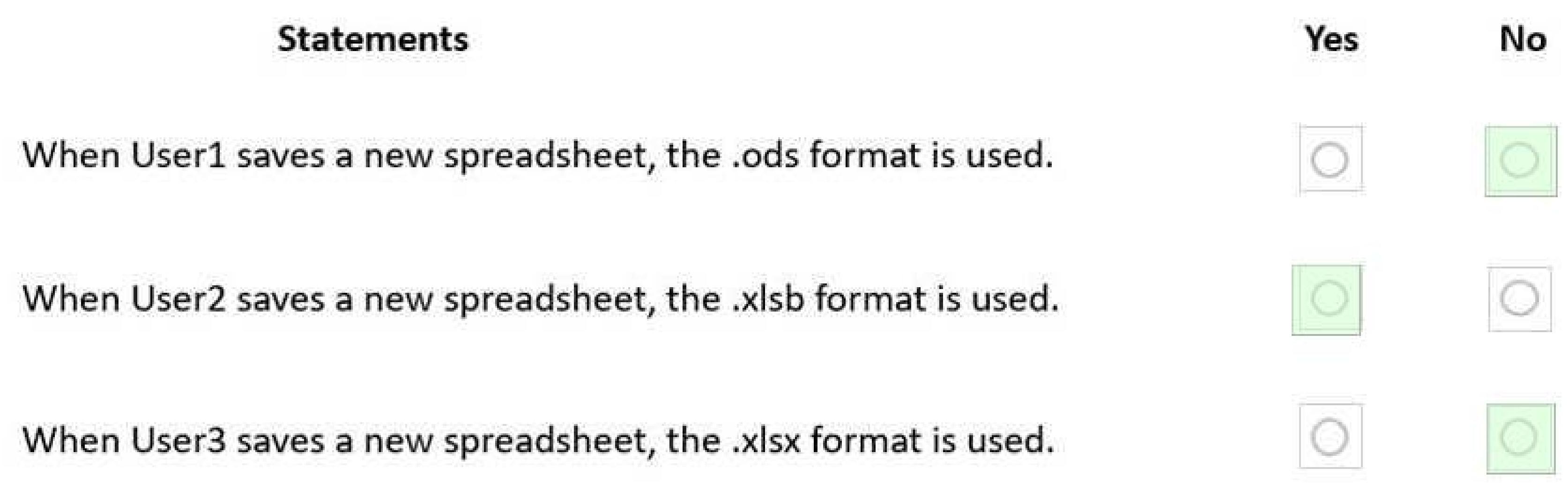
NOTE: Each correct selection is worth one point.

Hot Area:



Statements	Yes	No
When User1 saves a new spreadsheet, the .ods format is used.	○	○
When User2 saves a new spreadsheet, the .xlsb format is used.	○	○
When User3 saves a new spreadsheet, the .xlsx format is used.	○	○

Answer Area:



Statements	Yes	No
When User1 saves a new spreadsheet, the .ods format is used.	○	[✓ ○]
When User2 saves a new spreadsheet, the .xlsb format is used.	[✓ ○]	○
When User3 saves a new spreadsheet, the .xlsx format is used.	○	[✓ ○]

Section:
Explanation:
Box 1: No User1 is member of Group1 and Group2.
Policy1 with priority 0 is assigned to Group1: default file format for Excel is.ods.
Policy2 with priority 1 is assigned to Group2: default file format for Excel is.xlsb.
Note: Key points to remember about policy order Policies are assigned an order of priority.
Devices receive the first applied policy only.
You can change the order of priority for policies.
Default policies are given the lowest order of priority.
Box 2: Yes User2 is member of Group2.
Group2 and Group3 are members of Group1.
Box 3: No User3 is member of Group3.
Group2 and Group3 are members of Group1.
Reference: https://learn.microsoft.com/en-us/microsoft-365/security/defender-business/mdbpolicy-order

QUESTION 51
You have a Microsoft 365 subscription that contains 1,000 Android devices enrolled in Microsoft Intune. You create an app configuration policy that contains the following settings:
• Device enrollment type: Managed devices
• Profile Type: All Profile Types
• Platform: Android Enterprise
Which two types of apps can be associated with the policy? Each correct answer presents a complete solution. NOTE: Each correct selection is worth one point.

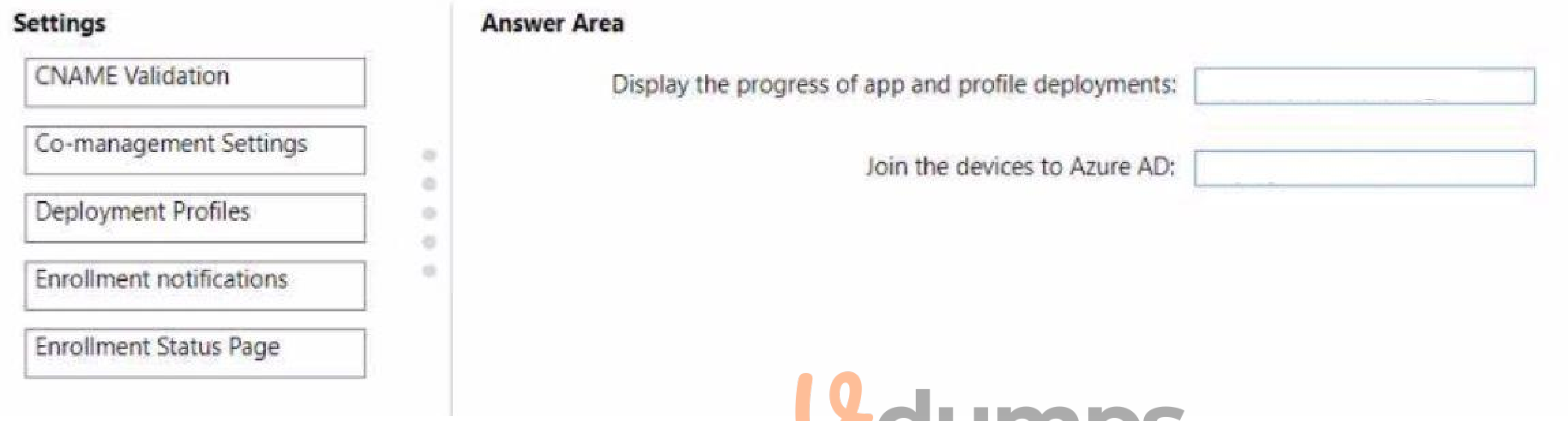
A. Built-in Android app
B. Managed Google Play store app
C. Web link
D. Android Enterprise system app
E. Android store app

Correct Answer: B, D
Section:

QUESTION 52
RAG DROP
You have a Microsoft 365 subscription that uses Microsoft Intune.

You plan to use Windows Autopilot to provision 25 Windows 11 devices.
You need to meet the following requirements during device provisioning:
* Display the progress of app and profile deployments.
* Join the devices to Azure AD.
What should you configure to meet each requirement? To answer drag the appropriate settings to the correct requirements. Each setting may be used once, more than once, or not at all. You may need to drag the split bar between panes or scroll to view content.
NOTE: Each correct selection is worth one point.

Select and Place:



Settings

CNAME Validation

Co-management Settings

Deployment Profiles

Enrollment notifications

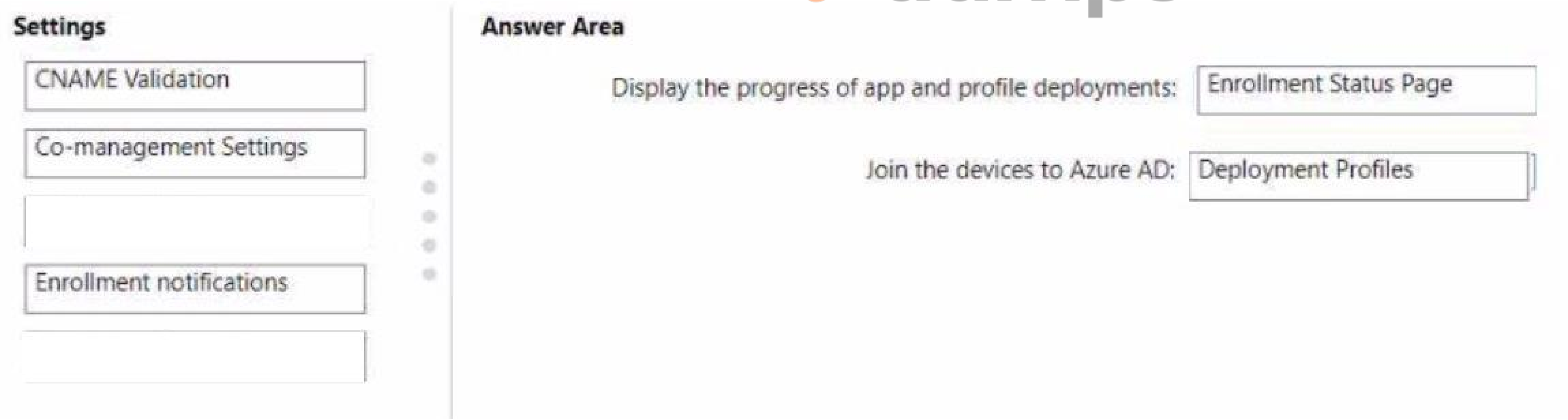
Enrollment Status Page

Answer Area

Display the progress of app and profile deployments:

Join the devices to Azure AD:

Correct Answer:



Settings

CNAME Validation

Co-management Settings

Enrollment notifications

Answer Area

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

Join the devices to Azure AD: Deployment Profiles

Section:
Explanation:

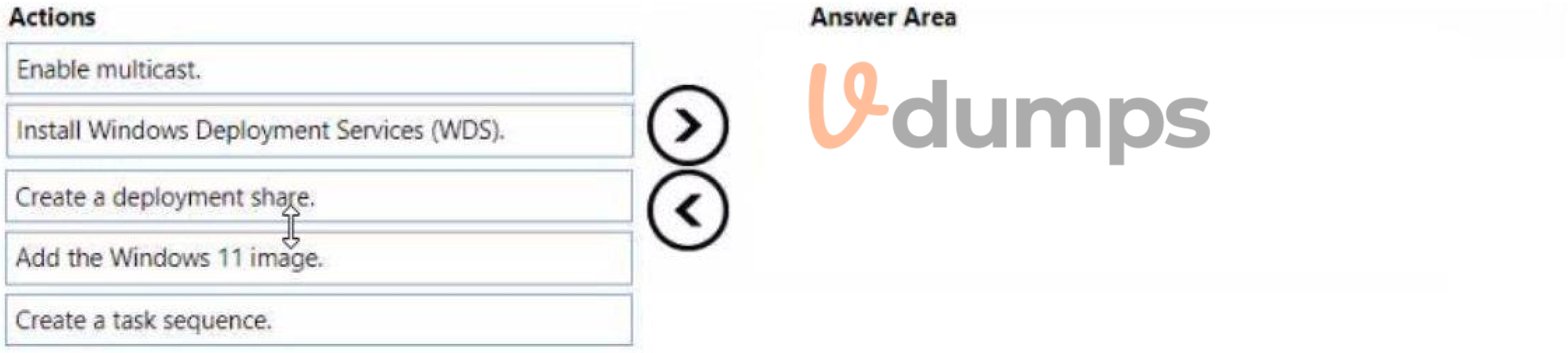
QUESTION 53
Your company has a Remote Desktop Gateway (RD Gateway).
You have a server named Server1 that is accessible by using Remote Desktop Services (RDS) through the RD Gateway.
You need to configure a Remote Desktop connection to connect through the gateway.
Which setting should you configure?

A. Connect from anywhere
B. Server authentication
C. Connection settings
D. Local devices and resources

Correct Answer: A
Section:
Explanation:
To connect to a remote server through the RD Gateway, you need to configure the Connect from anywhere setting in the Remote Desktop Connection client. This setting allows you to specify the domain name and port of the RD Gateway server, as well as the authentication method. The other settings are not related to the RD Gateway connection.Reference:Configure Remote Desktop Connection Settings for Remote Desktop Gateway

QUESTION 54
DRAG DROP
Your network contains an Active Directory domain.
You install the Microsoft Deployment Toolkit (MDT) on a server.
You have a custom image of Windows 11.
You need to deploy the image to 100 devices by using MDT.
Which three actions should you perform in sequence? To answer, move answer area and arrange them in the correct order.

Select and Place:

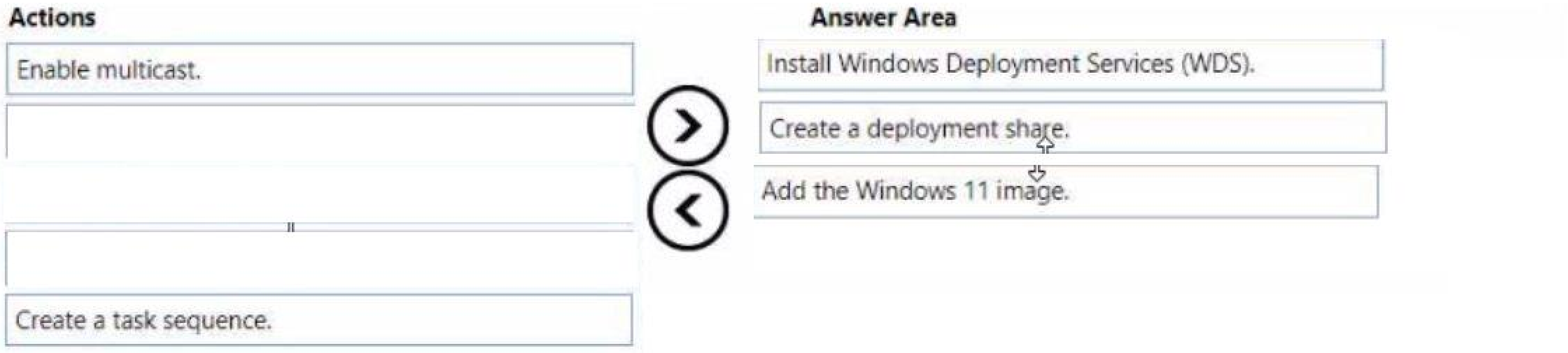


Actions

- Enable multicast.
- Install Windows Deployment Services (WDS).
- Create a deployment share.
- Add the Windows 11 image.
- Create a task sequence.

Answer Area

Correct Answer:



Actions

- Enable multicast.
- Create a task sequence.

Answer Area

- Install Windows Deployment Services (WDS).
- Create a deployment share.
- Add the Windows 11 image.

Section:

Explanation:
Install Windows Deployment Services (WDS)
Create a deployment share.
Add the Windows 11 image.

QUESTION 55
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

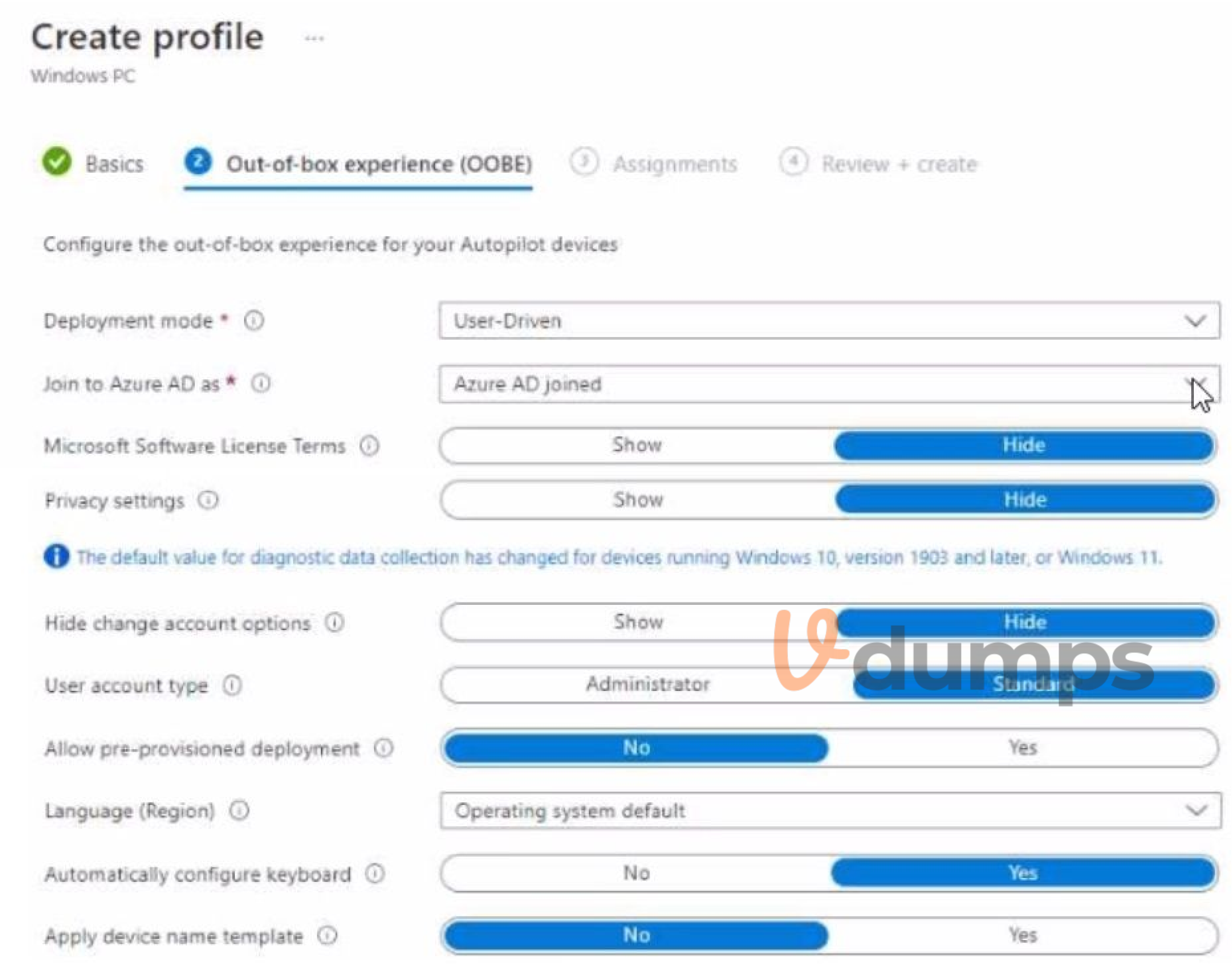
Correct Answer: C
Section:
Explanation:
To capture an image of a reference computer and make it ready for deployment to multiple computers, you need to run the sysprep command with the /generalize option. This option removes all unique system information from the Windows installation, such as the computer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

QUESTION 56
Your network contains an on-premises Active Directory domain. The domain contains two computers named Computer1 and Computer? that run Windows 10.
You install Windows Admin Center on Computer1.
You need to manage Computer2 from Computer1 by using Windows Admin Center.
What should you do on Computed?

A. Update the TrustedHosts list
B. Run the Enable-PSRemoting cmdlet
C. Allow Windows Remote Management (WinRM) through the Microsoft Defender firewall.
D. Add an inbound Microsoft Defender Firewall rule.

Correct Answer: B
Section:
Explanation:
To manage a remote computer from Windows Admin Center, you need to enable PowerShell remoting on the remote computer. You can do this by running the Enable-PSRemoting cmdlet, which configures the WinRM service, creates a listener, and allows inbound firewall rules for PowerShell remoting. The other options are not sufficient or necessary for this task.Reference:Installation and configuration for Windows Remote Management

QUESTION 57
HOTSPOT
You have a hybrid Azure AD tenant.
You configure a Windows Autopilot deployment profile as shown in the following exhibit.



Create profile ...

Windows PC

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

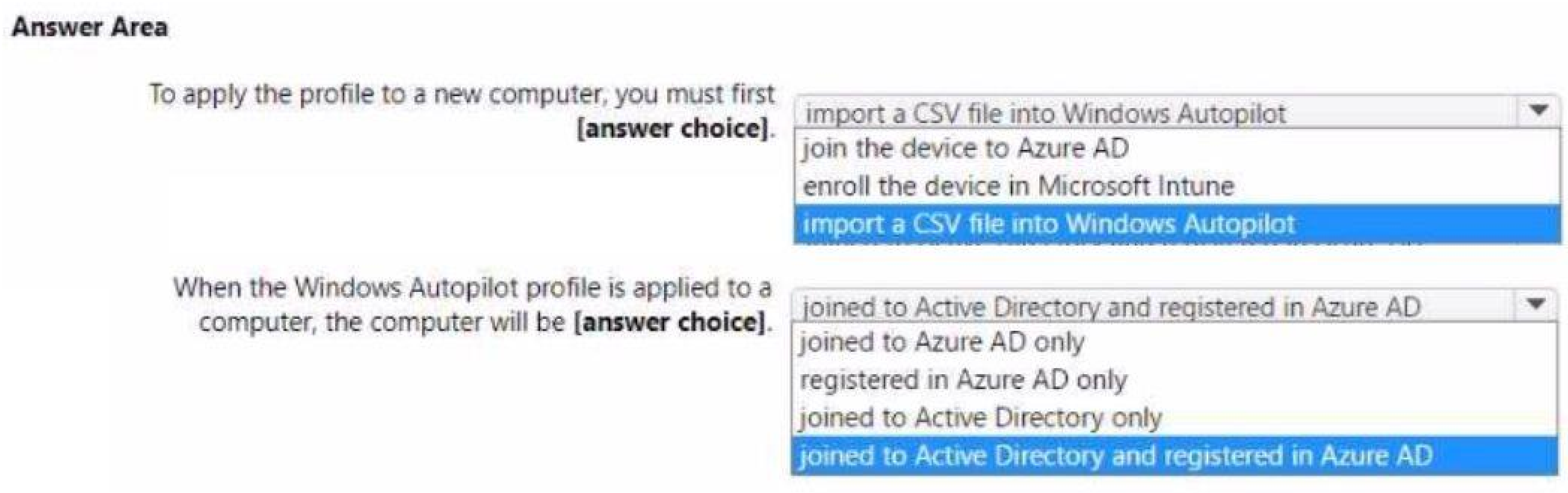
Deployment mode * ⓘ	User-Driven
Join to Azure AD as * ⓘ	Azure AD joined
Microsoft Software License Terms ⓘ	Show [✓ Hide]
Privacy settings ⓘ	Show [✓ Hide]

ⓘ The default value for diagnostic data collection has changed for devices running Windows 10, version 1903 and later, or Windows 11.

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

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

Hot Area:



Answer Area

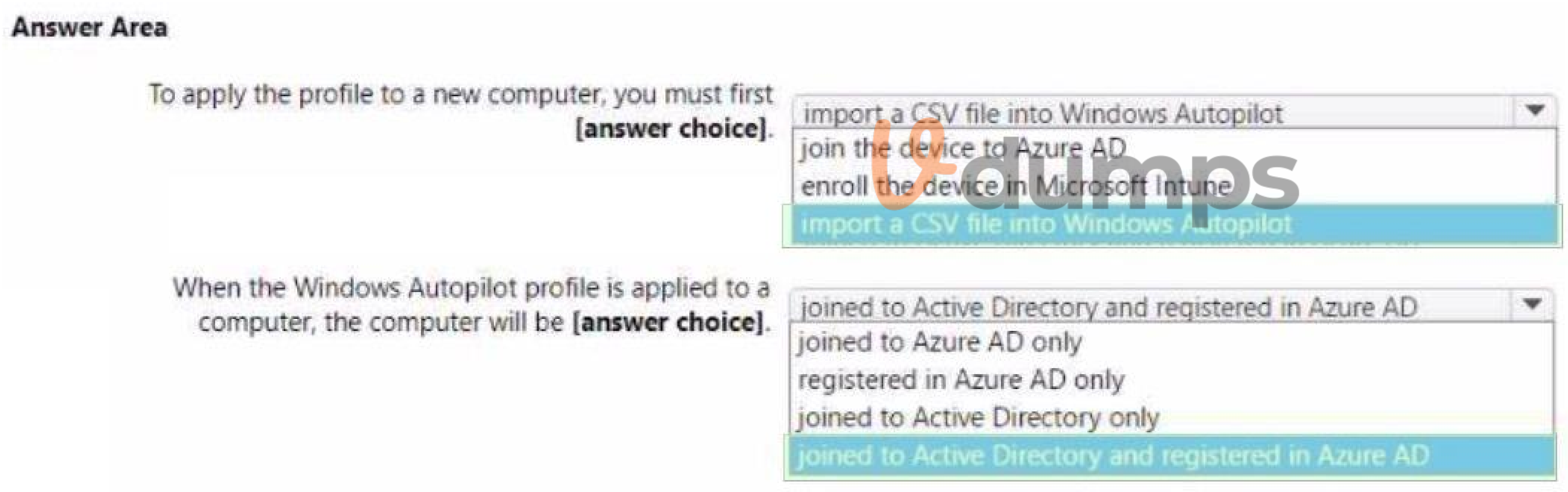
To apply the profile to a new computer, you must first **[answer choice]**.

- import a CSV file into Windows Autopilot
- 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 **[answer choice]**.

- joined to Active Directory and registered in Azure AD
- joined to Azure AD only
- registered in Azure AD only
- joined to Active Directory only
- joined to Active Directory and registered in Azure AD

Answer Area:



Answer Area

To apply the profile to a new computer, you must first **[answer choice]**.

- import a CSV file into Windows Autopilot
- 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 **[answer choice]**.

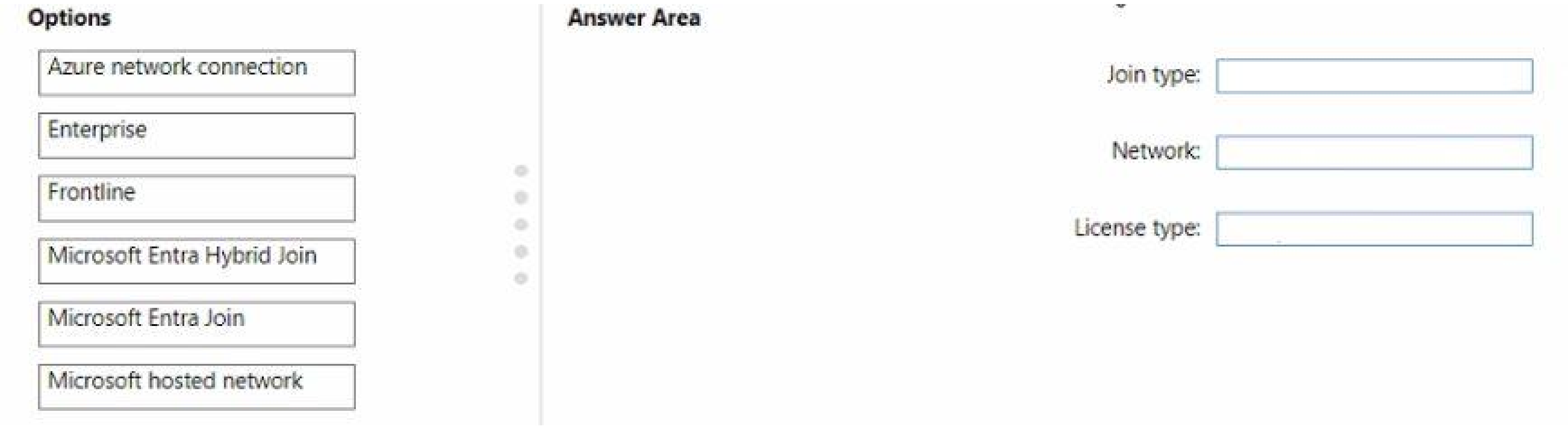
- joined to Active Directory and registered in Azure AD
- joined to Azure AD only
- registered in Azure AD only
- joined to Active Directory only
- joined to Active Directory and registered in Azure AD

Section:
Explanation:

QUESTION 58
DRAG DROP
Your on-premises network contains an Active Directory Domain Services (AD DS) domain.
You have an Azure subscription that contains a virtual network named VNet1. VNet1 contains five virtual machines and is NOT connected to the on-premises network.
You have a Microsoft 365 subscription that uses Microsoft Intune Suite.
You purchase Windows 365 Enterprise licenses.
You need to deploy Cloud PC. The solution must meet the following requirements:
* All users must be able to access their Cloud PC at any time without any restrictions.
* The users must be able to connect to the virtual machines on VNet1.

How should you configure the provisioning policy for Windows 365? To answer, drag the appropriate options to the correct settings. Each option 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.

Select and Place:



Options

- Azure network connection
- Enterprise
- Frontline
- Microsoft Entra Hybrid Join
- Microsoft Entra Join
- Microsoft hosted network

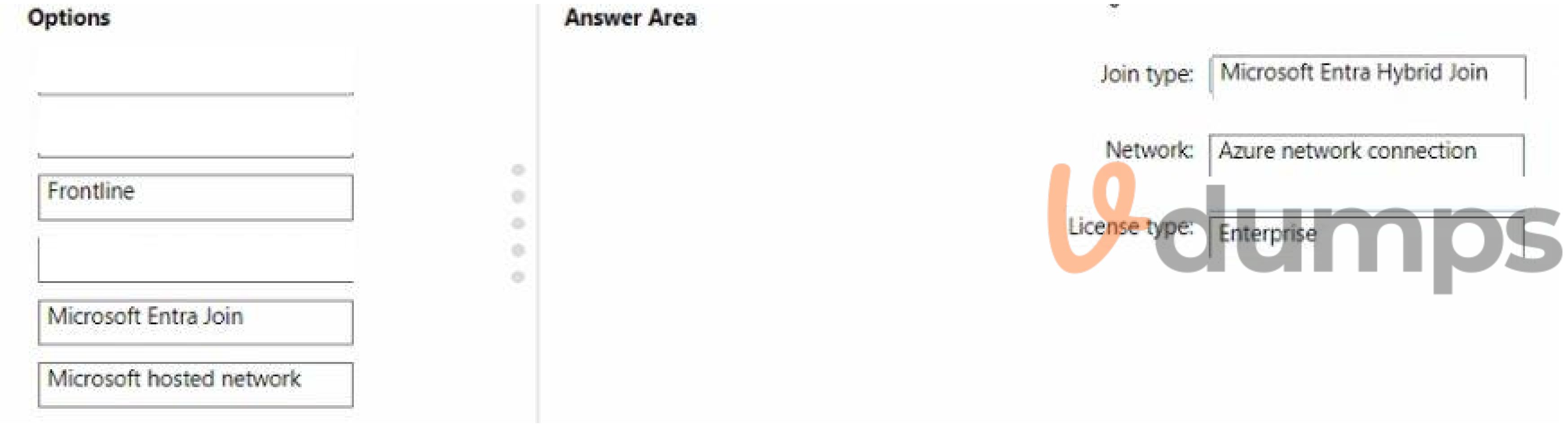
Answer Area

Join type:

Network:

License type:

Correct Answer:



Options

- Frontline
- Microsoft Entra Join
- Microsoft hosted network

Answer Area

Join type: Microsoft Entra Hybrid Join

Network: Azure network connection

License type: Enterprise

Section:
Explanation:

QUESTION 59
You have a Microsoft Intune subscription associated to an Azure AD tenant named contoso.com.
Users use one of the following three suffixes when they sign in to the tenant: us.contoso.com, eu.contoso.com, or contoso.com.
You need to ensure that the users are NOT required to specify the mobile device management (MDM) enrollment URL as part of the enrollment process. The solution must minimize the number of changes.
Which DNS records do you need?

A. three CNAME records
B. one CNAME record only
C. three TXT records
D. one TXT record only

Correct Answer: A
Section:

QUESTION 60

DRAG DROP

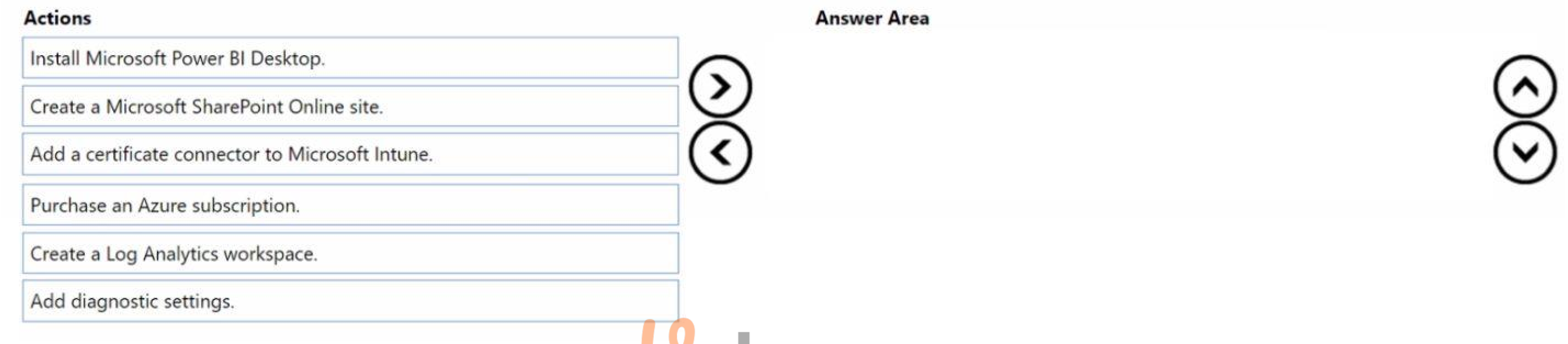
Your company has a Microsoft 365 E5 tenant.

All the devices of the company are enrolled in Microsoft Intune.

You need to create advanced reports by using custom queries and visualizations from raw Microsoft Intune data.

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.

Select and Place:



Actions

Install Microsoft Power BI Desktop.

Create a Microsoft SharePoint Online site.

Add a certificate connector to Microsoft Intune.

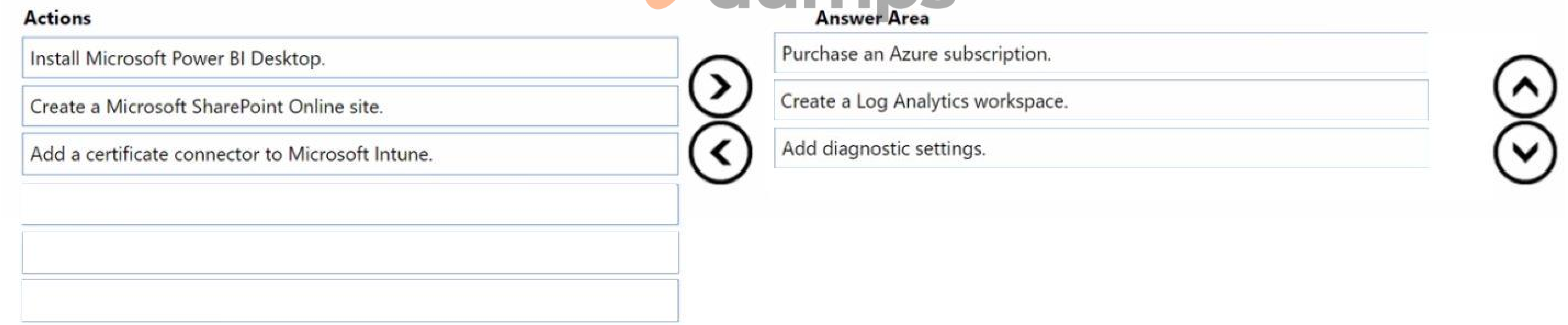
Purchase an Azure subscription.

Create a Log Analytics workspace.

Add diagnostic settings.

Answer Area

Correct Answer:



Actions

Install Microsoft Power BI Desktop.

