Microsoft

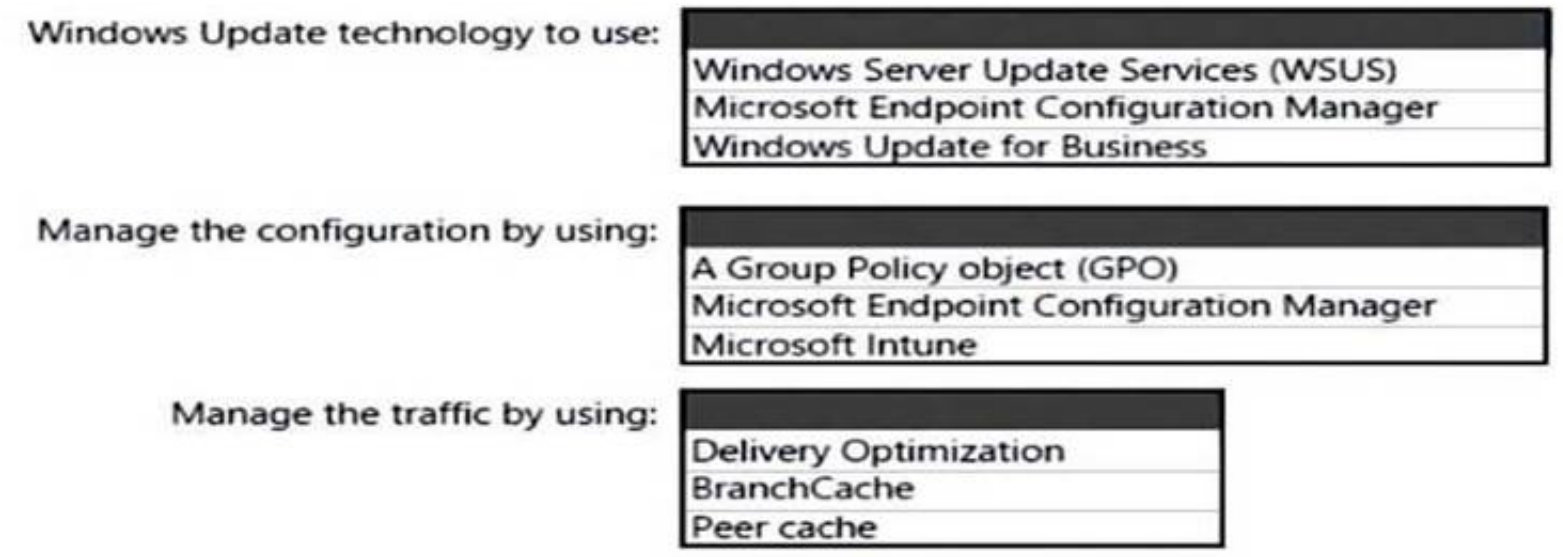
Exam Questions MD-102

Endpoint Administrator

NEW QUESTION 1
- (Exam Topic 4)
You have 100 computers that run Windows 10. You have no servers. All the computers are joined to Microsoft Azure Active Directory (Azure AD).
The computers have different update settings, and some computers are configured for manual updates. You need to configure Windows Update. The solution must meet the following requirements:

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

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



A. Mastered
B. Not Mastered

Answer: A

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

NEW QUESTION 2
- (Exam Topic 4)
You use Microsoft Intune and Intune Data Warehouse.
You need to create a device inventory report that includes the data stored in the data warehouse. What should you use to create the report?

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

Answer: D

Explanation:
You can use the Power BI Compliance app to load interactive, dynamically generated reports for your Intune tenant. Additionally, you can load your tenant data in Power BI using the OData link. Intune provides connection settings to your tenant so that you can view the following sample reports and charts related to:
Devices Enrollment
App protection policy Compliance policy
Device configuration profiles Software updates
Device inventory logs
Note: Load the data in Power BI using the OData link
With a client authenticated to Azure AD, the OData URL connects to the RESTful endpoint in the Data Warehouse API that exposes the data model to your reporting client. Follow these instructions to use Power BI Desktop to connect and create your own reports.

- Sign in to the Microsoft Endpoint Manager admin center.
- Select Reports > Intune Data warehouse > Data warehouse.
- Retrieve the custom feed URL from the reporting blade, for example:
- Open Power BI Desktop.

- Choose File > Get Data. Select OData feed.
- Choose Basic.
- Type or paste the OData URL into the URL box.
- Select OK.
- If you have not authenticated to Azure AD for your tenant from the Power BI desktop client, type your credentials. To gain access to your data, you must authorize with Azure Active Directory (Azure AD) using OAuth 2.0.
- Select Organizational account.
- Type your username and password.
- Select Sign In.
- Select Connect.
- Select Load.

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

NEW QUESTION 3
- (Exam Topic 4)
Your network contains an Active Directory domain named contoso.com. The domain contains two computers named Computer! and Computer2 that run Windows 10. On Computer1, you need to run the
Invoke-Command cmdlet to execute several PowerShell commands on Computed. What should you do first?

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

Answer: C

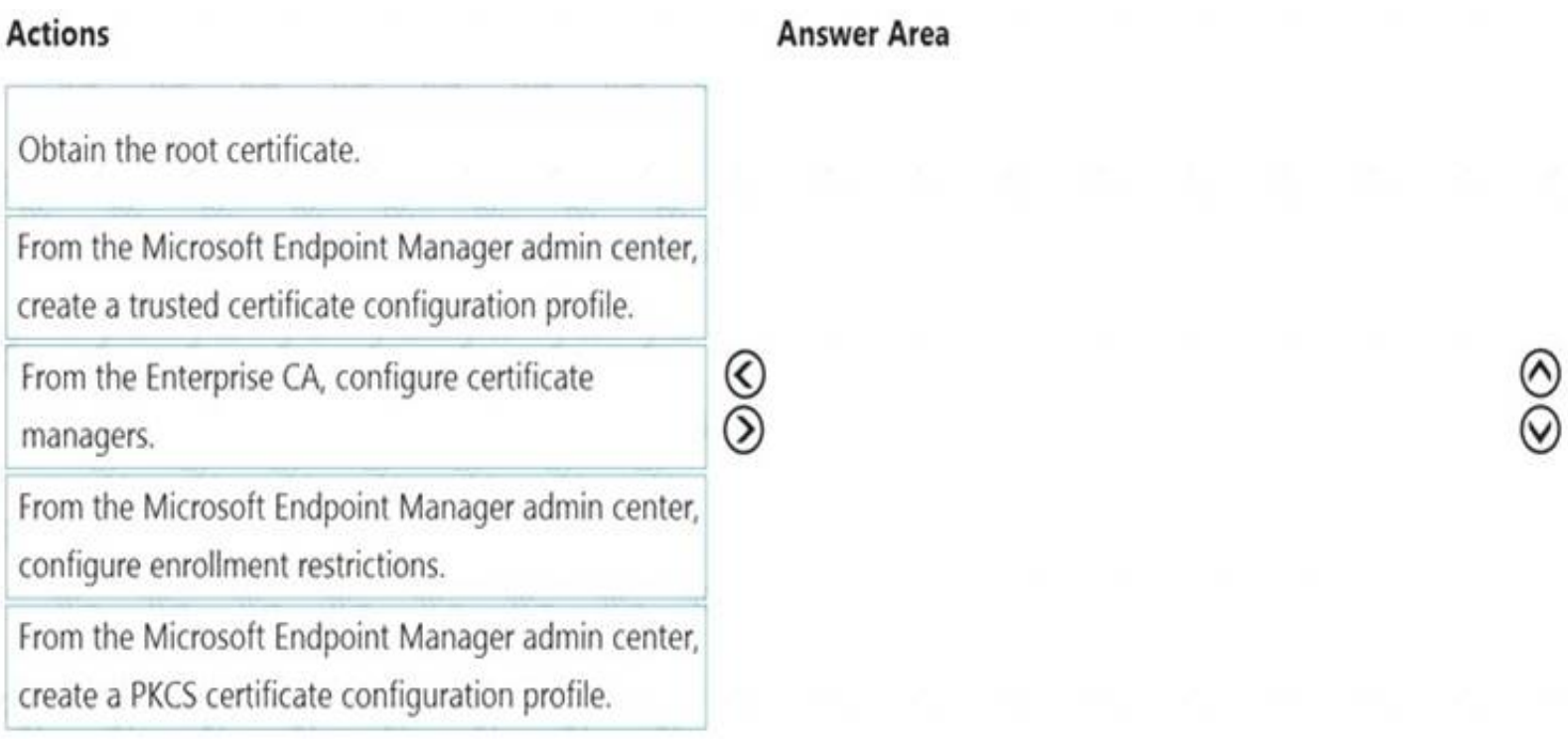
NEW QUESTION 4
- (Exam Topic 4)
You have a Microsoft 365 subscription that includes Microsoft Intune.
You need to implement a Microsoft Defender for Endpoint solution that meets the following requirements:
• Enforces compliance for Defender for Endpoint by using Conditional Access
• Prevents suspicious 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.

