MD-102 Q&As

Endpoint Administrator

Pass Microsoft MD-102 Exam with 100% Guarantee

Free Download Real Questions & Answers **PDF** and **VCE** file from:

https://www.pass4itsure.com/md-102.html

100% Passing Guarantee
100% Money Back Assurance

Following Questions and Answers are all new published by Microsoft Official Exam Center

QUESTION 1

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.	○	○

Correct Answer:

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

QUESTION 2

You have two computers named Computer1 and Computer2 that run Windows 10. Computer2 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 Computer2, configure the Remote Desktop settings.

B. From Windows Defender Firewall on Computer1, allow Remote Desktop.

C. From Windows Defender Firewall on Computer2, allow File and Printer Sharing.

D. From Computer1, configure the Remote Desktop Connection settings.

Correct Answer: D

How to gain access to local files:

You can gain access to your disk drives on the local computer during a Remote Desktop session. You can redirect the local disk drives, including the hard disk drives, CD-ROM disk drives, floppy disk drives, and mapped network disk drives

so that you can transfer files between the local host and the remote computer in the same way that you copy files from a network share. You can use Microsoft Windows Explorer to view the disk drives and files for each redirected disk drive.

Alternatively, you can view the files for each redirected disk drive in My Computer. The drives are displayed as "drive_letter on terminal_server_client_name" in both Windows Explorer and My Computer.

To view the disk drives and files for the redirected disk drive:

1.Click Start, point to All Programs (or Programs), point to

Accessories, point to Communications, and then click Remote Desktop Connection.

2.Click Options, and then click the

Local Resources tab.

3.Click Disk Drives, and then click

Connect.

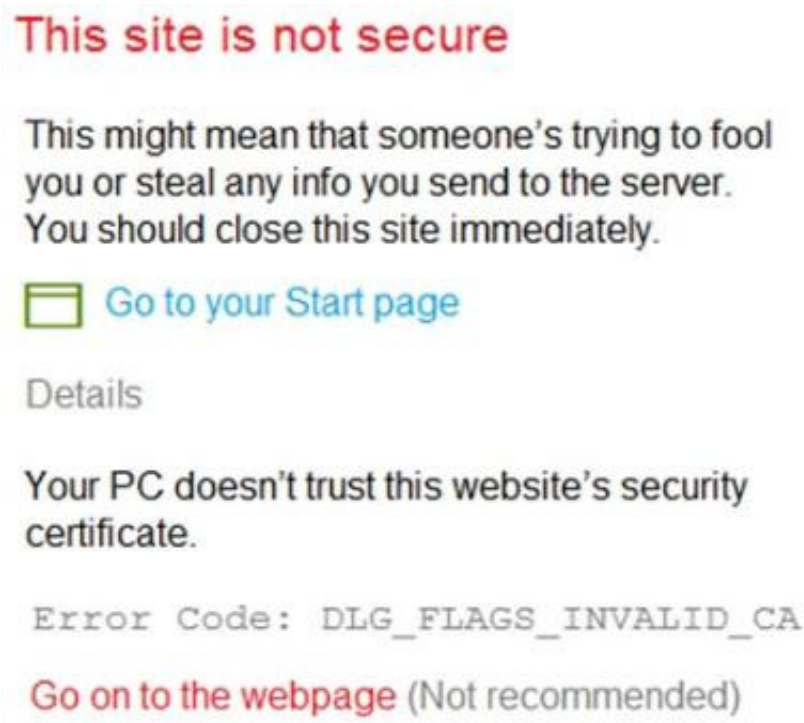
Reference:

https://support.microsoft.com/en-us/topic/how-to-gain-access-to-local-files-in-a-remote-desktop-session-to-a-windows-xp-based-or-to-a-windows-server-2003-based-host-computer-021ee183-e6be-4201-809e-c355c47b17f4

QUESTION 3

You use Windows Admin Center to remotely administer computers that run Windows 10.

When connecting to Windows Admin Center, you receive the message shown in the following exhibit.



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

A. Client Authentication Issuers

B. Personal

C. Trusted Root Certification Authorities

Correct Answer: C

"Error Code: DLG_FLAGS_INVALID_CA" while login to Admin Console after enabling HTTPS in PowerCenter.

Solution

To resolve this issue, add the CA-signed certificates to the "Trusted Root Certification Authorities" in the browser. After adding the certificates, restart the browser.

Reference:

https://knowledge.informatica.com/s/article/578585

QUESTION 4

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:

1.