Create a Microsoft SharePoint Online site.

Add a certificate connector to Microsoft Intune.

Answer Area

Purchase an Azure subscription.

Create a Log Analytics workspace.

Add diagnostic settings.

Section:

Explanation:

Purchase an Azure subscription.

Create a Log Analytics workspace.

Add diagnostic settings.

QUESTION 61

You manage 1,000 computers that run Windows 10. All the computers are enrolled in Microsoft Intune. You manage the servicing channel settings of the computers by using Intune.
You need to review the servicing status of a computer.
What should you do?

A. From Software updates, view the Per update ring deployment state.
B. From Software updates, view the audit logs.
C. From Device configuration - Profiles, view the device status.
D. From Device compliance, view the device compliance.

Correct Answer: A
Section:

QUESTION 62
You have a workgroup computer named Client1 that runs Windows 11 and connects to a public network.
You need to enable PowerShell remoting on Client1. The solution must ensure that PowerShell remoting connections are accepted from the local subnet only.
Which PowerShell command should you run?

A. Set-NetFirewallRule -Name 'WINRM-HTTP-In-TCP-PUBLIC' -RemoteAddress Any
B. Set-PSSessionConfiguration -AccessMode Local
C. Enable-PSRemoting -Force
D. Enable-PSRemoting -SkipNetworkProfileCheck

Correct Answer: D
Section:

QUESTION 63
Your network contains an Active Directory domain. The domain contains 10 computers that run Windows 10. Users in the finance department use the computers.
You have a computer named Computer1 that runs Windows 10.
From Computer1, you plan to run a script that executes Windows PowerShell commands on the finance department computers.
You need to ensure that you can run the PowerShell commands on the finance department computers from Computer.
What should you do on the finance department computers?

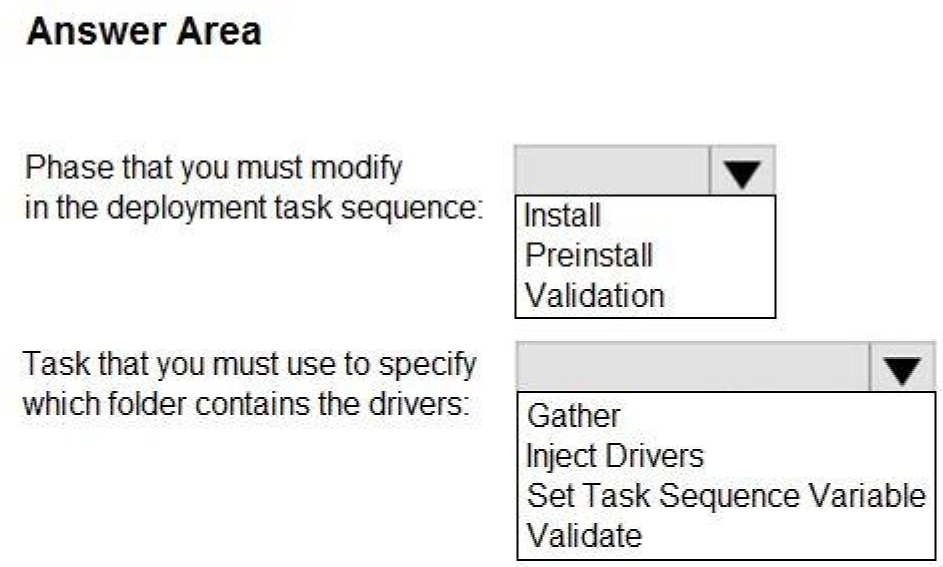
A. From Windows PowerShell, run the Enable-MMAgent cmdlet.
B. From the local Group Policy, enable the Allow Remote Shell Access setting.
C. From Windows PowerShell, run the Enable-PSRemoting cmdlet.
D. From the local Group Policy, enable the Turn on Script Execution setting.

Correct Answer: C
Section:
Explanation:
Enable-PSRemoting is specifically designed to enable remote PowerShell access. This cmdlet configures the necessary settings on the target computers to allow remote PowerShell connections. The other options are not directly related to enabling remote PowerShell: Enable-MMAgent is used for managing mobile devices. The 'Allow Remote Shell Access' group policy setting is primarily for enabling remote access for command prompt (cmd.exe), not PowerShell. The 'Turn on Script Execution' group policy setting controls whether scripts can run locally on a computer, but it doesn't enable remote PowerShell access. By running Enable-PSRemoting on the finance department computers, you'll ensure that they are ready to receive and execute PowerShell commands from Computer1.

QUESTION 64
HOTSPOT
You manage a Microsoft Deployment Toolkit (MDT) deployment share named DS1. DS1 contains an Out-of-Box Drivers folder named Windows 11 x64 that has subfolders in the format of {make name}\{model name}.

You need to modify a deployment task sequence to ensure that all the drivers in the folder that match the make and model of the computers are installed without using PnP detection or selection profiles.
What should you do? To answer, select the appropriate options in the answer area.
NOTE: Each correct selection is worth one point.

Hot Area:



Answer Area

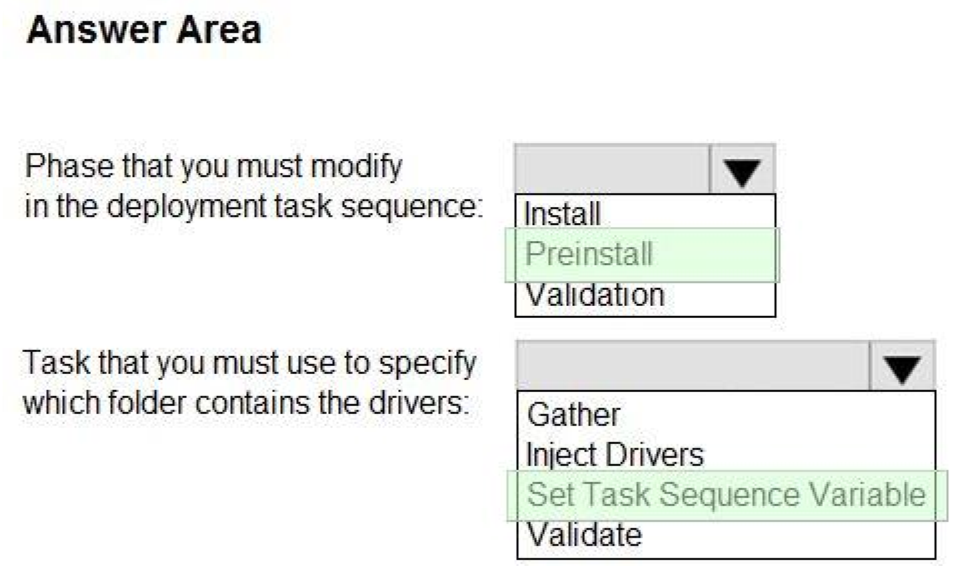
Phase that you must modify in the deployment task sequence:

Install
Preinstall
Validation

Task that you must use to specify which folder contains the drivers:

Gather
Inject Drivers
Set Task Sequence Variable
Validate

Answer Area:



Answer Area

Phase that you must modify in the deployment task sequence:

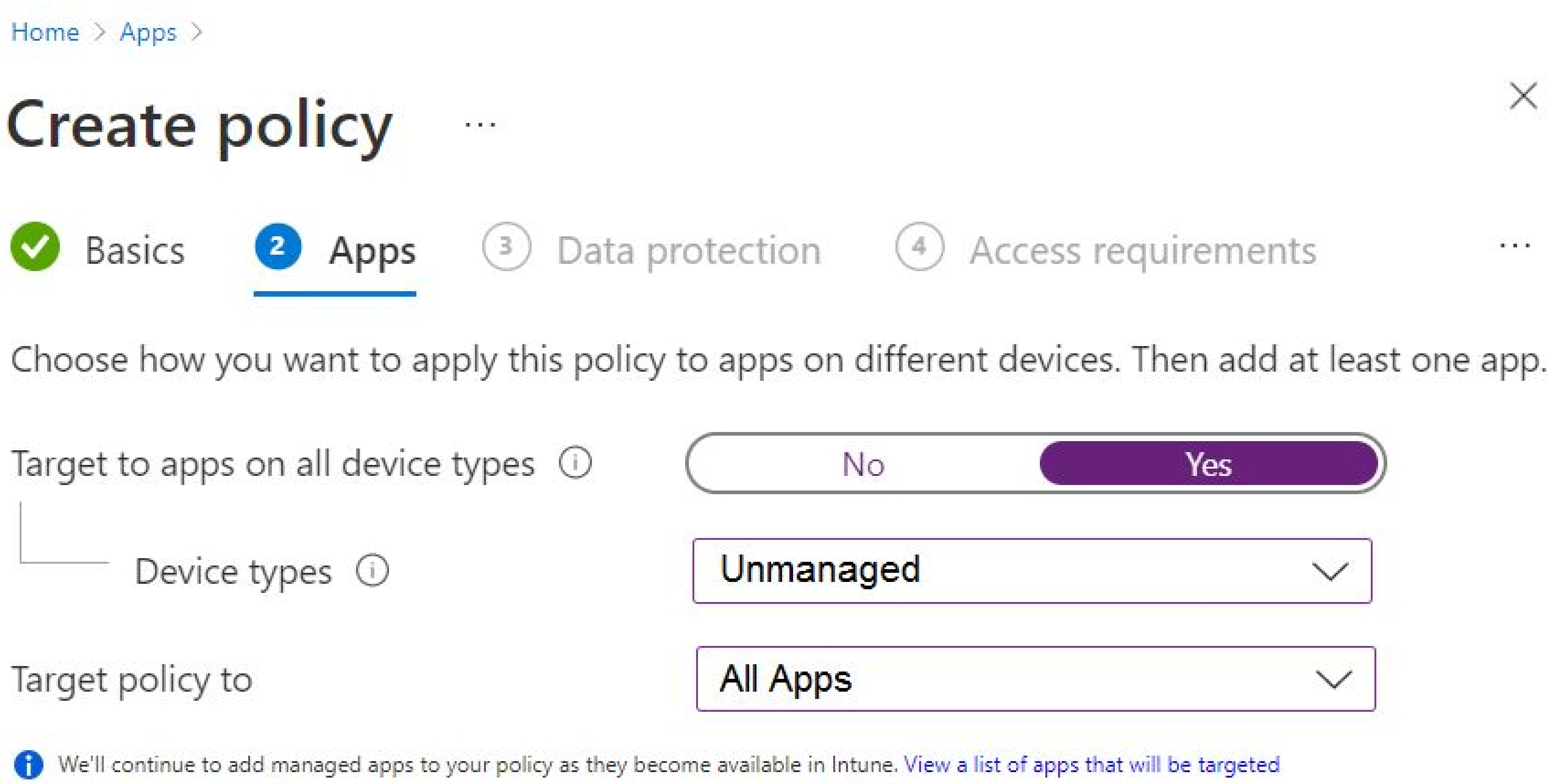
Install
[✓ Preinstall]
Validation

Task that you must use to specify which folder contains the drivers:

Gather
Inject Drivers
[✓ Set Task Sequence Variable]
Validate

Section:
Explanation:

QUESTION 65
HOTSPOT
You have a Microsoft 365 E5 subscription.
You create an app protection policy for Android device named Policy1 as shown in the following exhibit.



Home > Apps >

Create policy ...

✓ Basics ② Apps ③ Data protection ④ Access requirements ...

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

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

Device types ⓘ: Unmanaged

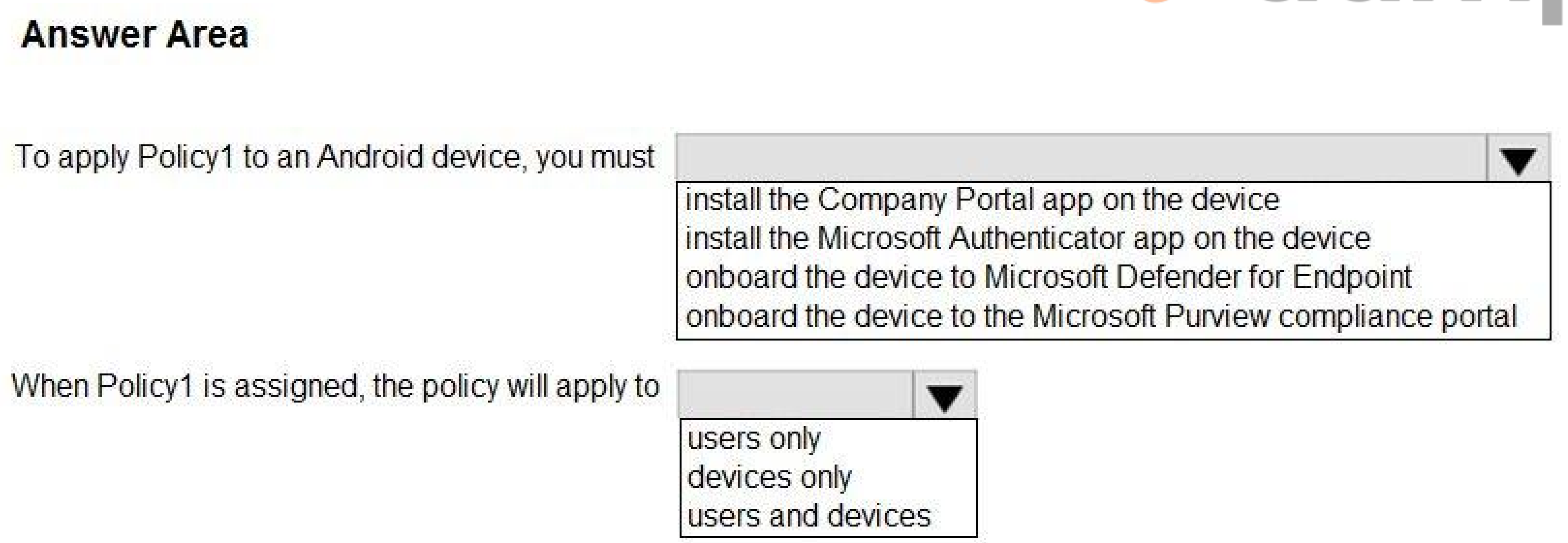
Target policy to: All Apps

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

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

NOTE: Each correct selection is worth one point.

Hot Area:



Answer Area

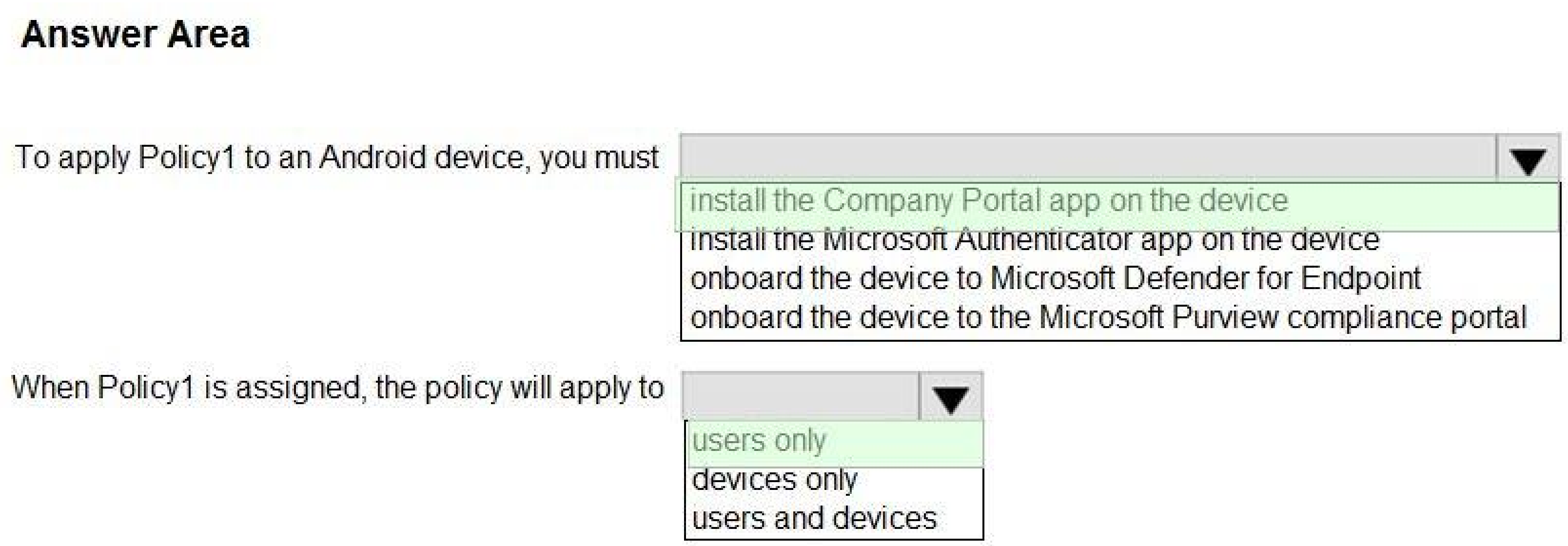
To apply Policy1 to an Android device, you must ▼

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

When Policy1 is assigned, the policy will apply to ▼

- users only
- devices only
- users and devices

Answer Area:



Answer Area

To apply Policy1 to an Android device, you must

- [✓ install the Company Portal app on the device]
- install the Microsoft Authenticator app on the device
- onboard the device to Microsoft Defender for Endpoint
- onboard the device to the Microsoft Purview compliance portal

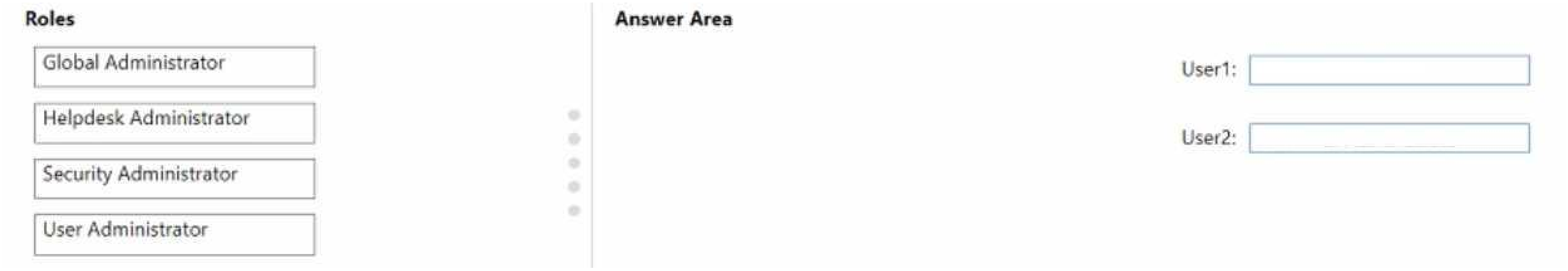
When Policy1 is assigned, the policy will apply to

- [✓ users only]
- devices only
- users and devices

Section:
Explanation:

QUESTION 66
DRAG DROP
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.

Select and Place:



Roles

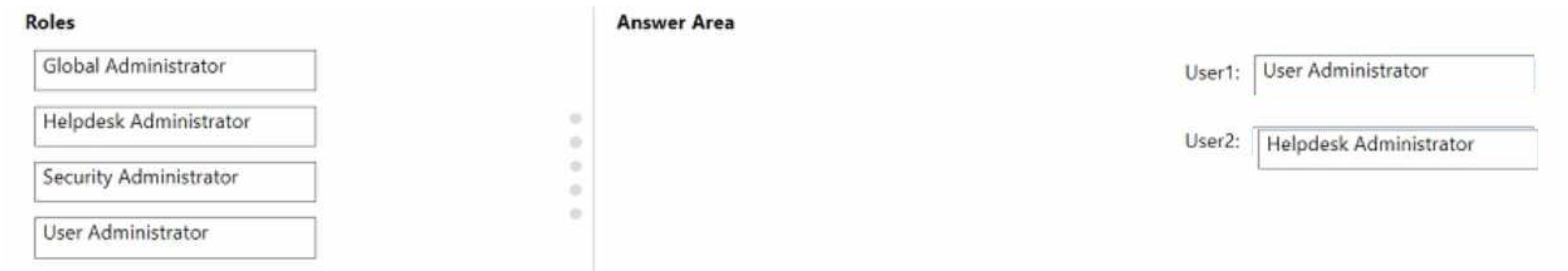
- Global Administrator
- Helpdesk Administrator
- Security Administrator
- User Administrator

Answer Area

User1:

User2:

Correct Answer:



Roles

Global Administrator

Helpdesk Administrator

Security Administrator

User Administrator

Answer Area

User1: User Administrator

User2: Helpdesk Administrator

Section:

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 monitor service health for non-administrative users1.

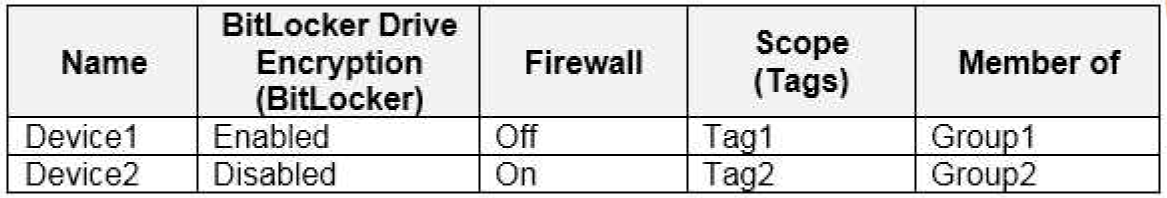
QUESTION 67

HOTSPOT

You have a Microsoft Intune subscription that has the following device compliance policy settings:

Mark devices with no compliance policy assigned as: Compliant Compliance status validity period (days): 14

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



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

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

Name: Policy1

Platform: Windows 10 and later

Require BitLocker: Require

Mark device noncompliant: 5 days after noncompliance

Scope (Tags): Tag1

Name: Policy2

Platform: Windows 10 and later

Firewall: Require

Mark device noncompliant: Immediately

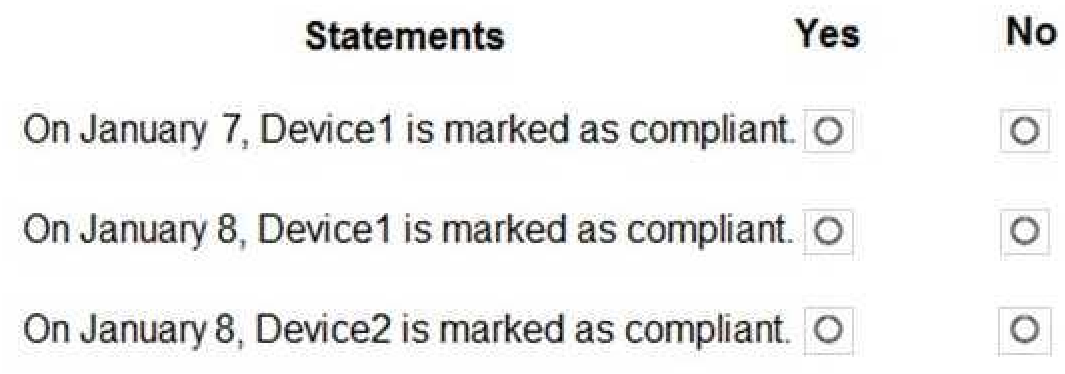
Scope (Tags): Tag2

On January 5, you assign Policy1 and Policy2 to Group1.

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

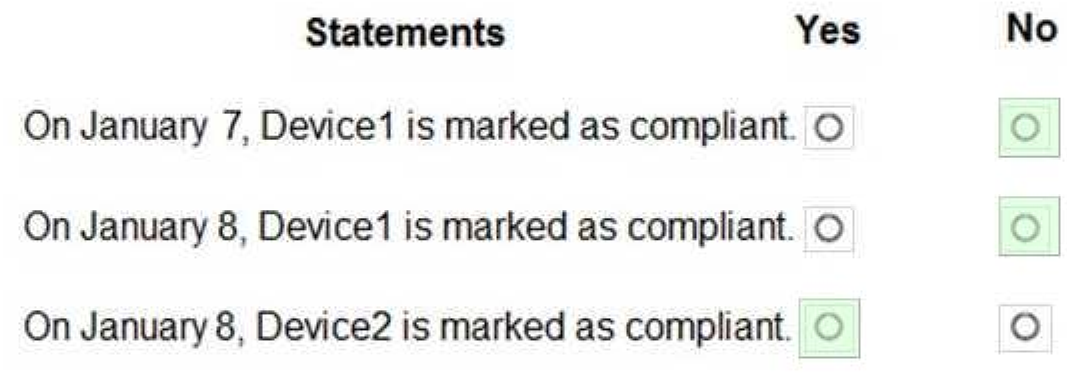
NOTE: Each correct selection is worth one point.

Hot Area:



Statements	Yes	No
On January 7, Device1 is marked as compliant.	○	○
On January 8, Device1 is marked as compliant.	○	○
On January 8, Device2 is marked as compliant.	○	○

Answer Area:



Statements	Yes	No
On January 7, Device1 is marked as compliant.	○	[✓ ○]
On January 8, Device1 is marked as compliant.	○	[✓ ○]
On January 8, Device2 is marked as compliant.	[✓ ○]	○

Section:

Explanation:

Box 1: No.

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

Box 2: No

For the same reason as Box1.

Box 3: Yes

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

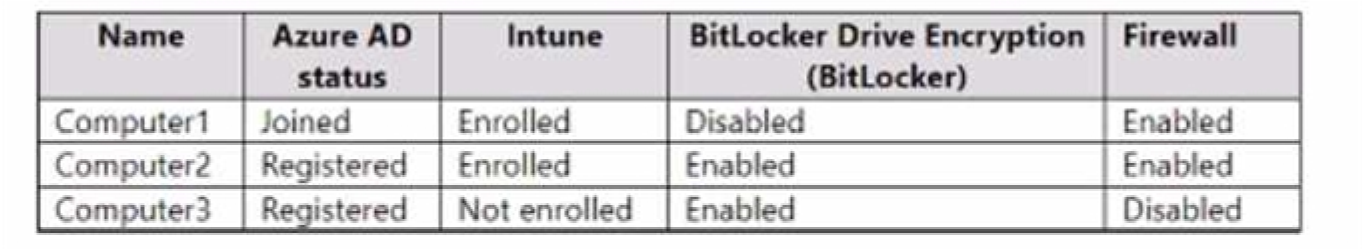
The Scope (tags) have nothing to do with whether the policy is applied or not. The tags are used in RBAC.

QUESTION 68

HOTSPOT

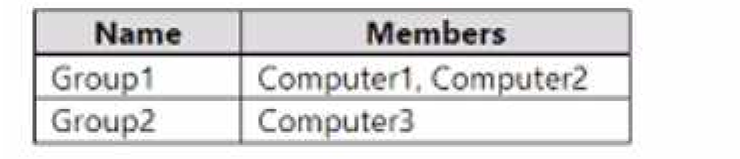
You have a Microsoft 365 subscription that includes Microsoft Intune.

You have computers that run Windows 11 as shown in the following table.



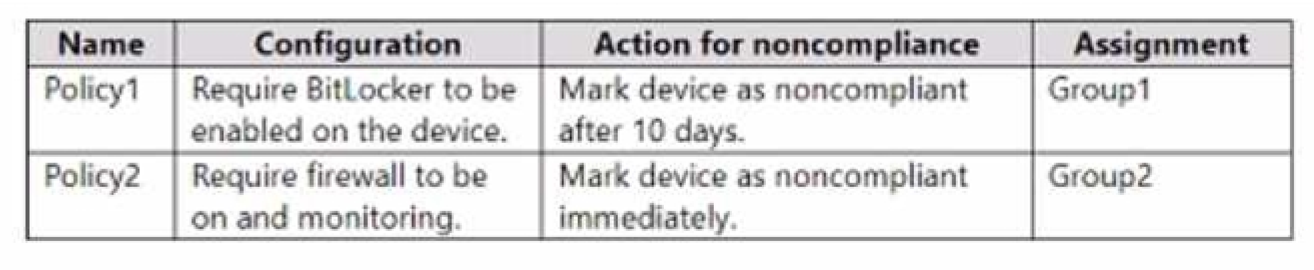
Name	Azure AD status	Intune	BitLocker Drive Encryption (BitLocker)	Firewall
Computer1	Joined	Enrolled	Disabled	Enabled
Computer2	Registered	Enrolled	Enabled	Enabled
Computer3	Registered	Not enrolled	Enabled	Disabled

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.



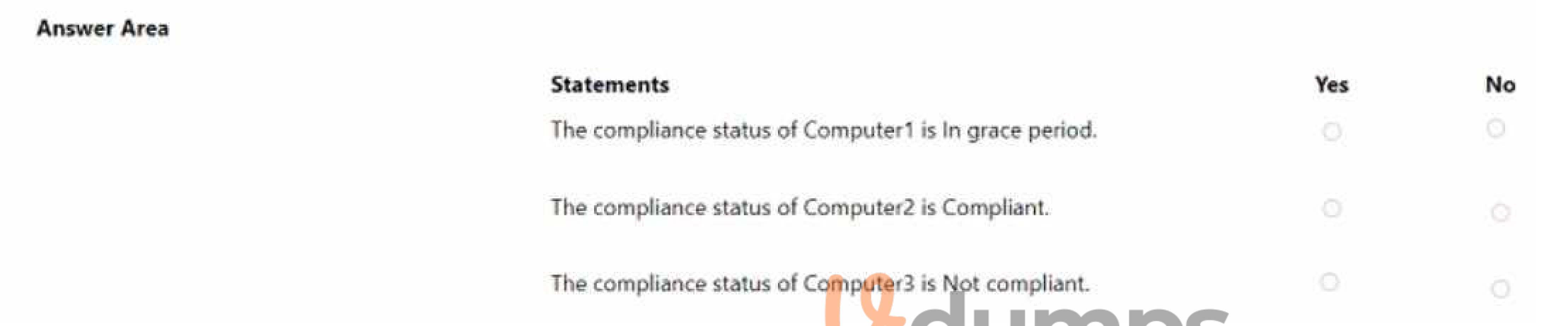
Name	Configuration	Action for noncompliance	Assignment
Policy1	Require BitLocker to be enabled on the device.	Mark device as noncompliant after 10 days.	Group1
Policy2	Require firewall to be on and monitoring.	Mark device as noncompliant immediately.	Group2

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.

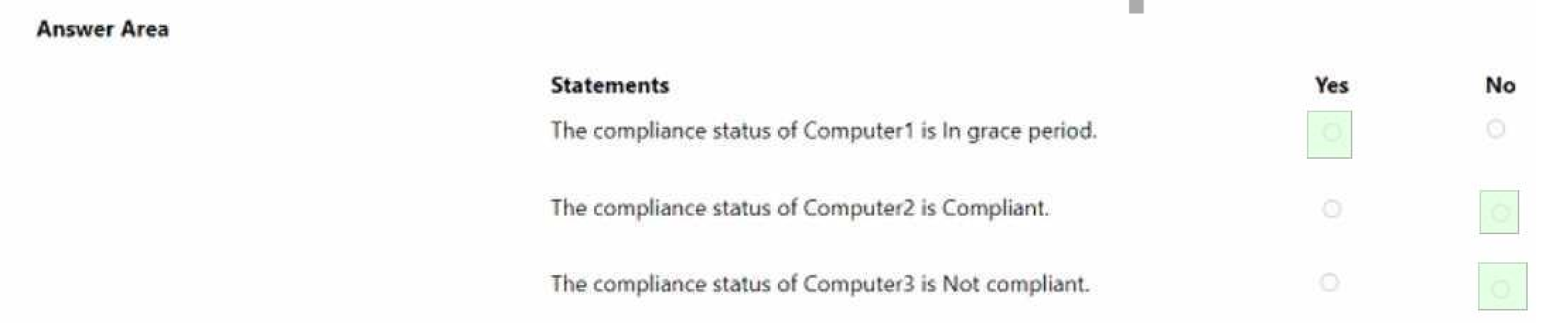
Hot Area:



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.	○	○

Answer Area:

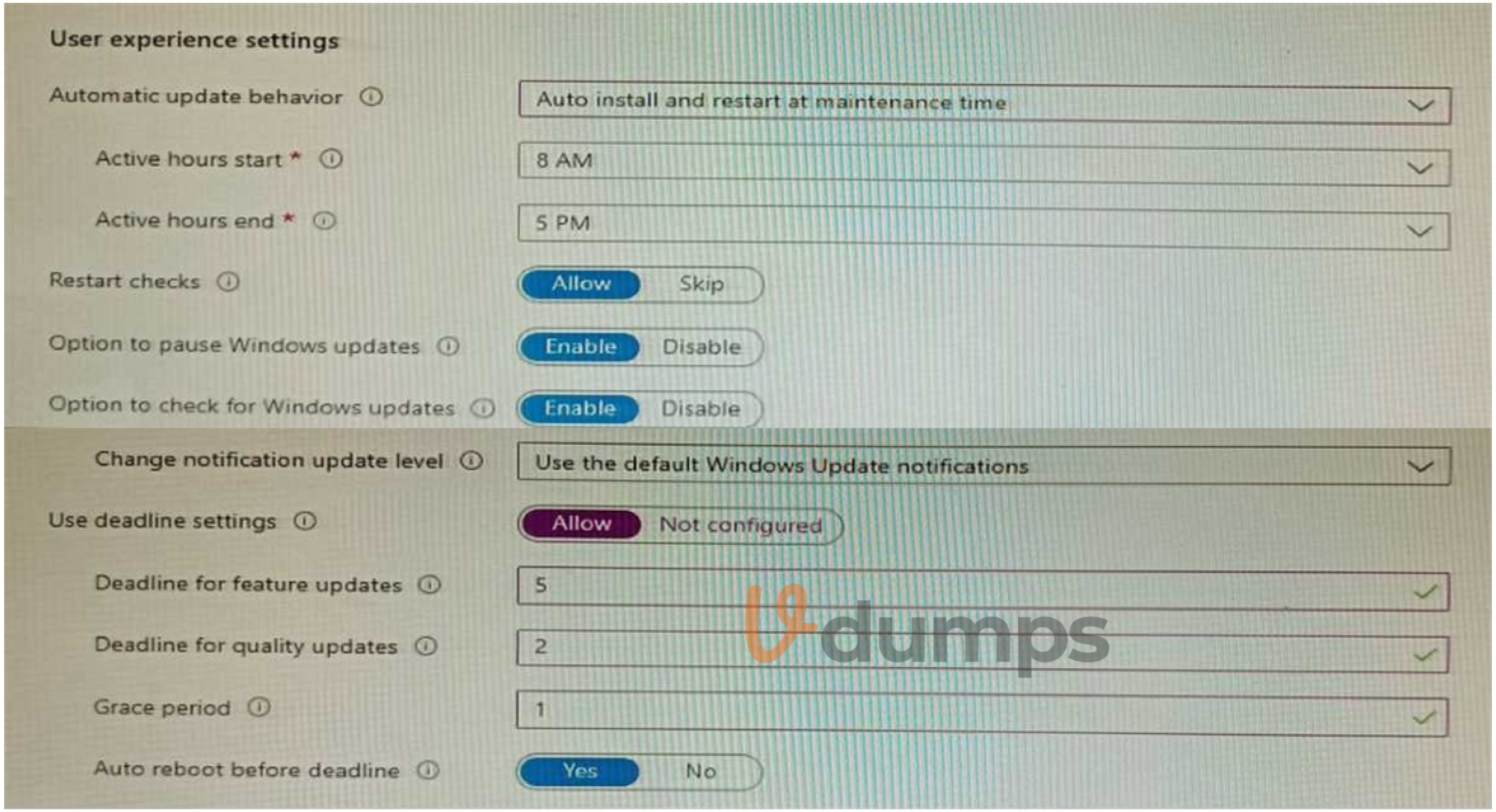


Answer Area

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.	○	[✓ ○]

Section:
Explanation:

QUESTION 69
HOTSPOT
You have a Microsoft 365 subscription that uses Microsoft Intune.
You plan to manage Windows updates by using Intune.
You create an update ring for Windows 10 and later and configure the User experience settings for the ring as shown in the following exhibit.