A. Mastered
B. Not Mastered

Answer: A

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

NEW QUESTION 5
- (Exam Topic 4)
You have a Microsoft Intune subscription that is configured to use a PFX certificate connector to an on-premises Enterprise certification authority (CA).
You need to use Intune to configure autoenrollment for Android devices by using public key pair (PKCS) certificates.
Which three actions should you perform in sequence? To answer, move the appropriate actions from the list of actions to the answer area and arrange them in the correct order.



A. Mastered
B. Not Mastered

Answer: A

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

NEW QUESTION 6
- (Exam Topic 4)
You have the devices shown in the following table.

Name	Operating system	Description
Device1	32-bit version of Windows 10	Retired device
Device2	64-bit version of Windows 11	New device
Server1	Windows Server 2019	File server

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

Answer Area

A. Mastered
B. Not Mastered

Answer: A

Explanation:

Answer Area

NEW QUESTION 7
- (Exam Topic 4)
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.

A. Mastered
B. Not Mastered

Answer: A

Explanation:

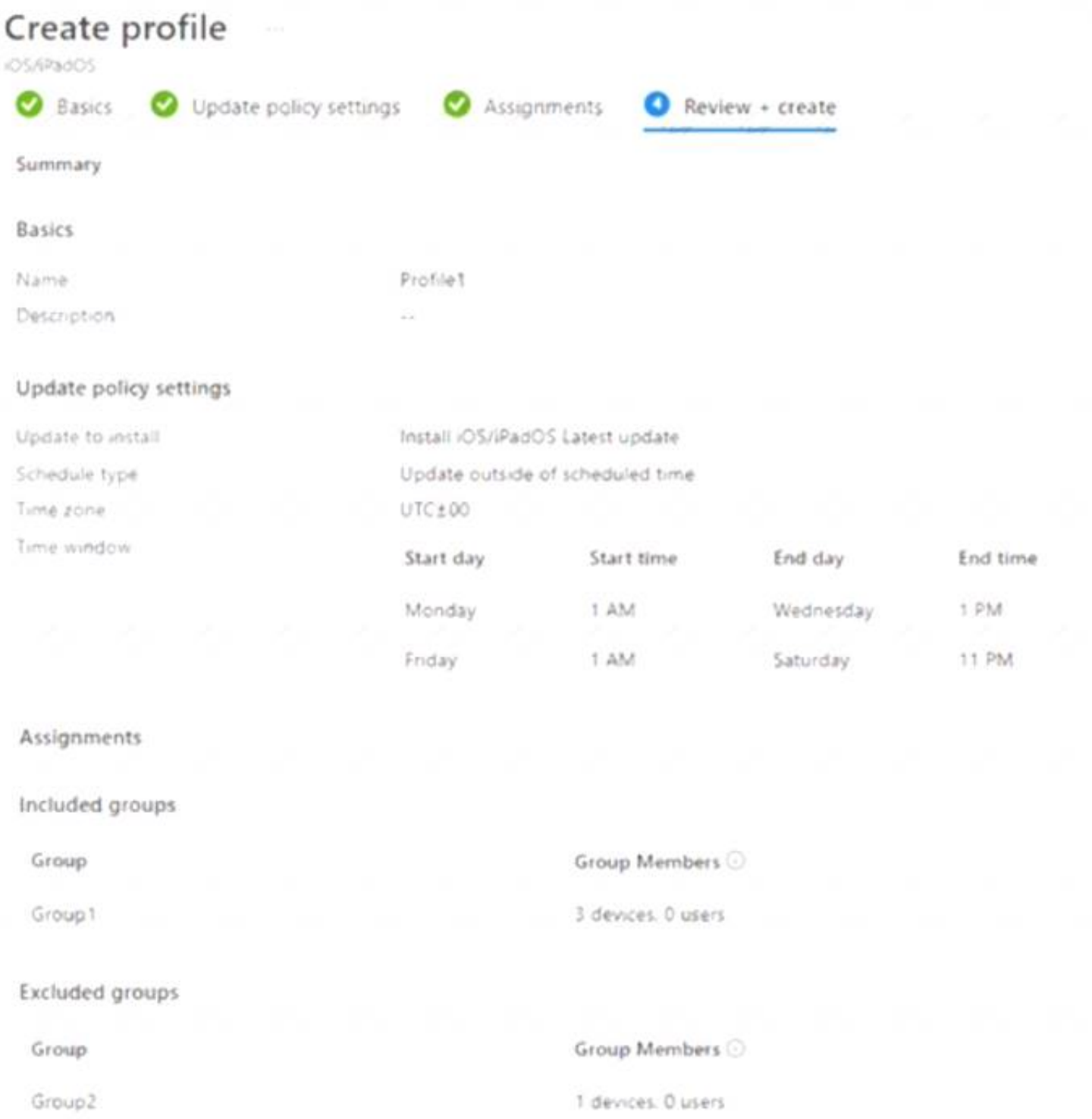
NEW QUESTION 8
- (Exam Topic 4)
You have a Microsoft 365 ES subscription that uses Microsoft Intune. Devices are enrolled in Intune as shown in the following table.

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.



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

Answer Area

Statements	Yes	No
If 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.		

A. Mastered
B. Not Mastered

Answer: A

Explanation:

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.		

NEW QUESTION 9
- (Exam Topic 4)

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

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

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

Name	Member
Group1	Device1, Device2, Device3
Group2	Device2

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

Create profile ...

Windows PC

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

Summary

Basics

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

Out-of-box experience (OOBE)