Requires BitLocker Drive Encryption (BitLocker) on each device

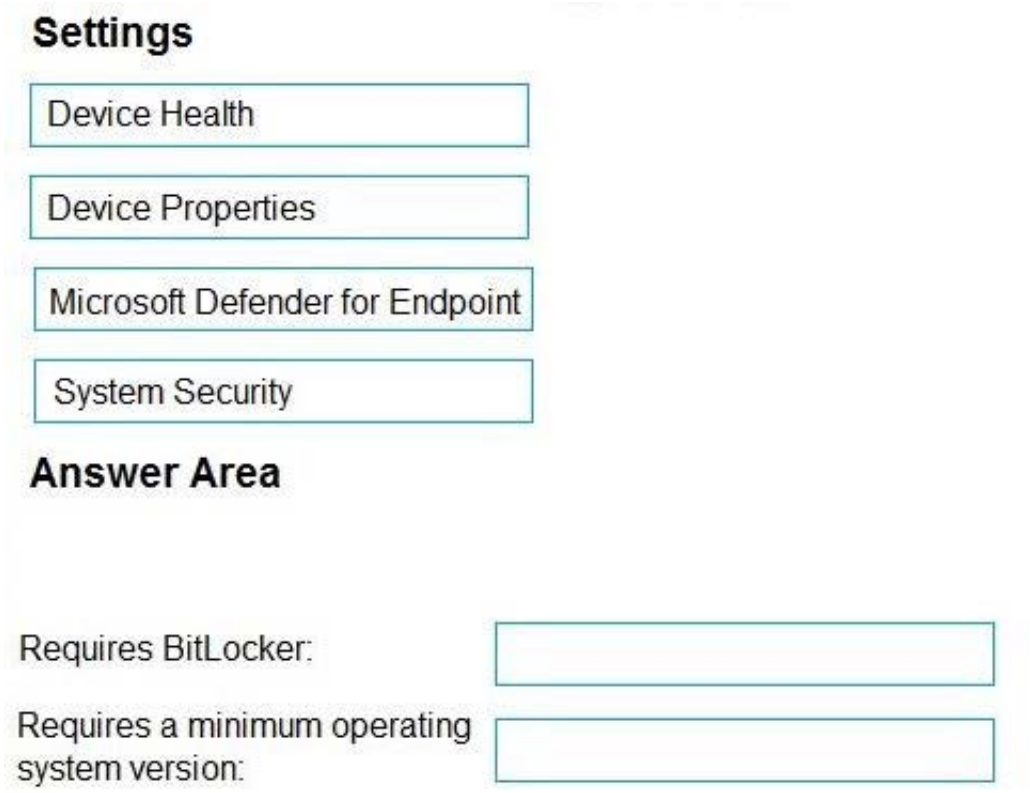
2.

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:



Correct Answer:

Device Compliance settings for Windows 10/11 in Intune

As part of your mobile device management (MDM) solution, use these settings to require BitLocker, set a minimum and maximum operating system, set a risk level using Microsoft Defender for Endpoint, and more.

Box 1: Device Health

Device Health

Windows Health Attestation Service evaluation rules

Require BitLocker:

Windows BitLocker Drive Encryption encrypts all data stored on the Windows operating system volume. BitLocker uses the Trusted Platform Module (TPM) to help protect the Windows operating system and user data. It also helps confirm

that a computer isn\\'t tampered with, even if its left unattended, lost, or stolen. If the computer is equipped with a compatible TPM, BitLocker uses the TPM to lock the encryption keys that protect the data. As a result, the keys can\\'t be

accessed until the TPM verifies the state of the computer.

Not configured (default) - This setting isn\\'t evaluated for compliance or non-compliance.

Require - The device can protect data that\\'s stored on the drive from unauthorized access when the system is off, or hibernates.

Box 2: Device Properties

Requires a minimum operating system version

Device Properties

Operating System Version

To discover build versions for all Windows 10/11 Feature Updates and Cumulative Updates (to be used in some of the fields below), see Windows release information. Be sure to include the appropriate version prefix before the build numbers,

like 10.0 for Windows 10 as the following examples illustrate.

Minimum OS version:

Enter the minimum allowed version in the major.minor.build.revision number format. To get the correct value, open a command prompt, and type ver.

Etc.

Reference:

https://learn.microsoft.com/en-us/mem/intune/protect/compliance-policy-create-windows

QUESTION 5

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:

Correct Answer:

QUESTION 6

HOTSPOT

You have 100 computers that run Windows 10. You have no servers. All the computers are joined to 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:

1.

The configuration must be managed from a central location.

2.

Internet traffic must be minimized.

3.