User experience settings

Automatic update behavior ⓘ: Auto install and restart at maintenance time

Active hours start * ⓘ: 8 AM

Active hours end * ⓘ: 5 PM

Restart checks ⓘ: [✓ Allow] Skip

Option to pause Windows updates ⓘ: [✓ Enable] Disable

Option to check for Windows updates ⓘ: [✓ Enable] Disable

Change notification update level ⓘ: Use the default Windows Update notifications

Use deadline settings ⓘ: [✓ Allow] Not configured

Deadline for feature updates ⓘ: 5

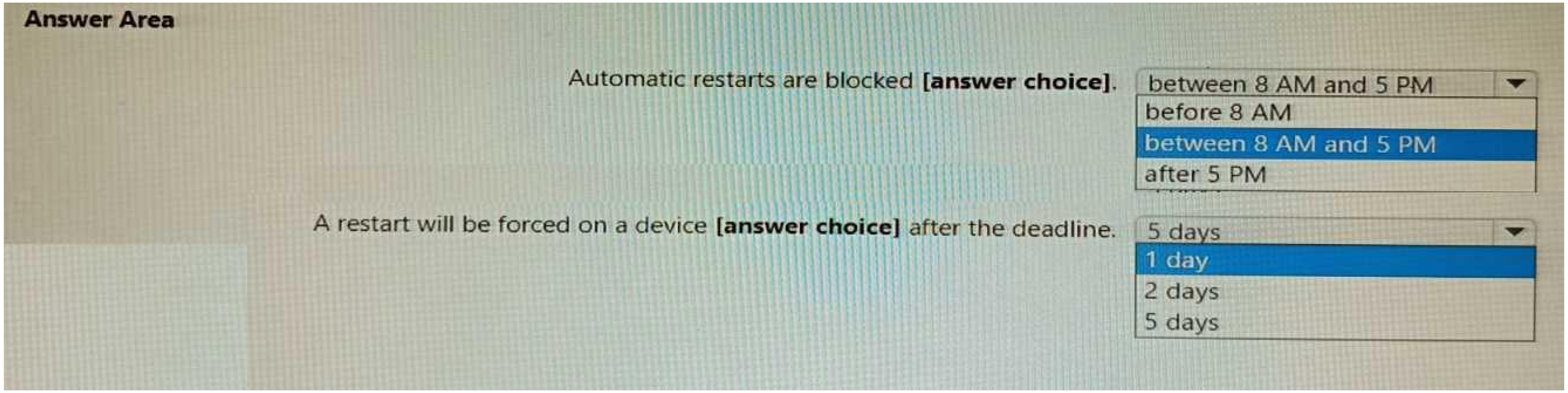
Deadline for quality updates ⓘ: 2

Grace period ⓘ: 1

Auto reboot before deadline ⓘ: [✓ Yes] No

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

Hot Area:



Answer Area

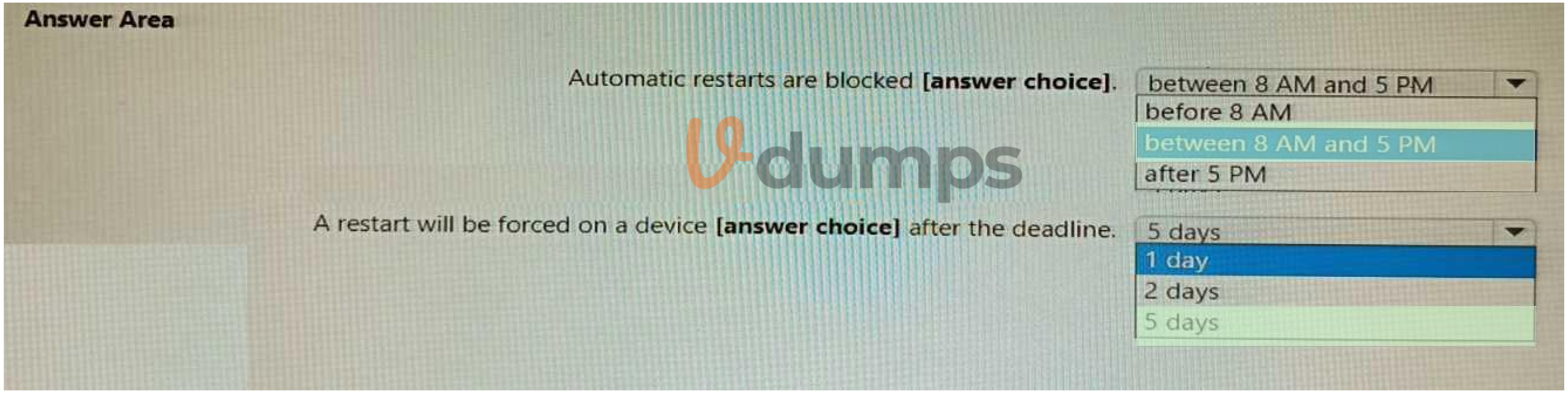
Automatic restarts are blocked **[answer choice]**.

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

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

5 days
- 1 day
- 2 days
- 5 days

Answer Area:



Answer Area

Automatic restarts are blocked **[answer choice]**.

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

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

5 days
- 1 day
- 2 days
- 5 days

Section:

Explanation:

QUESTION 70

You have a Microsoft 365 tenant.

You have devices enrolled in Microsoft Intune.

You assign a conditional access policy named Policy1 to a group named Group1. Policy! restricts devices marked as noncompliant from accessing Microsoft OneDrive for Business.

You need to identify which noncompliant devices attempt to access OneDrive for Business. What should you do?

A. From the Microsoft Entra admin center, review the Conditional Access Insights and Reporting workbook.

B. From the Microsoft Intune admin center, review Device compliance report.

C. From the Microsoft Intune admin center, review the Noncompliant devices report.

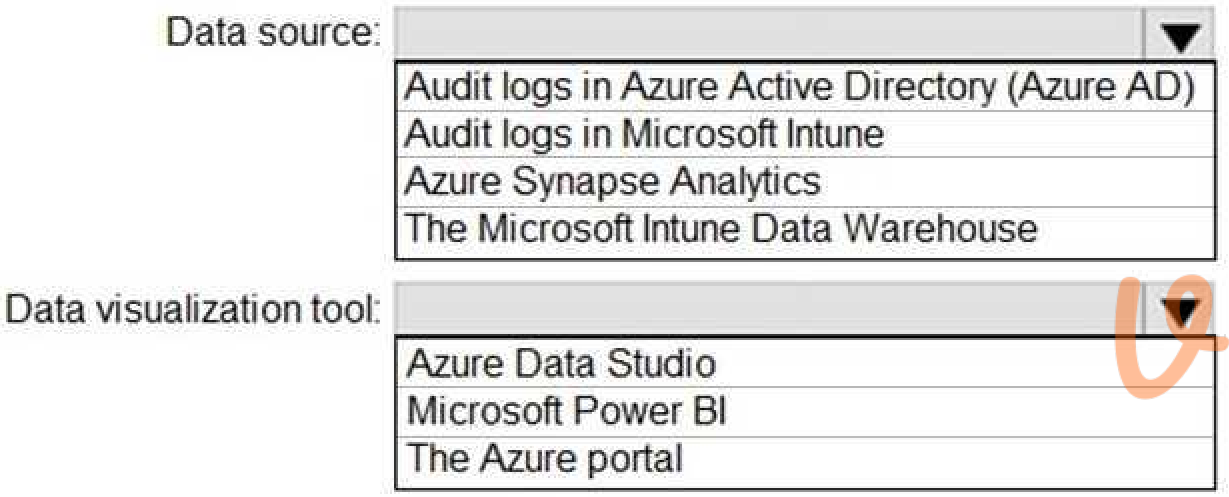
D. From the Microsoft Intune admin center, review the Setting compliance report.

Correct Answer: C
Section:

QUESTION 71

HOTSPOT
You use Microsoft Endpoint Manager to manage Windows 10 devices.
You are designing a reporting solution that will provide reports on the following:
Compliance policy trends
Trends in device and user enrolment
App and operating system version breakdowns of mobile devices
You need to recommend a data source and a data visualization tool for the design.
What should you recommend? To answer, select the appropriate options in the answer area.
NOTE: Each correct selection is worth one point.

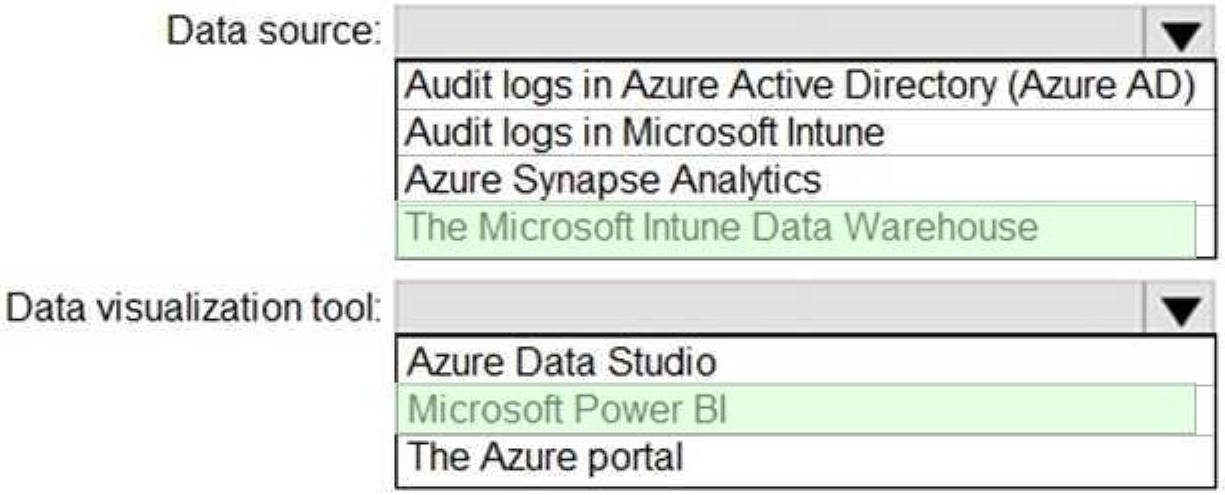
Hot Area:



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

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

Answer Area:



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

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

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

QUESTION 72
Your network contains an Active Directory domain. The domain contains 2,000 computers that run Windows 10. You implement hybrid Azure AD and Microsoft Intune.
You need to automatically register all the existing computers to Azure AD and enroll the computers in Intune. The solution must minimize administrative effort.
What should you use?

A. an Autodiscover address record
B. a Group Policy object (GPO)
C. an Autodiscover service connection point (SCP)
D. a Windows Autopilot deployment profile

Correct Answer: D
Section:

QUESTION 73
You have a Microsoft 365 E5 subscription that contains 100 iOS devices enrolled in Microsoft Intune.
You need to deploy a custom line-of-business (LOB) app to the devices by using Intune.
Which extension should you select for the app package file?

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

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

QUESTION 74
You have a Microsoft 365 E5 subscription that contains a user named User! and a web app named
Appl.
App1 must only accept modern authentication requests.
You plan to create a Conditional Access policy named CAPolicy1 that will have the following settings:
• Assignments
• Users or workload identities: User1
• Cloud apps or actions: App1
• Access controls
• Grant: Block access
You need to block only legacy authentication requests to Appl. Which condition should you add to CAPolicy1?

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

Correct Answer: E
Section:
Explanation:

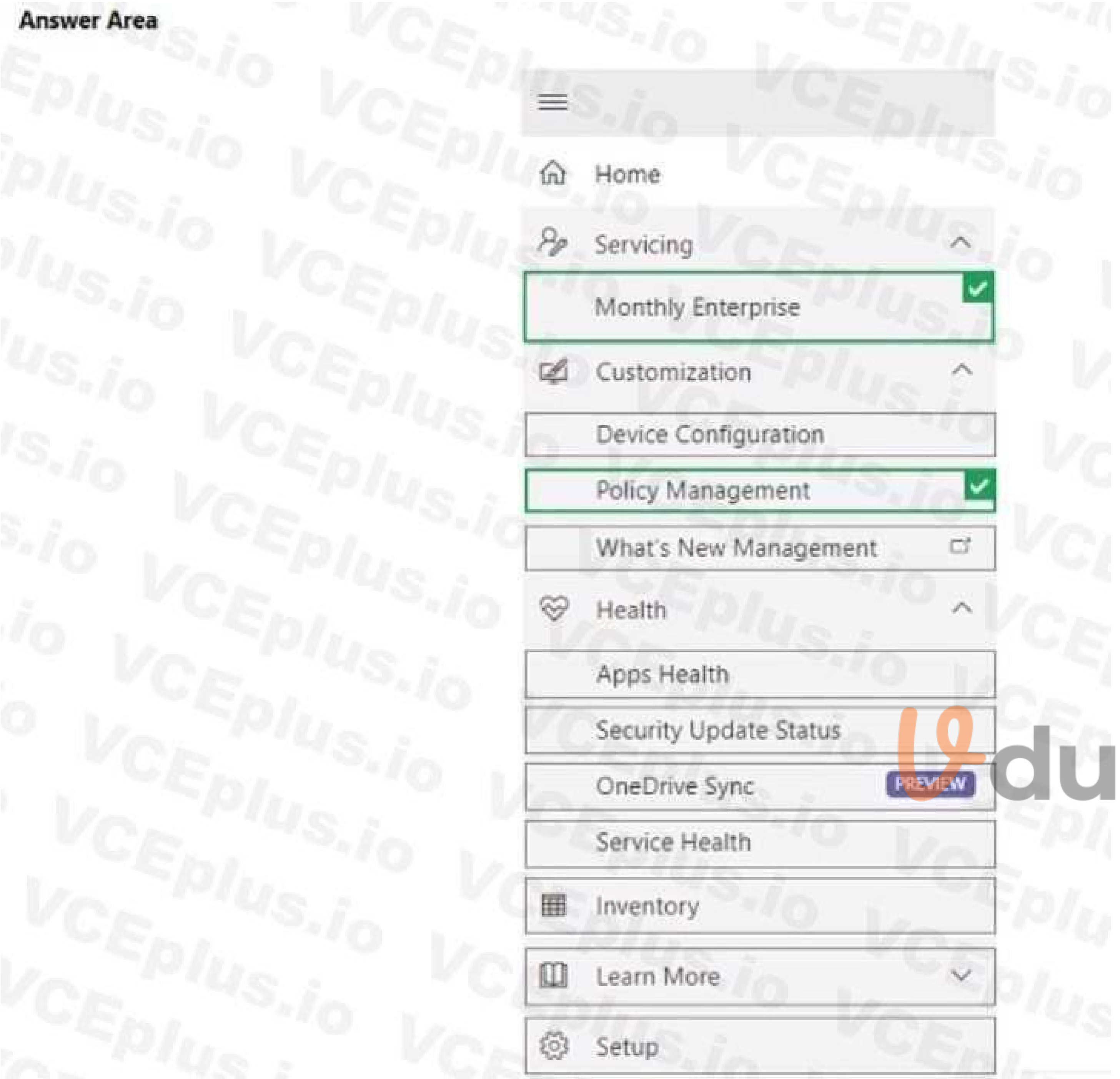
you can use the client apps condition to block legacy authentication requests to App11. Legacy authentication is a term that refers to authentication protocols that do not support modern authentication features such as multi-factor authentication or conditional access2. Examples of legacy authentication protocols include Basic Authentication, Digest Authentication, NTLM, and Kerberos2. To block legacy authentication requests, you need to configure the client apps condition to include Other clients, which covers any client that uses legacy authentication protocols13.

Reference: 1: Conditional Access: Block legacy authentication | Microsoft Learn https://learn.microsoft.com/en-us/mem/identity-protection/conditional-access/block-legacyauthentication 2: What is legacy authentication? | Microsoft Learn https://learn.microsoft.com/enus/ mem/identity-protection/conditional-access/legacy-authentication 3: Client apps condition in Azure Active Directory Conditional Access | Microsoft Learn https://learn.microsoft.com/enus/ mem/identity-protection/conditional-access/client-apps-condition

QUESTION 75

HOTSPOT
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.

Hot Area:

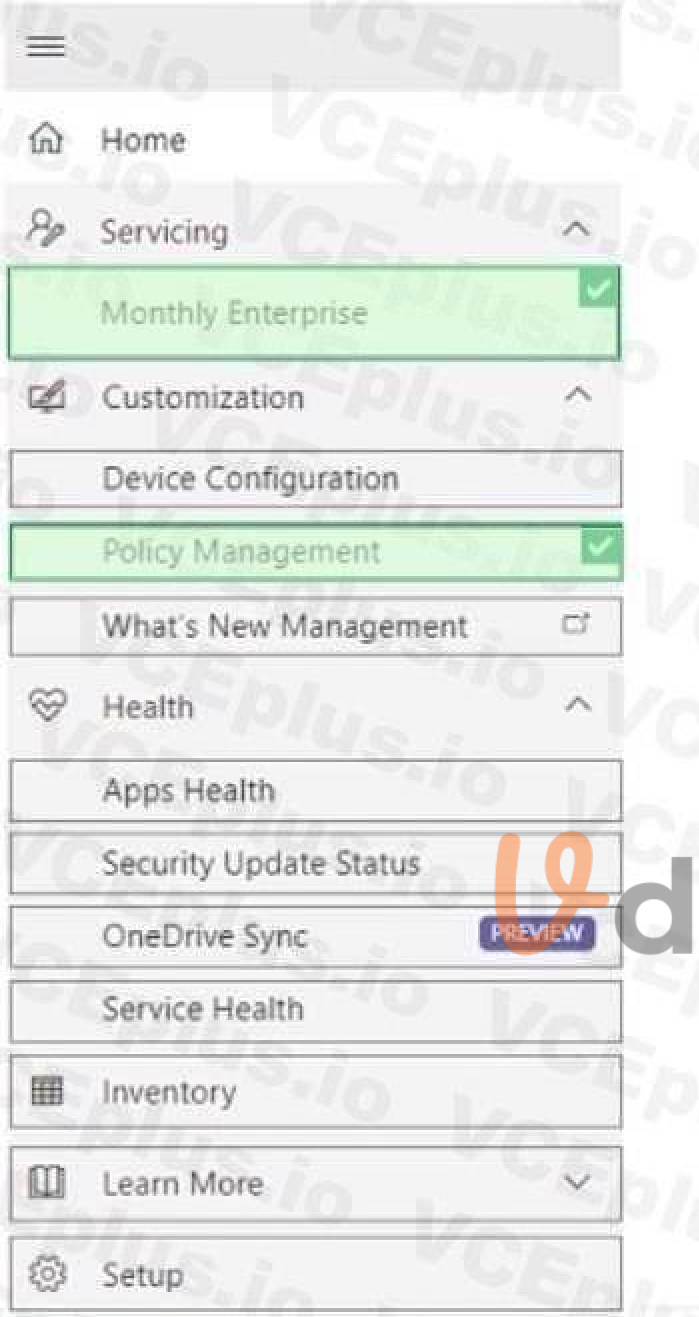


Answer Area

- 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

Answer Area:

Answer Area



Section:
Explanation:

QUESTION 76
You have a Microsoft 365 subscription.
You have 10 computers that run Windows 10 and are enrolled in mobile device management (MDM).
You need to deploy the Microsoft 36S Apps for enterprise suite to all the computers.
What should you do?

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

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

QUESTION 77
You have a Microsoft 365 subscription that uses Microsoft Intune Suite.
You use Microsoft Intune to manage devices.
You have a Windows 11 device named Device1 that is enrolled in Intune. Device1 has been offline for 30 days.
You need to remove Device1 from Intune immediately. The solution must ensure that if the device checks in again, any apps and data provisioned by Intune are removed. User-installed apps, personal data, and OEM-installed apps must be retained.
What should you use?

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

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

QUESTION 78
You have a Microsoft 365 subscription that uses Microsoft Intune Suite. You use Microsoft Intune to manage devices.
You need to review the startup times and restart frequencies of the devices. What should you use?

A. Azure Monitor
B. intune Data Warehouse
C. Microsoft Defender for Endpoint
D. Endpoint analytics

Correct Answer: D
Section:
Explanation:
Endpoint analytics is a feature of Microsoft Intune that provides insights into the performance and health of devices. You can use endpoint analytics to review the startup times and restart frequencies of the devices, as well as other metrics such as sign-in times, battery life, app reliability, and software inventory. Reference: https://docs.microsoft.com/en-us/mem/analytics/overview

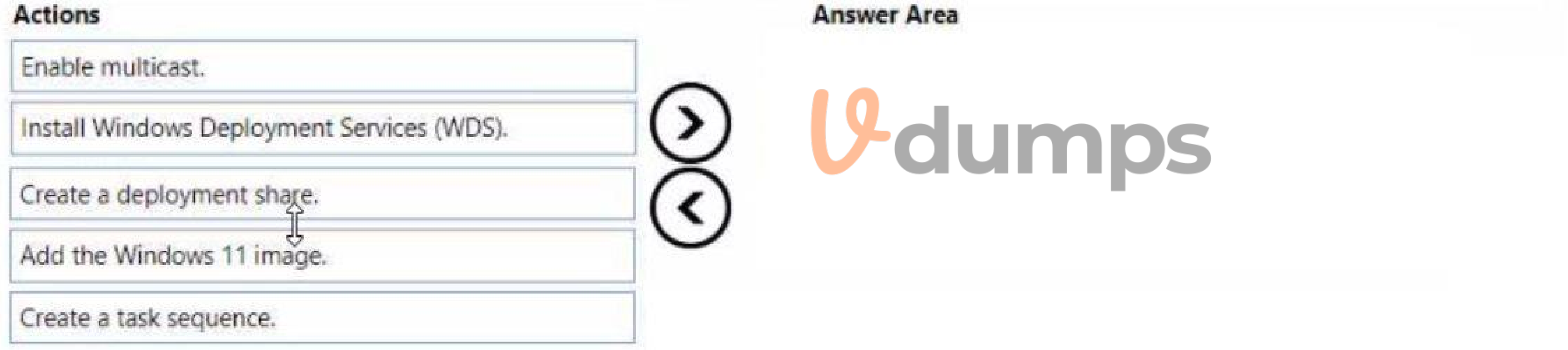
QUESTION 79
Your company has a Remote Desktop Gateway (RD Gateway).
You have a server named Server1 that is accessible by using Remote Desktop Services (RDS) through the RD Gateway.
You need to configure a Remote Desktop connection to connect through the gateway.
Which setting should you configure?

A. Connect from anywhere
B. Server authentication
C. Connection settings
D. Local devices and resources

Correct Answer: A
Section:
Explanation:
To connect to a remote server through the RD Gateway, you need to configure the Connect from anywhere setting in the Remote Desktop Connection client. This setting allows you to specify the domain name and port of the RD Gateway server, as well as the authentication method. The other settings are not related to the RD Gateway connection.Reference:Configure Remote Desktop Connection Settings for Remote Desktop Gateway

QUESTION 80
DRAG DROP
Your network contains an Active Directory domain.
You install the Microsoft Deployment Toolkit (MDT) on a server.
You have a custom image of Windows 11.
You need to deploy the image to 100 devices by using MDT.
Which three actions should you perform in sequence? To answer, move answer area and arrange them in the correct order.

Select and Place:

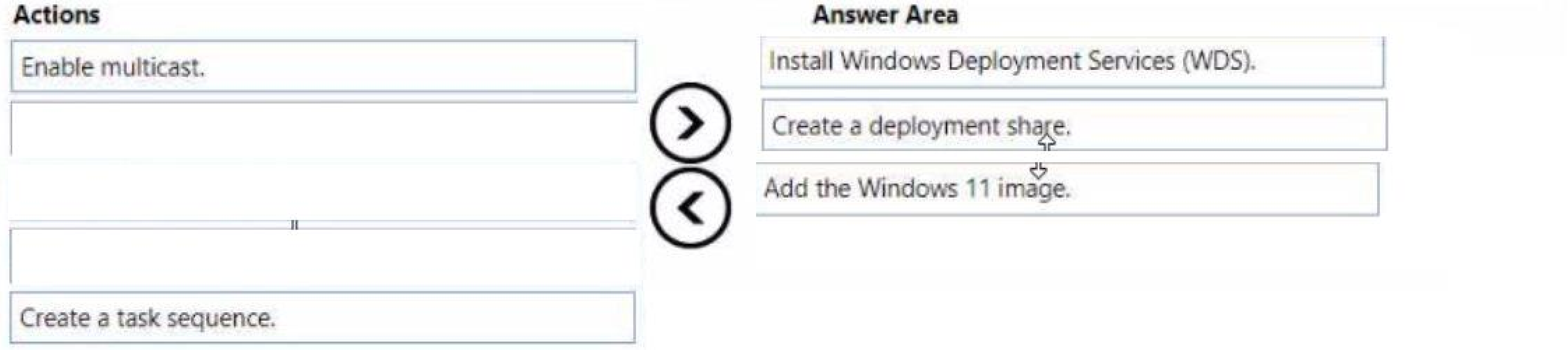


Actions

Enable multicast.
Install Windows Deployment Services (WDS).
Create a deployment share.
Add the Windows 11 image.
Create a task sequence.

Answer Area

Correct Answer:



Actions

Enable multicast.
Create a task sequence.

Answer Area

Install Windows Deployment Services (WDS).
Create a deployment share.
Add the Windows 11 image.

Section:
Explanation:

Install Windows Deployment Services (WDS)
Create a deployment share.
Add the Windows 11 image.

QUESTION 81

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

Correct Answer: C
Section:
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.Reference:Sysprep (Generalize) a Windows installation

QUESTION 82

Your network contains an on-premises Active Directory domain. The domain contains two computers named Computer1 and Computer? that run Windows 10.
You install Windows Admin Center on Computer1.
You need to manage Computer2 from Computer1 by using Windows Admin Center.
What should you do on Computed?

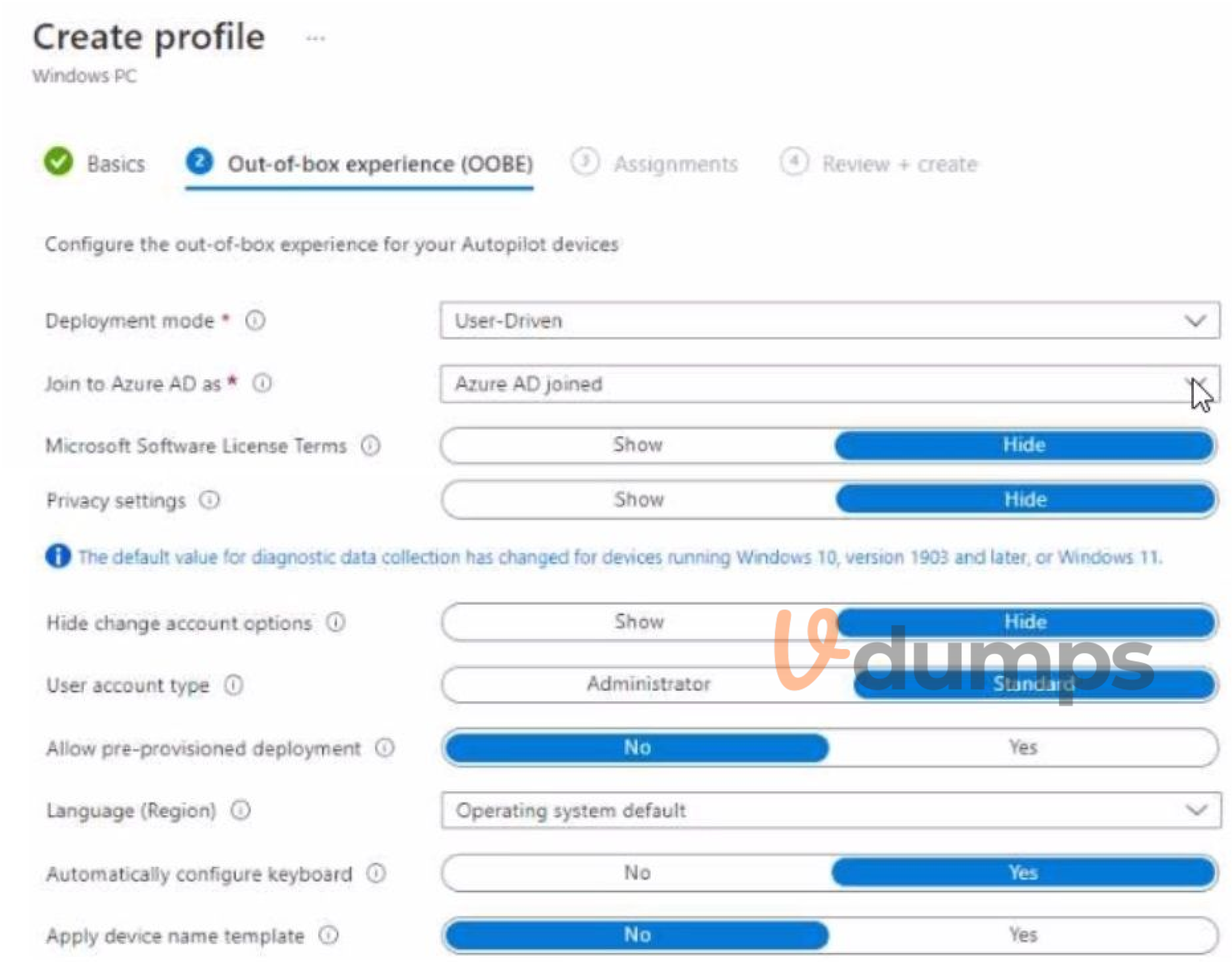
A. Update the TrustedHosts list
B. Run the Enable-PSRemoting cmdlet
C. Allow Windows Remote Management (WinRM) through the Microsoft Defender firewall.
D. Add an inbound Microsoft Defender Firewall rule.

Correct Answer: B
Section:
Explanation:

To manage a remote computer from Windows Admin Center, you need to enable PowerShell remoting on the remote computer. You can do this by running the Enable-PSRemoting cmdlet, which configures the WinRM service, creates a listener, and allows inbound firewall rules for PowerShell remoting. The other options are not sufficient or necessary for this task.Reference:Installation and configuration for Windows Remote Management

QUESTION 83

HOTSPOT
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 Assignments | 4 Review + create

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

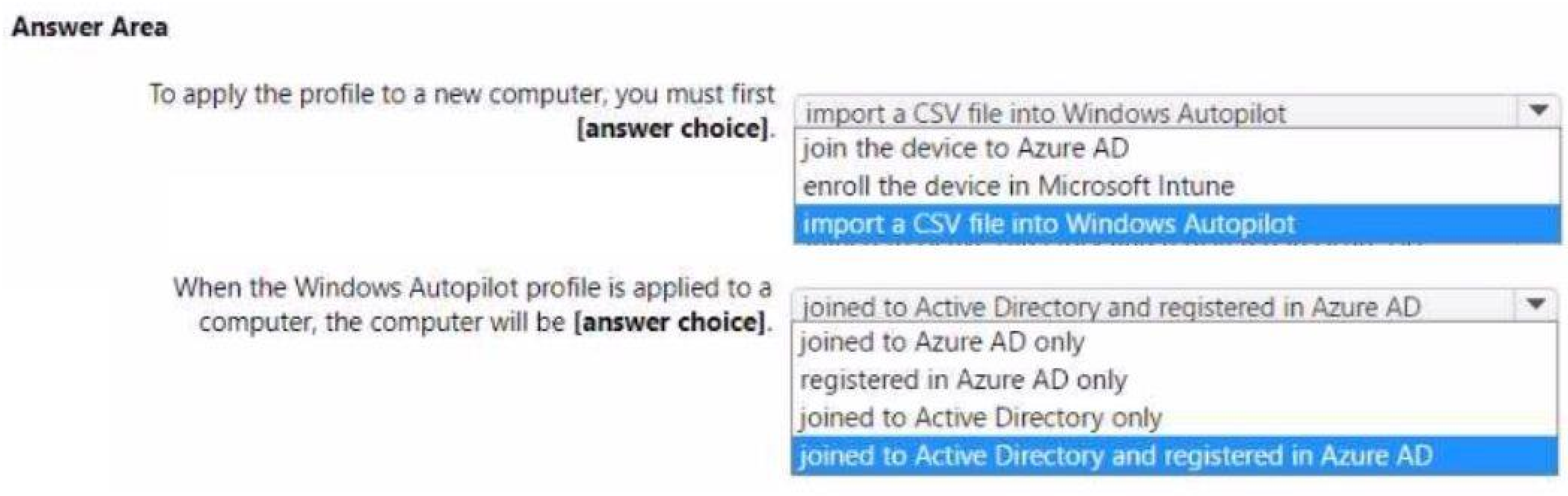
Deployment mode *	User-Driven
Join to Azure AD as *	Azure AD joined
Microsoft Software License Terms	Show [✓ Hide]
Privacy settings	Show [✓ Hide]

The default value for diagnostic data collection has changed for devices running Windows 10, version 1903 and later, or Windows 11.

Hide change account options	Show [✓ Hide]
User account type	Administrator [✓ Standard]
Allow pre-provisioned deployment	[✓ No] Yes
Language (Region)	Operating system default
Automatically configure keyboard	No [✓ Yes]
Apply device name template	[✓ No] Yes

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

Hot Area:



Answer Area

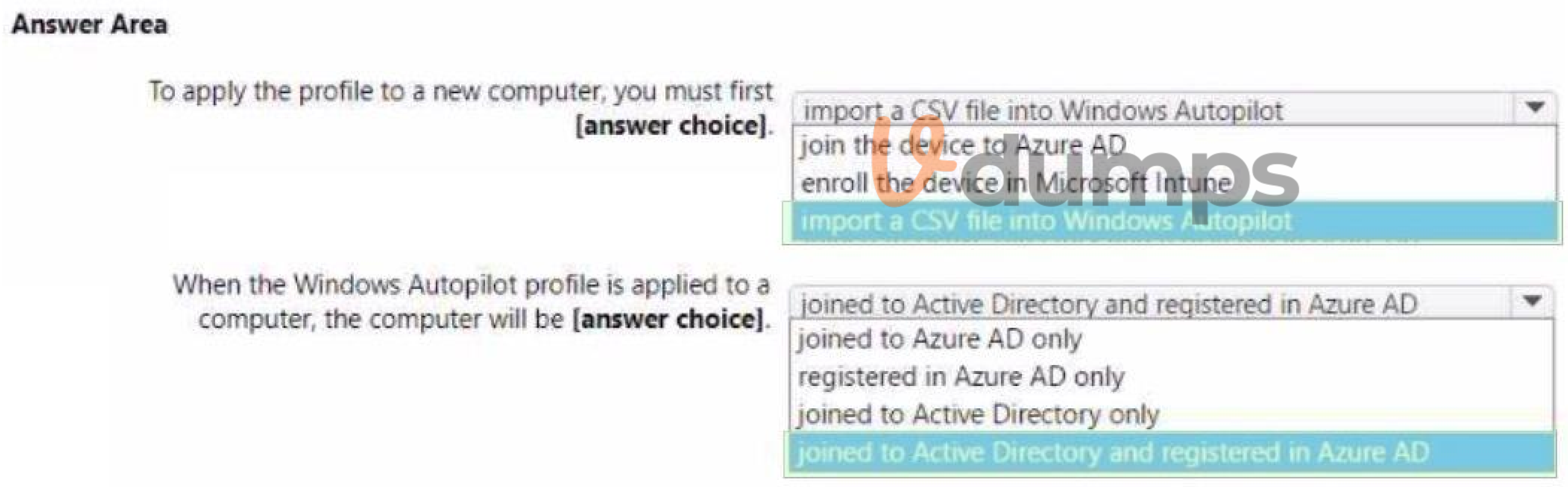
To apply the profile to a new computer, you must first **[answer choice]**.