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

Assignments

Included groups	Group1
Excluded groups	Group2

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

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

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

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

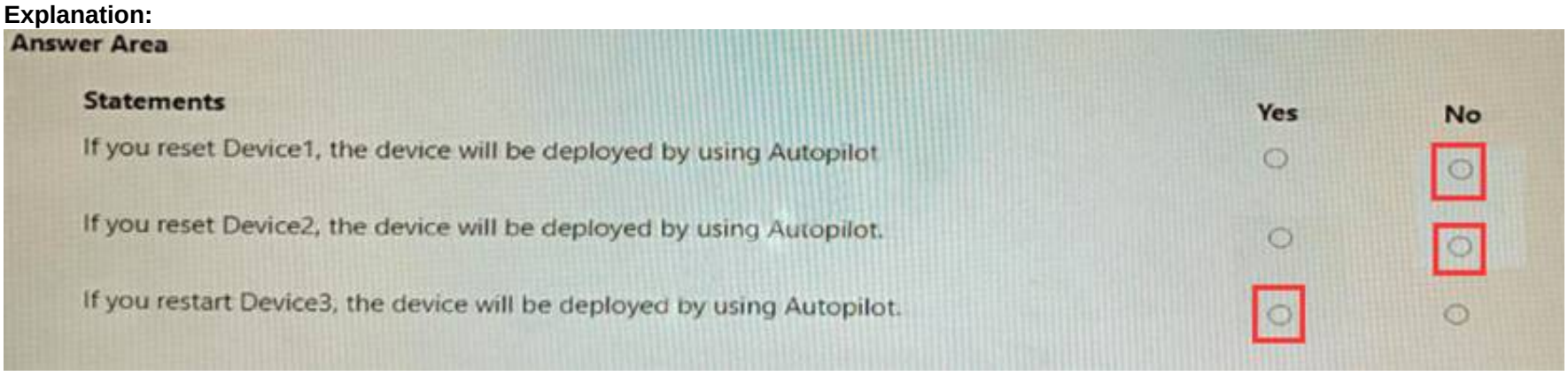
Answer Area

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

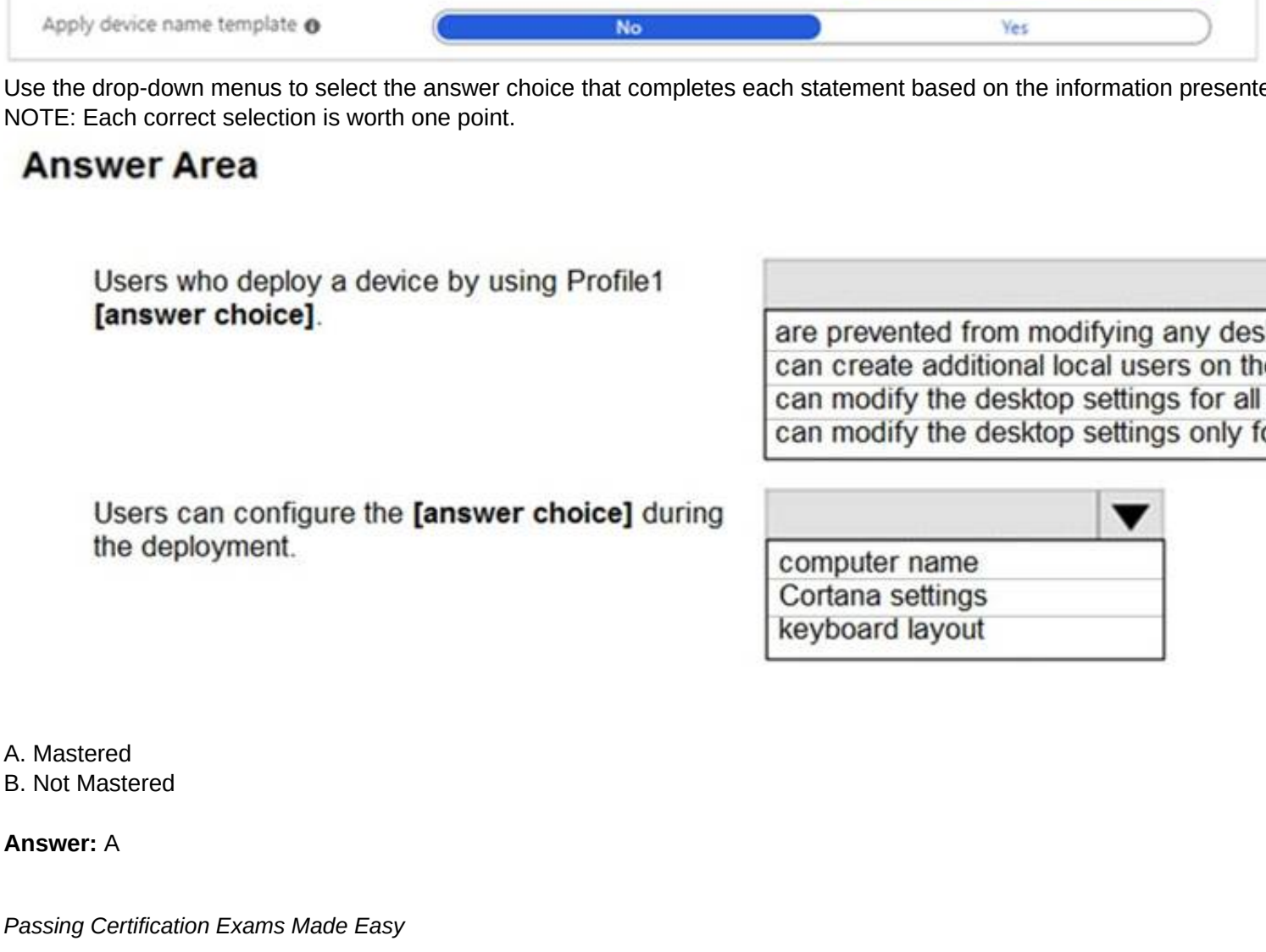
A. Mastered
B. Not Mastered

Answer: A

Explanation:



NEW QUESTION 10
- (Exam Topic 4)
You have a Microsoft Intune subscription.
You are creating a Windows Autopilot deployment profile named Profile1 as shown in the following exhibit.



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.

A. Mastered
B. Not Mastered

Answer: A

Explanation:

Answer Area

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

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

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

- computer name
- Cortana settings
- keyboard layout

NEW QUESTION 10
- (Exam Topic 4)
You have the MDM Security Baseline profile shown in the MDM exhibit. (Click the MDM tab.) You have the ASR Endpoint Security profile shown in the ASR exhibit. (Click the ASR 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 >

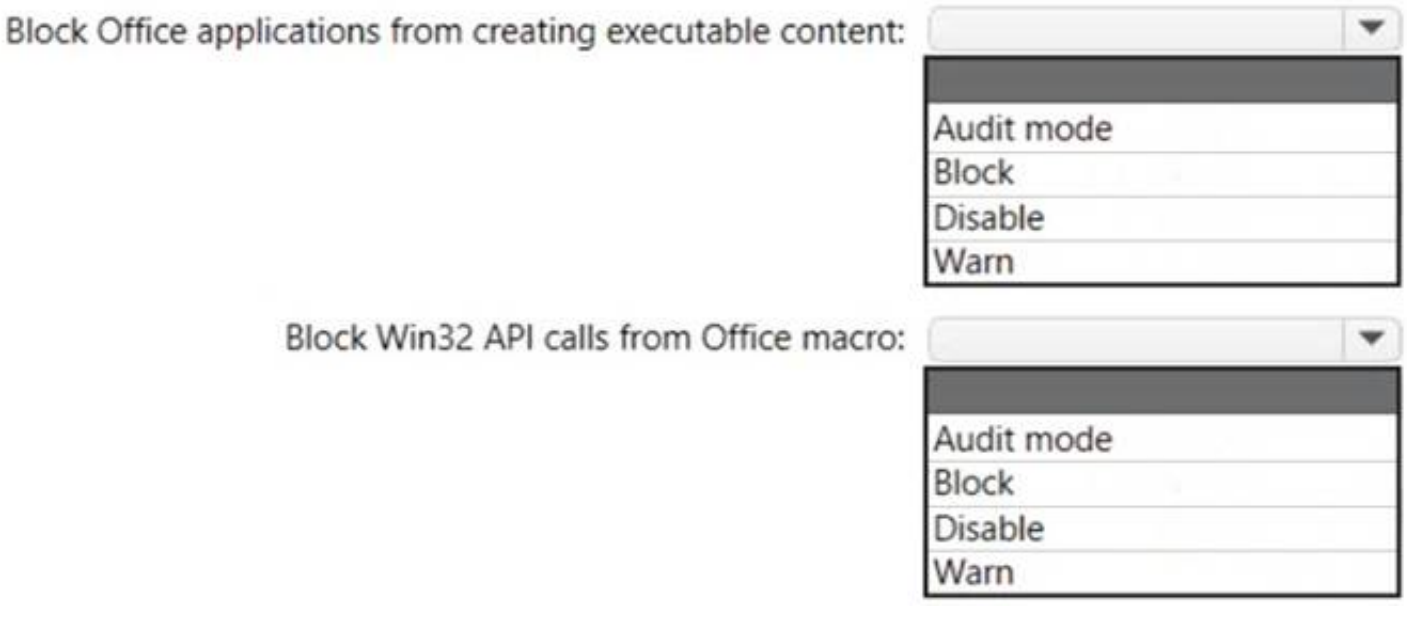
Edit profile

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
Block all Office applications from creating child processes	Audit mode
Block Win32 API calls from Office macro	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.