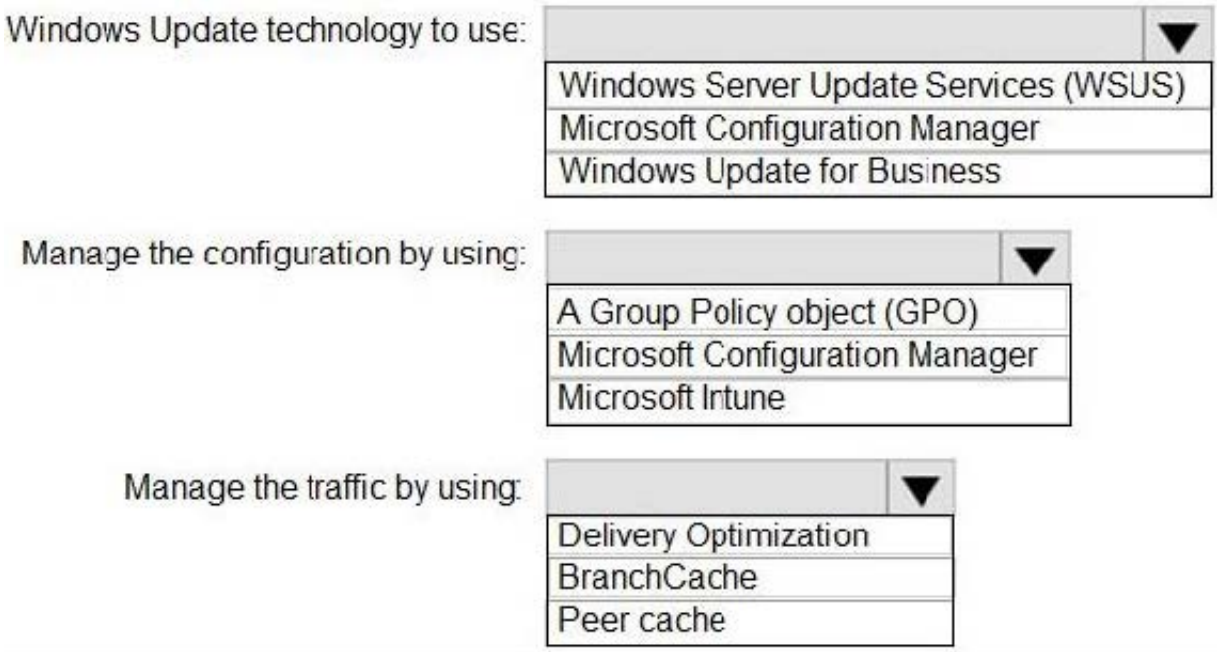
Costs must be minimized.

How should you configure Windows Update? To answer, select the appropriate options in the answer area.

NOTE: Each correct selection is worth one point.

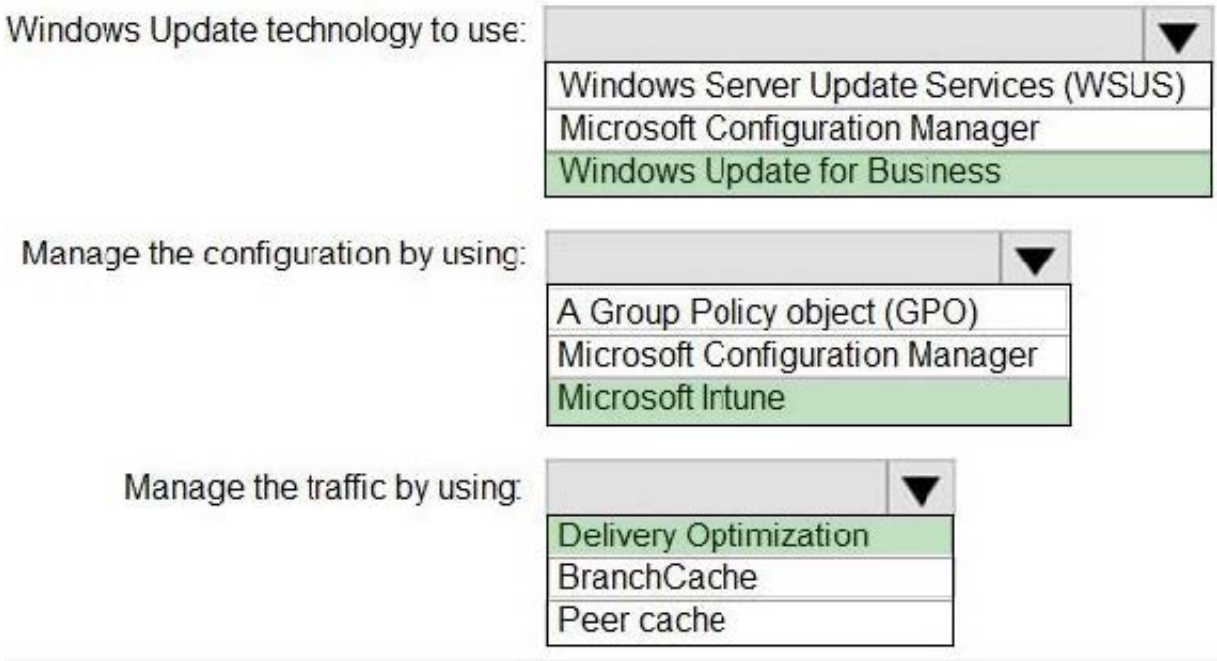
Hot Area:

Answer Area



Correct Answer:

Answer Area



QUESTION 7

You have an Azure AD group named Group1. Group1 contains two Windows 10 Enterprise devices named Device1 and Device2.

You create a device configuration profile named Profile1. You assign Profile1 to Group1.

You need to ensure that Profile1 applies to Device1 only.

What should you modify in Profile1?

A. Assignments

B. Settings

C. Scope (Tags)

D. Applicability Rules

Correct Answer: A

QUESTION 8

HOTSPOT

You have a Microsoft 365 subscription.

You use Microsoft Intune Suite to manage devices.

You have the iOS app protection policy shown in the following exhibit.