- import a CSV file into Windows Autopilot
- 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 **[answer choice]**.

- joined to Active Directory and registered in Azure AD
- joined to Azure AD only
- registered in Azure AD only
- joined to Active Directory only
- joined to Active Directory and registered in Azure AD

Answer Area:



Answer Area

To apply the profile to a new computer, you must first **[answer choice]**.

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

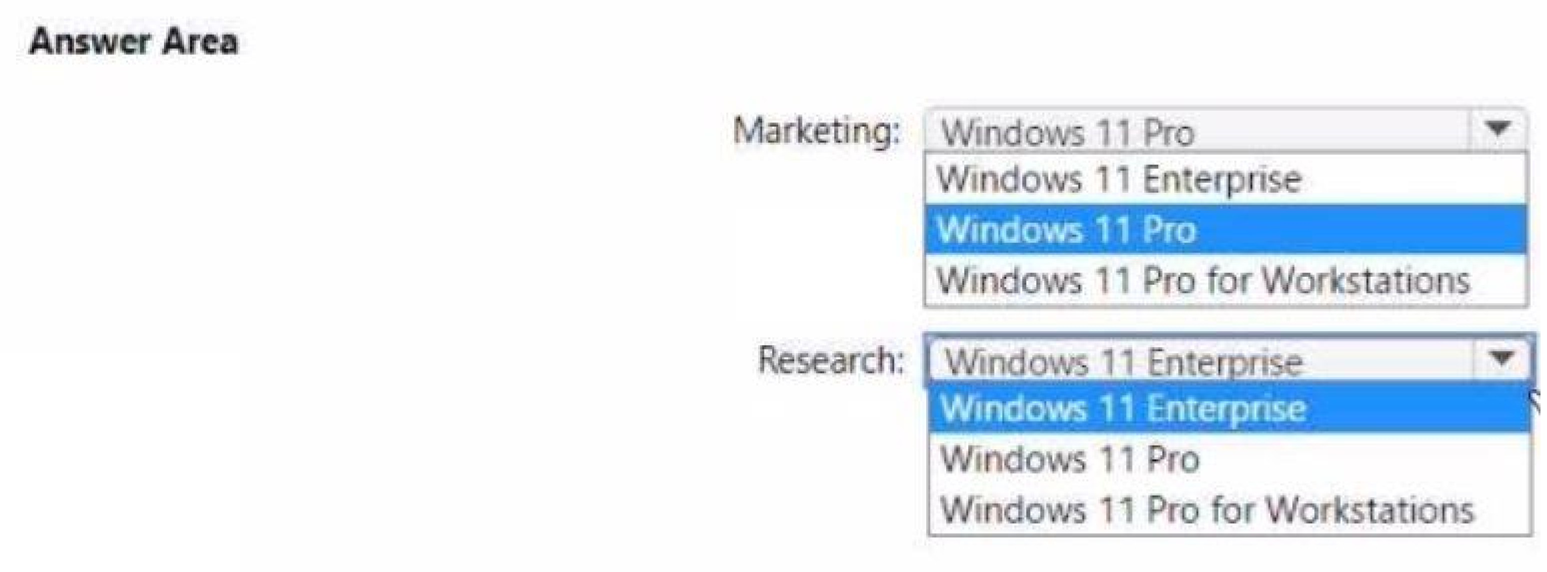
When the Windows Autopilot profile is applied to a computer, the computer will be **[answer choice]**.

- joined to Active Directory and registered in Azure AD
- joined to Azure AD only
- registered in Azure AD only
- joined to Active Directory only
- joined to Active Directory and registered in Azure AD

Section:
Explanation:

QUESTION 84
HOTSPOT
You have a Microsoft 365 subscription that uses Microsoft Intune Suite.
You use Microsoft Intune to manage devices.
You plan to create Windows 11 device builds for the marketing and research departments The solution must meet the following requirements:
* Marketing department devices must support Windows Update for Business.
* Research department devices must have support for feature update versions for up to 36 months from release.
What is the minimum Windows 11 edition required for each department? To answer, select the appropriate options in the answer area.
NOTE: Each correct selection is worth one point

Hot Area:



Answer Area

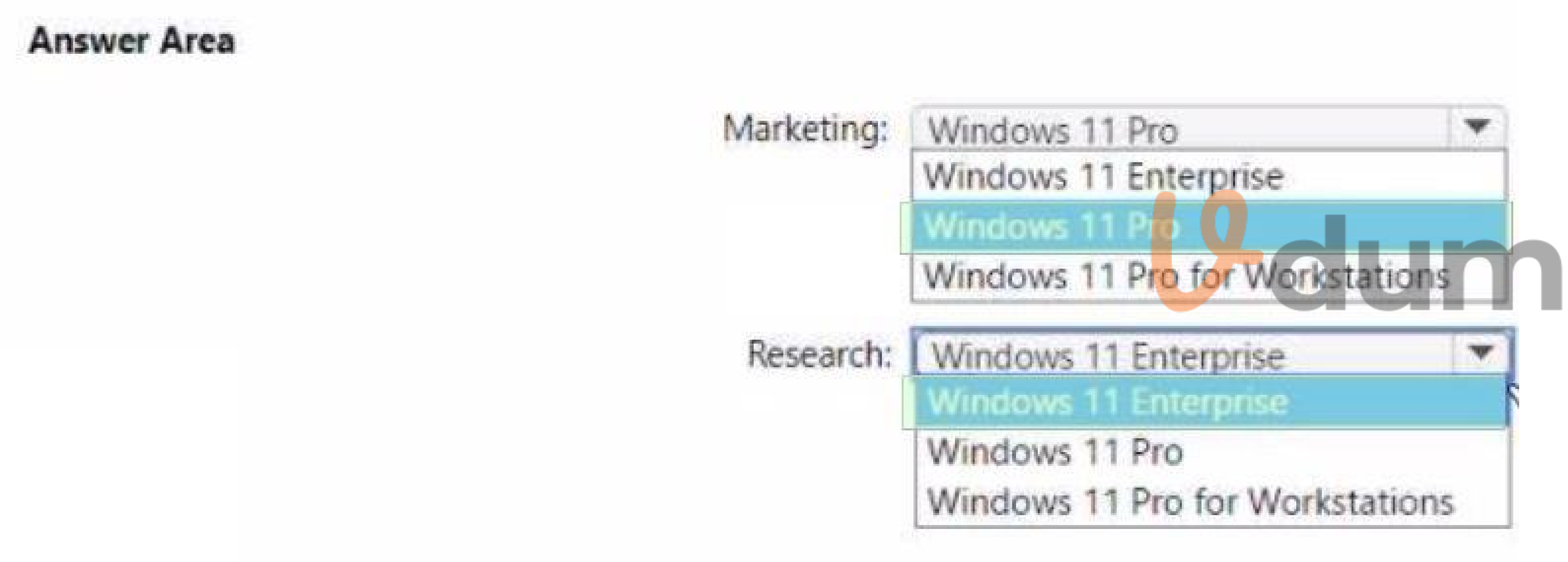
Marketing: Windows 11 Pro

- Windows 11 Enterprise
- Windows 11 Pro
- Windows 11 Pro for Workstations

Research: Windows 11 Enterprise

- Windows 11 Enterprise
- Windows 11 Pro
- Windows 11 Pro for Workstations

Answer Area:



Answer Area

Marketing: Windows 11 Pro

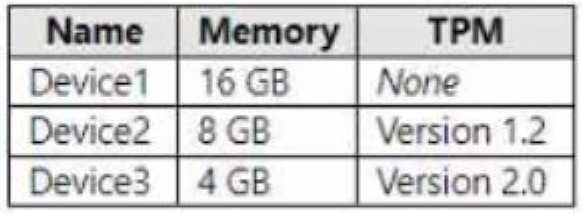
- Windows 11 Enterprise
- Windows 11 Pro
- Windows 11 Pro for Workstations

Research: Windows 11 Enterprise

- Windows 11 Enterprise
- Windows 11 Pro
- Windows 11 Pro for Workstations

Section:
Explanation:

QUESTION 85
You have an Azure AD tenant named contoso.com.
You plan to use Windows Autopilot to configure the Windows 10 devices shown in the following table.



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

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

A. Device2 only

B. Device3 only

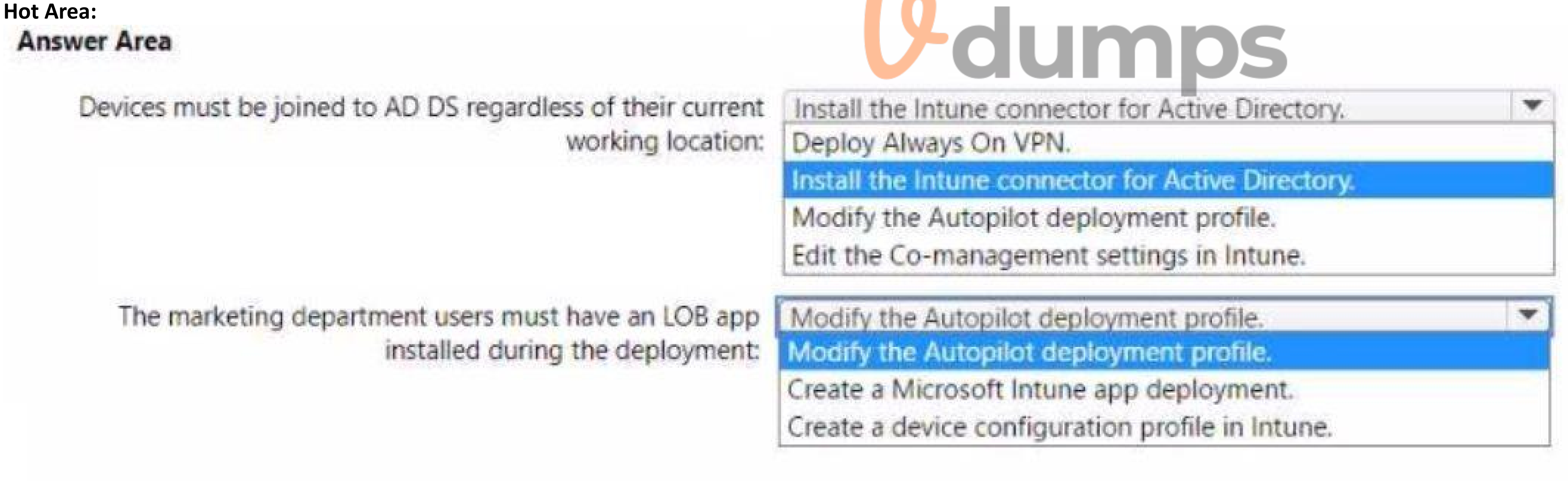
C. Device2 and Devnce3 only

D. Device 1, Device2, and Device3

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

QUESTION 86
HOTSPOT
Your network contains an on-premises Active Directory Domain Services (AD DS) domain that syncs with an Azure AD tenant.
You have a Microsoft 365 subscription
You plan to use Windows Autopilot to deploy new Windows devices.
You plan to create a deployment profile.
You need to ensure that The deployment meets the following requirements:
* Devices must be joined to AD DS regardless of their current working location.
* Users in the marketing department must have a line-of-business (LOB) app installed during the deployment.
The solution must minimize administrative effort.
What should you do for each requirement? To answer, select the appropriate options in the answer area.
NOTE: Each correct selection is worth one point.

Hot Area:



Answer Area

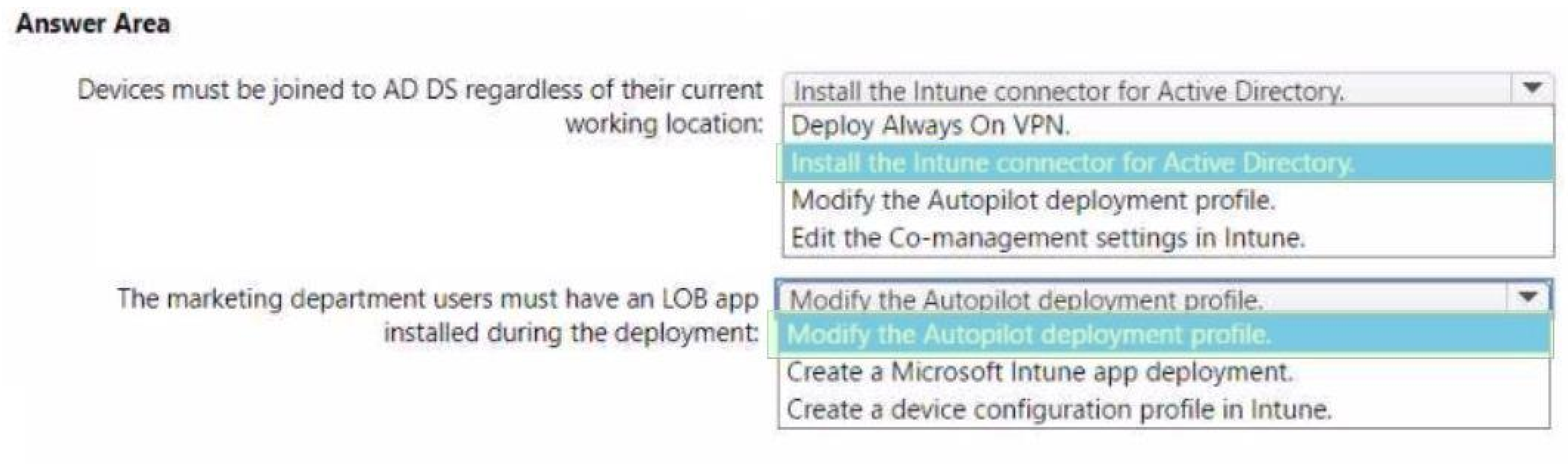
Devices must be joined to AD DS regardless of their current working location:

Install the Intune connector for Active Directory.
- Deploy Always On VPN.
- Install the Intune connector for Active Directory.
- Modify the Autopilot deployment profile.
- Edit the Co-management settings in Intune.

The marketing department users must have an LOB app installed during the deployment:

Modify the Autopilot deployment profile.
- Modify the Autopilot deployment profile.
- Create a Microsoft Intune app deployment.
- Create a device configuration profile in Intune.

Answer Area:



Answer Area

Devices must be joined to AD DS regardless of their current working location:

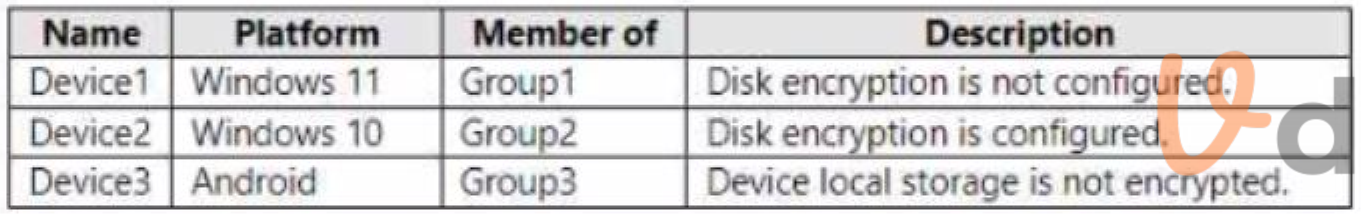
- Install the Intune connector for Active Directory. ▾
- Deploy Always On VPN.
- Install the Intune connector for Active Directory.
- Modify the Autopilot deployment profile.
- Edit the Co-management settings in Intune.

The marketing department users must have an LOB app installed during the deployment:

- Modify the Autopilot deployment profile. ▾
- Modify the Autopilot deployment profile.
- Create a Microsoft Intune app deployment.
- Create a device configuration profile in Intune.

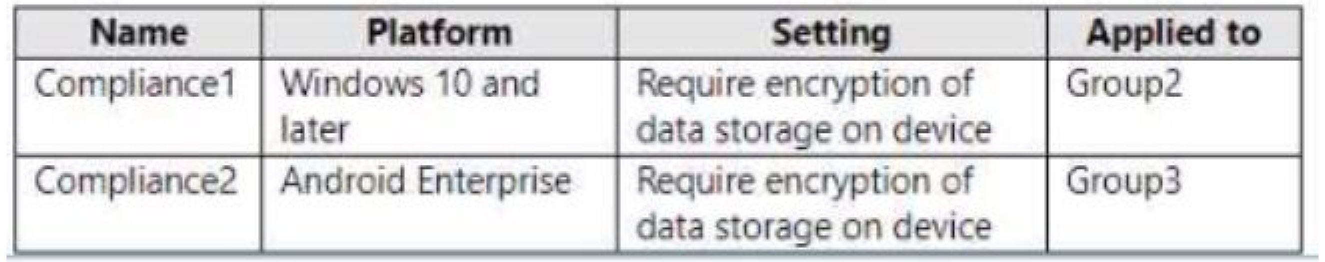
Section:
Explanation:

QUESTION 87
HOTSPOT
You have a Microsoft 365 subscription that contains a user named User1. The subscription contains devices enrolled in Microsoft intune as shown in the following table.



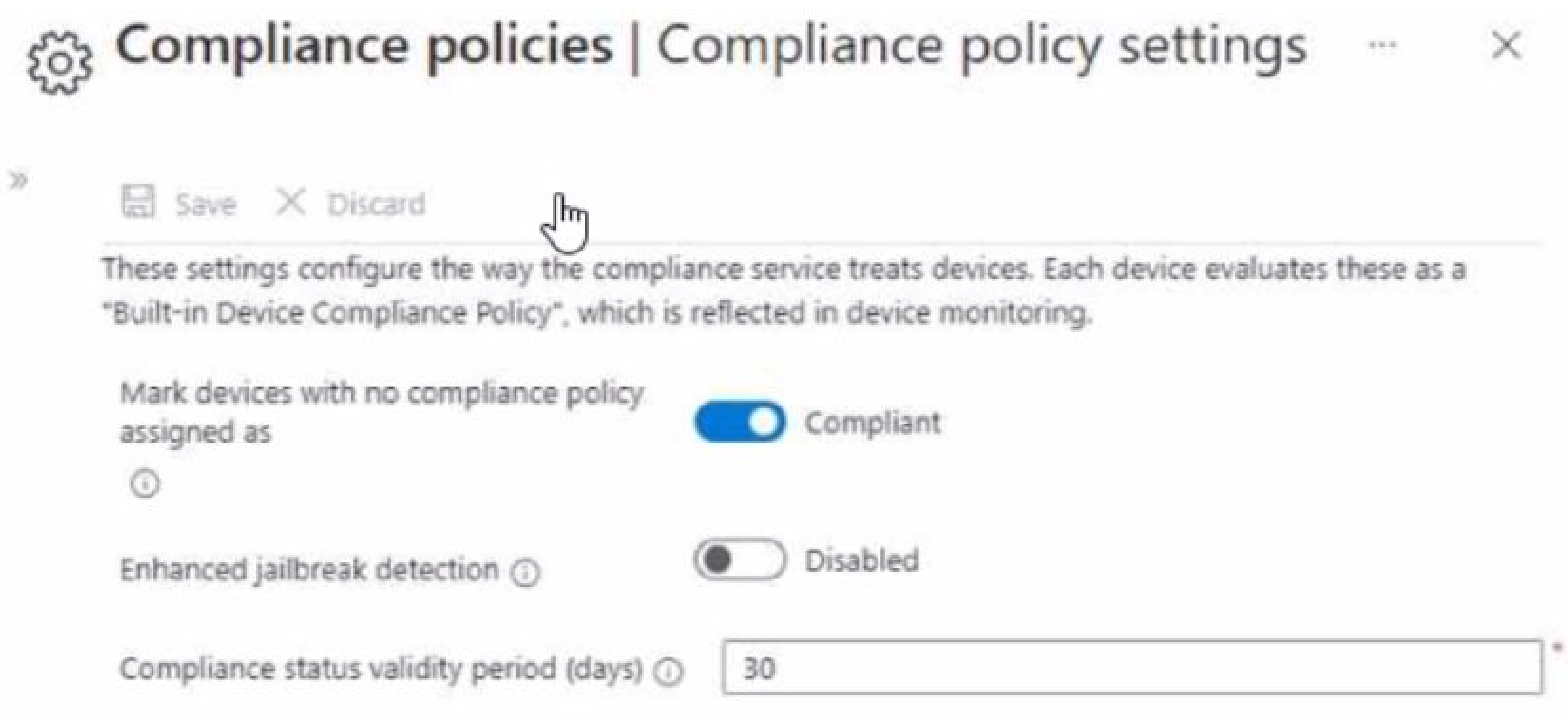
Name	Platform	Member of	Description
Device1	Windows 11	Group1	Disk encryption is not configured.
Device2	Windows 10	Group2	Disk encryption is configured.
Device3	Android	Group3	Device local storage is not encrypted.

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



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

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



Compliance policies | Compliance policy settings

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

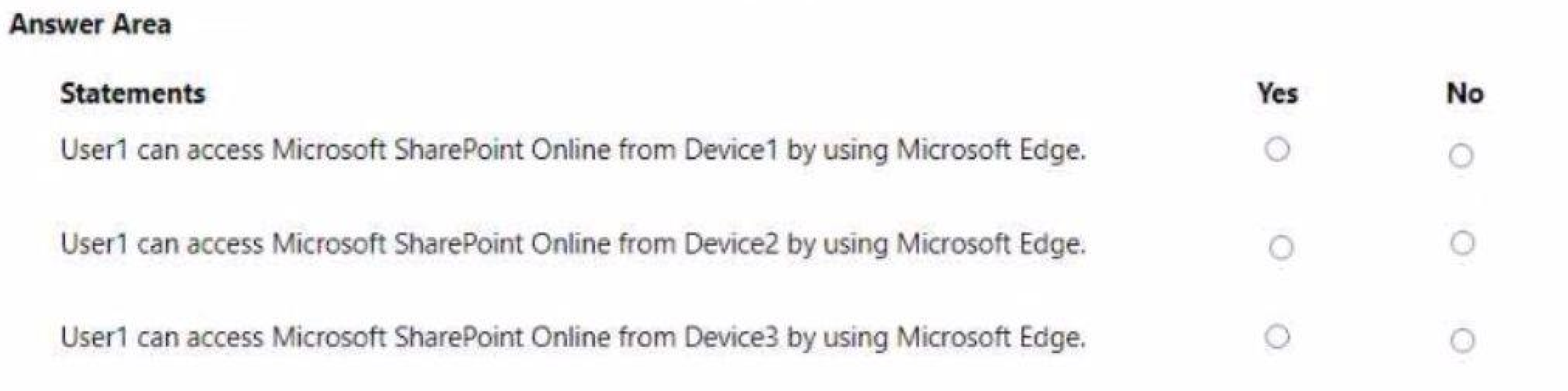
Mark devices with no compliance policy assigned as Compliant

Enhanced jailbreak detection Disabled

Compliance status validity period (days) 30

* Name: Policy1
* Assignments
o Users and groups: User1
o Cloud apps or actions: Office 365 SharePoint Online
* Access controls
o Grant Require device to be marked as compliant
* Enable policy: On
For each of the following statements, select Yes if the statement is true. Otherwise, select No. NOTE: Each correct selection is worth one point.

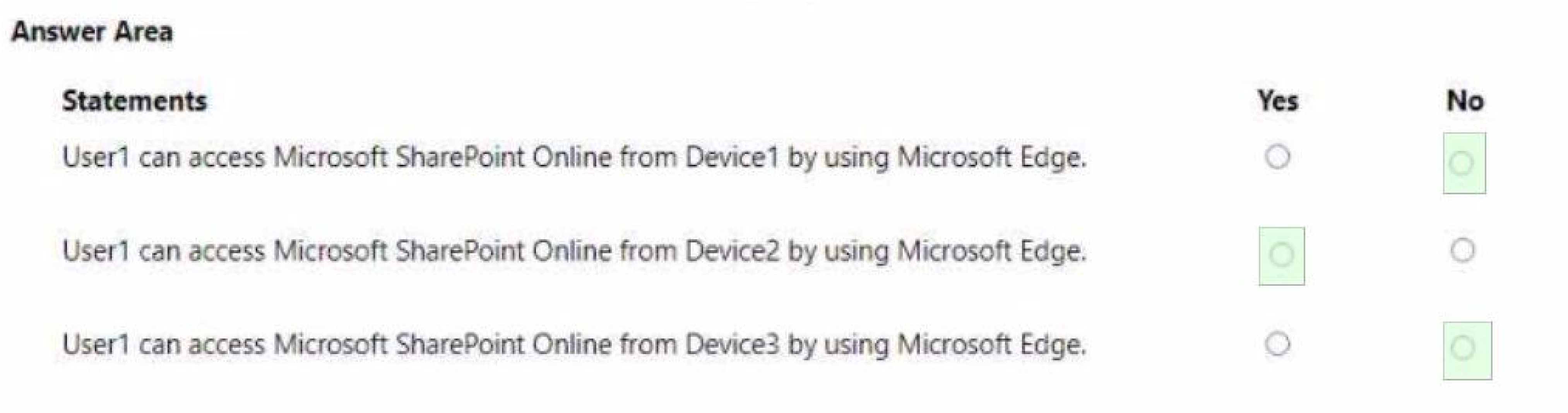
Hot Area:



Answer Area

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

Answer Area:



Answer Area

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

Section:
Explanation:

QUESTION 88
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

Correct Answer: D
Section:
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.

QUESTION 89
You have an Azure subscription.
You have an on-premises Windows 11 device named Device 1.
You plan to monitor Device1 by using Azure Monitor.
You create a data collection rule (DCR) named DCR1 in the subscription.
To what should you associate DCR1 ?

A. Azure Network Watcher
B. Device1

C. a Log Analytics workspace

D. a Monitored Object

Correct Answer: B
Section:
Explanation:
To monitor Device1 by using Azure Monitor, you should associate DCR1 with Device1. A data collection rule (DCR) defines the data collection process in Azure Monitor, such as what data to collect, how to transform it, and where to send it.A DCR can be associated with multiple virtual machines and specify different data sources, such as Azure Monitor Agent, custom logs, or Azure Event Hubs1.To associate a DCR with a virtual machine, you need to install the Azure Monitor Agent on the machine and then select the DCR from the list of available rules2.You can also use Azure Policy to automatically install the agent and associate a DCR with any virtual machines or virtual machine scale sets as they are created in your subscription3.
The other options are not correct for this scenario because:
Azure Network Watcher is a service that provides network performance monitoring and diagnostics for Azure resources.It is not related to data collection rules or Azure Monitor4.
A Log Analytics workspace is a destination where you can send the data collected by a data collection rule.It is not an entity that you can associate a DCR with5.
A Monitored Object is not a valid term in the context of Azure Monitor or data collection rules.

QUESTION 90
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.

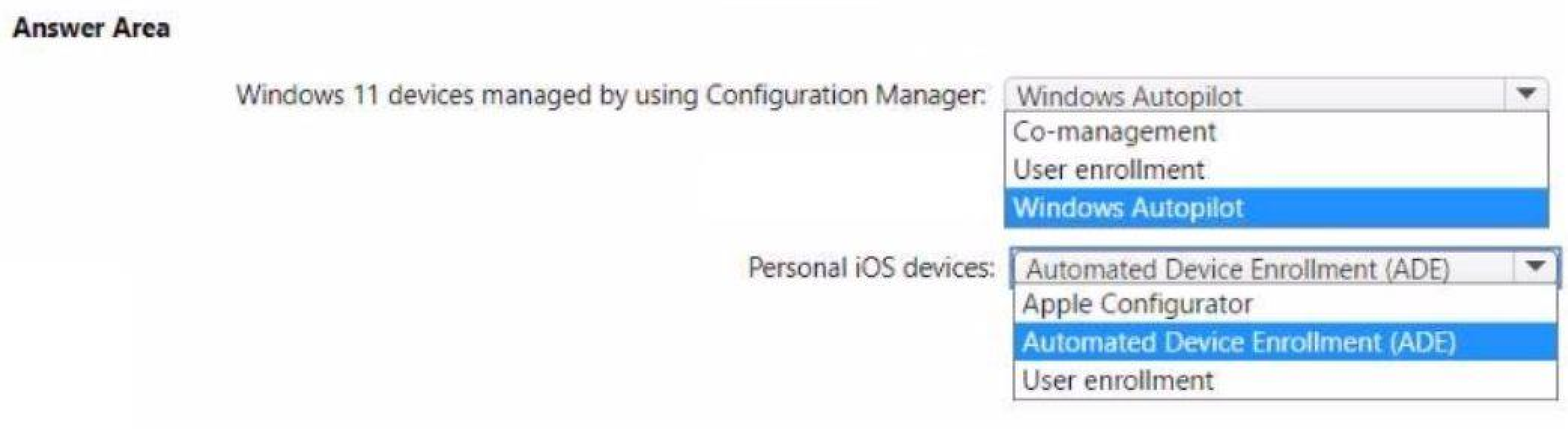
E. Create a device configuration profile.

Correct Answer: C, E
Section:
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.

QUESTION 91
HOTSPOT
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.

Hot Area:



Answer Area

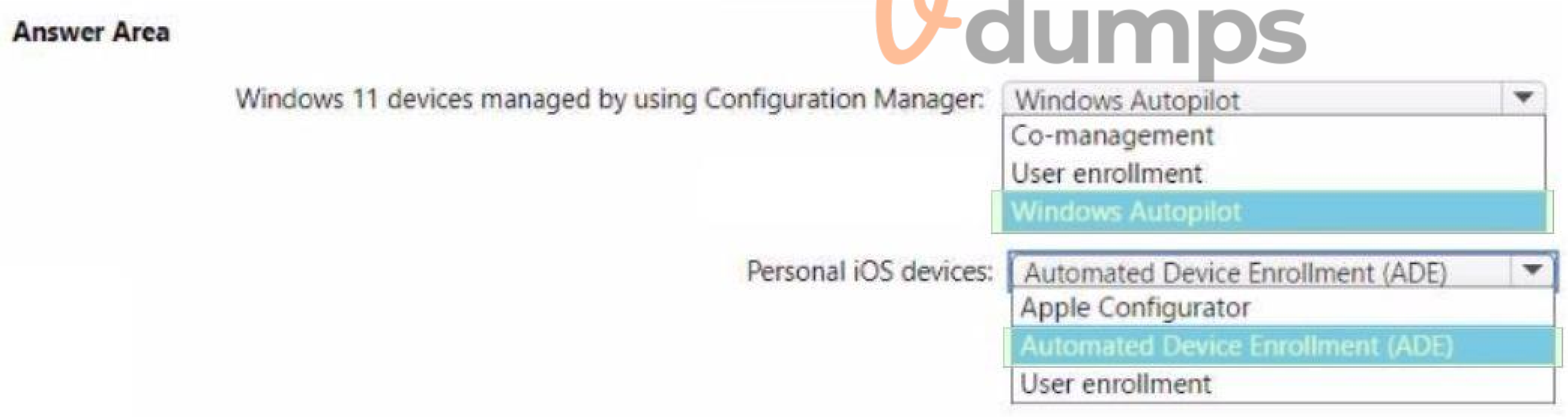
Windows 11 devices managed by using Configuration Manager: Windows Autopilot

- Co-management
- User enrollment
- Windows Autopilot

Personal iOS devices: Automated Device Enrollment (ADE)

- Apple Configurator
- Automated Device Enrollment (ADE)
- User enrollment

Answer Area:



Answer Area

Windows 11 devices managed by using Configuration Manager: Windows Autopilot

- Co-management
- User enrollment
- Windows Autopilot

Personal iOS devices: Automated Device Enrollment (ADE)

- Apple Configurator
- Automated Device Enrollment (ADE)
- User enrollment

Section:
Explanation:

QUESTION 92
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

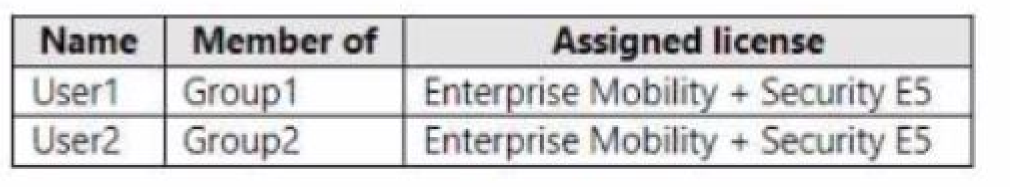
B. a device compliance policy

C. an MDM Security Baseline profile

D. a Group Policy Object (GPO)

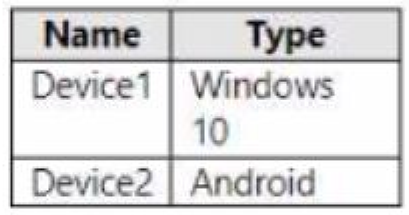
Correct Answer: A
Section:
Explanation:
A device configuration profile is a collection of settings that can be applied to devices enrolled in Microsoft Intune. You can use device configuration profiles to manage Windows 10 devices that are joined to Active Directory and enrolled in Intune. To ensure 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.Reference:[Use policy CSP settings to create custom device configuration profiles]

QUESTION 93
HOTSPOT
You have an Azure Active Directory Premium Plan 2 subscription that contains the users shown in the following table.



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

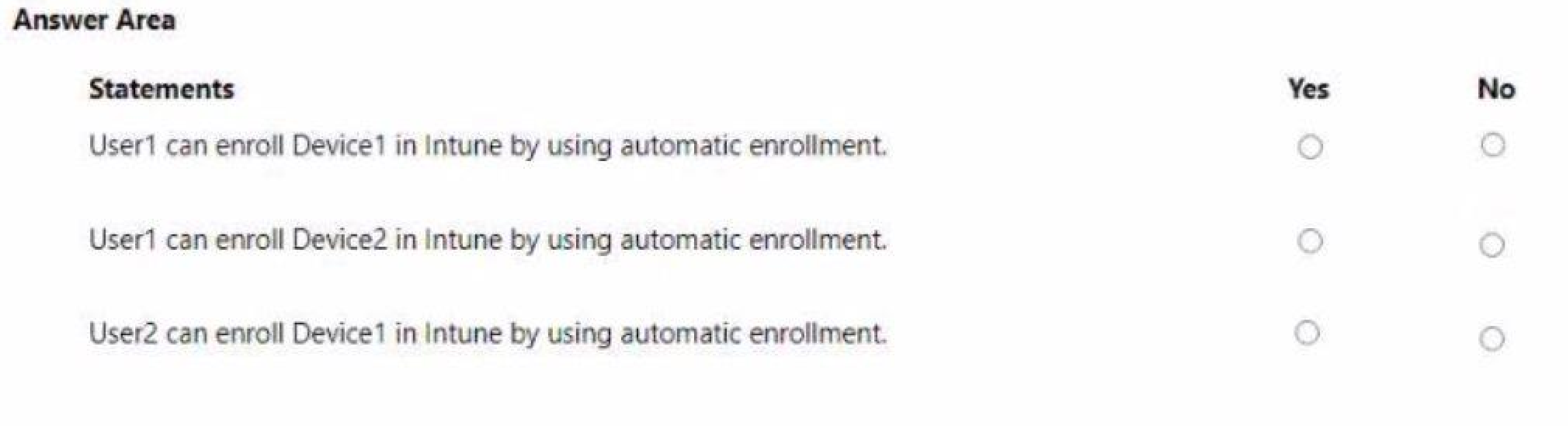
You purchase the devices shown in the following table.