Answer Area

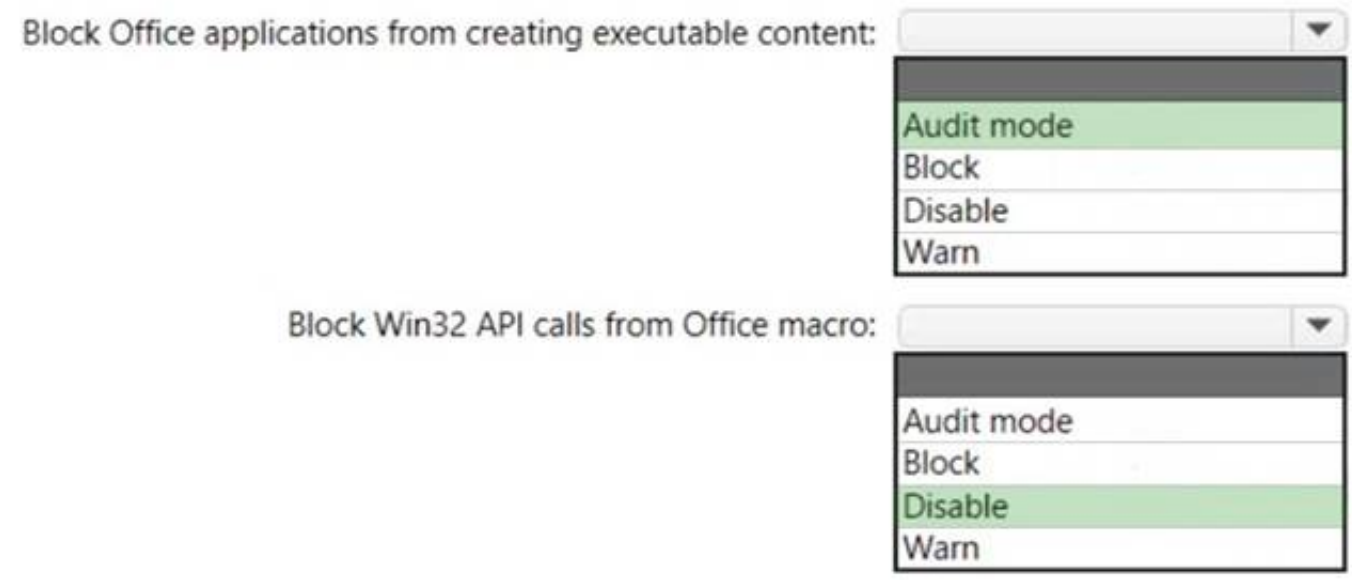


A. Mastered
B. Not Mastered

Answer: A

Explanation:

Answer Area



NEW QUESTION 15
- (Exam Topic 4)
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).

Answer: C

Explanation:
Reference:
https://www.manageengine.com/mobile-device-management/help/enrollment/mdm_creating_apns_certificate.ht 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

NEW QUESTION 19
- (Exam Topic 4)
You have a Microsoft 365 E5 subscription and 100 unmanaged iPad devices.
You need to deploy a specific iOS update to the devices. Users must be prevented from manually installing a more recent version of iOS.
Which two actions should you perform? Each correct answer presents part of the solution. NOTE: Each correct selection is worth one point.

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

Answer: CE

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

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

The other options are not correct for this scenario because:

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

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

NEW QUESTION 21
- (Exam Topic 4)
Note: This question is part of a series of questions that present the same scenario. Each question in the series contains a unique solution that might meet the stated goals. Some question sets might have more than one correct solution, while others might not have a correct solution.
After you answer a question in this section, you will NOT be able to return to it. As a result, these questions will not appear in the review screen.
Your network contains an Active Directory domain. The domain contains a computer named Computer1 that runs Windows 8.1.
Computer1 has apps that are compatible with Windows 10.
You need to perform a Windows 10 in-place upgrade on Computer1.
Solution: You copy the Windows 10 installation media to a Microsoft Deployment Toolkit (MDT) deployment share. You create a task sequence, and then you run the MDT deployment wizard on Computer1. Does this meet the goal?

A. Yes
B. No

Answer: B

NEW QUESTION 24
- (Exam Topic 4)
You have a Microsoft 365 subscription.
You plan to enable Microsoft Intune enrollment for the following types of devices:
• Existing Windows 11 devices managed by using Configuration Manager
• Personal iOS devices
The solution must minimize user disruption.
Which enrollment method should you use for each device type? To answer, select the appropriate options in the answer area.
NOTE: Each correct selection is worth one point.

Answer Area

A. Mastered
B. Not Mastered

Answer: A

Explanation:

Answer Area

NEW QUESTION 28
- (Exam Topic 4)
Your network contains an Active Directory domain. The domain contains a computer named Computer1 that runs Windows 8.1.
Computer1 has apps that are compatible with Windows 10.
You need to perform a Windows 10 in-place upgrade on Computer1.
Solution: You copy the Windows 10 installation media to a network share. You start Computer1 from Windows PE (WinPE), and then you run setup.exe from the network share.
Does this meet the goal?

A. Yes
B. No

Answer: B

NEW QUESTION 33
- (Exam Topic 4)
You have a Microsoft 365 subscription.
You plan to use Windows Autopilot to provision 25 Windows 11 devices. You need to configure the Out-of-box experience (OOBE) settings.
What should you create in the Microsoft Intune admin center?

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

Answer: B

NEW QUESTION 34
- (Exam Topic 4)
You have a Microsoft Intune subscription.
You have devices enrolled in intune as shown in the following table.

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

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

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

Answer: B

Explanation:
The correct answer is B because you need to create two app configuration policies for managed devices, one for iOS/iPadOS devices and one for Android devices1. App configuration policies let you customize the settings of apps for iOS/iPadOS or Android devices1. The settings are assigned to user groups and applied when the app runs1. The app developer or supplier provides the configuration settings (keys and values) that are exposed to Intune1. You can't use a single app configuration policy for both iOS/iPadOS and Android devices because they have different configuration settings2. References: 1: App configuration policies for Microsoft Intune | Microsoft Learn
https://learn.microsoft.com/en-us/mem/intune/apps/app-configuration-policies-overview 2: Add app configuration policies for managed iOS/iPadOS devices | Microsoft Learn https://learn.microsoft.com/en-us/mem/intune/apps/app-configuration-policies-use-ios

NEW QUESTION 37
- (Exam Topic 4)

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

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

You use Distributed File System (DFS) Replication to replicate images in a share named Production. You configure the following settings in the Bootstrap.ini file.

```
[Settings]
Priority=DefaultGateway, Default
[DefaultGateway]
10.1.1.1=NewYork
10.5.5.1=London
[NewYork]
DeployRoot=\\MDT1\Production$
[London]
DeployRoot=\\MDT2\Production$
KeyboardLocale=en-gb -
[Default]
DeployRoot=\\MDT3\Production$

KeyboardLocale=en-us -
```

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

Name	IP address
LT1	10.1.1.240
DT1	10.5.5.115
TB1	10.2.2.193

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

NOTE: Each correct selection is worth one point.

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

A. Mastered
B. Not Mastered

Answer: A

Explanation:

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

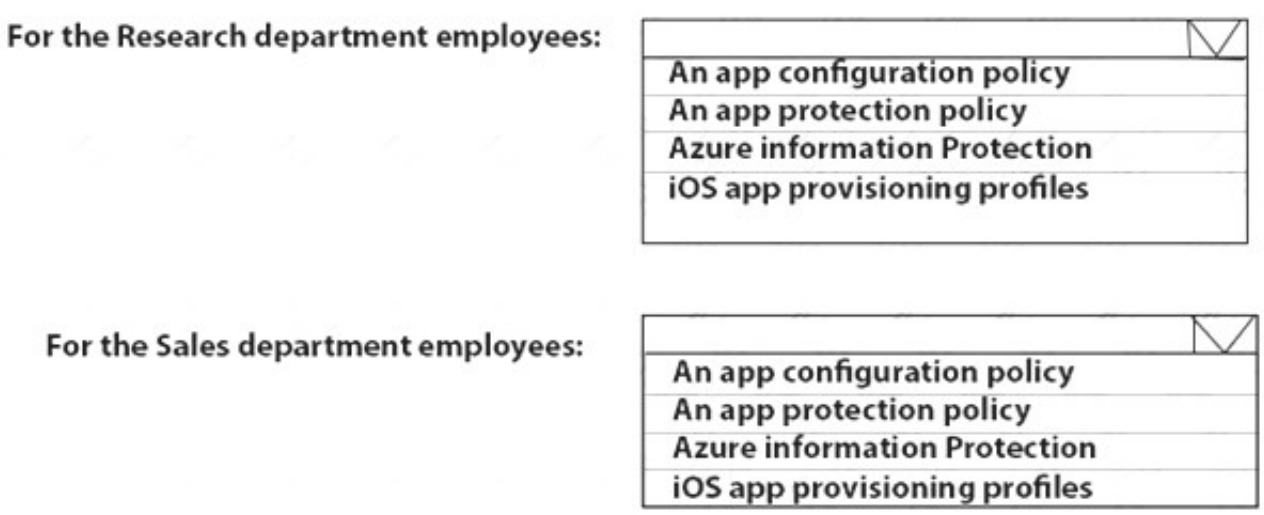
NEW QUESTION 38
- (Exam Topic 2)
What should you configure to meet the technical requirements for the Azure AD-joined computers?

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

Answer: A

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

NEW QUESTION 40
- (Exam Topic 2)
You need to recommend a solution to meet the device management requirements.
What should you include in the recommendation? To answer, select the appropriate options in the answer area. NOTE: Each correct selection is worth one point.

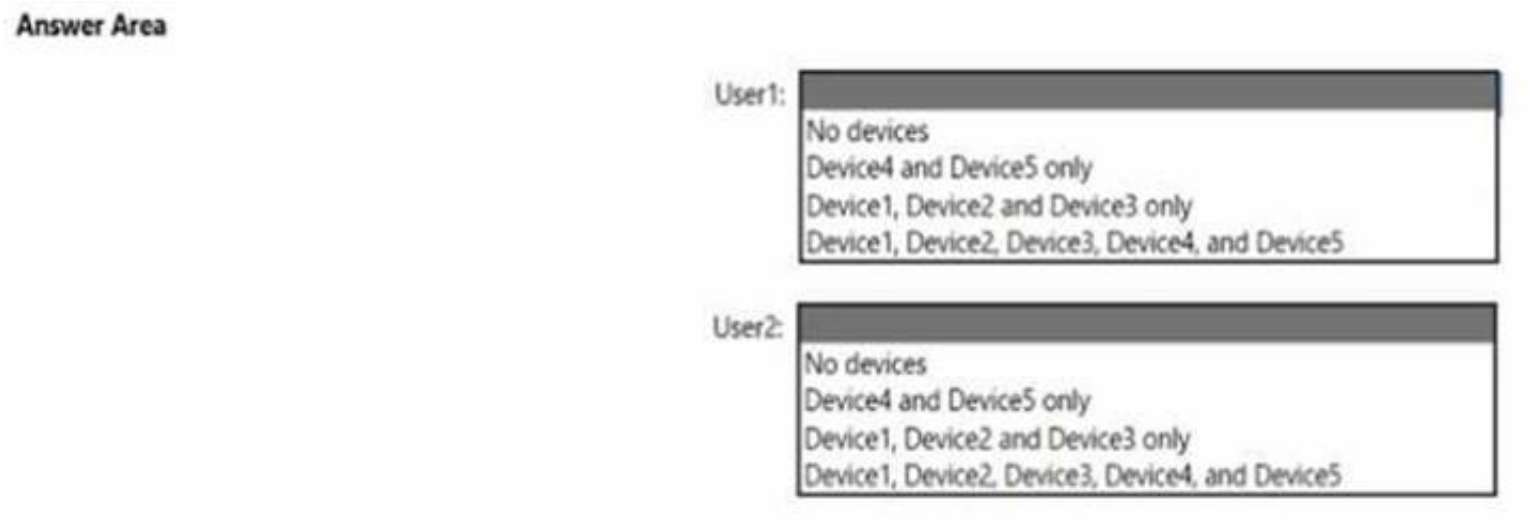


A. Mastered
B. Not Mastered

Answer: A

Explanation:
Reference:
https://github.com/MicrosoftDocs/IntuneDocs/blob/master/intune/app-protection-policy.md
https://docs.microsoft.com/en-us/azure/information-protection/configure-usage-rights#do-not-forward-option-fo

NEW QUESTION 42
- (Exam Topic 1)
User1 and User2 plan to use Sync your settings.
On which devices can the users use Sync your settings? To answer, select the appropriate options in the answer area.
NOTE: Each correct selection is worth one point.



A. Mastered
B. Not Mastered

Answer: A

Explanation:
Graphical user interface, text, application, email Description automatically generated
Reference:
https://www.jeffgilb.com/managing-local-administrators-with-azure-ad-and-intune/

NEW QUESTION 45
- (Exam Topic 1)
For each of the following statements, select Yes if the statement is true. Otherwise, select No.
NOTE: Each correct selection is worth one point.

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

A. Mastered
B. Not Mastered

Answer: A

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

NEW QUESTION 48
- (Exam Topic 4)
You have a Microsoft 365 E5 subscription that contains 100 iOS devices enrolled in Microsoft Intune. You need to ensure that notifications of iOS updates are deferred for 30 days after the updates are released. What should you create?

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

Answer: C

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

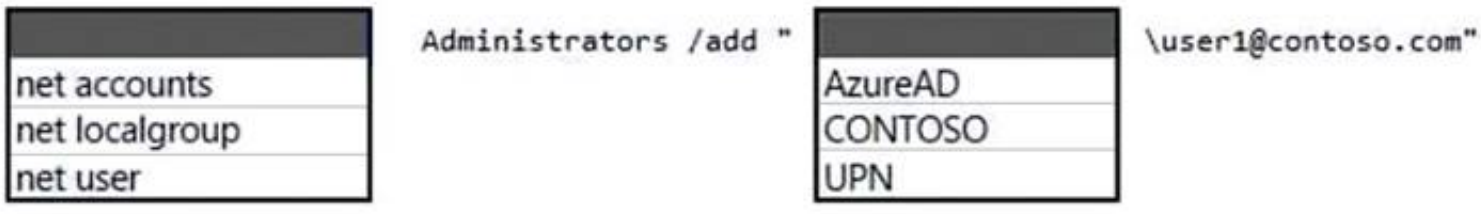
NEW QUESTION 52
- (Exam Topic 4)
Your company has an Azure AD tenant named contoso.com that contains several Windows 10 devices. When you join new Windows 10 devices to contoso.com, users are prompted to set up a four-digit pin. You need to ensure that the users are prompted to set up a six-digit pin when they join the Windows 10 devices to contoso.com.
Solution: From the Microsoft Entra admin center, you configure automatic mobile device management (MDM) enrollment. From the Microsoft Intune admin center, you create and assign a device restrictions profile.
Does this meet the goal?

A. Yes
B. No

Answer: B

NEW QUESTION 55
- (Exam Topic 4)
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.

Answer Area

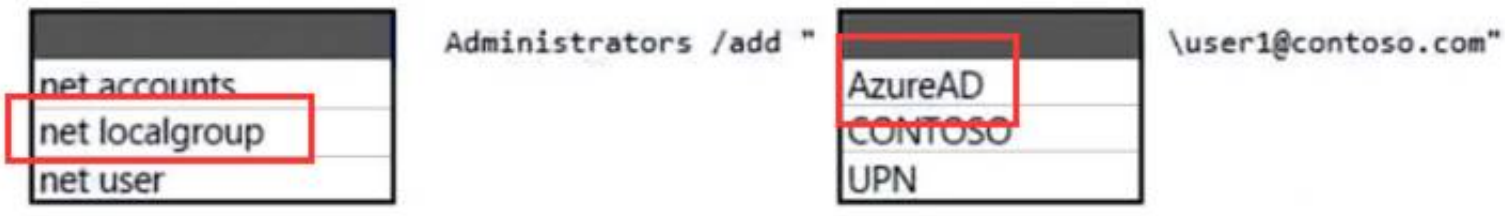


A. Mastered
B. Not Mastered

Answer: A

Explanation:

Answer Area



NEW QUESTION 59
- (Exam Topic 4)
You have a Microsoft 365 E5 subscription that contains 10 Android Enterprise devices. Each device has a corporate-owned work profile and is enrolled in Microsoft Intune.
You need to configure the devices to run a single app in kiosk mode.
Which Configuration settings should you modify in the device restrictions profile?

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

Answer: D

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

NEW QUESTION 60
- (Exam Topic 4)
You have an Azure AD tenant that contains the devices shown in the following table. You purchase Windows 11 Enterprise E5 licenses.
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

Answer: B

NEW QUESTION 63
- (Exam Topic 4)
You have a Microsoft 365 E5 subscription. The subscription contains 25 computers that run Windows 11 and are enrolled in Microsoft Intune. You need to onboard the devices to Microsoft Defender for Endpoint. What should you create in the Microsoft Intune admin center?

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

Answer: C

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

NEW QUESTION 68
- (Exam Topic 4)
You have a Microsoft 365 E5 subscription that contains 150 hybrid Azure AD joined Windows devices. All the devices are enrolled in Microsoft Intune. You need to configure Delivery Optimization on the devices to meet the following requirements:
• Allow downloads from the internet and from other computers on the local network.
• Limit the percentage of used bandwidth to 50. What should you use?

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

Answer: A

Explanation:
A configuration profile is the correct answer because it allows you to configure Delivery Optimization settings for Windows devices in Intune. You can specify the download mode, bandwidth limit, caching options, and more. A configuration profile is a template that contains one or more settings that you can apply to groups of devices. References:
- Windows 10 Delivery Optimization settings for Intune - Microsoft Intune | Microsoft Learn
- Delivery Optimization settings in Microsoft Intune

NEW QUESTION 71
- (Exam Topic 4)
Note: This question is part of a series of questions that present the same scenario. Each question in the series contains a unique solution that might meet the stated goals. Some question sets might have more than one correct solution, while others might not have a correct solution.
After you answer a question in this section, you will NOT be able to return to it. As a result, these questions will not appear in the review screen.
Your company has an Azure AD tenant named contoso.com that contains several Windows 10 devices. When you join new Windows 10 devices to contoso.com, users are prompted to set up a four-digit pin. You need to ensure that the users are prompted to set up a six-digit pin when they join the Windows 10 devices to contoso.com.
Solution: From the Microsoft Entra admin center, you configure the Authentication methods. Does this meet the goal?

A. Yes
B. No

Answer: B

NEW QUESTION 74
- (Exam Topic 4)
You have devices enrolled in Microsoft Intune as shown in the following table.

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

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

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

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

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

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

Answer Area

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

A. Mastered
B. Not Mastered

Answer: A

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

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

NEW QUESTION 77
- (Exam Topic 4)
You have the Microsoft Deployment Toolkit (MDT) installed. You install and customize Windows 11 on a reference computer
You need to capture an image of the reference computer and ensure that the image can be deployed to multiple computers.
Which command should you run before you capture the image?

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

Answer: C

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

NEW QUESTION 78
- (Exam Topic 4)
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.

Answer: C

NEW QUESTION 82
- (Exam Topic 4)
You have an Azure AD tenant named contoso.com.
You plan to use Windows Autopilot to configure the Windows 10 devices shown in the following table.

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

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

A. Device2 only

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

Answer: C

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

NEW QUESTION 85
- (Exam Topic 4)
You have a Microsoft 365 E5 subscription that contains a group named Group1.
You create a Conditional Access policy named CAPolicy1 and assign CAPolicy1 to Group1.
You need to configure CAPolicy1 to require the members of Group1 to reauthenticate every eight hours when they connect to Microsoft Exchange Online.
What should you configure?

A. Session access controls
B. an assignment that uses a User risk condition
C. an assignment that uses a Sign-in risk condition
D. Grant access controls

Answer: A

Explanation:
User sign-in frequency
Sign-in frequency defines the time period before a user is asked to sign in again when attempting to access a resource.
The Azure Active Directory (Azure AD) default configuration for user sign-in frequency is a rolling window of 90 days.
Sign-in frequency control

- Sign in to the Azure portal as a global administrator, security administrator, or Conditional Access administrator.
- Browse to Azure Active Directory > Security > Conditional Access.
- Select New policy.
- Give your policy a name. We recommend that organizations create a meaningful standard for the names of their policies.
- Choose all required conditions for customer’s environment, including the target cloud apps.
- Under Access controls > Session.

Select Sign-in frequency.
Choose Periodic reauthentication and enter a value of hours or days or select Every time.

- Save your policy. Reference:

https://docs.microsoft.com/en-us/azure/active-directory/conditional-access/howto-conditional-access-session-life

NEW QUESTION 88
- (Exam Topic 4)
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

Answer: D

NEW QUESTION 93
- (Exam Topic 4)
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

Answer: D

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. References:
https://docs.microsoft.com/en-us/mem/analytics/overview

NEW QUESTION 94
- (Exam Topic 4)
Your network contains an Active Directory domain named adatum.com. The domain contains two computers named Computer1 and Computer2 that run Windows

10. Remote Desktop is enabled on Computer2.
The domain contains the user accounts shown in the following table.

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

Computer2 contains the local groups shown in the following table.

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

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

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

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

Answer Area

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

A. Mastered
B. Not Mastered

Answer: A

Explanation:

Answer Area

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

NEW QUESTION 95
- (Exam Topic 4)
You have a hybrid deployment of Azure AD that contains 50 Windows 10 devices. All the devices are enrolled in Microsoft Intune.
You discover that Group Policy settings override the settings configured in Microsoft Intune policies. You need to ensure that the settings configured in Microsoft Intune override the Group Policy settings. What should you do?

A. From Group Policy Management Editor, configure the Computer Configuration settings in the Default Domain Policy.
B. From the Microsoft Intune admin center, create a custom device profile.
C. From the Microsoft Intune admin center, create an Administrative Templates device profile.
D. From Group Policy Management Editor, configure the User Configuration settings in the Default Domain Policy.

Answer: C

NEW QUESTION 96
- (Exam Topic 4)
You have a Microsoft 365 subscription that contains 1,000 iOS devices and includes Microsoft Intune. You need to prevent the printing of corporate data from managed apps on the devices, should you configure?

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

Answer: C

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

NEW QUESTION 97
- (Exam Topic 4)
You have an Azure Active Directory (Azure AD) tenant named contoso.com that contains the devices shown in the following table.

Name	Operating system	Azure AD status	Mobile device management (MDM)
Device1	Windows 8.1	Registered	*None*
Device2	Windows 10	Joined	*None*
Device3	Windows 10	Joined	Microsoft Intune

Contoso.com contains the Azure Active Directory groups shown in the following table.

Name	Members
Group1	Group2, Device1, Device3
Group2	Device2

You add a Windows Autopilot deployment profile. The profile is configured 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.

Statements	Yes	No
If Device1 starts in Out of Box Experience (OOBE) mode, the device will be deployed by using Autopilot.	○	○
If Device2 starts in Out of Box Experience (OOBE) mode, the device will be deployed by using Autopilot.	○	○
If Device3 starts in Out of Box Experience (OOBE) mode, the device will be deployed by using	○	○

A. Mastered
B. Not Mastered

Answer: A

Explanation:

Box 1: No
Device1 has no Mobile device Management (MDM) configured.
Note: Device1 is running Windows 8.1, and is registered, but not joined. Device1 is in Group1.
Profile1 is assigned to Group1. Box 2: No
Device2 has no Mobile device Management (MDM) configured. Note: Device2 is running Windows 10, and is joined.
Device2 is in Group2. Group2 is in Group1.
Profile1 is assigned to Group1. Box 3: Yes
Device3 has Mobile device Management (MDM) configured. Device3 is running Windows 10, and is joined

Device1 is in Group1.
Profile1 is assigned to Group1.
Mobile device management (MDM) enrollment: Once your Windows 10 device joins Azure AD, Autopilot ensures your device is automatically enrolled with MDMs such as Microsoft Intune. This program can automatically push configurations, policies and settings to the device, and install Office 365 and other business apps without you having to get IT admins to manually sort the device. Intune can also apply the latest updates from Windows Update for Business.
Reference: https://xo.xello.com.au/blog/windows-autopilot

NEW QUESTION 98
- (Exam Topic 4)
You have a Microsoft 365 subscription.
You have devices enrolled in Microsoft Intune as shown in the following table. To which devices can you deploy apps by using Intune?

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

Answer: E

NEW QUESTION 99
- (Exam Topic 4)
You have a Microsoft 365 subscription that uses Microsoft Intune Suite.
You use Microsoft Intune to manage devices. All devices are in the same time zone. You create an update rings policy and assign the policy to all Windows devices.
On the November 1, you pause the update rings policy. All devices remain online.
Without further modification to the policy, on which date will the devices next attempt to update?

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

Answer: C

NEW QUESTION 103
- (Exam Topic 4)
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

Answer: D

NEW QUESTION 105
- (Exam Topic 4)
You have a Hyper-V host that contains the virtual machines shown in the following table.

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

On which virtual machines can you install Windows 11?

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

Answer: E

NEW QUESTION 109
- (Exam Topic 4)
You have a Microsoft 365 E5 subscription that uses Microsoft Intune.
You add apps to Intune as shown in the following table.

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

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

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

Answer: D

NEW QUESTION 113
- (Exam Topic 4)
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.

Answer: BCF

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. References: How to Enable WinRM via Group Policy, Installation and configuration for Windows Remote Management

NEW QUESTION 115
- (Exam Topic 4)
You have a Microsoft 365 subscription.
You use Microsoft Intune Suite to manage devices.
You have the iOS app protection policy shown in the following exhibit.

Access requirements

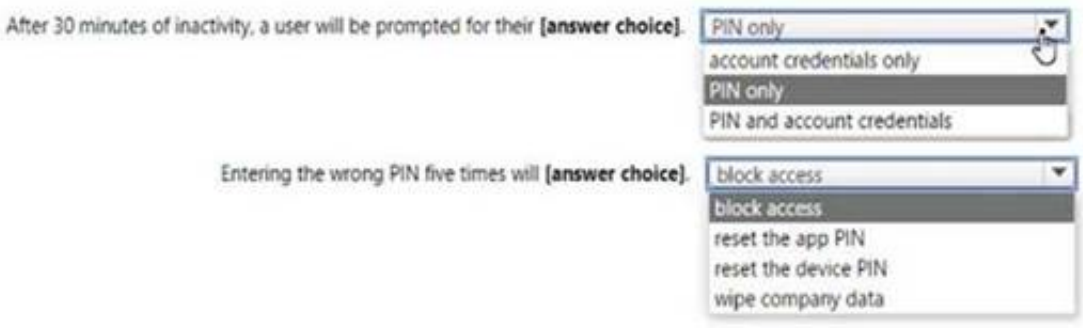
PIN for access	Require
PIN type	Numeric
Simple PIN	Allow
Select minimum PIN length	6
Touch ID instead of PIN for access (iOS 8+/iPadOS)	Allow
Override biometrics with PIN after timeout	Require
Timeout (minutes of inactivity)	30
Face ID instead of PIN for access (iOS 11+/iPadOS)	Block
PIN reset after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

Conditional launch

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

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

Answer Area



A. Mastered
B. Not Mastered

Answer: A

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

NEW QUESTION 119
- (Exam Topic 4)
You have devices that are not rooted enrolled in Microsoft Intune as shown in the following table.

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

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

Answer Area

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

A. Mastered
B. Not Mastered

Answer: A

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

- Device1 is marked as noncompliant because it is rooted and the device compliance policy Policy1 blocks rooted devices under the Device health setting1.
- Device2 is marked as compliant because it is not rooted and it is within the network location Network1 that is specified in the device compliance policy Policy11.
- Device3 is marked as noncompliant because it is outside the network location Network1 that is specified in the device compliance policy Policy11. The device compliance location setting requires devices to be in a specific network range to be compliant2.

NEW QUESTION 124
- (Exam Topic 4)
You have an Azure Active Directory (Azure AD) tenant that contains the users shown in the following table.

Name	Member of
User1	Group1
User2	Group2

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

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

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

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

A. Mastered
B. Not Mastered

Answer: A

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

NEW QUESTION 125
- (Exam Topic 4)
You have a Microsoft 365 E5 subscription that contains 100 Windows 10 devices enrolled in Microsoft Intune. You need to create Endpoint security policies to meet the following requirements:

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

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

Answer Area

Manage

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

A. Mastered
B. Not Mastered

Answer: A

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

NEW QUESTION 128
- (Exam Topic 4)
Your network contains an on-premises Active Directory domain and an Azure AD tenant.
The Default Domain Policy Group Policy Object (GPO) contains the settings shown in the following table.

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

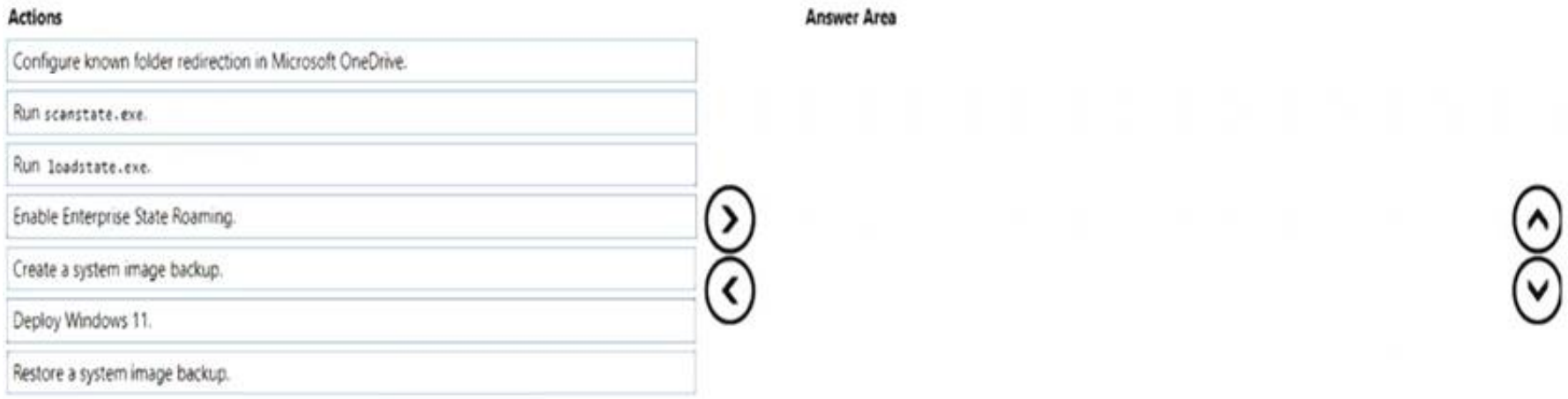
Which device configuration profile type template should you use?

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

Answer: A

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

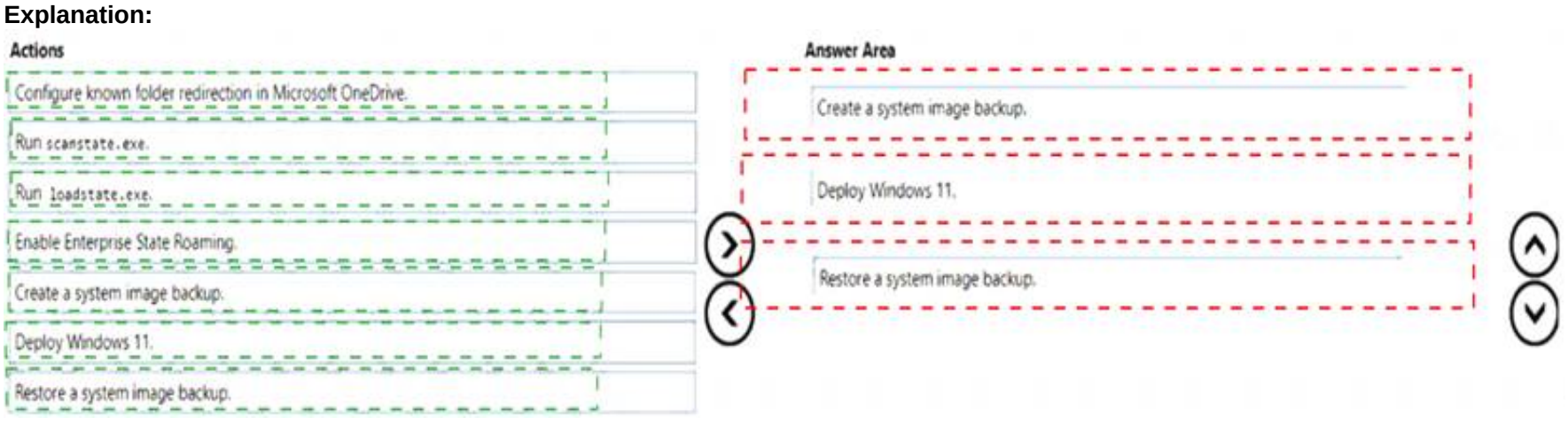
NEW QUESTION 131
- (Exam Topic 4)
You have 100 computers that run Windows 10.
You plan to deploy Windows 11 to the computers by performing a wipe and load installation. You need to recommend a method to retain the user settings and the user data.
Which three actions should you recommend be performed in sequence? To answer, move the appropriate actions from the list of actions to the answer area and arrange them in the correct order.



A. Mastered
B. Not Mastered

Answer: A

Explanation:



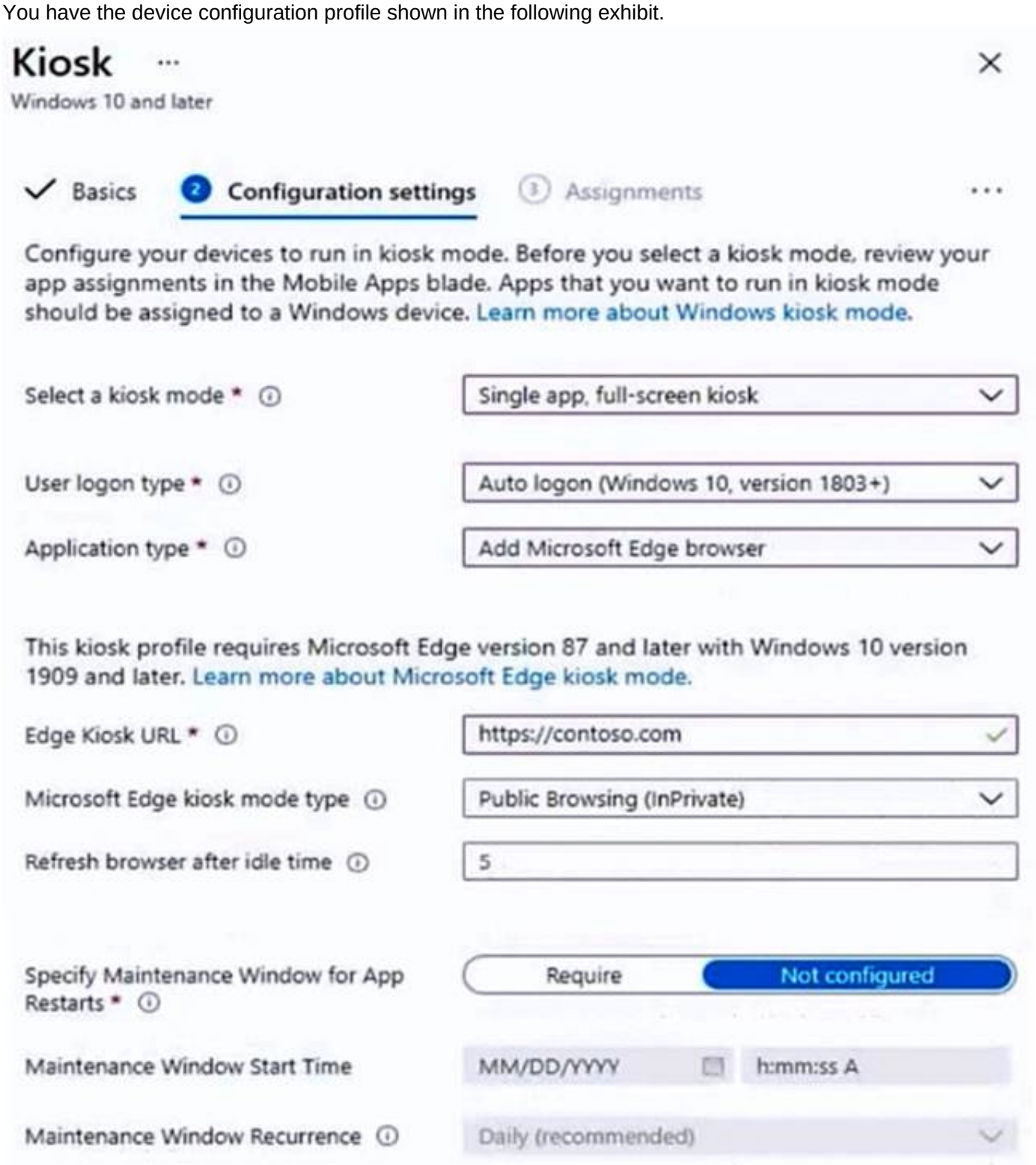
NEW QUESTION 135
- (Exam Topic 4)
Your network contains an Active Directory domain. The domain contains a computer named Computer! that runs Windows 11. You need to enable the Windows Remote Management (WinRM) service on Computer1 and perform the following configurations:
• For the WinRM service, set Startup type to Automatic.
• Create a listener that accepts requests from any IP address.
• Enable a firewall exception for WS-Management communications. Which PowerShell cmdlet should you use?

A. Connect-WSMan
B. Enable-PSRemoting
C. Invoke-WSManAction

D. Enable-PSSessionConfiguration

Answer: B

NEW QUESTION 137
- (Exam Topic 4)
You have the device configuration profile shown in the following exhibit.



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

Answer Area

Users	can access any URL. cannot view the address bar in Microsoft Edge. can only access URLs that include contoso.com. can only access URLs that start with https://contoso.com/ .
Windows 10 devices can have	a single Microsoft Edge instance that has a single tab. a single Microsoft Edge instance that has multiple tabs. multiple Microsoft Edge instances that have multiple tabs. multiple Microsoft Edge instances that each has a single tab.

A. Mastered
B. Not Mastered

Answer: A

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

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

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

NEW QUESTION 141
- (Exam Topic 4)
You have a Microsoft 365 subscription that includes Microsoft Intune. You have computers that run Windows 11 as shown in the following table.

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

You have the groups shown in the following table.

Name	Members
Group1	Computer1, Computer2
Group2	Computer3

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

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

The next day, you review the compliance status of the computers.
For each of the following statements, select Yes if the statement is true. Otherwise, select No. NOTE: Each correct selection is worth one point.

Answer Area

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

A. Mastered
B. Not Mastered

Answer: A

Explanation:

Answer Area

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

NEW QUESTION 142
- (Exam Topic 4)
Your company standardizes on Windows 10 Enterprise for all users.
Some users purchase their own computer from a retail store. The computers run Windows 10 Pro.
You need to recommend a solution to upgrade the computers to Windows 10 Enterprise, join the computers to Azure AD, and install several Microsoft Store apps. The solution must meet the following
requirements:
• Ensure that any applications installed by the users are retained.

• Minimize user intervention.
What is the best recommendation to achieve the goal? More than one answer choice may achieve the goal. Select the BEST answer.

A. Windows Autopilot
B. Microsoft Deployment Toolkit (MDT)
C. a Windows Configuration Designer provisioning package
D. Windows Deployment Services (WDS)

Answer: A

NEW QUESTION 144
- (Exam Topic 4)
You have a Microsoft 365 subscription that contains a user named User1. User! is assigned a Windows 10/11 Enterprise E3 license. You use Microsoft Intune Suite to manage devices. User1 activates the following devices:
• Device1: Windows 11 Enterprise
• Device2: Windows 10 Enterprise
• Device3: Windows 11 Enterprise
How many more devices can User1 activate?

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

Answer: A

NEW QUESTION 147
- (Exam Topic 4)
Your network contains an Active Directory domain named contoso.com. The domain contains a computer named Computer1 that runs Windows 10. You have the groups shown in the following table.

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

Which groups can you add to Group4?

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

Answer: C

NEW QUESTION 149
.....

Thank You for Trying Our Product

We offer two products:

1st - We have Practice Tests Software with Actual Exam Questions

2nd - Questons and Answers in PDF Format

MD-102 Practice Exam Features:

* MD-102 Questions and Answers Updated Frequently

* MD-102 Practice Questions Verified by Expert Senior Certified Staff

* MD-102 Most Realistic Questions that Guarantee you a Pass on Your FirstTry

* MD-102 Practice Test Questions in Multiple Choice Formats and Updatesfor 1 Year

100% Actual & Verified — Instant Download, Please Click
Order The MD-102 Practice Test Here