Access requirements

PIN for access	Require
PIN type	Numeric
Simple PIN	Allow
Select minimum PIN length	6
Touch ID instead of PIN for access (iOS8+/iPadOS)	Allow
Override biometrics with PIN after timeout	Require
Timeout (minutes of inactivity)	30
Face ID instead of PIN for access (iOS11+/iPadOS)	Block
PIN reset after number of days	No
Number of days	0
App PIN when device PIN is set	Require
Work or school account credentials for access	Require
Recheck the access requirements after /minutes of inactivity	30

Conditional launch

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

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

Hot Area:

Answer Area

After 30 minutes of inactivity, a user will be prompted for their
- account credentials only
- PIN only
- PIN and account credentials

Entering the wrong PIN five times will
- block access
- reset the app PIN
- reset the device PIN
- wipe company data

Correct Answer:

Answer Area

After 30 minutes of inactivity, a user will be prompted for their
- account credentials only
- PIN only
- PIN and account credentials

Entering the wrong PIN five times will
- block access
- reset the app PIN
- reset the device PIN
- wipe company data

QUESTION 9

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. Policy1 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: A

https://learn.microsoft.com/en-us/azure/active-directory/conditional-access/howto-conditional-access-insights-reporting

QUESTION 10

HOTSPOT

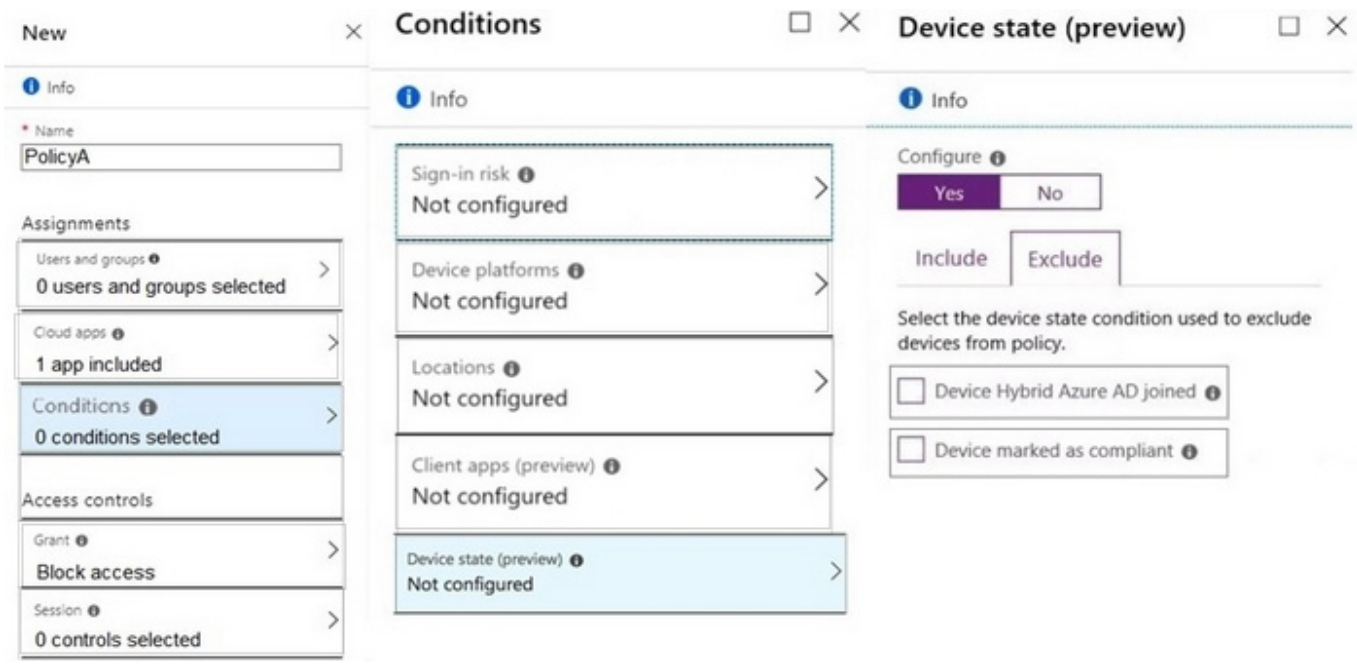
You need a new conditional access policy that has an assignment for Office 365 Exchange Online.

You need to configure the policy to meet the technical requirements for Group4.

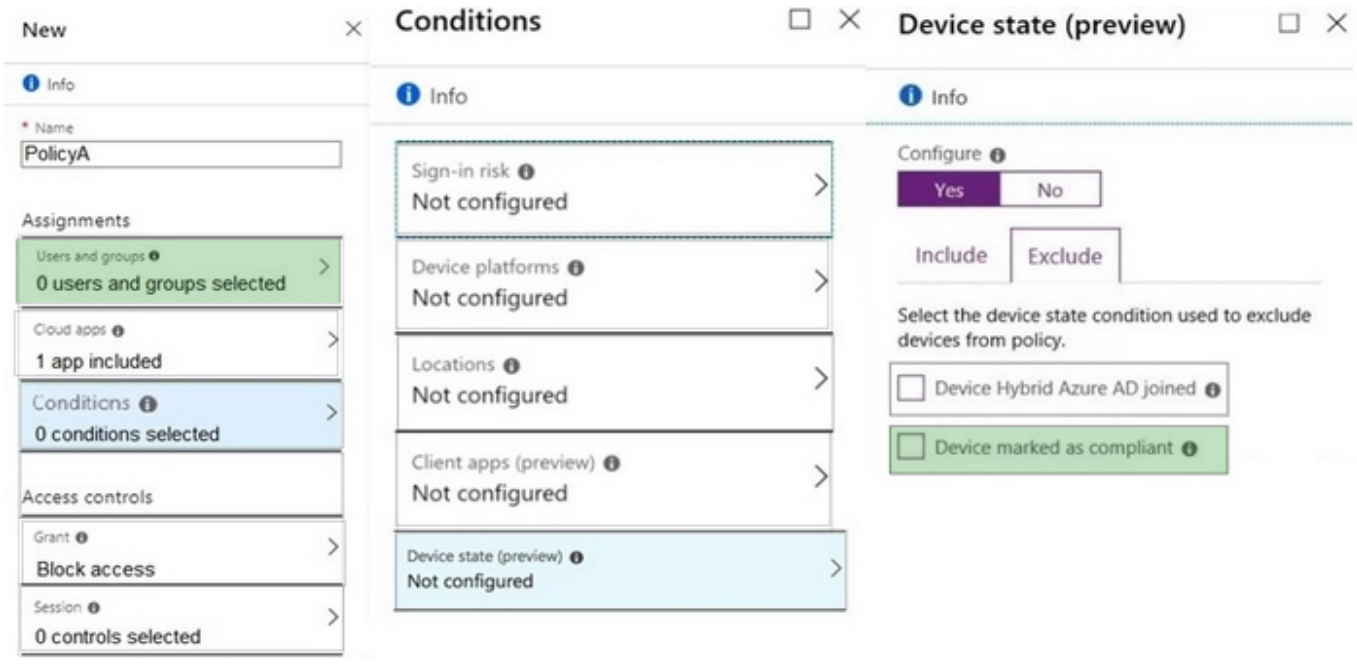
Which two settings should you configure in the policy? To answer, select the appropriate settings in the answer area.

NOTE: Each correct selection is worth one point.

Hot Area:



Correct Answer:



References: https://docs.microsoft.com/en-us/azure/active-directory/conditional-access/overview https://docs.microsoft.com/en-us/azure/active-directory/conditional-access/conditions https://docs.microsoft.com/en-us/intune/device-compliance-get-started

QUESTION 11

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.	○	○

Correct Answer:

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.	○	○

QUESTION 12

DRAG DROP

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

Name	Platform	Enrolled in Microsoft Intune
Device1	Windows 10	Yes
Device2	Android Enterprise	Yes
Device3	iOS/iPadOS	Yes

You need to configure the Microsoft Edge settings for each device.

What should you use? To answer, drag the appropriate Intune features to the correct devices. 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:

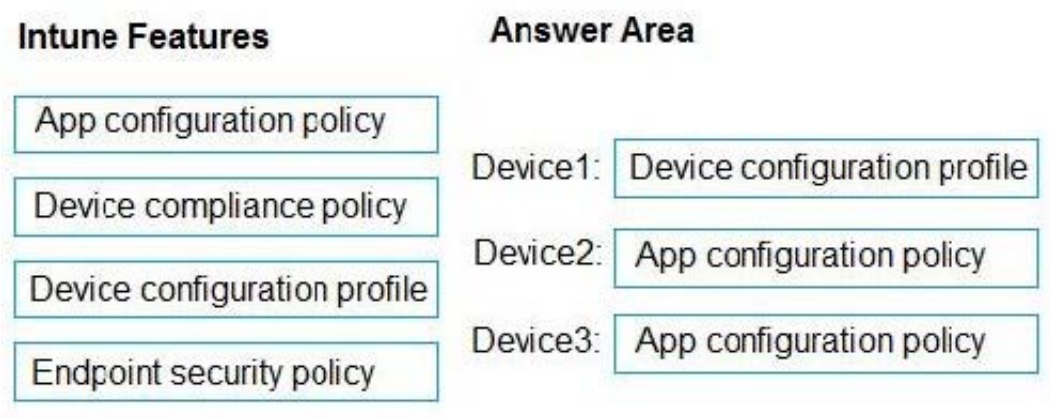
Intune Features

- App configuration policy
- Device compliance policy
- Device configuration profile
- Endpoint security policy

Answer Area

Device1: [ ]
Device2: [ ]
Device3: [ ]

Correct Answer:



Box 1: Device configuration profile Windows 10

Configure Microsoft Edge policy settings with Microsoft Intune You can configure Microsoft Edge policies and settings by adding a device configuration profile to Microsoft Intune. Using Intune to manage and enforce policies is equivalent to using Active Directory Group Policy or configuring local Group Policy Object (GPO) settings on user devices.

Box 2: App configuration policy Android Enterprise

App configuration policies for Microsoft Intune App configuration policies can help you eliminate app setup problems by letting you assign configuration settings to a policy that is assigned to end-users before they run the app. The settings are then supplied automatically when the app is configured on the end-users device, and end-users don\\'t need to take action. The configuration settings are unique for each app.

You can create and use app configuration policies to provide configuration settings for both iOS/iPadOS or Android apps. These configuration settings allow an app to be customized by using app configuration and management. The configuration policy settings are used when the app checks for these settings, typically the first time the app is run.

Box 3: App configuration policy iOS

Reference: https://learn.microsoft.com/en-us/deployedge/configure-edge-with-intune https://learn.microsoft.com/en-us/mem/intune/apps/manage-microsoft-edge https://learn.microsoft.com/en-us/mem/intune/apps/app-configuration-policies-overview

QUESTION 13

HOTSPOT

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

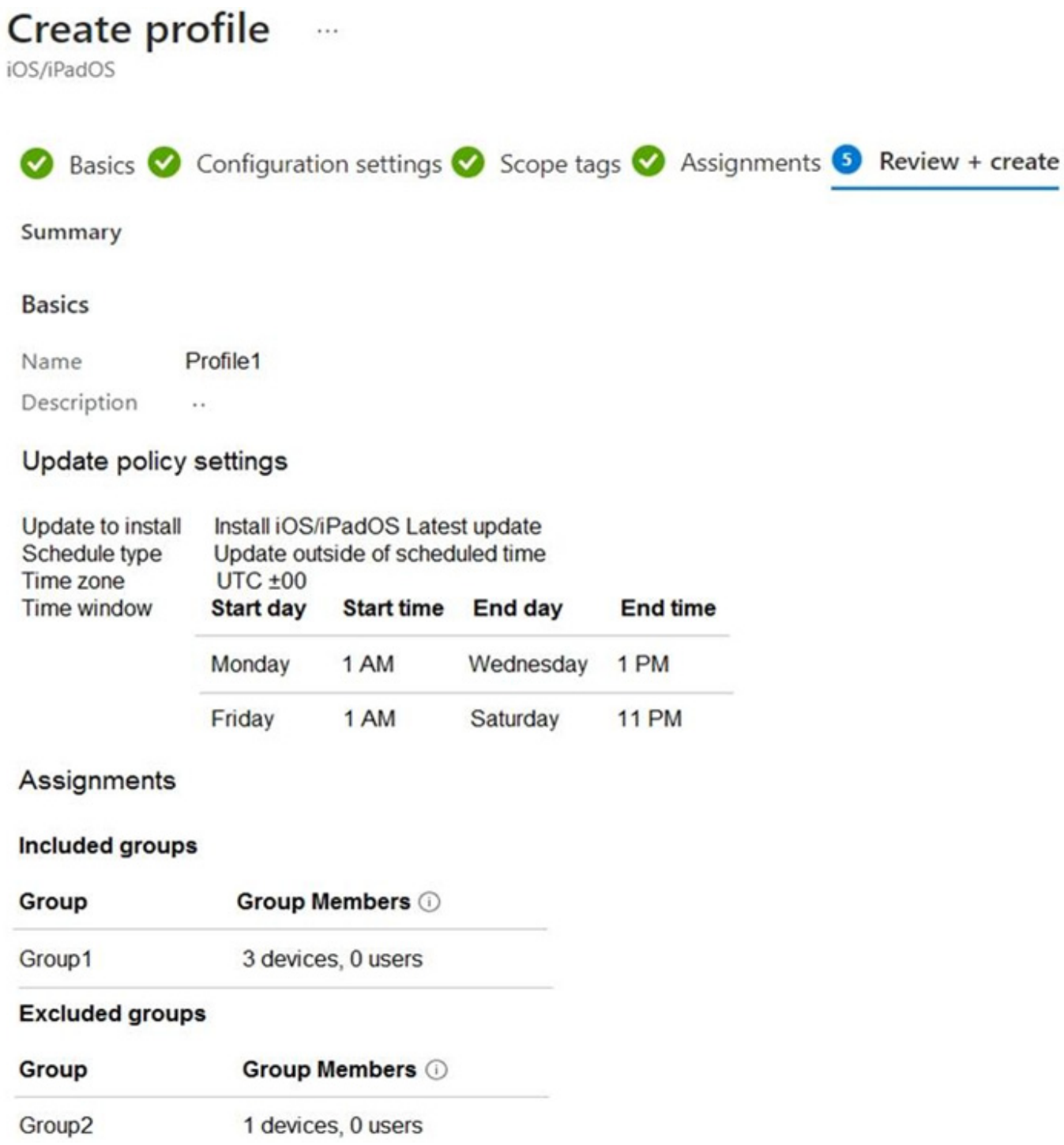
Devices are enrolled in Intune as shown in the following table.

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

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

Name	Members
Group1	Device1, Device2, Device3
Group2	Device2

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



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.	○	○

Correct Answer:

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.	○	○

QUESTION 14

HOTSPOT

You have a Microsoft 365 subscription that contains 1,000 iOS devices. The devices are enrolled in Microsoft Intune as follows:

1.

Two hundred devices are enrolled by using the Intune Company Portal.

2.

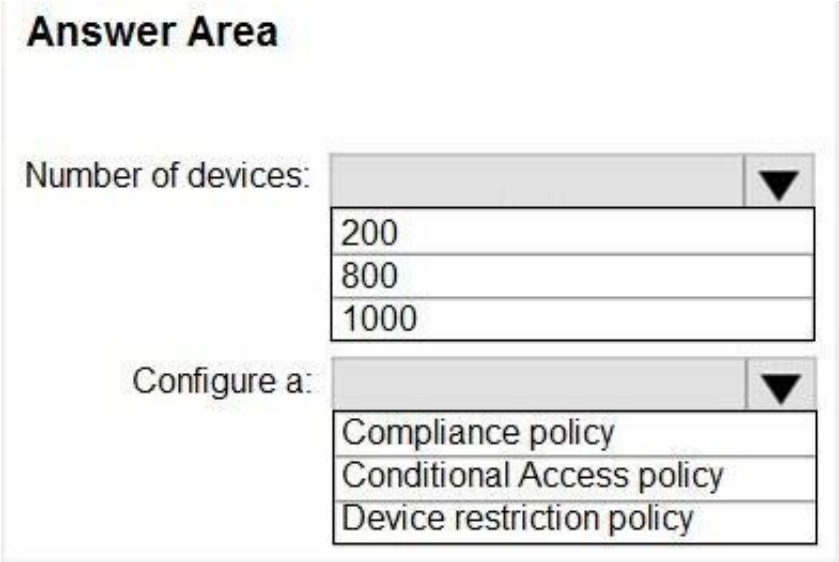
Eight hundred devices are enrolled by using Apple Automated Device Enrollment (ADE).

You create an iOS/iPadOS software updates policy named Policy1 that is configured to install iOS/iPadOS 15.5.

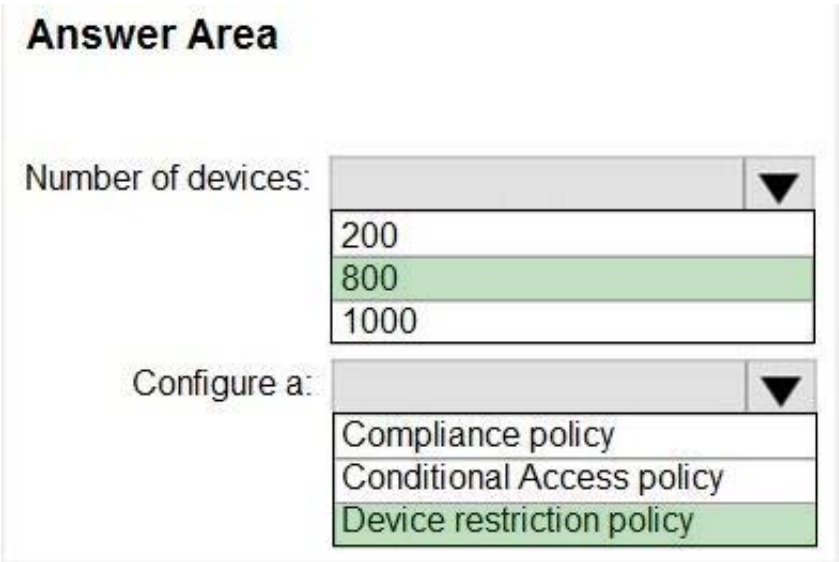
How many iOS devices will Policy1 update, and what should you configure to ensure that only iOS/iPadOS 15.5 is installed? To answer, select the appropriate options in the answer area.

NOTE: Each correct selection is worth one point.

Hot Area:



Correct Answer:



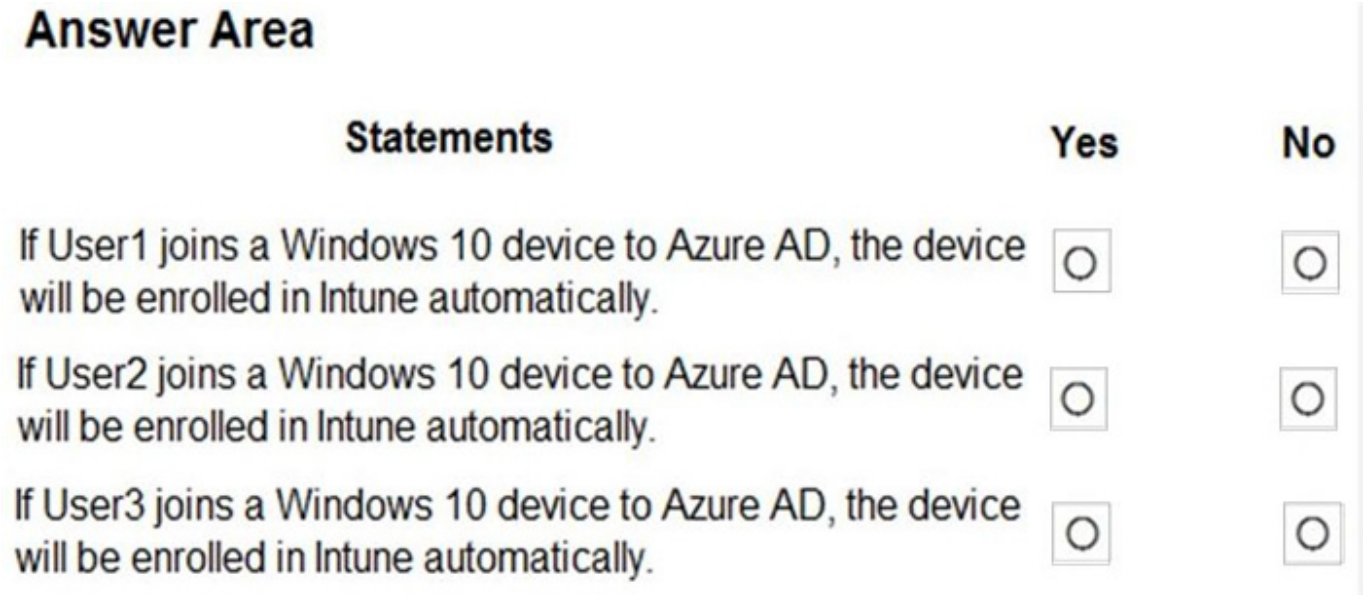
QUESTION 15

HOTSPOT

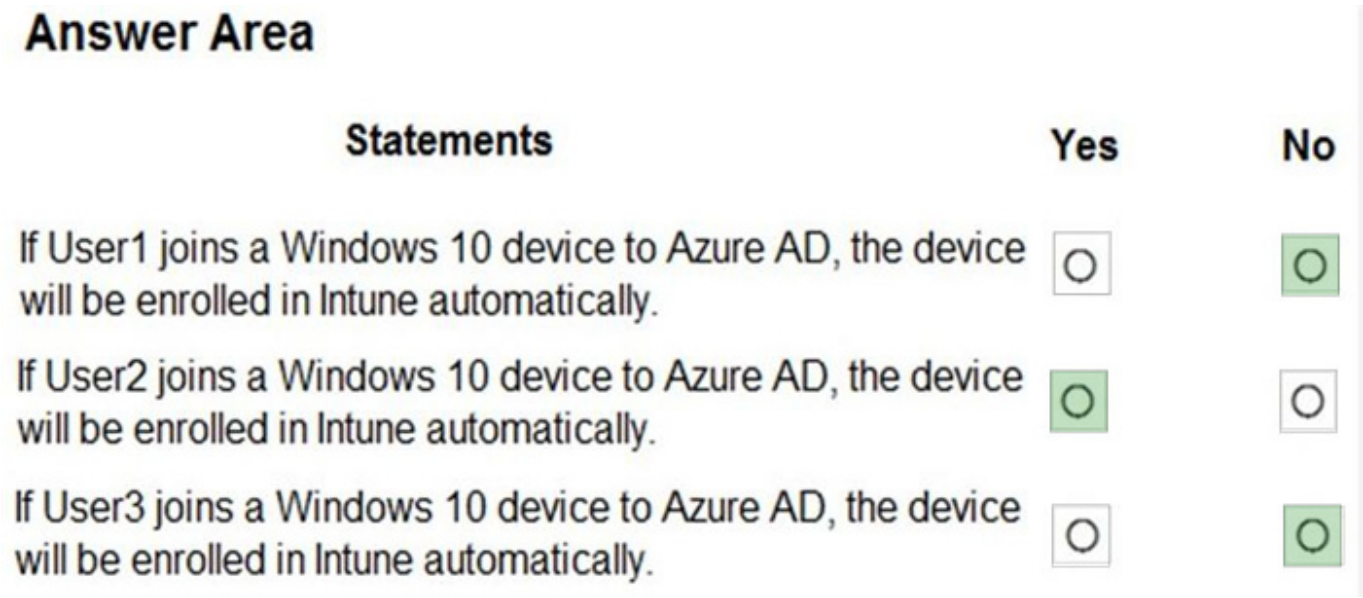
For each of the following statements, select Yes if the statement is true. Otherwise, select No.

NOTE: Each correct selection is worth one point.

Hot Area:



Correct Answer:



Box 1: No

User1 is a Cloud device administrator.

Local administrative privileges are required when enrolling an already configured Windows 10 device in Intune.

Cloud Device Administrator

Users in this role can enable, disable, and delete devices in Azure AD and read Windows 10 BitLocker keys (if present) in the Azure portal. The role does not grant permissions to manage any other properties on the device.

Note: The Windows 10 devices are joined to Azure AD and enrolled in Microsoft Intune.

Box 2: Yes

User2 is an Azure AD joined device local administrator.

Azure AD Joined Device Local Administrator

This role is available for assignment only as an additional local administrator in Device settings. Users with this role become local machine administrators on all Windows 10 devices that are joined to Azure Active Directory. They do not have

the ability to manage devices objects in Azure Active Directory.

Box 3: No

User3 is a Global reader.

Global Reader

Users in this role can read settings and administrative information across Microsoft 365 services but can\\'t take management actions.

Reference:

https://docs.microsoft.com/en-us/troubleshoot/mem/intune/no-permission-to-enroll-windows-devices

https://learn.microsoft.com/en-us/azure/active-directory/roles/permissions-reference