Name	Type
Device1	Windows 10
Device2	Android

You configure automatic mobile device management (MDM) and mobile application management (MAM) enrollment by using the following settings:
* MDM user scope: Group1
* MAM user scope: Group2
For each of the following statements, select Yes if the statement is true. Otherwise, select No. NOTE: Each correct selection is worth one point.

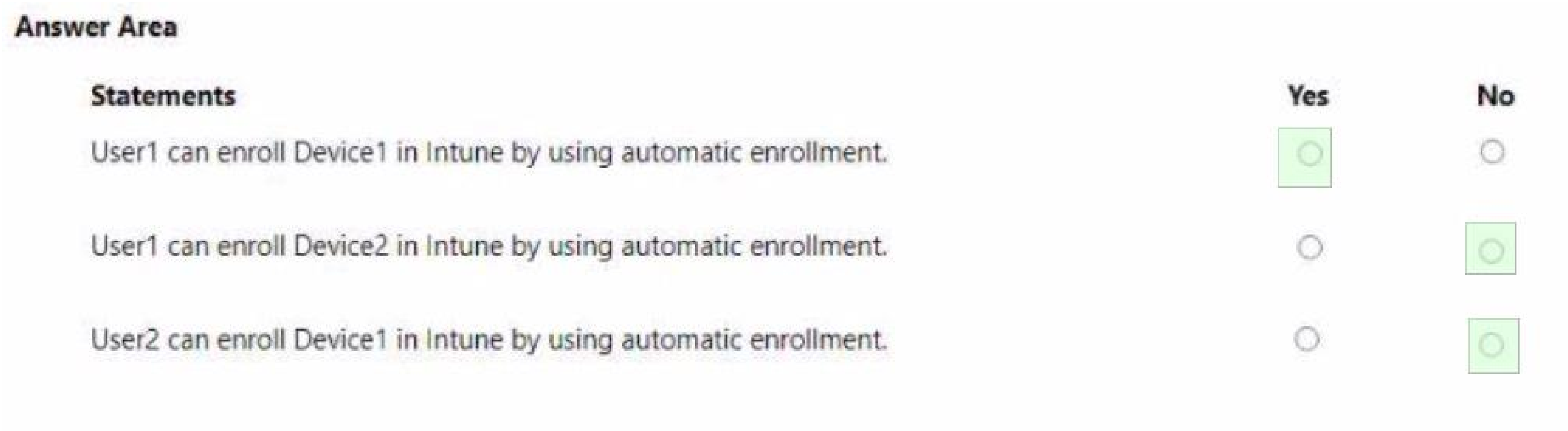
Hot Area:



Answer Area

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

Answer Area:



Answer Area

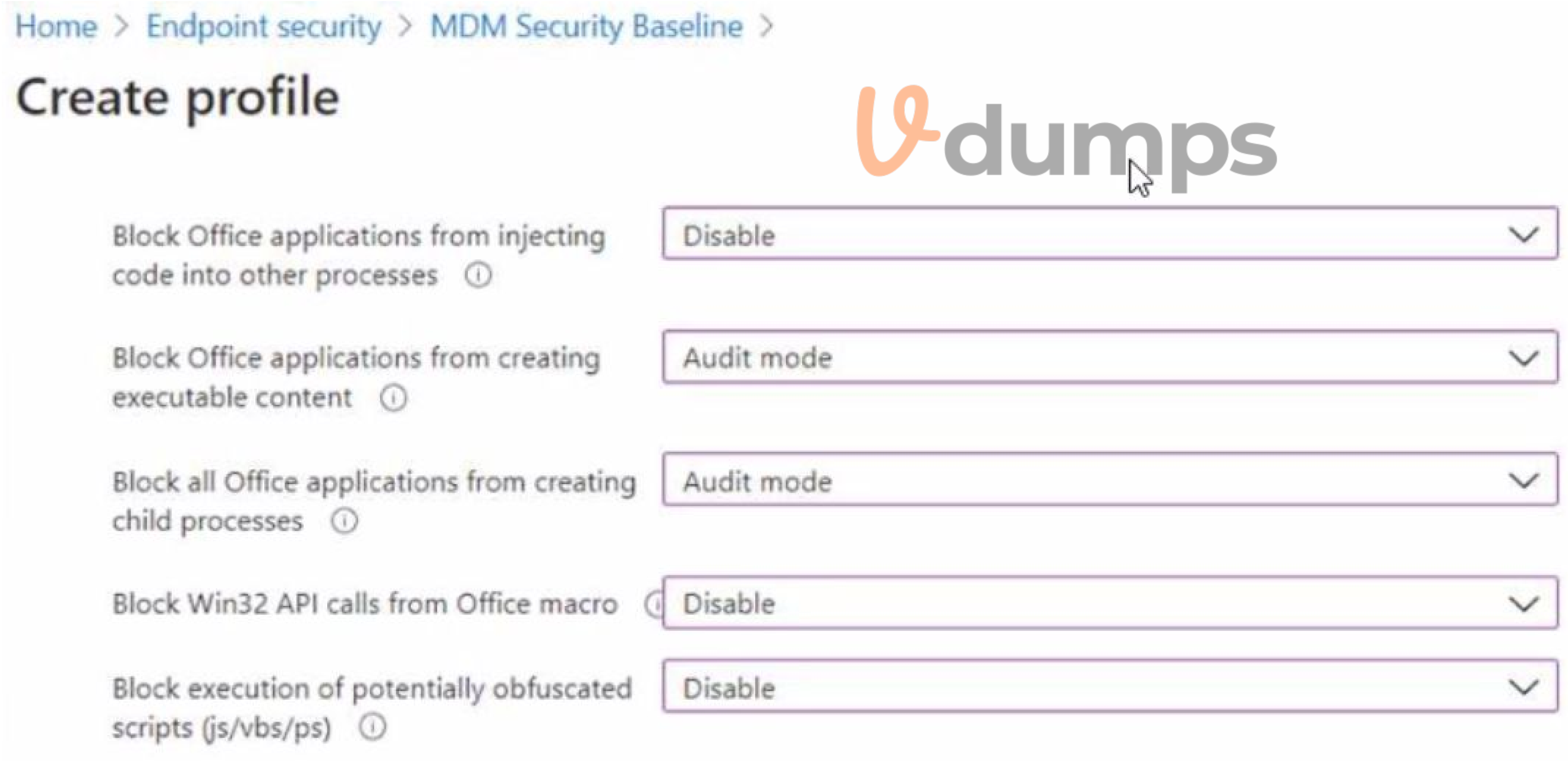
Statements	Yes	No
User1 can enroll Device1 in Intune by using automatic enrollment.	[✓ ○]	○
User1 can enroll Device2 in Intune by using automatic enrollment.	○	[✓ ○]
User2 can enroll Device1 in Intune by using automatic enrollment.	○	[✓ ○]

Section:
Explanation:

QUESTION 94

HOTSPOT

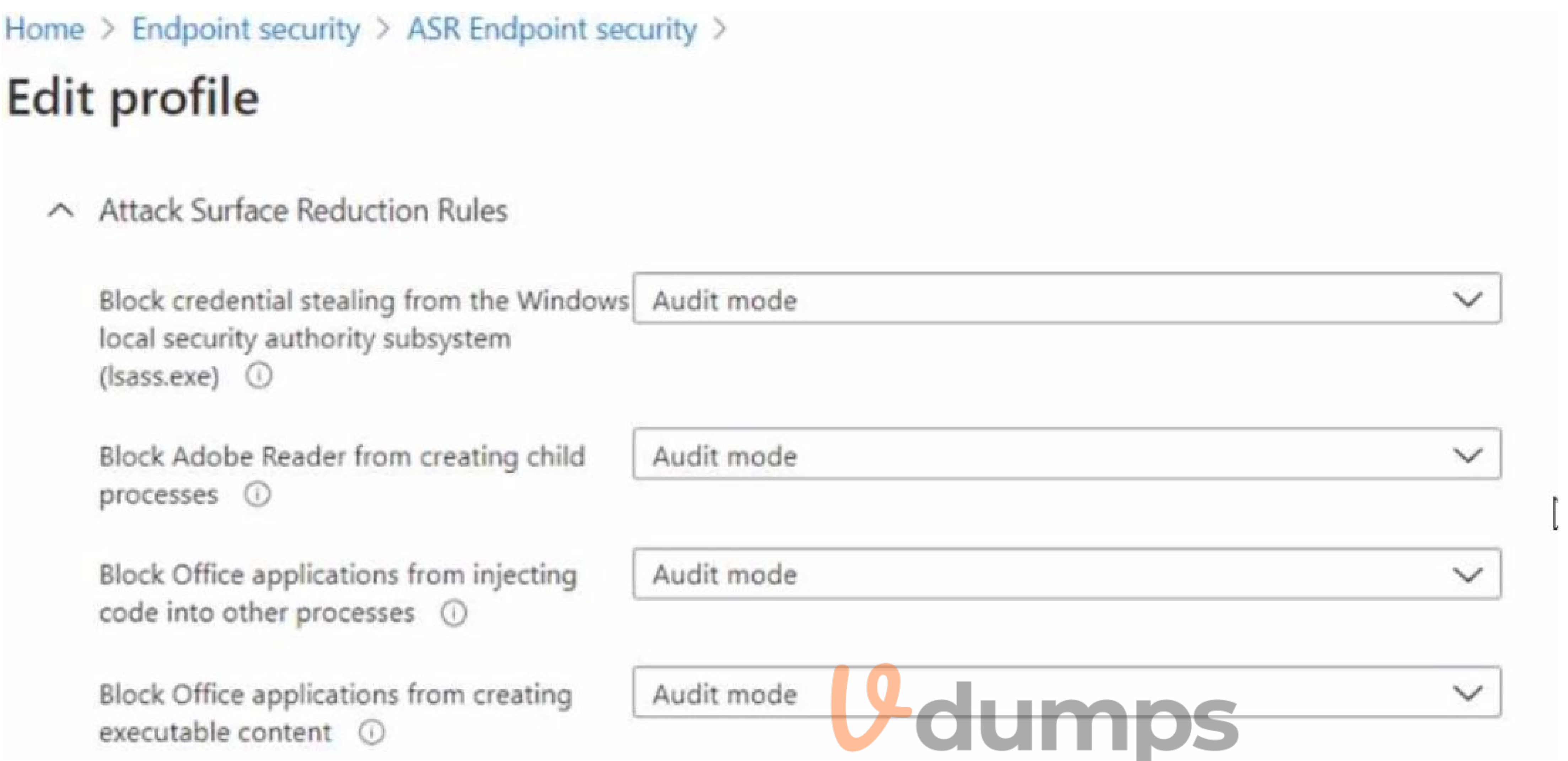
You have the MDM Security Baseline profile shown in the MDM exhibit. (Click the MDM tab.)



Home > Endpoint security > MDM Security Baseline >

Create profile

Block Office applications from injecting code into other processes ⓘ	Disable
Block Office applications from creating executable content ⓘ	Audit mode
Block all Office applications from creating child processes ⓘ	Audit mode
Block Win32 API calls from Office macro ⓘ	Disable
Block execution of potentially obfuscated scripts (js/vbs/ps) ⓘ	Disable



Home > Endpoint security > ASR Endpoint security >

Edit profile

Attack Surface Reduction Rules

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

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

* Block Office applications from creating executable content

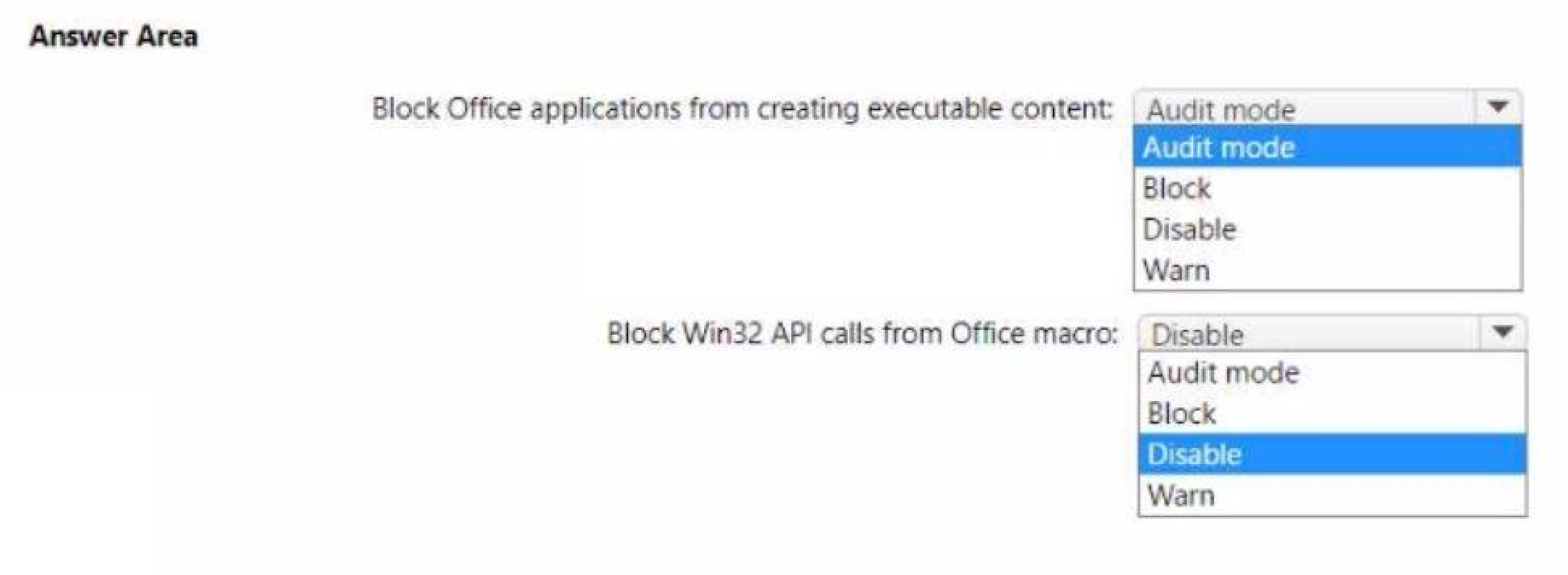
* Block Win32 API calls from Office macro

Currently, the settings are disabled locally on each device.

What are the effective settings on the devices? To answer, select the appropriate options in the answer area.

NOTE: Each correct selection is worth one point.

Hot Area:



Answer Area

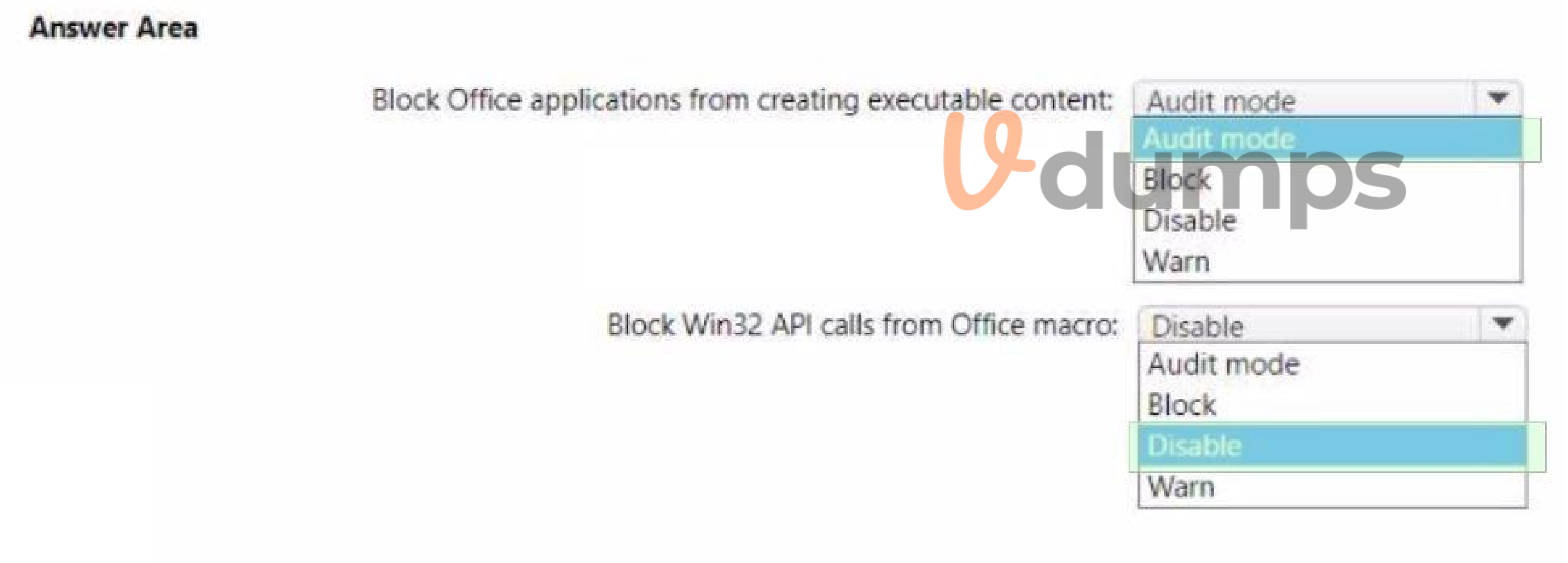
Block Office applications from creating executable content: Audit mode

- Audit mode
- Block
- Disable
- Warn

Block Win32 API calls from Office macro: Disable

- Audit mode
- Block
- Disable
- Warn

Answer Area:



Answer Area

Block Office applications from creating executable content: Audit mode

- Audit mode
- Block
- Disable
- Warn

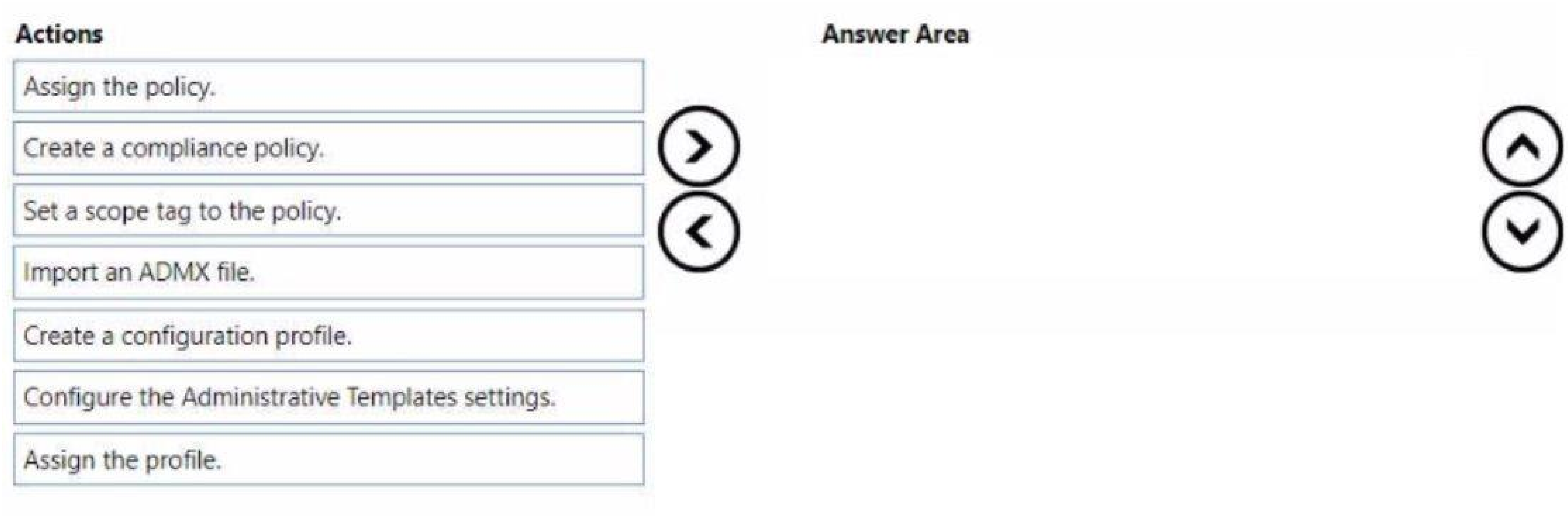
Block Win32 API calls from Office macro: Disable

- Audit mode
- Block
- Disable
- Warn

Section:
Explanation:

QUESTION 95
DRAG DROP
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.

Select and Place:

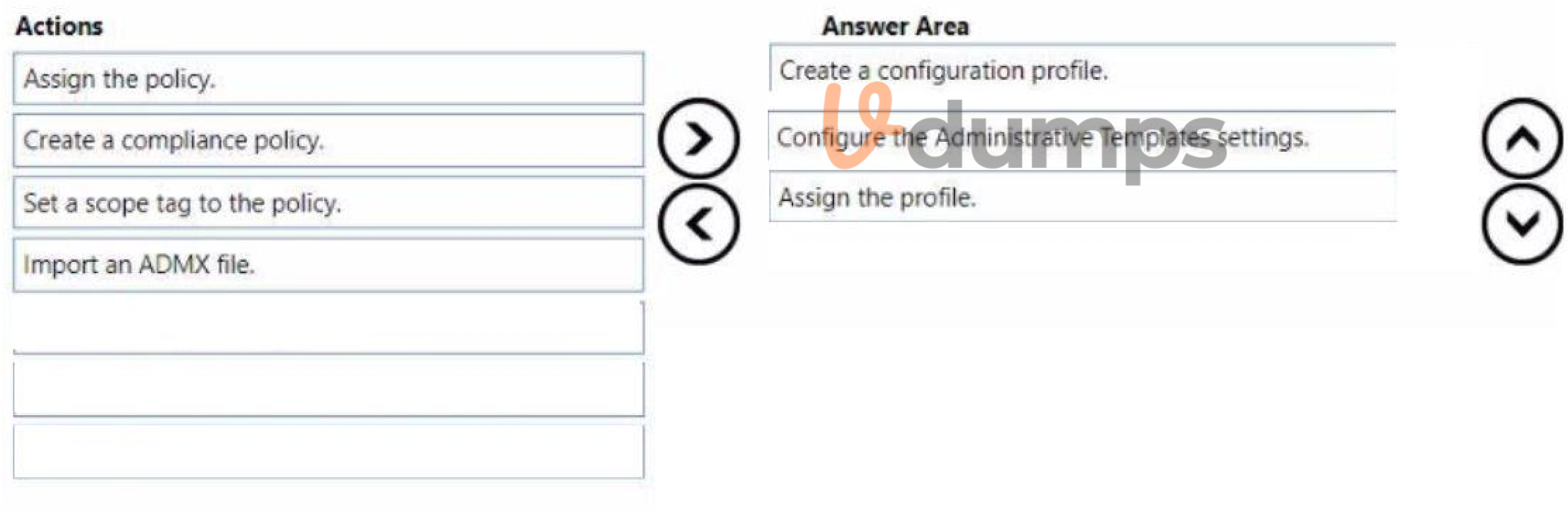


Actions

- 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

Correct Answer:



Actions

- Assign the policy.
- Create a compliance policy.
- Set a scope tag to the policy.
- Import an ADMX file.

Answer Area

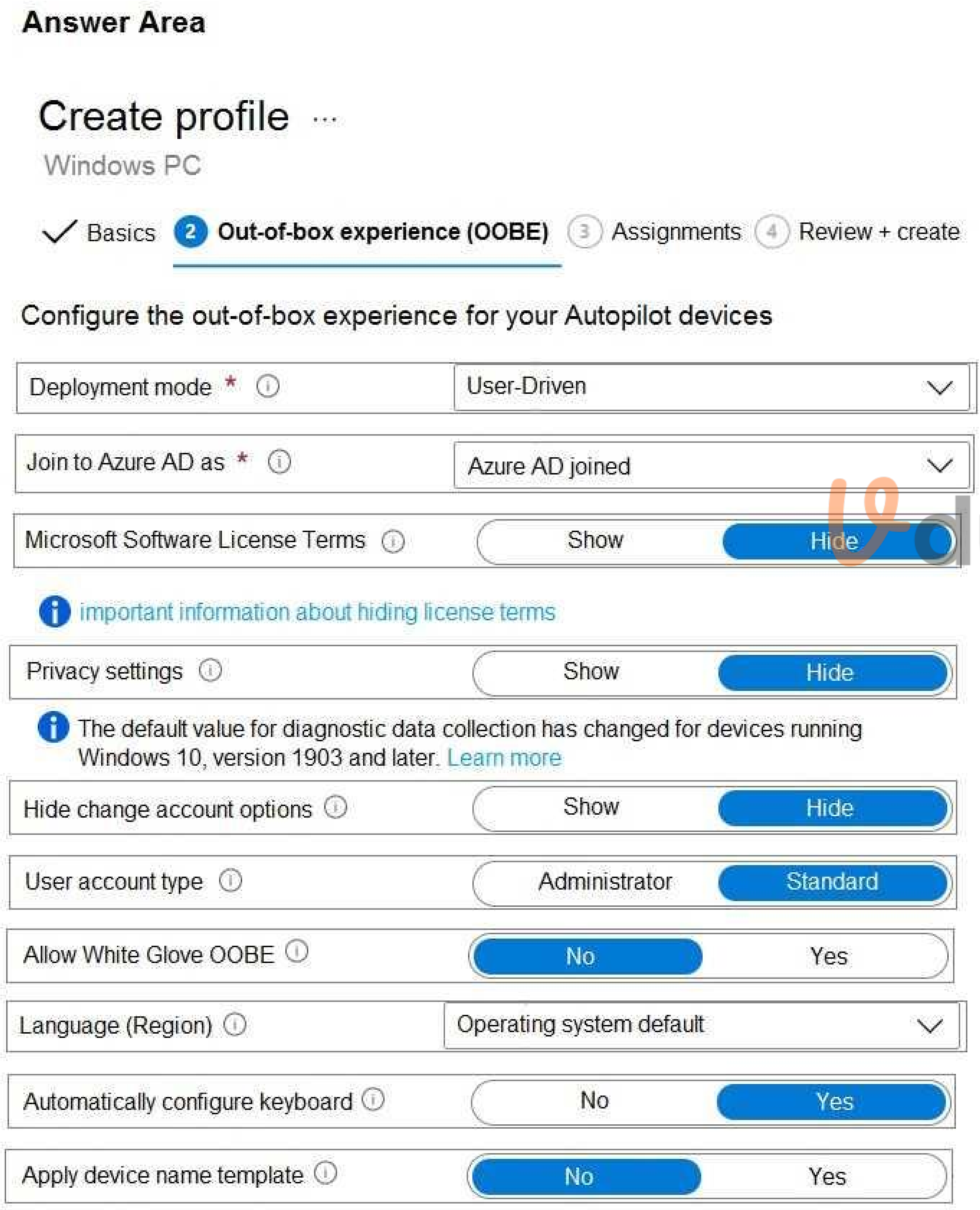
- Create a configuration profile.
- Configure the Administrative Templates settings.
- Assign the profile.

Section:
Explanation:
Create a configuration profile.
Configure the Administrative Templates settings.
Assign the profile.

QUESTION 96
HOTSPOT
You create a Windows Autopilot deployment profile.
You need to configure the profile settings to meet the following requirements:

Automatically enroll new devices and provision system apps without requiring end-user authentication.
Include the hardware serial number in the computer name.
Which two settings should you configure? To answer, select the appropriate settings in the answer area.
NOTE: Each correct selection is worth one point.

Hot Area:



Answer Area

Create profile ...

Windows PC

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

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

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

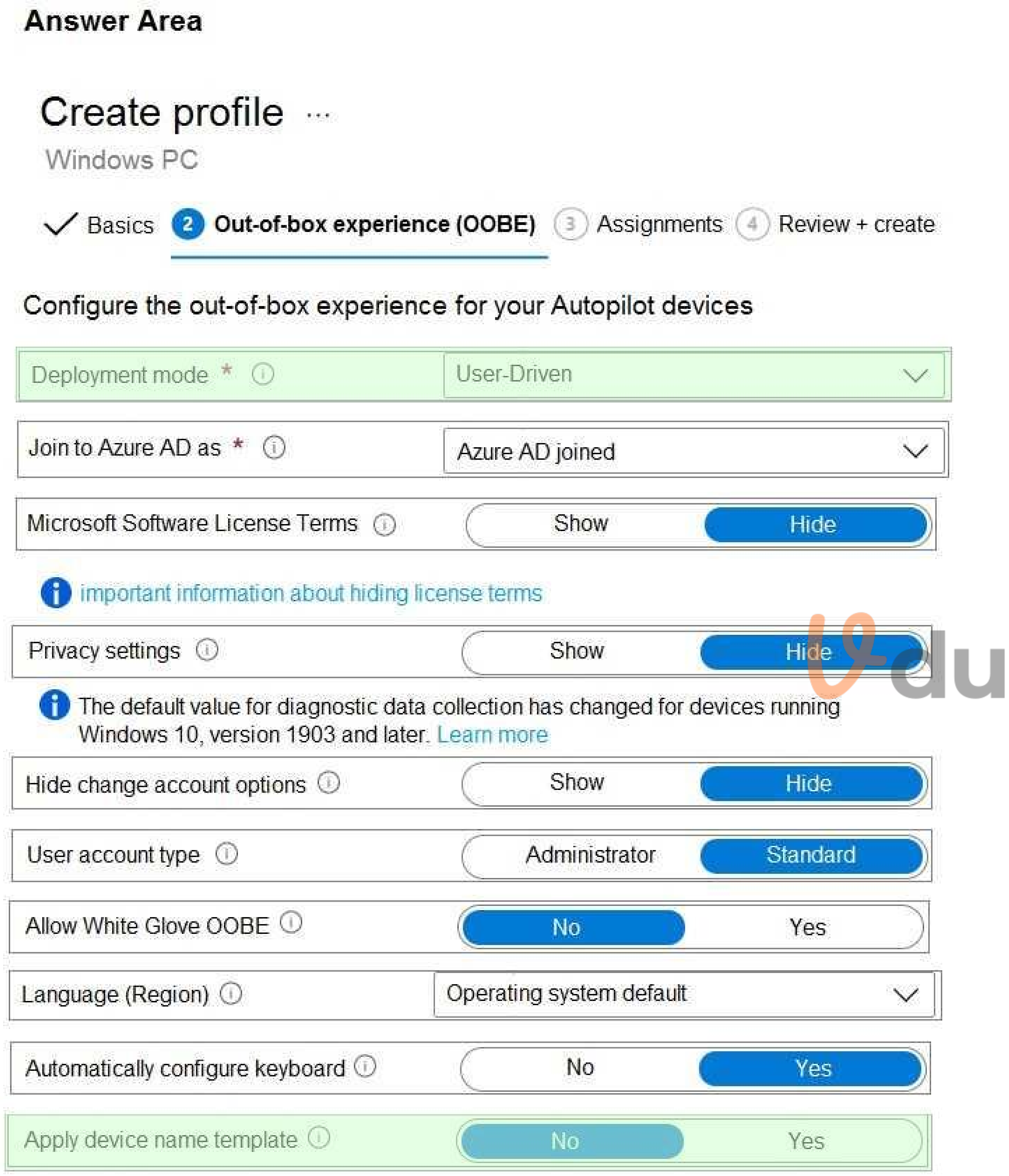
important information about hiding license terms

Privacy settings	Show [✓ Hide]

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

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

Answer Area:



Answer Area

Create profile ···

Windows PC

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

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

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

ⓘ important information about hiding license terms

Privacy settings ⓘ	Show [✓ Hide]

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

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

Section:

Explanation:

Reference:

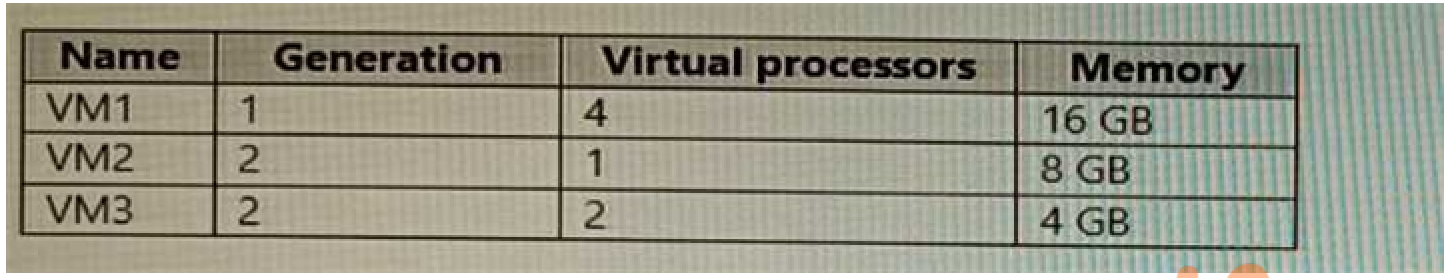
https://docs.microsoft.com/en-us/mem/autopilot/profiles

QUESTION 97
You have a computer named Computer! that runs Windows 11.
A user named User1 plans to use Remote Desktop to connect to Computer1.
You need to ensure that the device of User1 is authenticated before the Remote Desktop connection is established and the sign in page appears.
What should you do on Computer1?

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

Correct Answer: B
Section:

QUESTION 98
You have a Hyper-V host that contains the virtual machines shown in the following table.



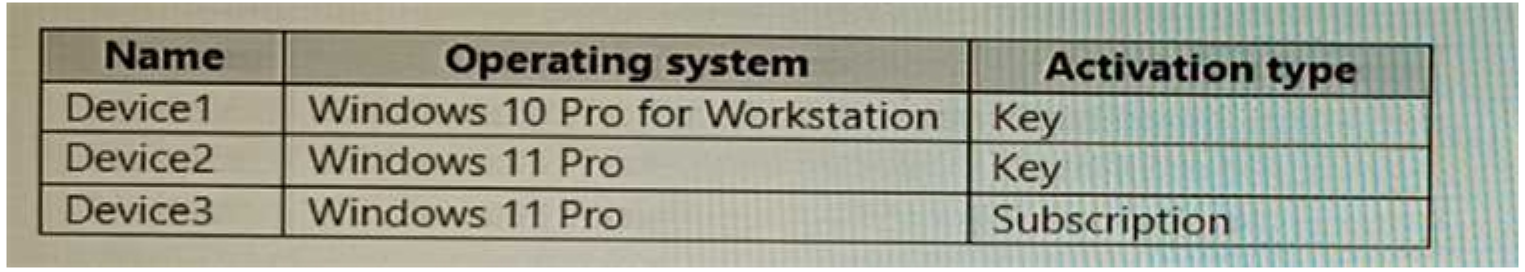
Name	Generation	Virtual processors	Memory
VM1	1	4	16 GB
VM2	2	1	8 GB
VM3	2	2	4 GB

On which virtual machines can you install Windows 11?

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

Correct Answer: E
Section:

QUESTION 99
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

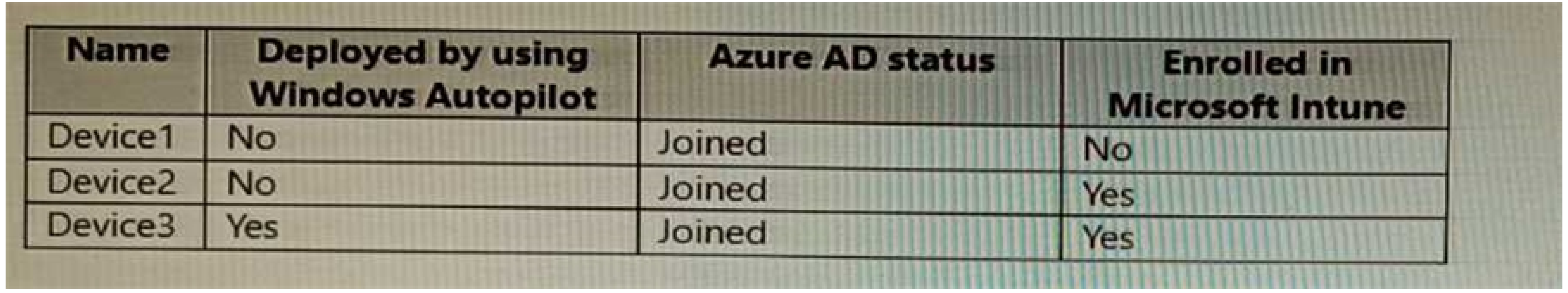
D. Device1, Device2, and Device3

Correct Answer: A
Section:

QUESTION 100

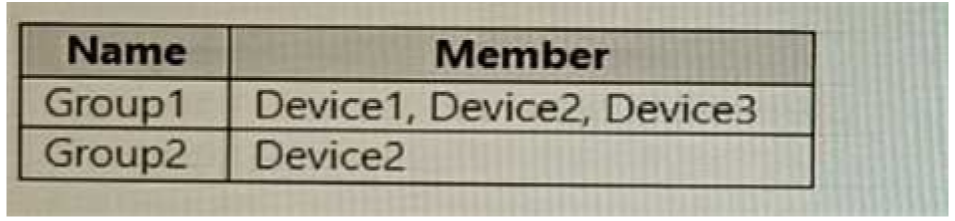
HOTSPOT

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



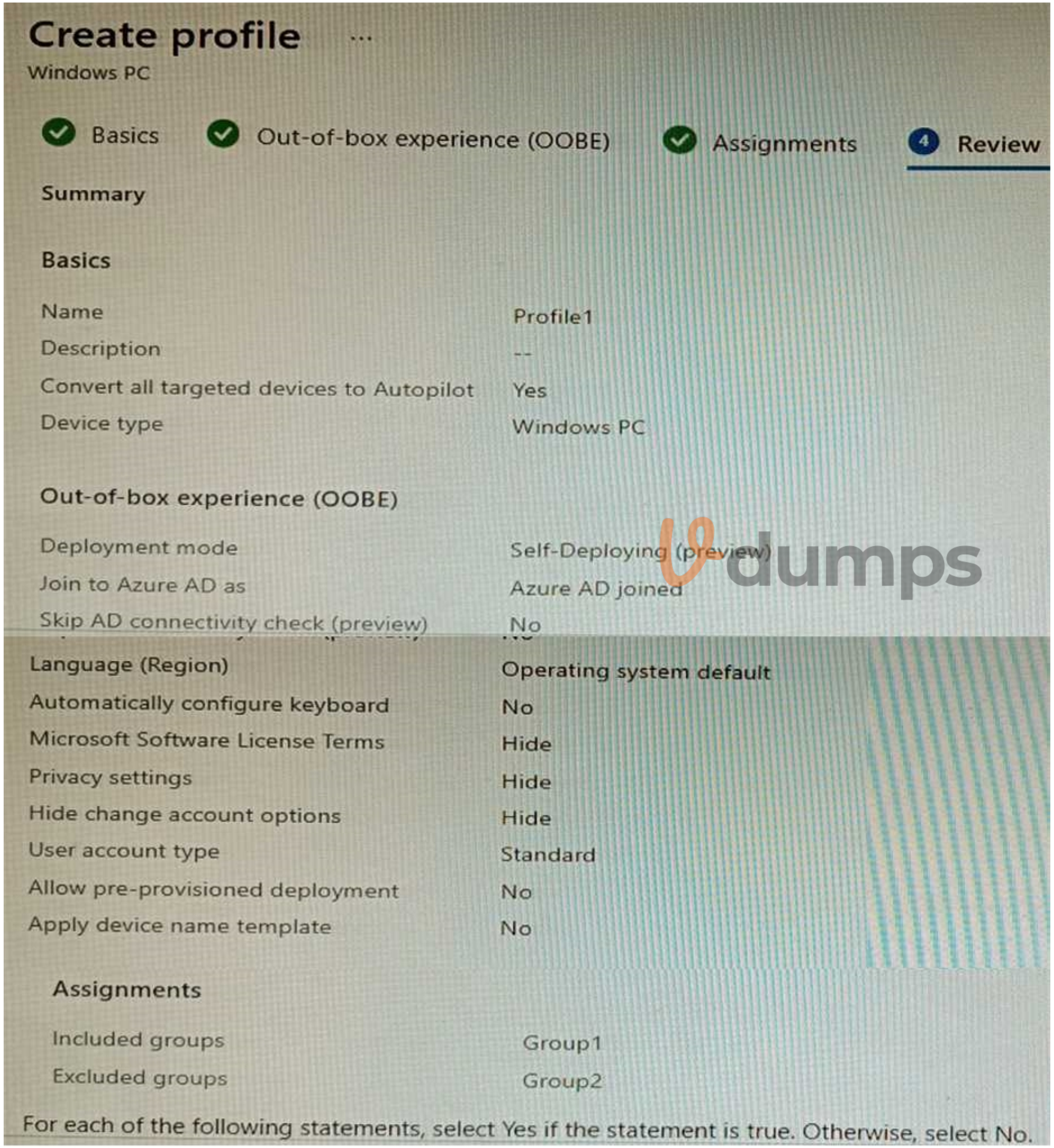
Name	Deployed by using Windows Autopilot	Azure AD status	Enrolled in Microsoft Intune
Device1	No	Joined	No
Device2	No	Joined	Yes
Device3	Yes	Joined	Yes

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

Summary

Basics

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

Out-of-box experience (OOBE)

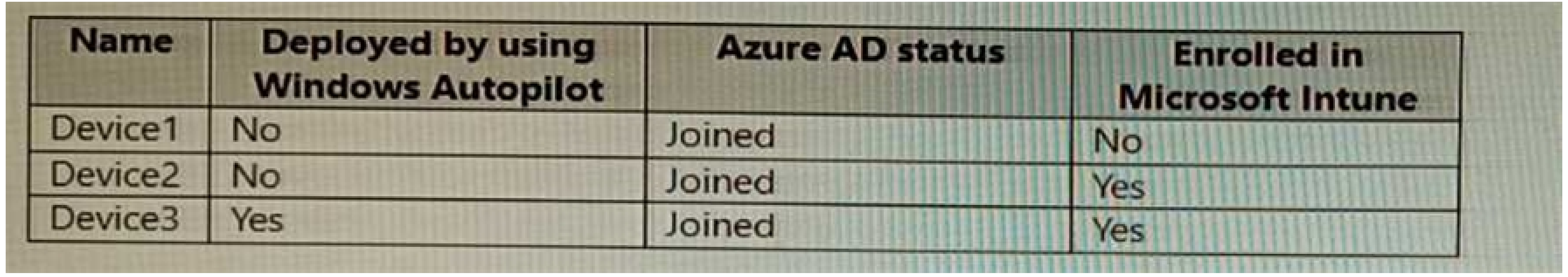
Deployment mode	Self-Deploying (preview)
Join to Azure AD as	Azure AD joined
Skip AD connectivity check (preview)	No
Language (Region)	Operating system default
Automatically configure keyboard	No
Microsoft Software License Terms	Hide
Privacy settings	Hide
Hide change account options	Hide
User account 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.

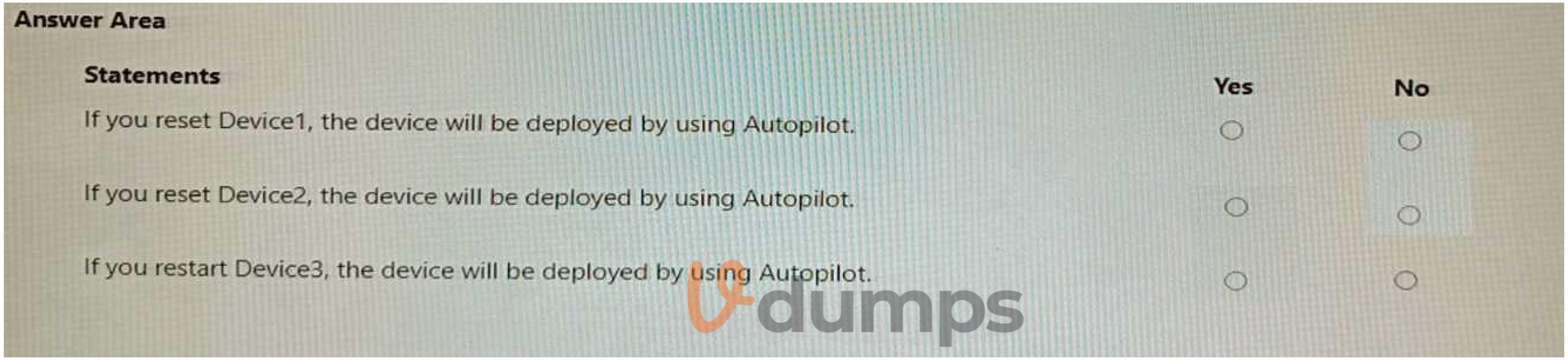
You have an Azure AD tenant named contoso.com that contains the devices shown in the following table.



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.

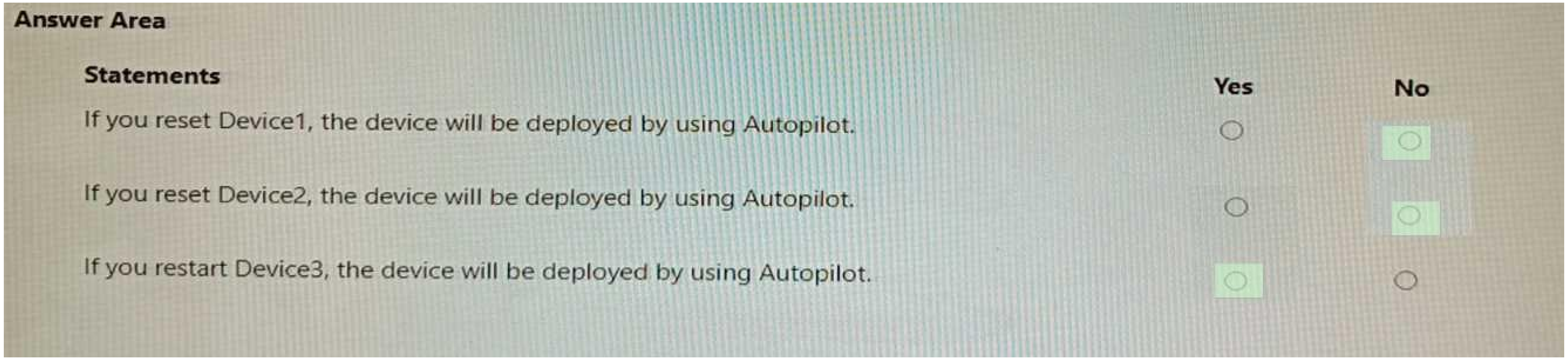
Hot Area:



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.	○	○

Answer Area:



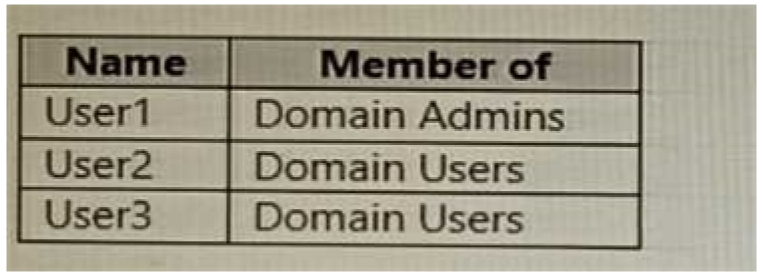
Answer Area

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.	[✓ ○]	○

Section:
Explanation:

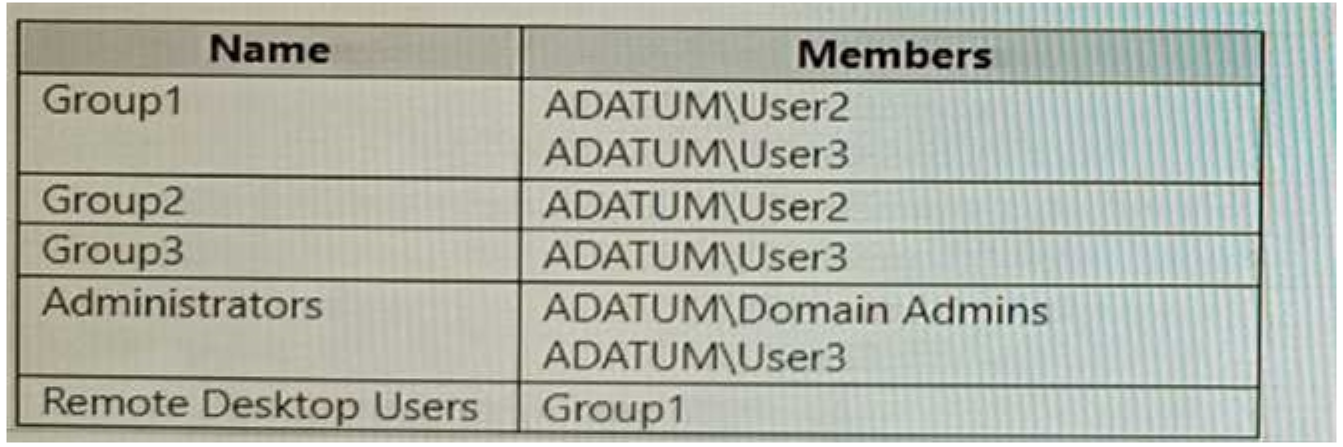
QUESTION 101
HOTSPOT

Your network contains an Active Directory domain named adatum.com. The domain contains two computers named Computer1 and Computer2 that run Windows 10. Remote Desktop is enabled on Computer2.
The domain contains the user accounts shown in the following table.



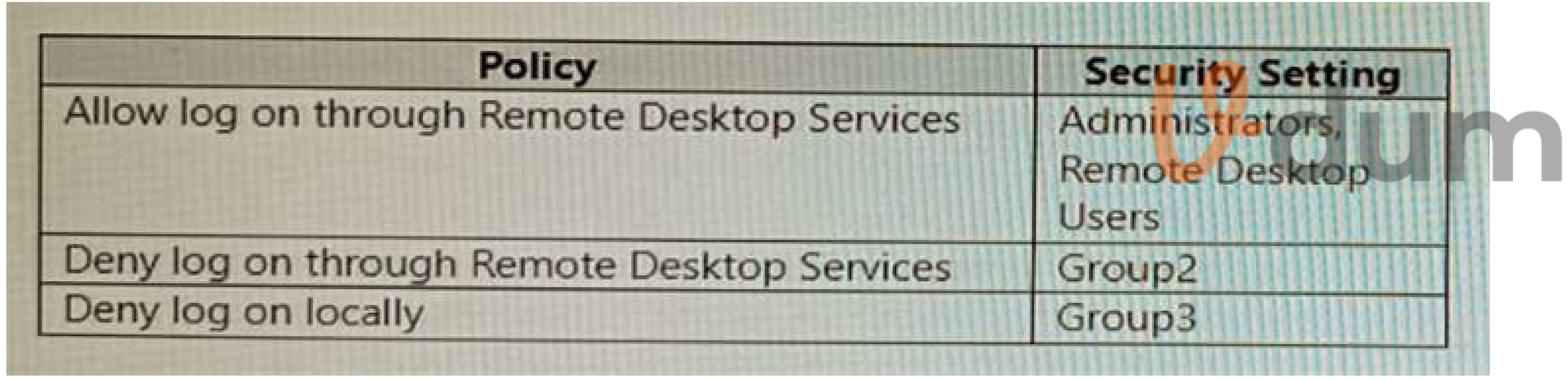
Name	Member of
User1	Domain Admins
User2	Domain Users
User3	Domain Users

Computer2 contains the local groups shown in the following table.



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

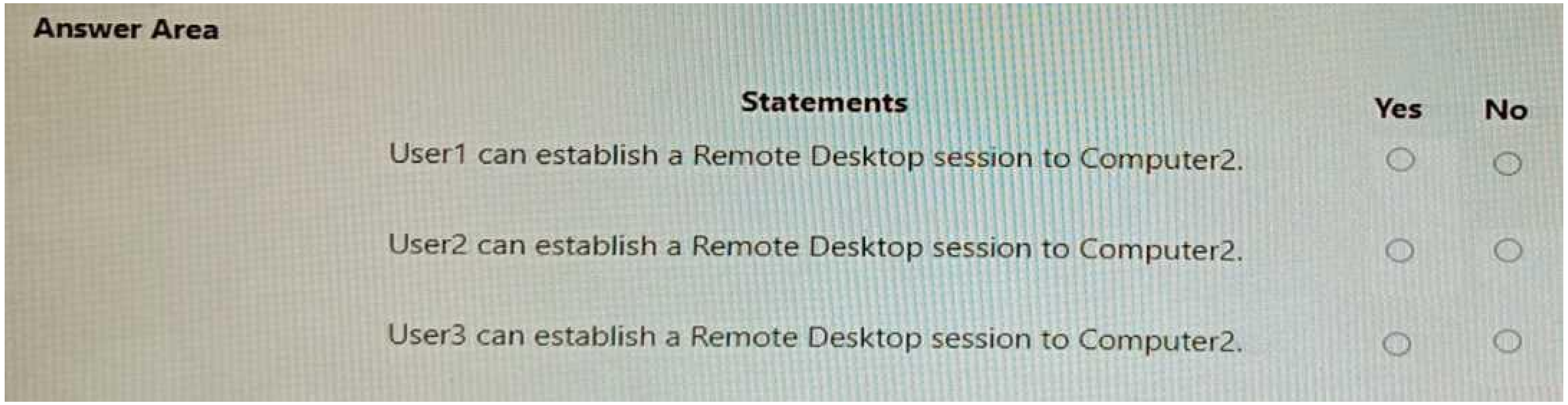
The relevant user rights assignments for Computed are shown in the following table.



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

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

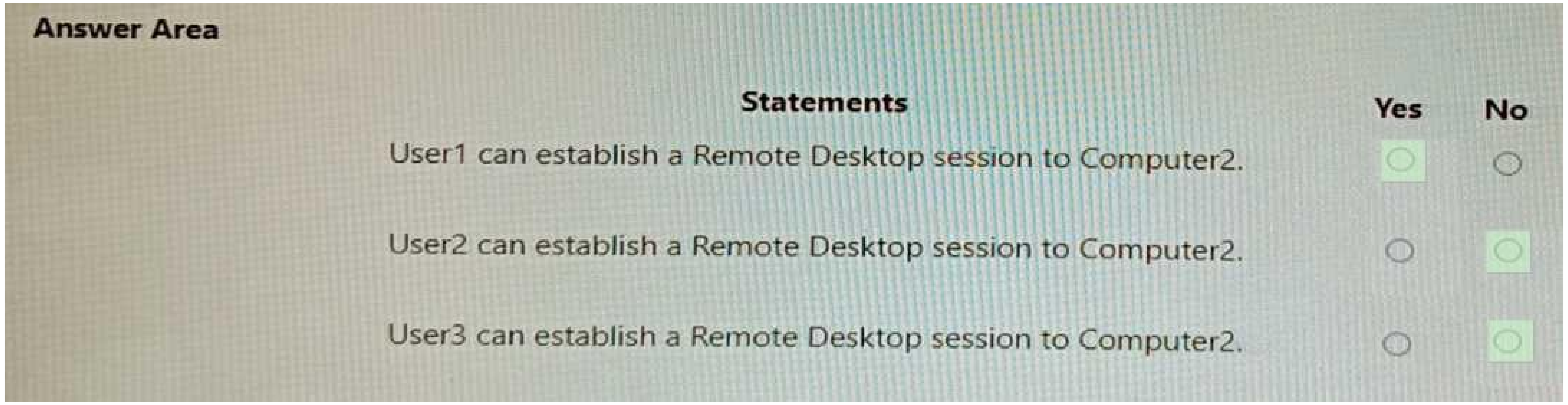
Hot Area:



Answer Area

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

Answer Area:



Answer Area

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

Section:
Explanation:

QUESTION 102
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.

Correct Answer: D
Section:

QUESTION 103
You have a Windows 10 device named Computer1 enrolled in Microsoft Intune.
You need to configure Computer1 as a public workstation that will run a single customer-facing, full-screen application.
Which configuration profile type template should you use in Microsoft Intune admin center?

A. Shared multi-user device
B. Device restrictions
C. Kiosk
D. Endpoint protection

Correct Answer: C
Section:

QUESTION 104
You have a Microsoft 365 subscription.
You have devices enrolled in Microsoft Intune as shown in the following table.

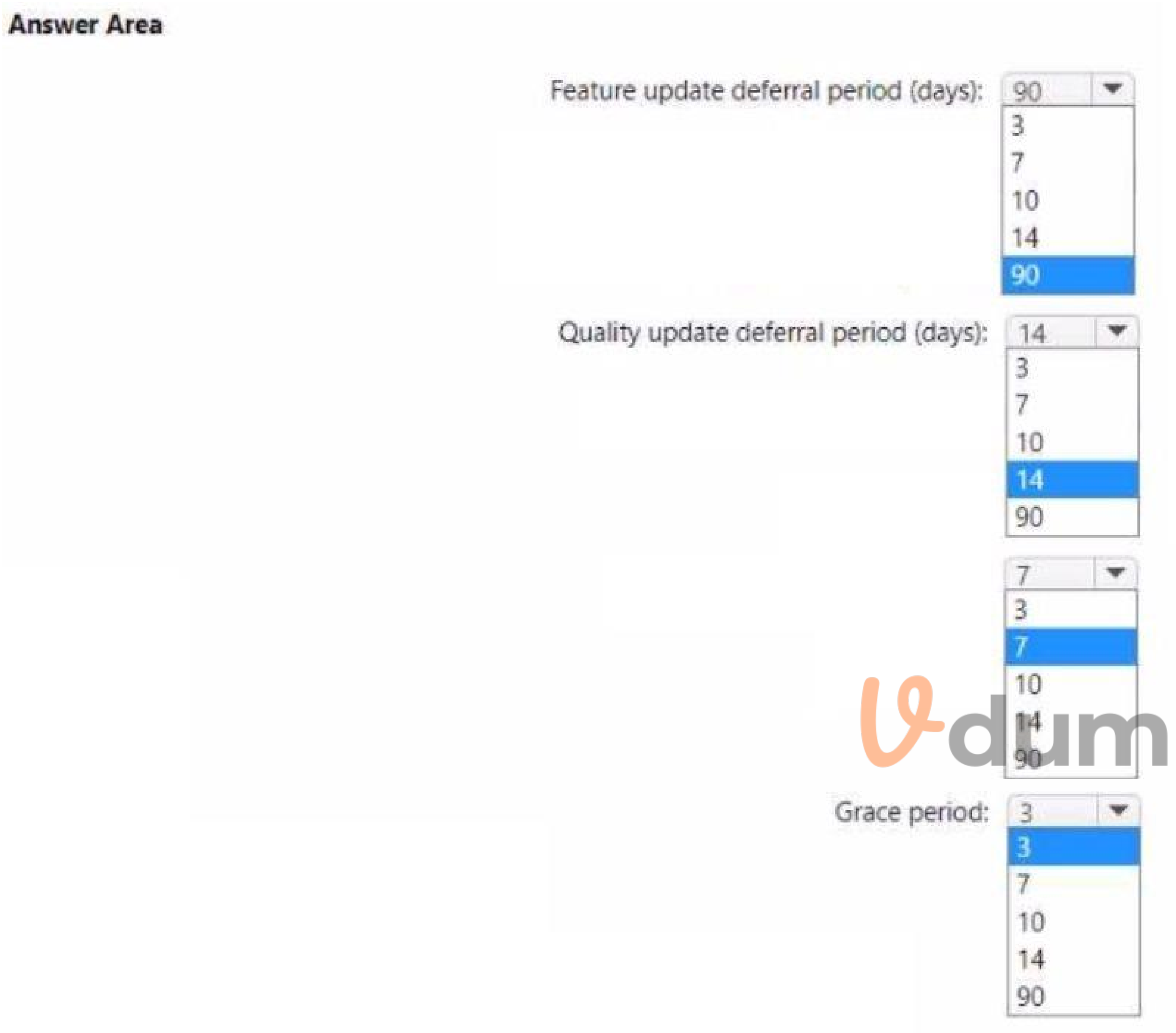
To which devices can you deploy apps by using Intune?

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

Correct Answer: E
Section:

QUESTION 105
HOTSPOT
You have a Microsoft 365 subscription that uses Microsoft Intune Suite.
You use Microsoft Intune to manage devices.
You need to configure an update ring that meets the following requirements:
* Fixes and improvements to existing Windows functionality can be deferred for 14 days but will install automatically seven days after that date.
* The installation of new Windows features can be deferred for 90 days but will install automatically 10 days after that date.
* Devices must restart automatically three days after an update is installed.
How should you configure the update ring? To answer, select the appropriate options in the answer are a. NOTE: Each correct selection is worth one point.

Hot Area:



Answer Area

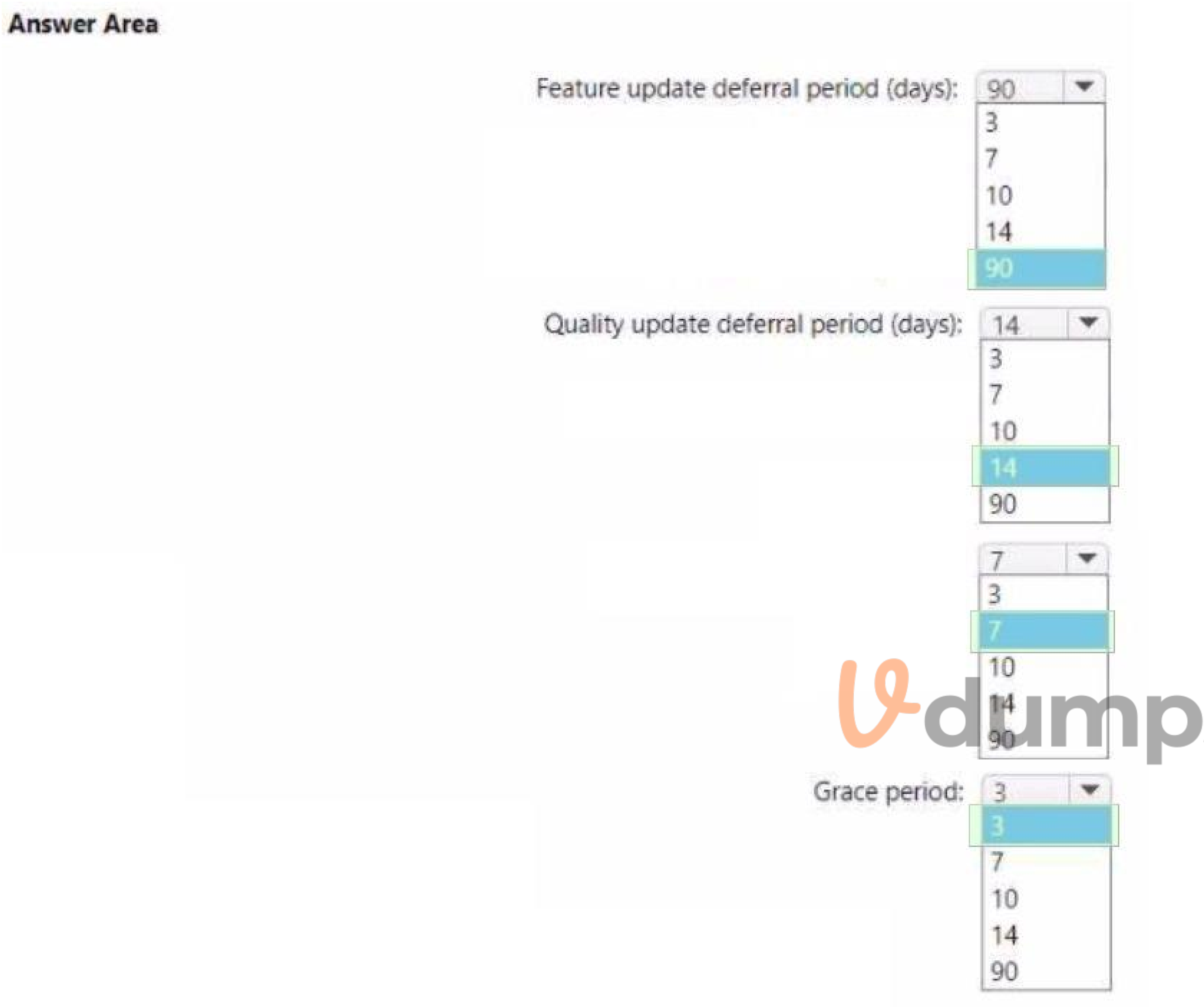
Feature update deferral period (days): 90

Quality update deferral period (days): 14

7

Grace period: 3

Answer Area:



Answer Area

Feature update deferral period (days): 90

Quality update deferral period (days): 14

7

Grace period: 3

Section:
Explanation:

QUESTION 106
You manage 1.000 devices by using Microsoft Intune. You review the Device compliance trends report. For how long will the report display trend data?

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

Correct Answer: B
Section:

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

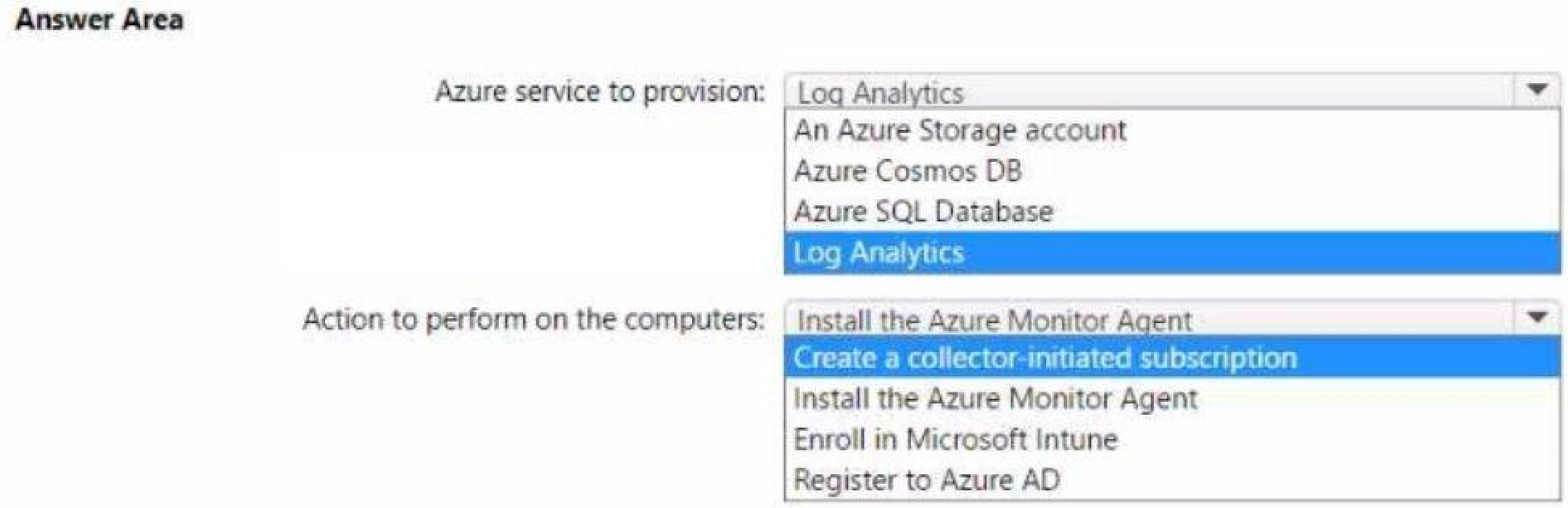
QUESTION 107
You have a Microsoft 365 subscription that contains 500 computers that run Windows 11. The computers are Azure AD joined and are enrolled in Microsoft Intune.
You plan to manage Microsoft Defender Antivirus on the computers.
You need to prevent users from disabling Microsoft Defender Antivirus,
What should you do?

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

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

QUESTION 108
HOTSPOT
You have 1,000 computers that run Windows 10 and are members of an Active Directory domain.
You need to capture the event togs from the computers to Azure.
What should you do? To answer, select the appropriate options in the answer area.
NOTE: Each correct selection is worth one point.

Hot Area:



Answer Area

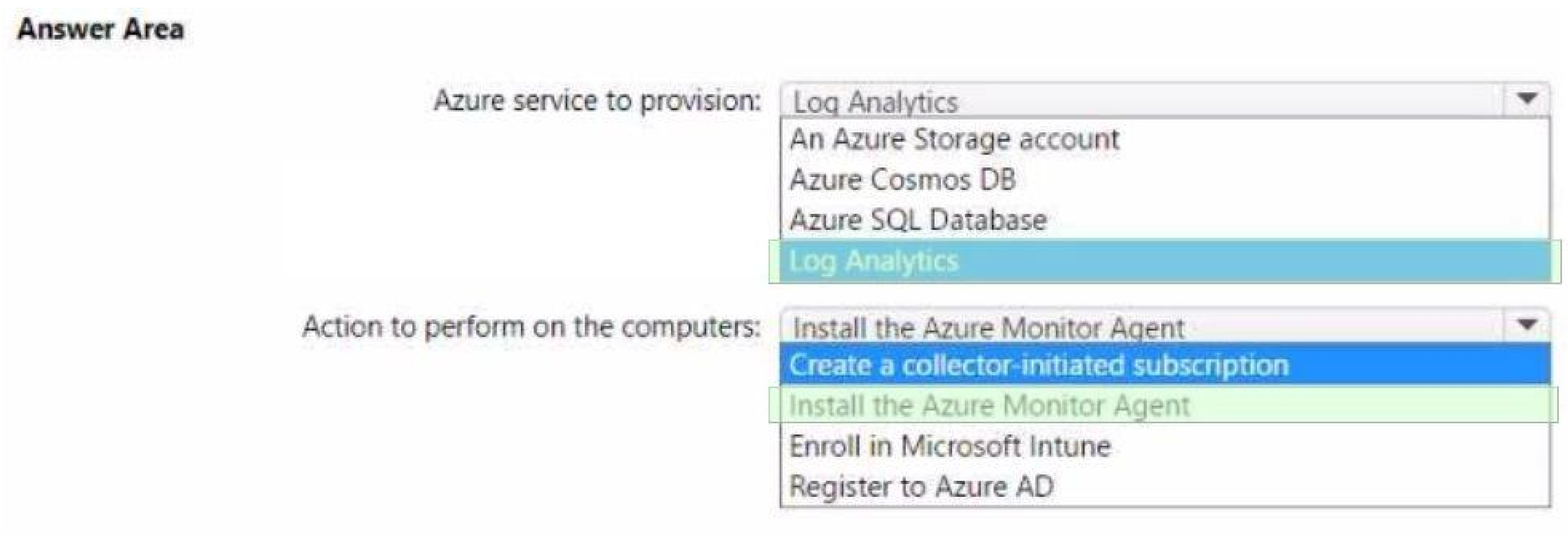
Azure service to provision: Log Analytics

- An Azure Storage account
- Azure Cosmos DB
- Azure SQL Database
- Log Analytics

Action to perform on the computers: Install the Azure Monitor Agent

- Create a collector-initiated subscription
- Install the Azure Monitor Agent
- Enroll in Microsoft Intune
- Register to Azure AD

Answer Area:



Answer Area

Azure service to provision: Log Analytics

An Azure Storage account
Azure Cosmos DB
Azure SQL Database
Log Analytics

Action to perform on the computers: Install the Azure Monitor Agent

Create a collector-initiated subscription
Install the Azure Monitor Agent
Enroll in Microsoft Intune
Register to Azure AD

Section:
Explanation:

QUESTION 109
You have 200 computers that run Windows 10 and are joined to an Active Directory domain.
You need to enable Windows Remote Management (WinRM) on all the computers by using Group Policy.
Which three actions should you perform? Each correct answer presents part of the solution.
NOTE: Each correct selection is worth one point.

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

Correct Answer: B, C, F
Section:
Explanation:
To enable WinRM on domain computers using Group Policy, you need to perform the following actions:
Enable the Allow remote server management through WinRM setting under Computer Configuration > Policies > Administrative Templates > Windows Components > Windows Remote Management (WinRM) > WinRM Service. This setting allows you to specify the IP address ranges that can connect to the WinRM service.
Set the Startup Type of the Windows Remote Management (WS-Management) service to Automatic under Computer Configuration > Preferences > Control Panel Settings > Services. This setting ensures that the WinRM service starts automatically on the computers.
Enable the Windows Defender Firewall: Allow inbound remote administration exception setting under Computer Configuration > Policies > Security Settings > Windows Firewall and Advanced Security > Windows Firewall and Advanced Security > Inbound Rules. This setting creates a firewall rule that allows incoming TCP connections on port 5985 for WinRM.Reference:How to Enable WinRM via Group Policy,Installation and configuration for Windows Remote Management

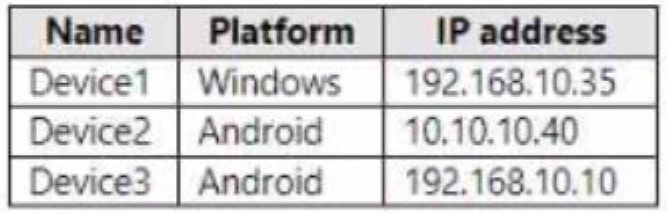
QUESTION 110
You have a Microsoft 365 Business Standard subscription and 100 Windows 10 Pro devices.
You purchase a Microsoft 365 E5 subscription.
You need to upgrade the Windows 10 Pro devices to Windows 10 Enterprise. The solution must minimize administrative effort.

Which upgrade method should you use?

A. Windows Autopilot
B. a Microsoft Deployment Toolkit (MDT) lite-touch deployment
C. Subscription Activation
D. an in-place upgrade by using Windows installation media

Correct Answer: C
Section:
Explanation:
Subscription Activation is a feature that allows you to upgrade from Windows 10 Pro or Windows 11 Pro to Windows 10 Enterprise or Windows 11 Enterprise without needing a product key or reinstallation. You just need to assign a subscription license (such as Microsoft 365 E5) to the user in Azure AD, and then sign in to the device with that user account. The device will automatically activate Windows Enterprise edition using the firmware-embedded activation key for Windows Pro edition. This method minimizes administrative effort and simplifies the upgrade process.Reference:Windows subscription activation,Deploy Windows Enterprise licenses

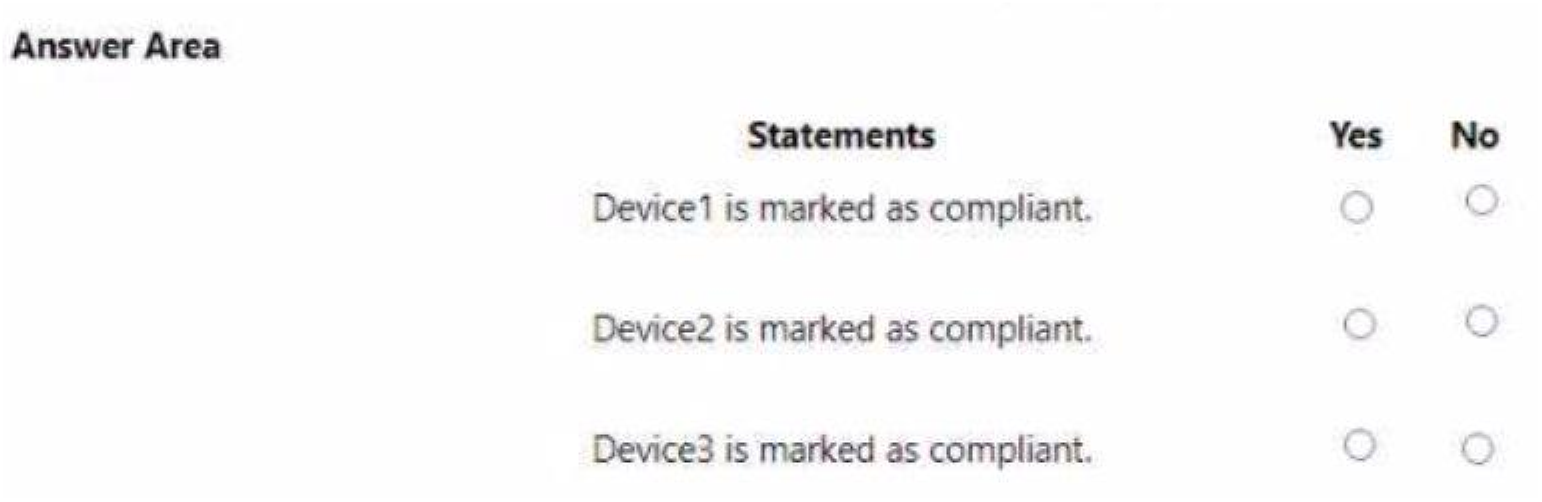
QUESTION 111
HOTSPOT
You have devices that are not rooted enrolled in Microsoft Intune as shown in the following table.



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

The devices are members of a group named Group1.
In Intune, you create a device compliance location that has the following configurations:
* Name: Network1
* IPv4 range: 192.168.0.0/16
In Intune. you create a device compliance policy for the Android platform. The policy has the following configurations:
* Name: Policy1
* Device health: Rooted devices: Block
* Locations: Location: Network1
* Mark device noncompliant: Immediately
* Assigned: Group1
The Intune device compliance policy has the following configurations:
* Mark devices with no compliance policy assigned as: Compliant
* Enhanced jailbreak detection: Enabled
* Compliance status validity period (days): 20
For each of the following statements, select Yes if the statement is true. Otherwise, select No.
NOTE: Each correct selection is worth one point.

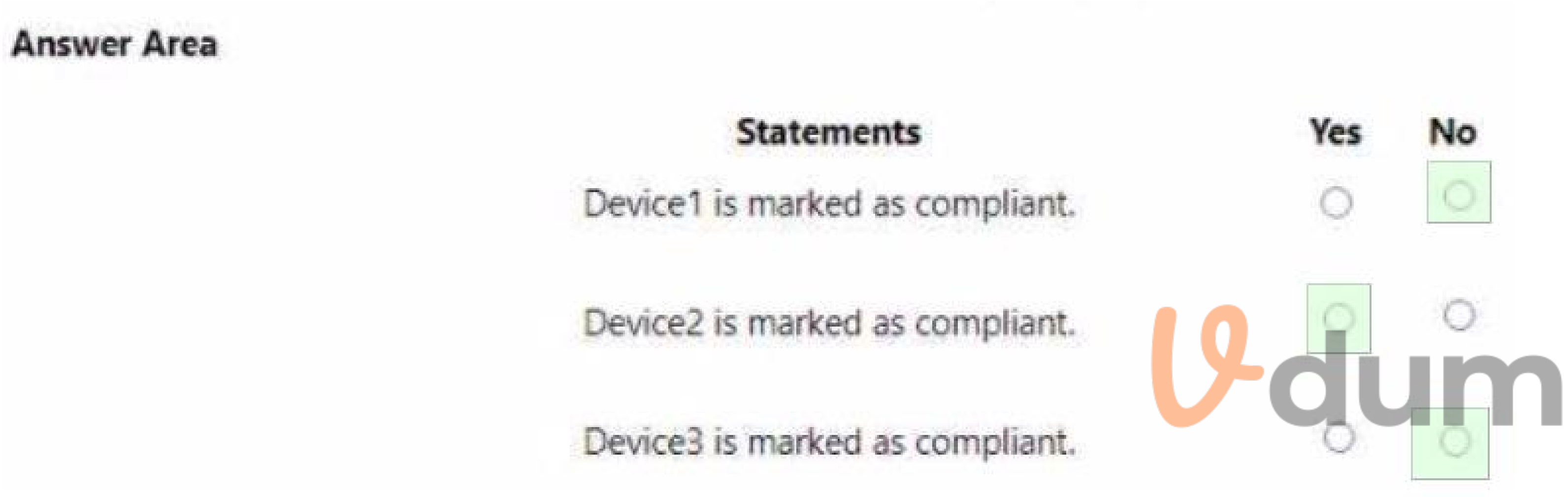
Hot Area:



Answer Area

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

Answer Area:



Answer Area

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

Section:
Explanation:

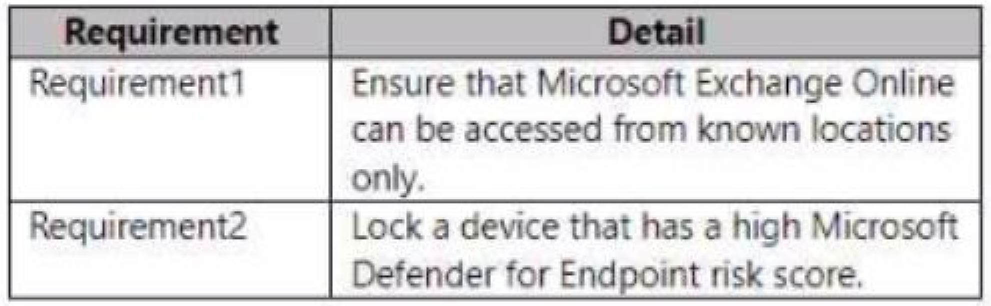
QUESTION 112
You need to implement mobile device management (MDM) for personal devices that run Windows 11. The solution must meet the following requirements:
* Ensure that you can manage the personal devices by using Microsoft Intune.
* Ensure that users can access company data seamlessly from their 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

Correct Answer: A
Section:
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.

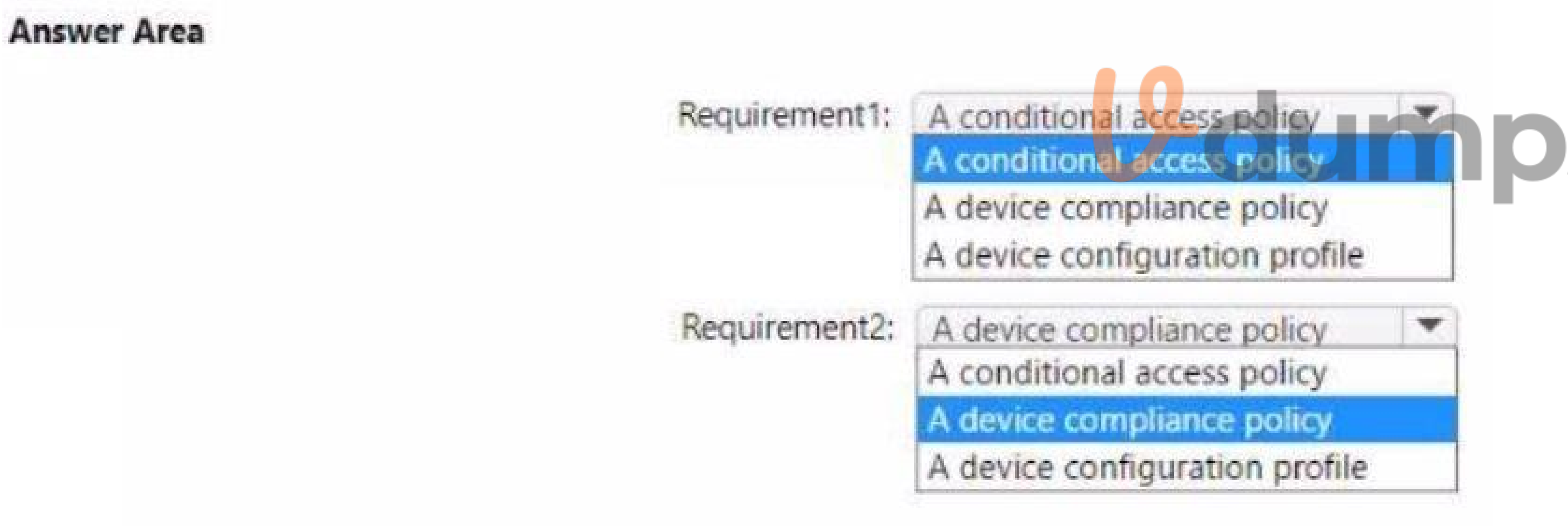
QUESTION 113
HOTSPOT
You have a Microsoft 365 subscription.
All computers are enrolled in Microsoft Intune.
You have business requirements for securing your Windows 11 environment as shown in the following table.



Requirement	Detail
Requirement1	Ensure that Microsoft Exchange Online can be accessed from known locations only.
Requirement2	Lock a device that has a high Microsoft Defender for Endpoint risk score.

What should you implement to meet each requirement? To answer, select the appropriate options in the answer are a. NOTE: Each correct selection is worth one point.

Hot Area:

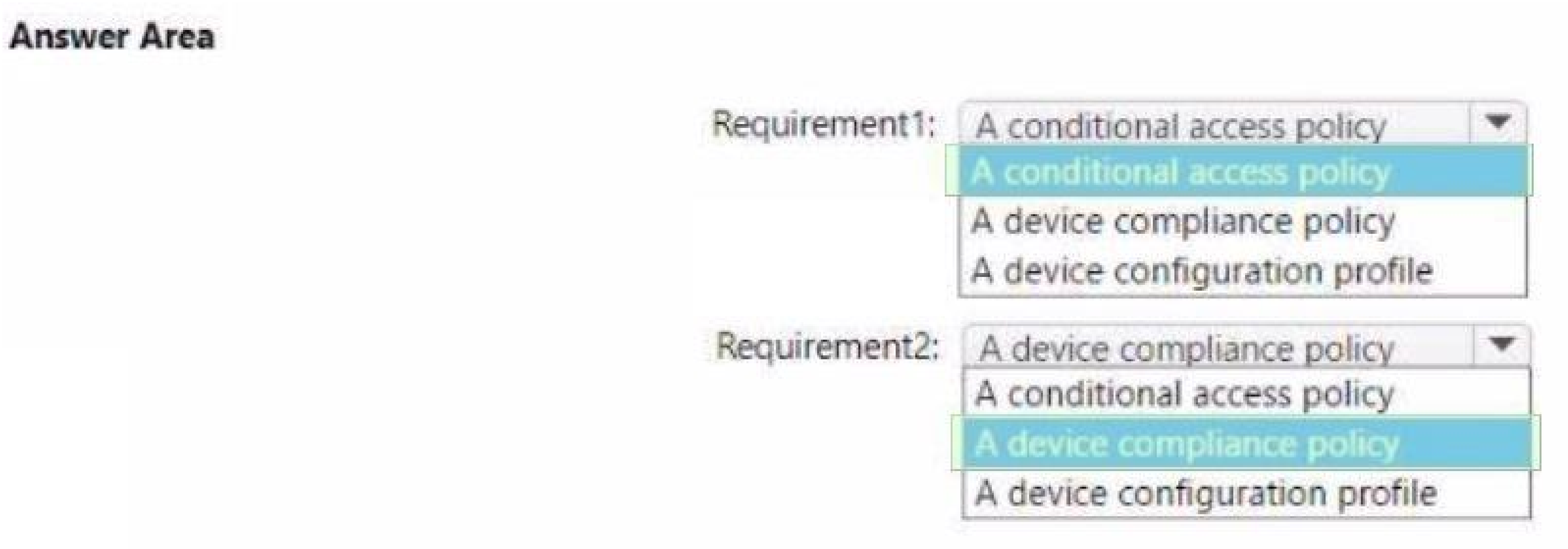


Answer Area

Requirement1: A conditional access policy
- A conditional access policy
- A device compliance policy
- A device configuration profile

Requirement2: A device compliance policy
- A conditional access policy
- A device compliance policy
- A device configuration profile

Answer Area:



Answer Area

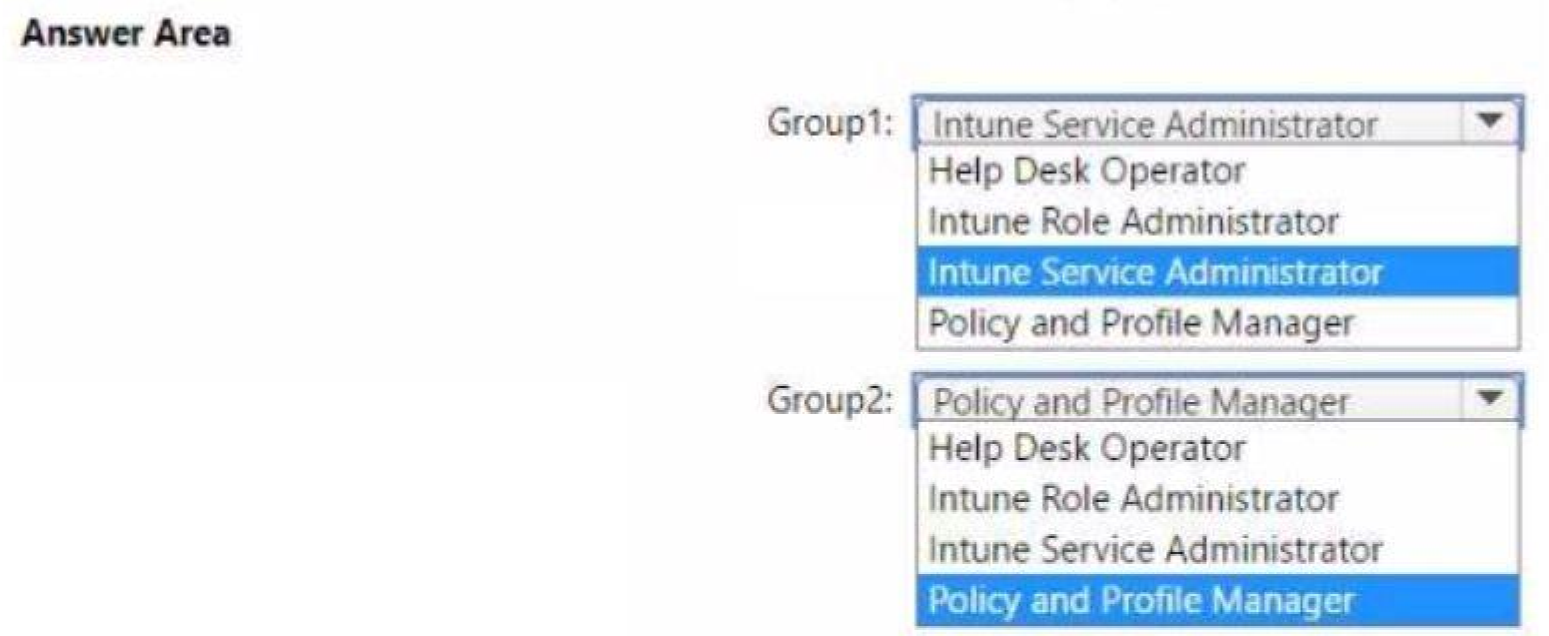
Requirement1: A conditional access policy ▼
- [✓ A conditional access policy]
- A device compliance policy
- A device configuration profile

Requirement2: A device compliance policy ▼
- A conditional access policy
- [✓ A device compliance policy]
- A device configuration profile

Section:
Explanation:

QUESTION 114
HOTSPOT
You have a Microsoft 365 subscription that contains two security groups named Group1 and Group2. Microsoft 365 uses Microsoft Intune Suite.
You use Microsoft Intune to manage devices.
You need to assign roles in Intune to meet the following requirements:
* The members of Group1 must manage Intune roles and assignments.
* The members of Group2 must assign existing apps and policies to users and devices.
The solution must follow the principle of least privilege.
Which role should you assign to each group? To answer, select the appropriate options in the answer area.
NOTE: Each correct selection is worth one point.

Hot Area:

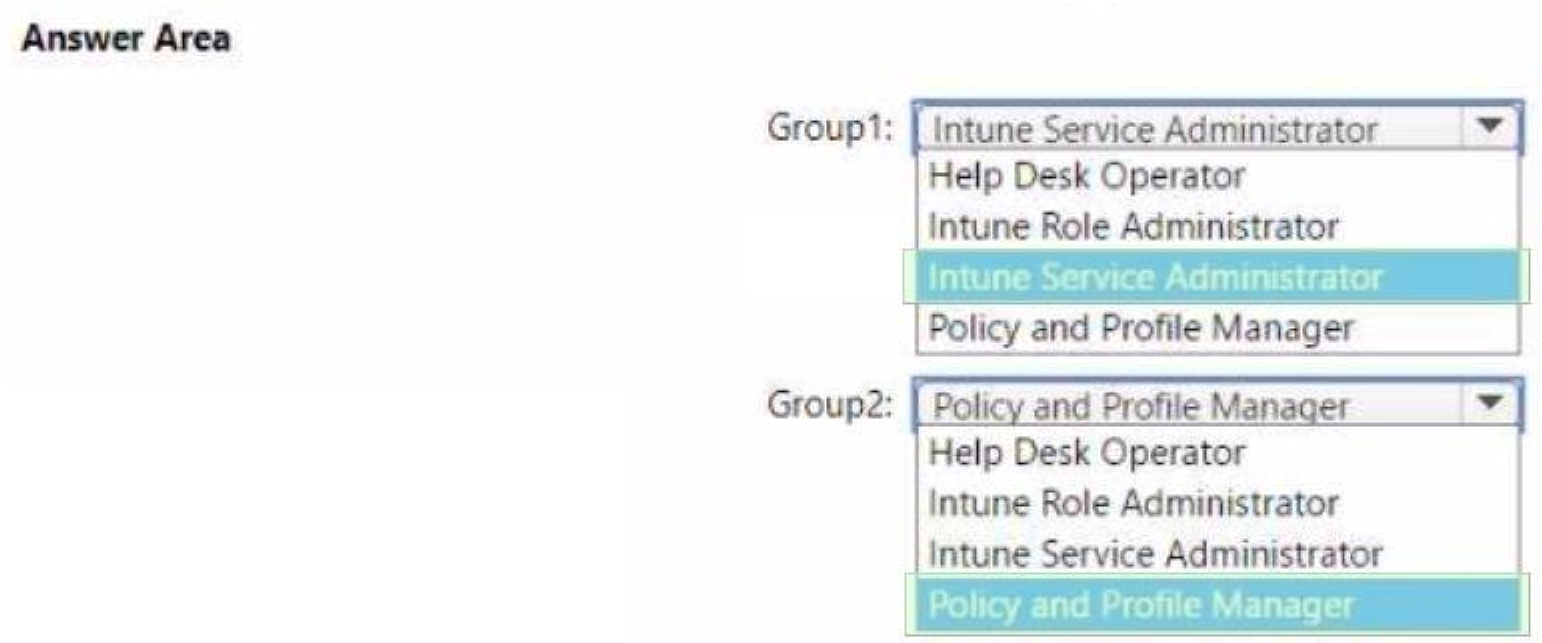


Answer Area

Group1: Intune Service Administrator ▼
- Help Desk Operator
- Intune Role Administrator
- [✓ Intune Service Administrator]
- Policy and Profile Manager

Group2: Policy and Profile Manager ▼
- Help Desk Operator
- Intune Role Administrator
- Intune Service Administrator
- [✓ Policy and Profile Manager]

Answer Area:



Answer Area

Group1: Intune Service Administrator

- Help Desk Operator
- Intune Role Administrator
- Intune Service Administrator
- Policy and Profile Manager

Group2: Policy and Profile Manager

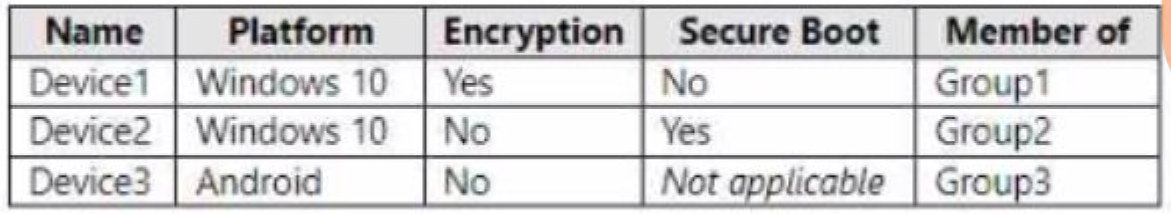
- Help Desk Operator
- Intune Role Administrator
- Intune Service Administrator
- Policy and Profile Manager

Section:
Explanation:

QUESTION 115

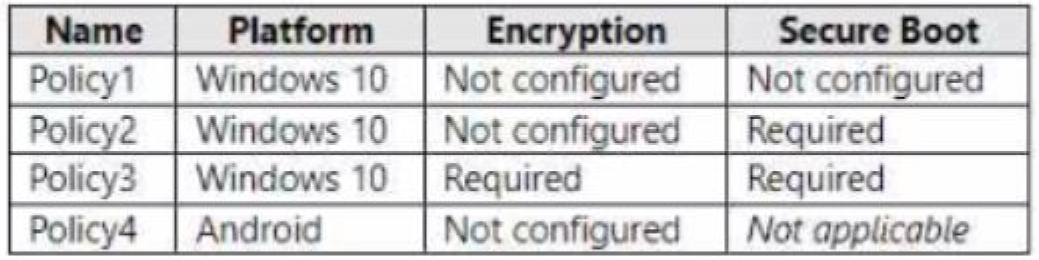
HOTSPOT

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



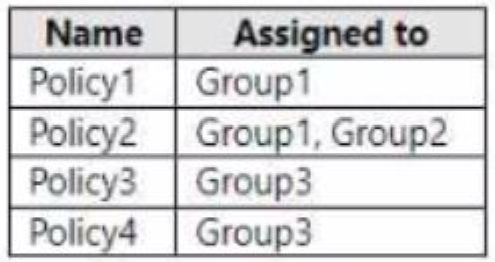
Name	Platform	Encryption	Secure Boot	Member of
Device1	Windows 10	Yes	No	Group1
Device2	Windows 10	No	Yes	Group2
Device3	Android	No	*Not applicable*	Group3

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*

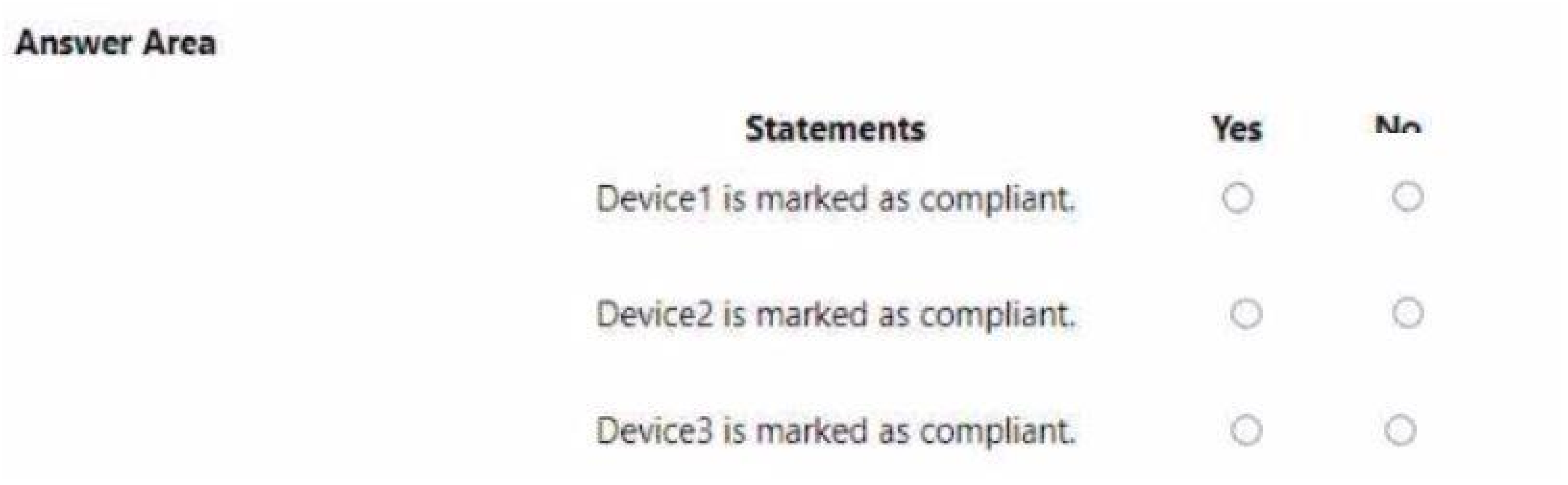
The device compliance policies have the assignments shown in the following table.



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.

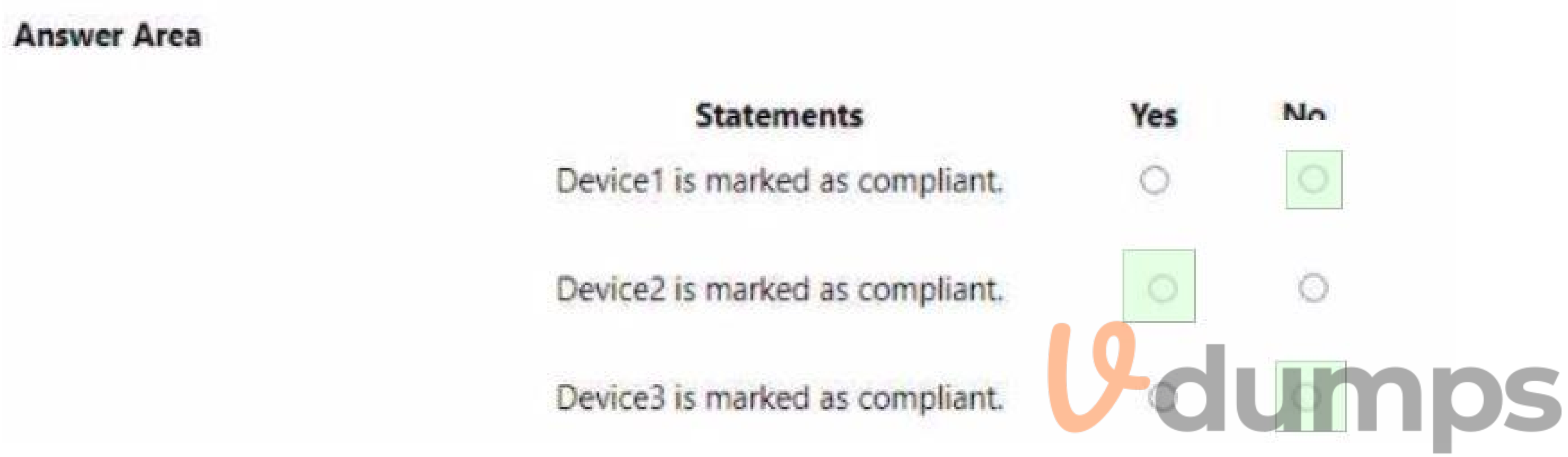
Hot Area:



Answer Area

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

Answer Area:



Answer Area

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

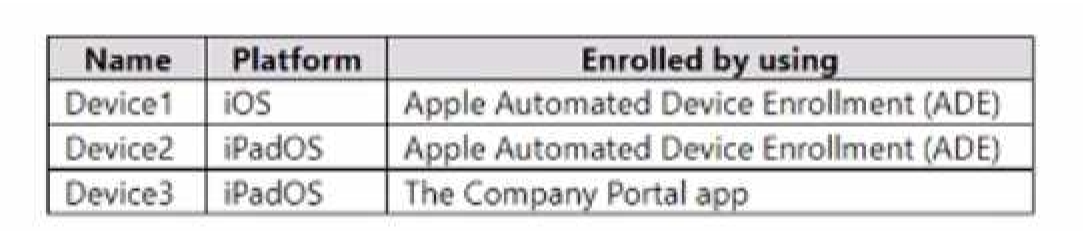
Section:
Explanation:

QUESTION 116
You have a Microsoft 365 subscription that uses Microsoft Intune Suite.
You use Microsoft Intune to manage devices.
You need to ensure that the startup performance of managed Windows 11 devices is captured and available for review in the Intune admin center.
What should you configure?

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

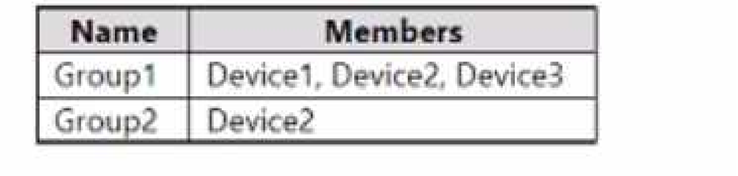
Correct Answer: D
Section:

QUESTION 117
HOTSPOT
You have a Microsoft 365 ES subscription that uses Microsoft Intune.
Devices are enrolled in Intune as shown in the following table.



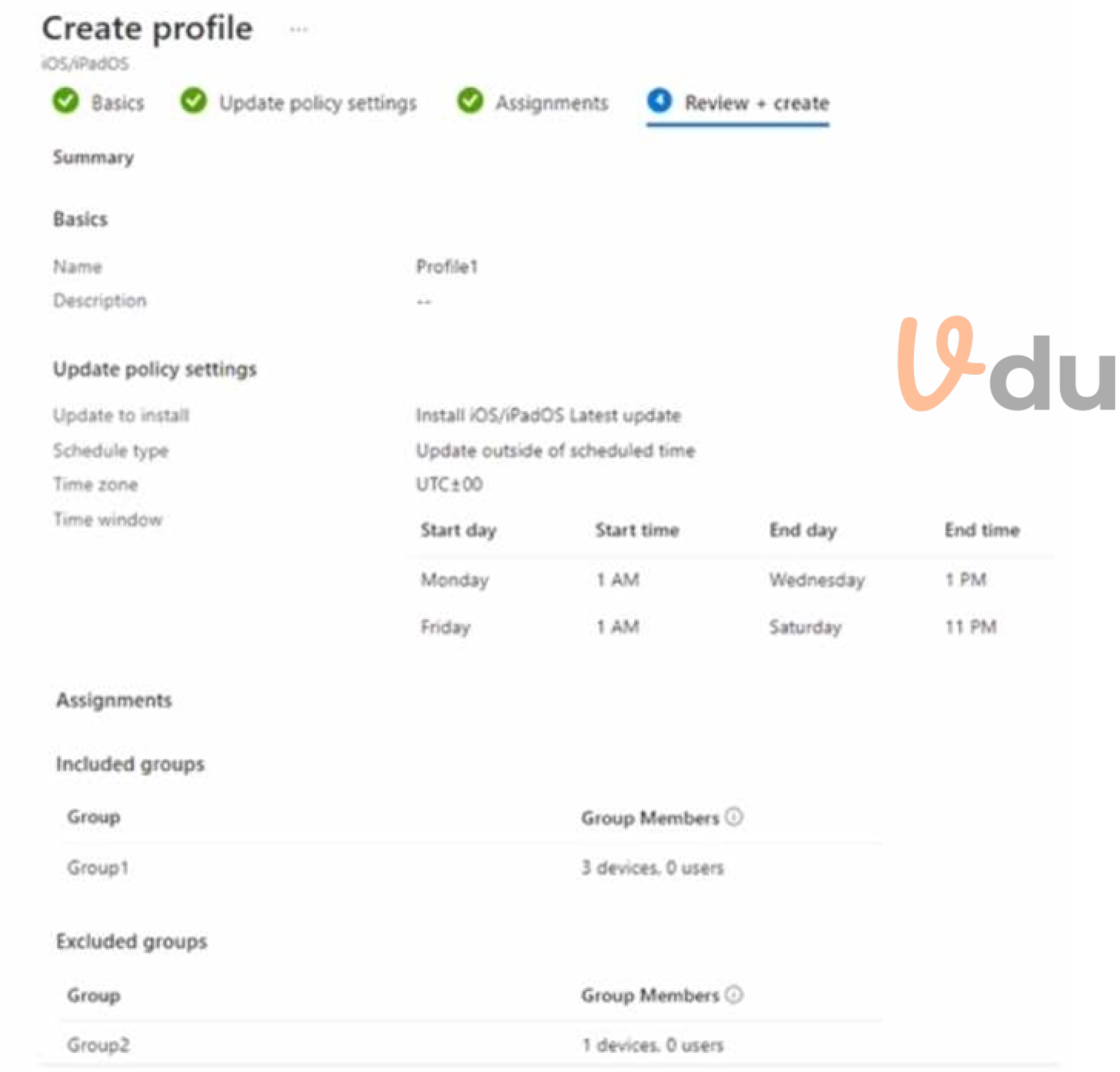
Name	Platform	Enrolled by using
Device1	iOS	Apple Automated Device Enrollment (ADE)
Device2	iPadOS	Apple Automated Device Enrollment (ADE)
Device3	iPadOS	The Company Portal app

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



Name	Members
Group1	Device1, Device2, Device3
Group2	Device2

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



Create profile

iOS/iPadOS

Summary

Basics

Name	Profile1
Description	--

Update policy settings

Update to install	Install iOS/iPadOS Latest update
Schedule type	Update outside of scheduled time
Time zone	UTC±00
Time window	

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

Assignments

Included groups

Group	Group Members
Group1	3 devices, 0 users

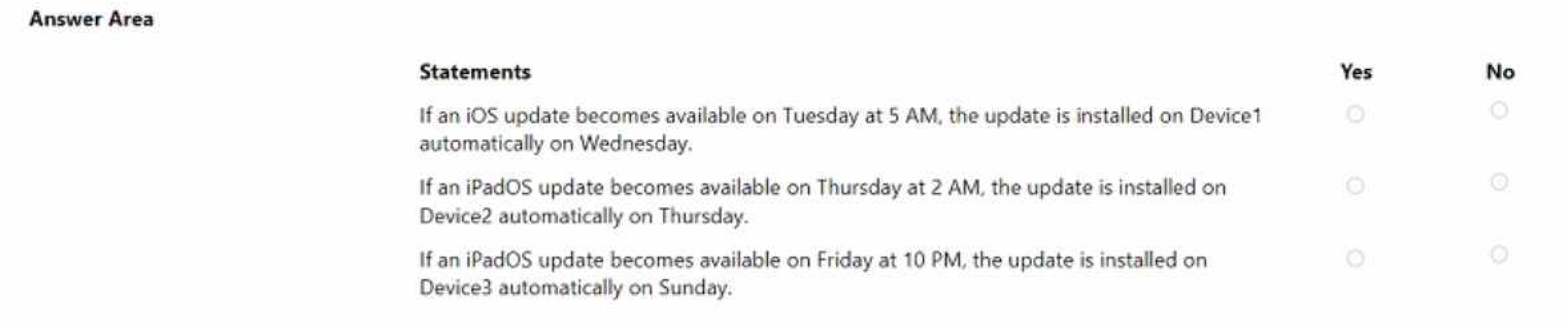
Excluded groups

Group	Group Members
Group2	1 devices, 0 users

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

NOTE: Each correct selection is worth one point.

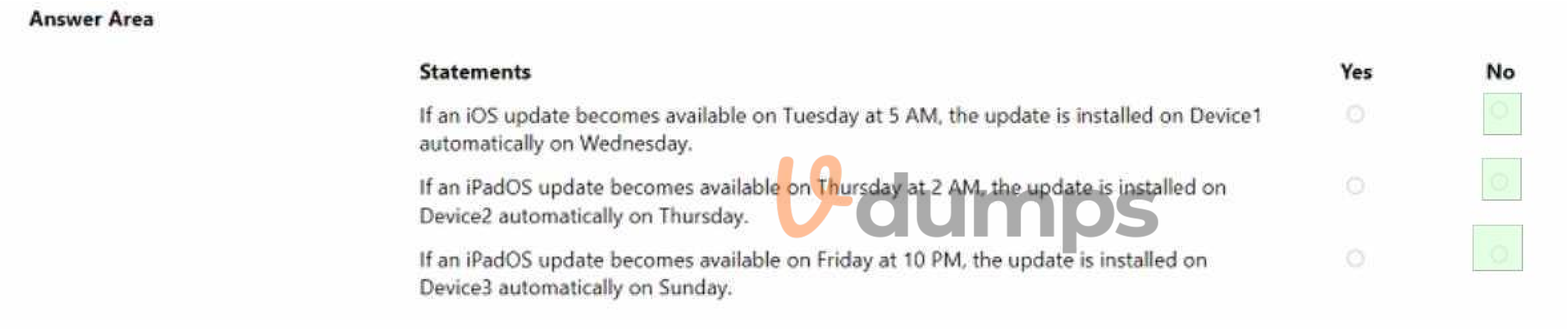
Hot Area:



Answer Area

Statements	Yes	No
If an iOS update becomes available on Tuesday at 5 AM, the update is installed on Device1 automatically on Wednesday.	○	○
If an iPadOS update becomes available on Thursday at 2 AM, the update is installed on Device2 automatically on Thursday.	○	○
If an iPadOS update becomes available on Friday at 10 PM, the update is installed on Device3 automatically on Sunday.	○	○

Answer Area:

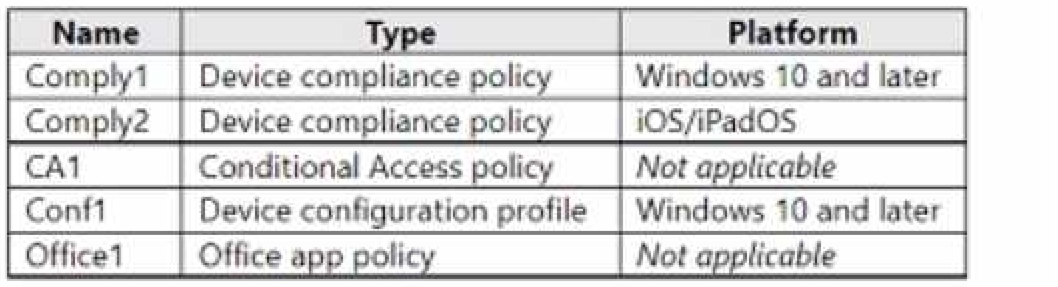


Answer Area

Statements	Yes	No
If an iOS update becomes available on Tuesday at 5 AM, the update is installed on Device1 automatically on Wednesday.	○	[✓ ○]
If an iPadOS update becomes available on Thursday at 2 AM, the update is installed on Device2 automatically on Thursday.	○	[✓ ○]
If an iPadOS update becomes available on Friday at 10 PM, the update is installed on Device3 automatically on Sunday.	○	[✓ ○]

Section:
Explanation:

QUESTION 118
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

Correct Answer: B
Section:

QUESTION 119

You use Microsoft Defender for Endpoint to protect computers that run Windows 10.
You need to assess the differences between the configuration of Microsoft Defender for Endpoint and the Microsoft-recommended configuration baseline.
Which tool should you use?

A. Microsoft Defender for Endpoint Power 81 app

B. Microsoft Secure Score

C. Endpoint Analytics

D. Microsoft 365 Defender portal

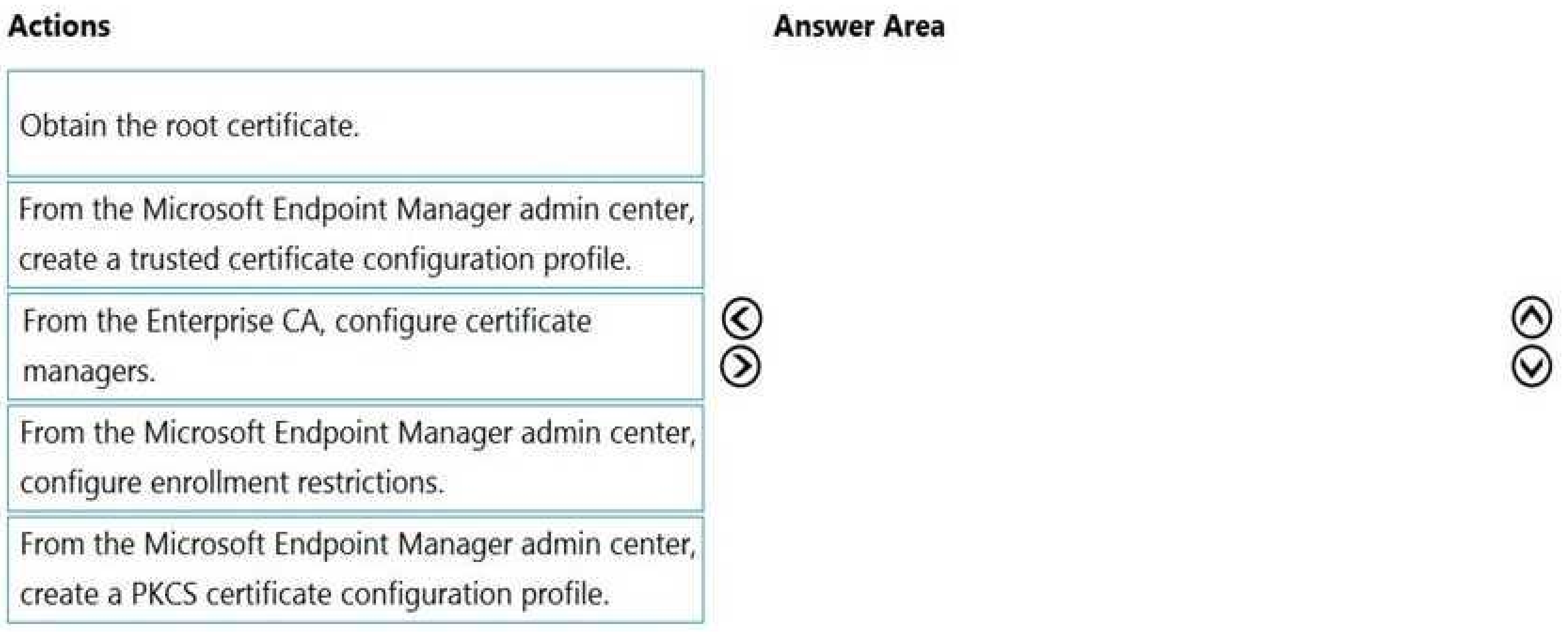
Correct Answer: B
Section:

QUESTION 120

DRAG DROP

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.

Select and Place:



Actions

Answer Area

Obtain the root certificate.

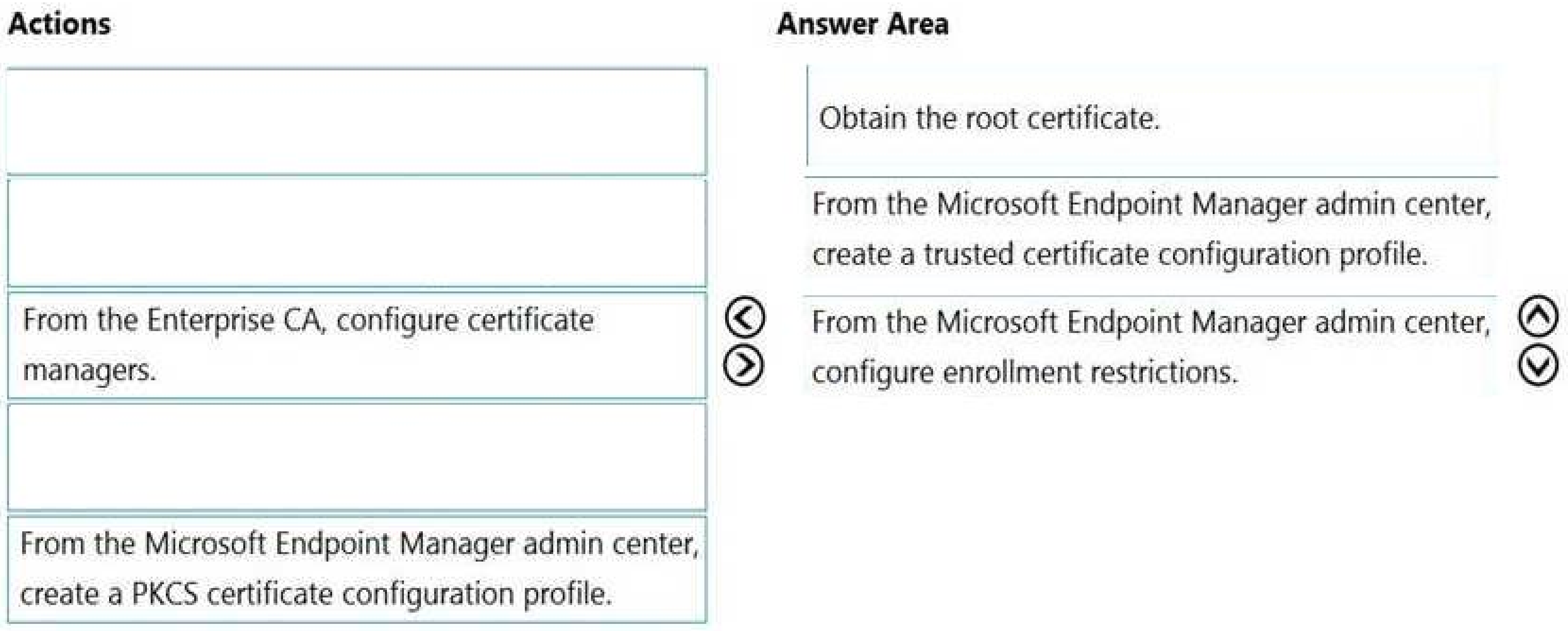
From the Microsoft Endpoint Manager admin center, create a trusted certificate configuration profile.

From the Enterprise CA, configure certificate managers.

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

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

Correct Answer:



Actions

From the Enterprise CA, configure certificate managers.

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

Answer Area

Obtain the root certificate.

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

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

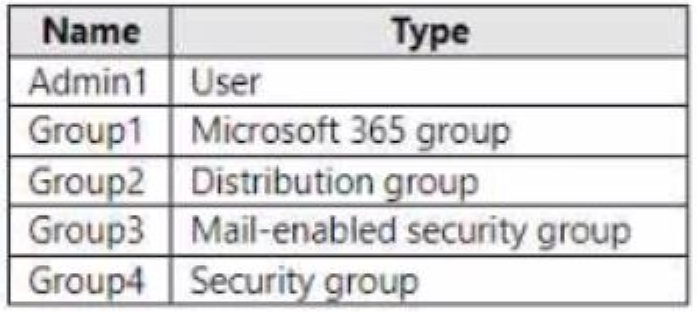
Section:
Explanation:
Reference:
https://docs.microsoft.com/en-us/mem/intune/protect/certificates-pfx-configure

QUESTION 121
You have a Microsoft 365 subscription that contains 1,000 iOS devices and includes Microsoft Intune. You need to prevent the printing of corporate data from managed apps on the devices, should you configure?

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

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

QUESTION 122
You have a Microsoft 365 tenant that contains the objects shown in the following table.



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

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

A. Group3 and Group4 only
B. Admin1, Group3, and Group4 only
C. Group1, Group3, and Group4 only
D. Group1, Group2, Group3, and Group4 only
E. Admin1, Group1. Group2, Group3, andGroup4

Correct Answer: C
Section:
Explanation:
In the Microsoft Intune admin center, you can assign apps to users or devices. Users can be assigned to apps by using user groups or individual user accounts. Devices can be assigned to apps by using device groups. In this scenario, the objects shown in the table are as follows:
Admin1 is an individual user account that belongs to theGlobal administratorsrole group.
Group1 is a user group that contains 100 users.
Group2 is a device group that contains 50 devices.
Group3 is a user group that contains 200 users.
Group4 is a device group that contains 150 devices.
Since App1 is a Microsoft 365 Apps app, it can only be assigned to users, not devices. Therefore, Group2 and Group4 are not valid objects for app assignment. Admin1 is also not a valid object for app assignment, because individual user accounts can only be used for testing purposes, not for production deployment. Therefore, the only valid objects for app assignment are Group1 and Group3, which are user groups.

QUESTION 123
You plan to deploy Windows 11 Pro to 200 new computers by using the Microsoft Deployment Toolkit (MDT) and Windows Deployment Services (WDS).
The company has a Volume Licensing Agreement and uses a product key to activate Windows 11.
You need to ensure that the new computers will be configured to have the correct product key during the installation.
What should you configure?

A. an MDT task sequence
B. the Device settings in Azure AD
C. a WDS boot image
D. a Windows Autopilot deployment profile

Correct Answer: A
Section:
Explanation:
https://learn.microsoft.com/en-us/answers/questions/856939/how-to-place-windows-product-key-in-the-rules-on-t#:~:text=You%20may%20set%20the%20Product%20Key%20per%20Task%20Sequence%20in%20customsettings.ini

QUESTION 124
You have a Microsoft 365 subscription that includes Microsoft Intune. The subscription contains corporate-owned, fully managed Android Enterprise devices.
You plan to deploy a configuration profile that will have a device restrictions profile type named Profile1. Profile1 will assign maintenance windows for system updates.
What should you configure from the Configuration settings for Profile1?

A. Device experience
B. General

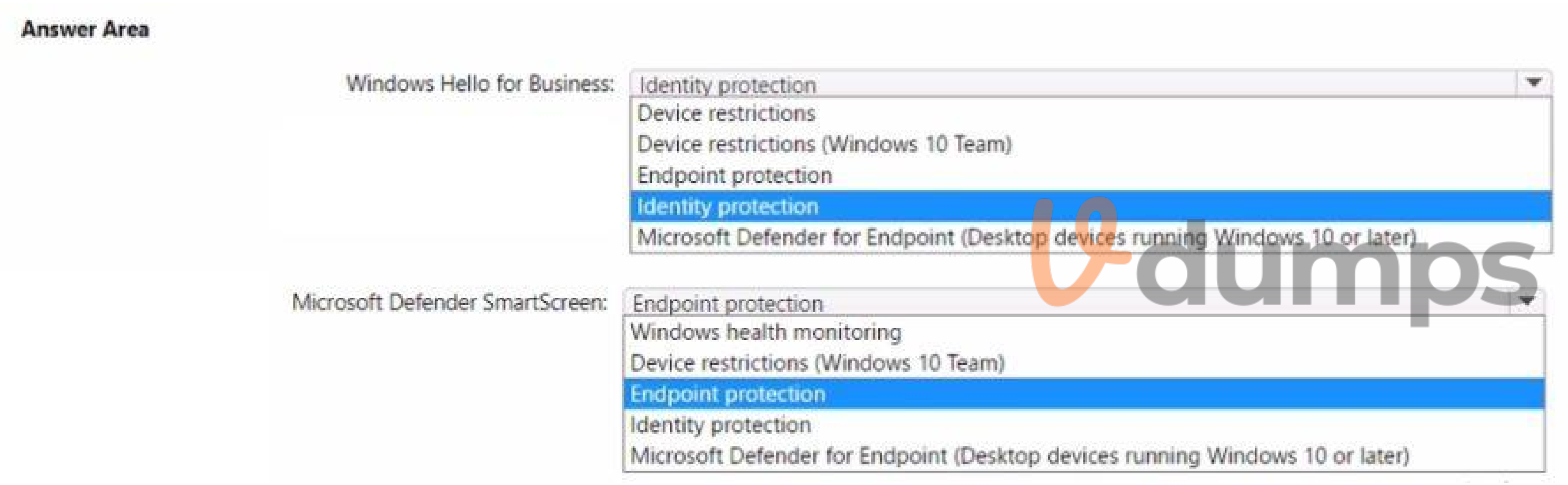
C. Connectivity

D. Power Settings Explanation

Correct Answer: A
Section:

QUESTION 125
HOTSPOT
You have a Microsoft 365 subscription.
You have 25 Microsoft Surface Hub devices that you plan to manage by using Microsoft Intune.
You need to configure the devices to meet the following requirements:
* Enable Windows Hello for Business.
* Configure Microsoft Defender SmartScreen to block users from running unverified files.
Which profile type template should you use for each requirement? To answer, select the appropriate options in the answer are a. NOTE: Each correct selection is worth one point.

Hot Area:



Answer Area

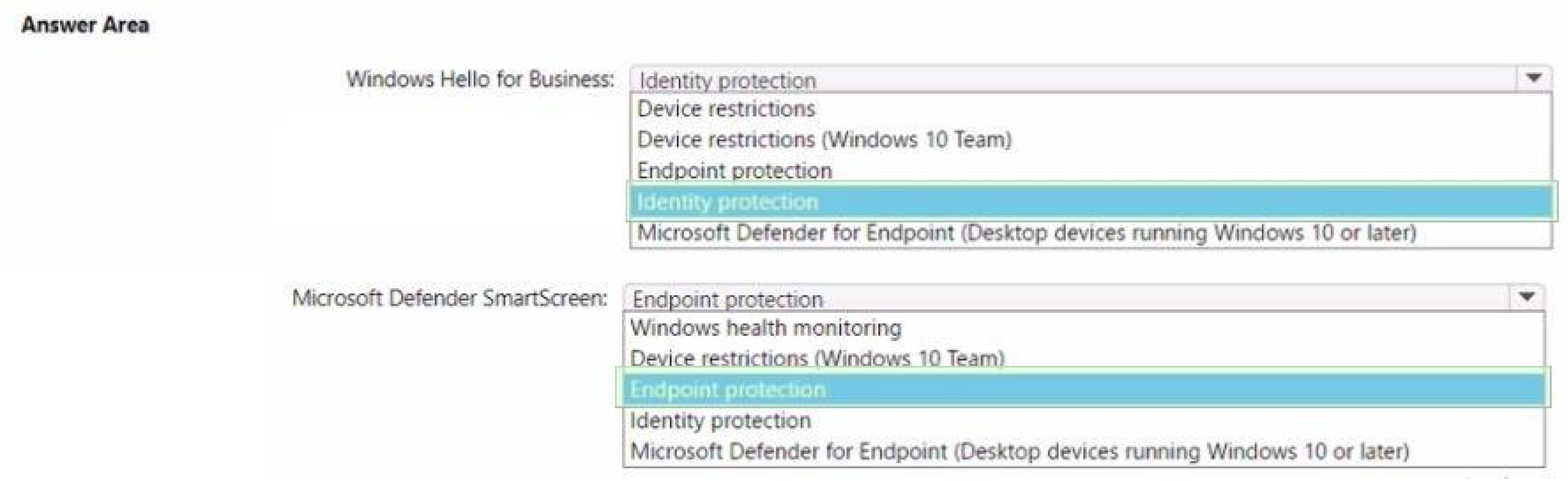
Windows Hello for Business: Identity protection

- Device restrictions
- Device restrictions (Windows 10 Team)
- Endpoint protection
- Identity protection
- Microsoft Defender for Endpoint (Desktop devices running Windows 10 or later)

Microsoft Defender SmartScreen: Endpoint protection

- Windows health monitoring
- Device restrictions (Windows 10 Team)
- Endpoint protection
- Identity protection
- Microsoft Defender for Endpoint (Desktop devices running Windows 10 or later)

Answer Area:



Answer Area

Windows Hello for Business: Identity protection

- Device restrictions
- Device restrictions (Windows 10 Team)
- Endpoint protection
- Identity protection
- Microsoft Defender for Endpoint (Desktop devices running Windows 10 or later)

Microsoft Defender SmartScreen: Endpoint protection

- Windows health monitoring
- Device restrictions (Windows 10 Team)
- Endpoint protection
- Identity protection
- Microsoft Defender for Endpoint (Desktop devices running Windows 10 or later)

Section:

Explanation:

QUESTION 126

HOTSPOT

You have a Microsoft 365 E5 subscription.

You use Microsoft Intune to manage Windows 365 Cloud PC devices.

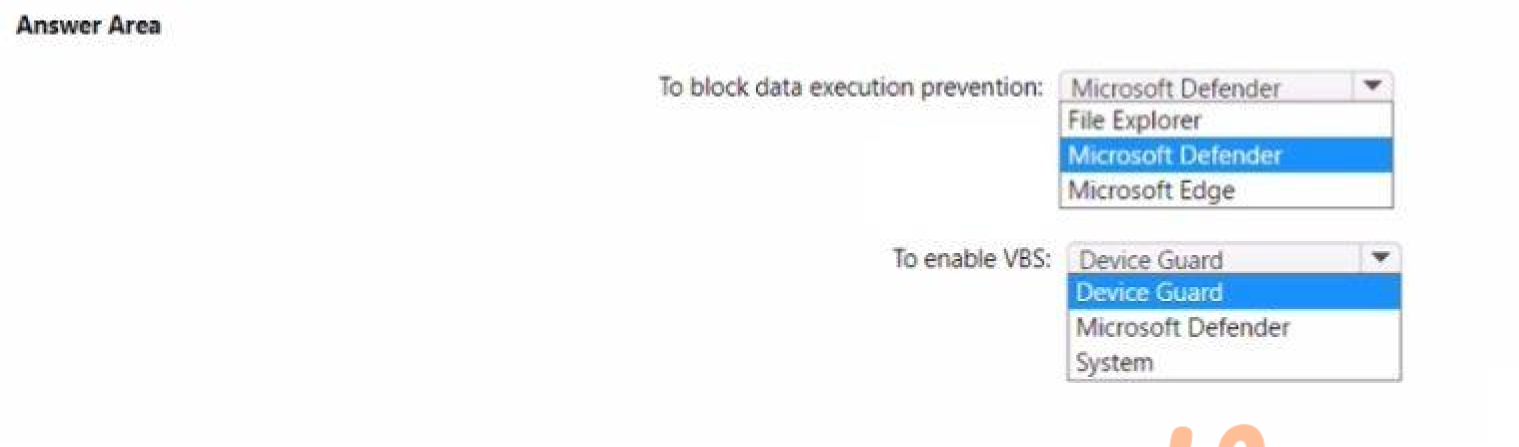
You need to deploy a Windows 365 Security Baseline to the Cloud PC devices. The solution must meet the following requirements:

* Block data execution prevention.

* Enable virtualization-based security (V8S) and Secure Boot.

What should you configure for the Windows 365 Security Baseline profile? To answer, select the appropriate options in the answer area.

Hot Area:

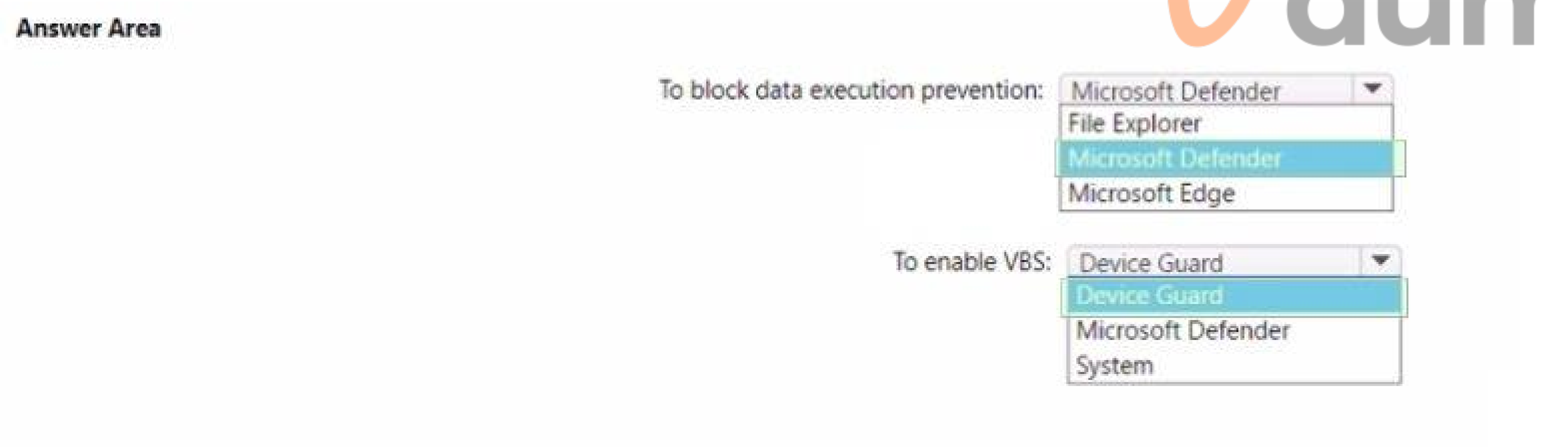


Answer Area

To block data execution prevention: Microsoft Defender
- File Explorer
- Microsoft Defender
- Microsoft Edge

To enable VBS: Device Guard
- Device Guard
- Microsoft Defender
- System

Answer Area:



Answer Area

To block data execution prevention: Microsoft Defender
- File Explorer
- Microsoft Defender
- Microsoft Edge

To enable VBS: Device Guard
- Device Guard
- Microsoft Defender
- System

Section:

Explanation:

QUESTION 127

RAG DROP

You have a Microsoft 365 subscription that uses Microsoft Intune.

You plan to use Windows Autopilot to provision 25 Windows 11 devices.

You need to meet the following requirements during device provisioning:

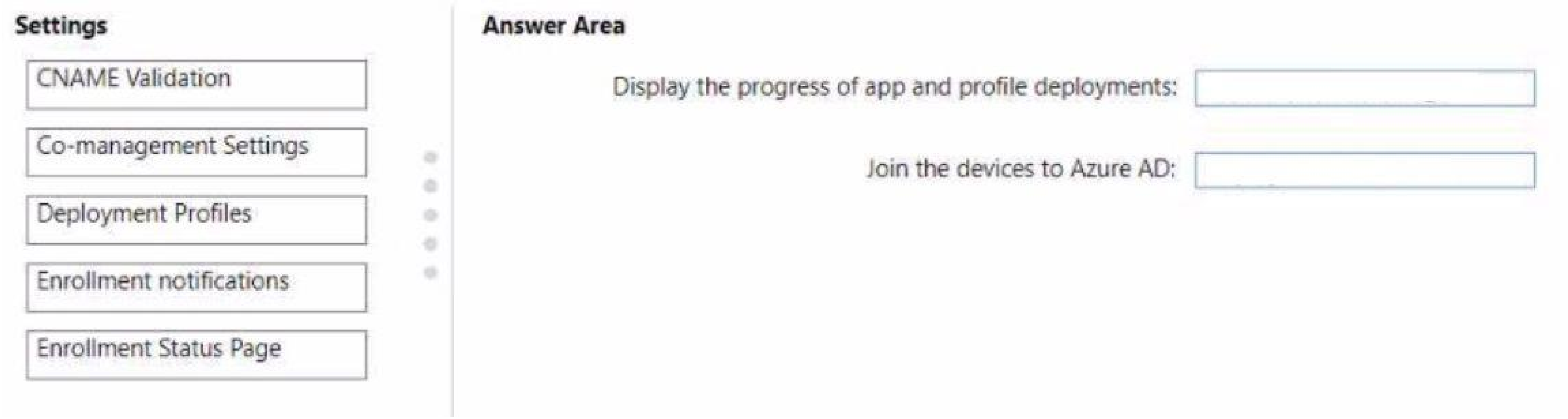
* Display the progress of app and profile deployments.

* Join the devices to Azure AD.

What should you configure to meet each requirement? To answer drag the appropriate settings to the correct requirements. Each setting may be used once, more than once, or not at all. You may need to drag the split bar between panes or scroll to view content.

NOTE: Each correct selection is worth one point.

Select and Place:



Settings

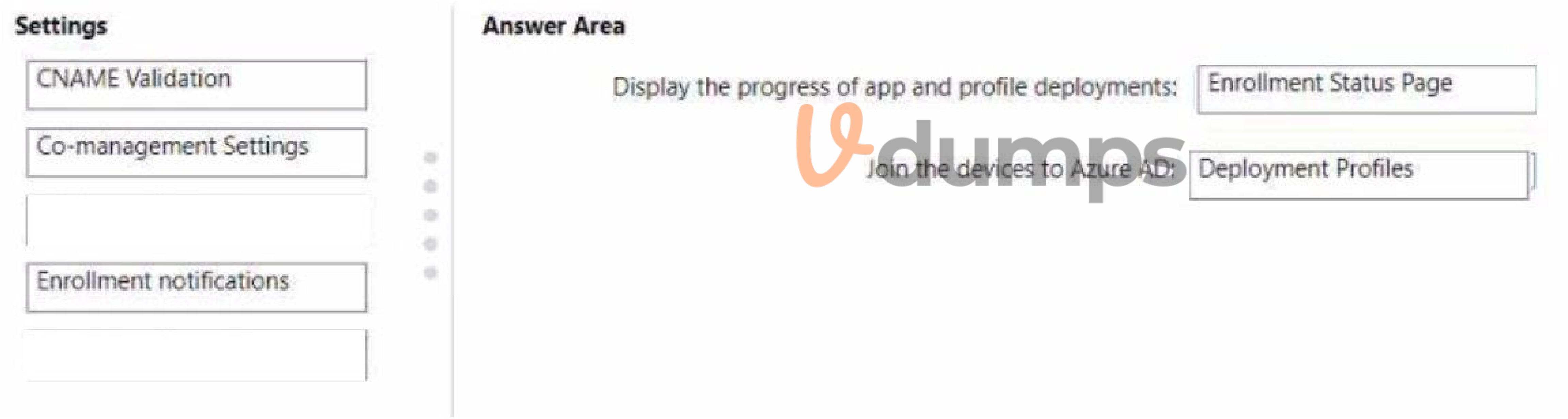
- CNAME Validation
- Co-management Settings
- Deployment Profiles
- Enrollment notifications
- Enrollment Status Page

Answer Area

Display the progress of app and profile deployments:

Join the devices to Azure AD:

Correct Answer:



Settings

- CNAME Validation
- Co-management Settings
- Enrollment notifications

Answer Area

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

Join the devices to Azure AD: Deployment Profiles

Section:
Explanation: