2passeasy

Exam Questions MD-102

Endpoint Administrator

https://www.2passeasy.com/dumps/MD-102/

NEW QUESTION 1
- (Exam Topic 4)
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

Answer: A

NEW QUESTION 2
- (Exam Topic 4)
You have a Microsoft 365 subscription that contains 100 devices enrolled in Microsoft Intune. You need to review the startup processes and how often each device restarts.
What should you use?

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

Answer: B

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

≫ The configuration must be managed from a central location.

≫ Internet traffic must be minimized.

≫ Costs must be minimized.

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

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

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

Manage the traffic by using:	Delivery Optimization
	BranchCache
	Peer cache

A. Mastered
B. Not Mastered

Answer: A

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

NEW QUESTION 4

- (Exam Topic 4)
You have an Azure AD tenant named contoso.com.
You need to ensure that users are not added automatically to the local Administrators group when they join their Windows 11 device to contoso.com.
What should you configure?

A. Windows Autopilot
B. provisioning packages for Windows
C. Security defaults in Azure AD
D. Device settings in Azure AD

Answer: D

Explanation:
To ensure that users are not added automatically to the local Administrators group when they join their Windows 11 device to contoso.com, you should configure the Device settings in Azure AD. The Device settings allow you to manage which users can join devices to Azure AD and whether they are added as local administrators or standard users. By default, users who join devices to Azure AD are added to the local Administrators group, but you can change this setting to None or Selected1.
The other options are not relevant for this scenario because:

≫   Windows Autopilot is a service that allows you to pre-configure new devices and enroll them automatically to Azure AD and Microsoft Intune. It does not control the local administrator role of the users who join the devices2.

≫   Provisioning packages for Windows are files that contain custom settings and policies that can be applied to Windows devices during the setup process. They do not affect the Azure AD join process or the local administrator role of the users3.

≫   Security defaults in Azure AD are a set of basic identity security mechanisms that are enabled by default to protect your organization from common attacks. They do not include any settings related to device management or local administrator role4.
References: Manage device identities using the Microsoft Entra admin center, Windows Autopilot, Provisioning packages for Windows 10, What are security defaults?

NEW QUESTION 5
- (Exam Topic 4)
You have 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.

Answer Area
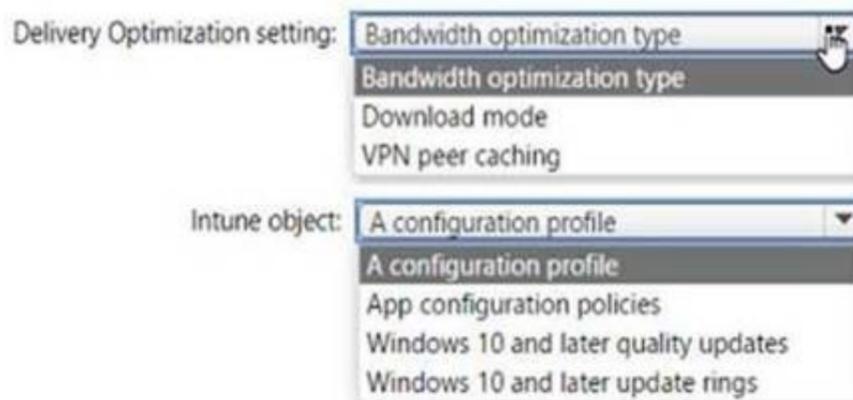
A. Mastered
B. Not Mastered

Answer: A

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. References: https://docs.microsoft.com/en-us/mem/intune/configuration/delivery-optimization-windows

NEW QUESTION 6
- (Exam Topic 4)
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.

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:

A. Mastered
B. Not Mastered

Answer: A

Explanation:

Settings

CNAME Validation

Co-management Settings

Deployment Profiles

Enrollment notifications

Enrollment Status Page

Answer Area

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

Join the devices to Azure AD: | Deployment Profiles |

NEW QUESTION 7
- (Exam Topic 4)
You have a Microsoft Intune subscription that is configured to use a PFX certificate connector to an on-premises Enterprise certification authority (CA).
You need to use Intune to configure autoenrollment for Android devices by using public key pair (PKCS) certificates.
Which three actions should you perform in sequence? To answer, move the appropriate actions from the list of actions to the answer area and arrange them in the correct order.

Actions

Obtain the root certificate.

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

From the Enterprise CA, configure certificate managers.

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

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

Answer Area

A. Mastered
B. Not Mastered

Answer: A

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

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

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

Answer: A

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

NEW QUESTION 9
- (Exam Topic 4)
Your network contains an on-premises Active Directory Domain Services {AD DS) domain that syncs with an Azure AD tenant by using Azure AD Connect.
You use Microsoft Intune and Configuration Manager to manage devices.
You need to recommend a deployment plan for new Windows 11 devices. The solution must meet the following requirements:
• Devices for the marketing department must be joined to the AD DS domain only. The IT department will install complex applications on the devices at build time, before giving the devices to the marketing department users.
• Devices for The sales department must be Azure AD joined. The devices will be shipped directly from the manufacturer to The homes of the sales department users.
• Administrative effort must be minimized.
Which deployment method should you recommend for each department? To answer, select the appropriate options in the answer area. NOTE: Each correct selection is worth one point.

A. Mastered
B. Not Mastered

Answer: A

Explanation:

NEW QUESTION 10
- (Exam Topic 4)
You have a Microsoft 365 E5 subscription that uses Microsoft Intune. You have the Windows 11 devices shown in the following table.

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

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

Basics Edit

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

Compliance settings Edit

Device Health

Require BitLocker	Require

Actions for noncompliance Edit

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

Scope tags Edit

Default

Assignments Edit

Included groups

Group
Group1
Group3

Excluded groups

Group
Group2

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

Answer Area

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

A. Mastered
B. Not Mastered

Answer: A

Explanation:

Answer Area

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

NEW QUESTION 10
- (Exam Topic 4)
You have a computer named Computer! that runs Windows 11.
A user named User1 plans to use Remote Desktop to connect to Computer1.
You need to ensure that the device of User1 is authenticated before the Remote Desktop connection is established and the sign in page appears.
What should you do on Computer1?

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

Answer: B

NEW QUESTION 11
- (Exam Topic 4)
You have a Microsoft 365 subscription that contains 1,000 iOS devices. The devices are enrolled in Microsoft Intune as follows:
• Two hundred devices are enrolled by using the Intune Company Portal.
• Eight hundred devices are enrolled by using Apple Automated Device Enrollment (ADE).
You create an iOS/iPadOS software updates policy named Policy 1 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.

Answer Area

Number of devices:
| 200 |
| 800 |
| 1000 |

Configure a:
| Compliance policy |
| Conditional Access policy |
| Device restriction policy |

A. Mastered
B. Not Mastered

Answer: A

Explanation:
Policy 1 will update 800 iOS devices that are enrolled by using Apple Automated Device Enrollment (ADE). This is because ADE devices are supervised devices that support software update policies in Intune1. Devices that are enrolled by using the Intune Company Portal are not supervised devices and do not support software update policies2.
To ensure that only iOS/iPadOS 15.5 is installed, you should configure a device restriction policy that restric visibility of software updates. This will prevent users from manually updating the OS to a newer version than the one you specified in Policy 11. You can use the Deployment Workbench to create and assign a device restriction profile to your ADE devices3.

NEW QUESTION 16
- (Exam Topic 4)
You have a Microsoft 365 subscription. All devices run Windows 10.
You need to prevent users from enrolling the devices in the Windows Insider Program.
What two configurations should you perform from the Microsoft Intune admin center? Each correct answer is a complete solution.
NOTE: Each correct selection is worth one point.

A. a device restrictions device configuration profile
B. an app configuration policy
C. a Windows 10 and later security baseline

D. a custom device configuration profile
E. a Windows 10 and later update ring

Answer: AE

NEW QUESTION 19
- (Exam Topic 4)
You have a Microsoft 365 E5 subscription.
You need to download a report that lists all the devices that are NOT enrolled in Microsoft Intune and are assigned an app protection policy.
What should you select in the Microsoft Endpoint Manager admin center?

A. App
B. and then App protection policies
C. App
D. and then Monitor
E. Devices, and then Monitor
F. Reports, and the Device compliance

Answer: A

Explanation:
App report: You can search by platform and app, and then this report will provide two different app protection statuses that you can select before generating the report. The statuses can be Protected or Unprotected.
Reference:
https://docs.microsoft.com/en-us/mem/intune/apps/app-protection-policies-monitor

NEW QUESTION 24
- (Exam Topic 4)
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

Answer: A

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. References: Configure Remote Desktop Connection Settings for Remote Desktop Gateway

NEW QUESTION 28
- (Exam Topic 4)
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.

Answer Area

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

A. Mastered
B. Not Mastered

Answer: A

Explanation:

Answer Area

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

NEW QUESTION 30
- (Exam Topic 4)
You have a Microsoft 365 E5 subscription that contains 1,000 Windows 11 devices. All the devices are enrolled in Microsoft Intune.
You plan to integrate Intune with Microsoft Defender for Endpoint.
You need to establish a service-to-service connection between Intune and Defender for Endpoint. Which settings should you configure in the Microsoft Endpoint Manager admin center?

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

Answer: A

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

NEW QUESTION 32
- (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.

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 ❶	User-Driven ⌄
* Join to Azure AD as ❶	Azure AD joined ⌄
Microsoft Software License Terms ❶	Show / **Hide**

Important information about hiding license terms

| Privacy settings ❶ | 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 ❶	Show / **Hide**
User account type ❶	Administrator / **Standard**
Allow White Glove OOBE ❶	**No** / Yes
Language (Region) ❶	Operating system default ⌄
Automatically configure keyboard ❶	No / **Yes**
Apply device name template ❶	**No** / Yes

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

Answer Area

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

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 35

- (Exam Topic 4)
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

Answer: C

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 least 1 GHz
clock speed and2 cores.

≫ A system firmware that supports UEFI
andSecure Boot.

≫ A Trusted Platform Module (TPM)
version2.0
or higher.

≫ At least 4 GB

≫ At least 64 GB
of system memory (RAM). of storage space.
In this scenario, the virtual machines that run Windows 10 have the following specifications:

≫ 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.

NEW QUESTION 39
- (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 42
- (Exam Topic 4)
You have a Microsoft 365 subscription that contains the devices shown in the following table.

Name	Type
Device1	Windows 10
Device2	iOS
Device3	Android Enterprise

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

Settings	Answer Area
Require BitLocker.	Device1: Setting
Prevent jailbroken devices from having corporate access.	Device2: Setting
Prevent rooted devices from having corporate access.	Device3: Setting
Require Secure Boot to be enabled on the device.	

A. Mastered
B. Not Mastered

Answer: A

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

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

Name	Type
Device1	Windows 10
Device2	iOS
Device3	Android Enterprise

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

Settings	Answer Area
Require BitLocker.	Device1:
Prevent jailbroken devices from having corporate access.	Device2:
Prevent rooted devices from having corporate access.	Device3:
Require Secure Boot to be enabled on the device.	

A. Mastered
B. Not Mastered

Answer: A

Explanation:

Settings	Answer Area
Require BitLocker.	Device1: [ ] Require BitLocker.
Prevent jailbroken devices from having corporate access.	Device2: [ ] Prevent jailbroken devices from having corporate access.
Prevent rooted devices from having corporate access.	Device3: [ ] Prevent rooted devices from having corporate access.
Require Secure Boot to be enabled on the device.	
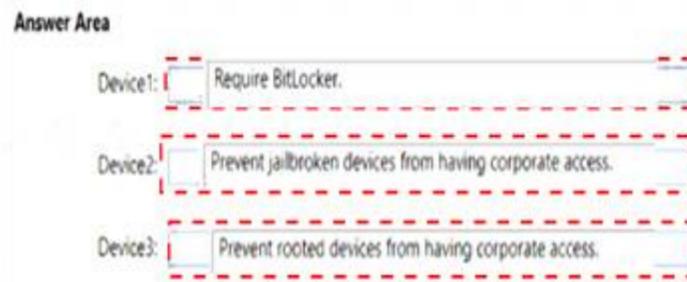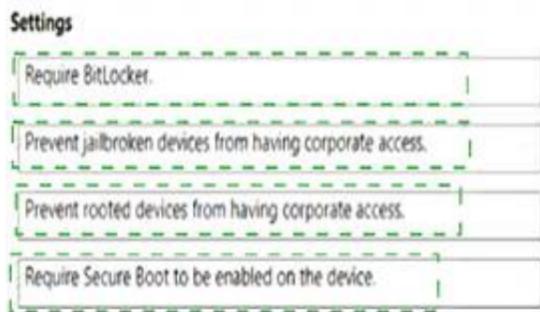
NEW QUESTION 46
- (Exam Topic 4)
Your network contains an Active Directory domain. The domain contains a computer named Computer1 that runs Windows 8.1.
Computer1 has apps that are compatible with Windows 10.
You need to perform a Windows 10 in-place upgrade on Computer1.
Solution: You copy the Windows 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 50
- (Exam Topic 4)
You have a Microsoft Intune deployment that contains the resources shown in the following table.

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

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

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

Answer: B

NEW QUESTION 53
- (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 58
- (Exam Topic 3)
You need to meet the requirements for the MKG department users. What should you do?

A. Assign the MKG department users the Purchaser role in Microsoft Store for Business
B. Download the APPX file for App1 from Microsoft Store for Business
C. Add App1 to the private store
D. Assign the MKG department users the Basic Purchaser role in Microsoft Store for Business
E. Acquire App1 from Microsoft Store for Business

Answer: E

Explanation:
 References:
https://docs.microsoft.com/en-us/microsoft-store/distribute-apps-from-your-private-store Enable the users in the MKG department to use App1.
The private store is a feature in Microsoft Store for Business and Education that organizations receive during the signup process. When admins add apps to the private store, all employees in the organization can view and download the apps. Your private store is available as a tab in Microsoft Store app, and is usually named for your company or organization. Only apps with online licenses can be added to the private store.
Reference:
https://docs.microsoft.com/en-us/microsoft-store/distribute-apps-from-your-private-store

NEW QUESTION 62
- (Exam Topic 3)
What is the maximum number of devices that User1 and User2 can enroll in Intune? To answer, select the appropriate options in the answer area.
NOTE: Each correct selection is worth one point.

User1 can enroll a maximum of:
- 5 devices
- 10 devices
- 15 devices
- 1,000 devices
- An unlimited number of devices

User2 can enroll a maximum of:
- 5 devices
- 10 devices
- 15 devices
- 1,000 devices
- An unlimited number of devices

A. Mastered
B. Not Mastered

Answer: A

Explanation:

User1 can enroll a maximum of:
- 5 devices
- 10 devices
- 15 devices
- 1,000 devices
- An unlimited number of devices

User2 can enroll a maximum of:
- 5 devices
- 10 devices
- 15 devices
- 1,000 devices
- An unlimited number of devices

NEW QUESTION 66
- (Exam Topic 3)
You need to meet the technical requirements for the iOS devices. Which object should you create in Intune?

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

Answer: D

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

NEW QUESTION 71
- (Exam Topic 2)
What should you upgrade before you can configure the environment to support co-management?

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

Answer: B

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

NEW QUESTION 73
- (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 77
- (Exam Topic 1)
You need to ensure that computer objects can be created as part of the Windows Autopilot deployment. The solution must meet the technical requirements.
To what should you grant the right to create the computer objects?

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

Answer: C

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

NEW QUESTION 80
- (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 81
- (Exam Topic 4)
You have computer that run Windows 10 and connect to an Azure Log Analytics workspace. The workspace is configured to collect all available events from Windows event logs. The computers have the logged events shown in the following table.

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

Which events are collected in the Log Analytics workspace?

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

Answer: E

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

NEW QUESTION 86
- (Exam Topic 4)
You have a Microsoft 365 E5 subscription.
You create an app protection policy for Android devices named Policy1 as shown in the following exhibit.

Home > Apps >

Create policy · · ·   ✕

✅ Basics   ② **Apps**   ① Data protection   ④ Access requirements   · · ·

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

Target to apps on all device types ⓘ   Yes   **No**

    Device types * ⓘ   Unmanaged   ⌄

Target policy to   All Apps   ⌄

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

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

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

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

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

| users only |
| devices only |
| users and devices |

A. Mastered
B. Not Mastered

Answer: A

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

NEW QUESTION 90
- (Exam Topic 4)
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 A
D. add an enterprise application.
E. From the Microsoft Intune admin center, add an app.

Answer: D

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. References:
https://docs.microsoft.com/en-us/mem/intune/apps/apps-win32-app-management

NEW QUESTION 95
- (Exam Topic 4)
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.
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.	○	○

A. Mastered
B. Not Mastered

Answer: A

Explanation:

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.	○	○

NEW QUESTION 99
- (Exam Topic 4)
You have two computers that run Windows 10. The computers are enrolled in Microsoft Intune as shown in the following table.

Name	Member of
Computer1	Group1
Computer2	Group1, Group2

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

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

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

Name	Include	Exclude
Ring1	Group1	Group2
Ring2	Group2	Group1

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

Quality deferral on Computer1:

| 3 days |
| 7 days |
| 10 days |
| 13 days |
| No effect |

Quality deferral on Computer2:

| 3 days |
| 7 days |
| 10 days |
| 13 days |
| No effect |

A. Mastered
B. Not Mastered

Answer: A

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

NEW QUESTION 103
- (Exam Topic 4)
You have a Microsoft 365 subscription that uses Microsoft Intune and contains the users shown in the following table.

Name	Member of	License
User1	Group1	None
User2	Group1	Microsoft 365 E3
User3	Group2	Microsoft 365 E5

Group2 has been assigned in the Enrollment Status Page. You have the devices shown in the following table.

Name	Operating system	Department
Device1	Windows 10 Pro	Marketing
Device2	Windows 11 Home	Research
Device3	Windows 10 Pro	Marketing

You capture and upload the hardware IDs of the devices in the marketing department. You configure Windows Autopilot.

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 complete the Autopilot process on Device1.		
User2 can complete the Autopilot process on Device1.		
User3 can view device setup information during the enrollment phase of Device1.		

A. Mastered
B. Not Mastered

Answer: A

Explanation:

Answer Area

Statements	Yes	No
User1 can complete the Autopilot process on Device1.		☐
User2 can complete the Autopilot process on Device1.	☐	
User3 can view device setup information during the enrollment phase of Device1.		☐

NEW QUESTION 104
- (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 109
- (Exam Topic 4)
You have groups that use the Dynamic Device membership type as shown in the following table.

Name	Syntax
Group1	(device.deviceOwnership -eq "Company")
Group2	(device.deviceOwnership -eq "Personal")

You are deploying Microsoft 365 apps.
You have devices enrolled in Microsoft Intune as shown in the following table.

Name	Ownership	Platform
LT1	Company	Windows 10 Enterprise x64
LT2	Personal	Windows 10 Enterprise x64
LT3	Company	MacOS Big Sur

In the Microsoft Endpoint Manager admin center, you create a Microsoft 365 Apps app as shown in the exhibit. (Click the Exhibit tab.)

App Information Edit

Name	Microsoft 365 Apps for Windows 10
Description	Microsoft 365 Apps for Windows 10
Publisher	Microsoft
Category	Productivity
Show this as a featured app in the Company Portal	No
Information URL	https://products.office.com/en-us/explore-office-for-home
Privacy URL	https://privacy.microsoft.com/en-US/privacystatement
Developer	Microsoft
Owner	Microsoft
Notes	...
Logo	Office
	Teams, Word
Architecture	64-bit
Update channel	Current Channel
Remove other versions	Yes
Version to install	Latest
Use shared computer activation	No
Accept the Microsoft Software License Teams on behalf of users	No
Install background service for Microsoft Search in Bing	No
Apps to be installed as part of the suite	1 language(s) selected

Assignments Edit

Group mode	Group
⌄ Required	
⊕ Included	Group1
Available for enrolled devices	

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
LT1 will have Microsoft Office 365 installed	○	○
LT2 will have Microsoft Office 365 installed	○	○
LT3 will have Microsoft Office 365 installed	○	○

A. Mastered
B. Not Mastered

Answer: A

Explanation:
Graphical user interface, text, application Description automatically generated
Reference:
https://docs.microsoft.com/en-us/mem/intune/apps/apps-add-office365
https://docs.microsoft.com/en-us/mem/intune/apps/apps-deploy https://docs.microsoft.com/en-us/mem/intune/apps/apps-add

NEW QUESTION 110
- (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 112
- (Exam Topic 4)
You have a Microsoft 365 subscription that uses Microsoft Intune Suite. You use Microsoft Intune to deploy and manage Windows devices.
You have 100 devices from users that left your company.
You need to repurpose the devices for new users by removing all the data and applications installed by the previous users. The solution must minimize administrative effort.
What should you do?

A. Deploy a new configuration profile to the devices.
B. Perform a Windows Autopilot reset on the devices.
C. Perform an in-place upgrade on the devices.
D. Perform a clean installation of Windows 11 on the devices.

Answer: B

NEW QUESTION 115
- (Exam Topic 4)
You have a Microsoft 365 subscription that contains a user named User1 and uses Microsoft Intune Suite. You use Microsoft Intune to manage devices that run Windows 11.
User1 provides remote support for 75 devices in the marketing department.
You need to add User1 to the Remote Desktop Users group on each marketing department device. What should you configure?

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

Answer: D

NEW QUESTION 117
- (Exam Topic 4)
You have a Microsoft 365 E5 subscription that contains the users shown in the following table.

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

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

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

Answer: B

Explanation:

* Admin1
An application admin has full access to enterprise applications, applications registrations, and application proxy settings.
* Admin2
Mark your app as publisher verified.
In Azure AD this user must be a member of one of the following roles: Application Admin, Cloud Application Admin, or Global Admin.
* Admin3
Office Apps admin - Assign the Office Apps admin role to users who need to do the following:
- Use the Office cloud policy service to create and manage cloud-based policies for Office
- Create and manage service requests
- Manage the What's New content that users see in their Office apps
- Monitor service health Reference:
Office Apps admin - Assign the Office Apps admin role to users who need to do the following https://docs.microsoft.com/en-us/azure/active-directory/develop/mark-app-as-publisher-verified

NEW QUESTION 120
- (Exam Topic 4)
You have an Azure AD tenant named contoso.com that contains a user named Used. User! has a user principal name (UPN) of user1@contoso.com.
You join a Windows 11 device named Client 1 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:
net localgroup Administrators /add "AzureAD\user1@contoso.com"
This command will add the Azure AD user with the UPN of user1@contoso.com to the local Administrators group of the device1. You need to use the AzureAD prefix and double backslashes to specify the user's domain2. You also need to enclose the user's name in quotation marks if it contains special characters like @1.
You can run this command from an elevated command prompt on Client1, or remotely by using PowerShell or other tools1. You can also use the Intune Role Administrator role or the Additional local administrators on all Azure AD joined devices setting to manage the local administrators group on Azure AD joined devices34.

NEW QUESTION 125
- (Exam Topic 4)
You have an Azure AD tenant named contoso.com that contains the devices shown in the following table.

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

AH devices contain an app named App1 and are enrolled in Microsoft Intune.
You need to prevent users from copying data from App1 and pasting the data into other apps.
Which type of policy and how many policies should you create in Intune? To answer, select the appropriate options in the answer area.
NOTE: Each correct selection is worth one point.

Answer Area

A. Mastered
B. Not Mastered

Answer: A

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

NEW QUESTION 129
- (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 131
- (Exam Topic 4)
You have a Microsoft 365 subscription that uses Microsoft Intune Suite. You use Microsoft Intune to manage devices.
Auto-enrollment in Intune is configured.
You have 100 Windows 11 devices in a workgroup.
You need to connect the devices to the corporate wireless network and enroll 100 new Windows devices in Intune.
What should you use?

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

Answer: C

NEW QUESTION 133
- (Exam Topic 4)
You have a Microsoft 365 E5 subscription.
You create a new update rings policy named Policy1 as shown in the following exhibit.

Update ring settings Edit

Update settings

Microsoft product updates	Allow
Windows drivers	Allow
Quality update deferral period (days)	0
Feature update deferral period (days)	30
Upgrade Windows 10 devices to Latest Windows 11 release	No
Set feature update uninstall period (2 - 60 days)	10
Servicing channel	General Availability channel

User experience settings

Automatic update behavior	Auto install at maintenance time
Active hours start	8 AM
Active hours end	5 PM
Restart checks	Allow
Option to pause Windows updates	Enable
Option to check for Windows updates	Enable
Change notification update level	Use the default Windows Update notifications
Use deadline settings	Allow
Deadline for feature updates	30
Deadline for quality updates	0
Grace period	0
Auto reboot before deadline	No

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

Answer Area

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

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

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

1 day	▼
1 day	
30 days	
60 days	

A. Mastered
B. Not Mastered

Answer: A

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

NEW QUESTION 135
- (Exam Topic 4)
You have a Microsoft 365 subscription that contains 1,000 Android devices enrolled in Microsoft Intune. You create an app configuration policy that contains the following settings:
• Device enrollment type: Managed devices

• Profile Type: All Profile Types
• Platform: Android Enterprise
Which two types of apps can be associated with the policy? Each correct answer presents a complete solution. NOTE: Each correct selection is worth one point.

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

Answer: BD

NEW QUESTION 136
- (Exam Topic 4)
You have a Microsoft 365 tenant that contains the objects shown in the following table. You are creating a compliance policy named Compliance1.
Which objects can you specify in Compliance1 as additional recipients of noncompliance notifications?

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

Answer: C

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

NEW QUESTION 139
- (Exam Topic 4)
You have a Microsoft 365 tenant that contains the objects shown in the following table.

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

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

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

Answer: C

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

NEW QUESTION 143
- (Exam Topic 4)
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

Answer: C

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. References: Windows subscription activation, Deploy Windows Enterprise
licenses

NEW QUESTION 145
- (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 150
- (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 152
- (Exam Topic 4)
Your company has a computer named Computer1 that runs Windows 10. Computed was used by a user who left the company.
You plan to repurpose Computer1 and assign the computer to a new user. You need to redeploy Computer1 by using Windows Autopilot.
Which three actions should you perform in sequence? To answer, move the appropriate actions from the list of actions to the answer area and arrange them in the correct order.

A. Mastered
B. Not Mastered

Answer: A

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

➢ Generate a JSON file that contains the computer information. This file specifies the Autopilot profile to be applied during the deployment. You can use the Get-AutopilotProfilesForExistingDevices PowerShell script to generate this file1.

⟫ Reset the computer. You can use the Windows Automatic Redeployment feature to trigger a reset from the login screen by pressing Ctrl + R and providing an administrator account2. Alternatively, you can use the Windows Autopilot Reset feature to remotely reset the device from Intune1.

⟫ Upload the file by running azcopy.exe. This step copies the JSON file to a blob storage account in Azure, where it can be accessed by the device during the deployment. You need to specify the storage account name, access key, and container name as parameters for azcopy.exe1.

NEW QUESTION 157
- (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 160
- (Exam Topic 4)
You have a Microsoft 365 E5 subscription that contains the groups shown in the following table.

Name	Description
Group1	Azure AD group that contains a user named User1
Group2	Azure AD group that contains iOS devices

You create a Conditional Access policy named CAPolicy1 that will block access to Microsoft Exchange Online from iOS devices. You assign CAPolicy1 to Group1.
You discover that User1 can still connect to Exchange Online from an iOS device. You need to ensure that CAPolicy1 is enforced.
What should you do?

A. Configure a new terms of use (TOU).
B. Assign CAPolicy1 to Group2.
C. Enable CAPolicy1
D. Add a condition in CAPolicy1 to filter for devices.

Answer: B

Explanation:
Common signals that Conditional Access can take in to account when making a policy decision include the following signals:
* User or group membership
Policies can be targeted to specific users and groups giving administrators fine-grained control over access.
* Device

Users with devices of specific platforms or marked with a specific state can be used when enforcing Conditional Access policies.
Use filters for devices to target policies to specific devices like privileged access workstations.
* Etc.
Reference: https://learn.microsoft.com/en-us/azure/active-directory/conditional-access/overview

NEW QUESTION 161
- (Exam Topic 4)
You have a Microsoft 365 subscription that contains 500 Android Enterprise devices. All the devices are enrolled in Microsoft Intune.
You need to deliver bookmarks to the Chrome browser on the devices What should you create?

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

Answer: D

NEW QUESTION 162
- (Exam Topic 4)
You have an Azure AD tenant named contoso.com. You have the devices shown in the following table.

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

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

Answer Area

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

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

A. Mastered
B. Not Mastered

Answer: A

Explanation:

Answer Area

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

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

NEW QUESTION 163
- (Exam Topic 4)
You have the device configuration profile shown in the following exhibit.

Kiosk ...

Windows 10 and later

✓ Basics   ② Configuration settings   ③ Assignments   ...

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

Select a kiosk mode * ⓘ	Single app, full-screen kiosk ⌄
User logon type * ⓘ	Auto logon (Windows 10, version 1803+) ⌄
Application type * ⓘ	Add Microsoft Edge browser ⌄

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

Edge Kiosk URL * ⓘ	https://contoso.com ✓
Microsoft Edge kiosk mode type ⓘ	Public Browsing (InPrivate) ⌄
Refresh browser after idle time ⓘ	5
Specify Maintenance Window for App Restarts * ⓘ	Require / **Not configured**
Maintenance Window Start Time	MM/DD/YYYY 🗓 / h:mm:ss A
Maintenance Window Recurrence ⓘ	Daily (recommended) ⌄

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

Answer Area

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

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

A. Mastered
B. Not Mastered

Answer: A

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

❯ Kiosk mode: Enabled

> Kiosk type: Multi-app

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

> Address bar: Disabled

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

NEW QUESTION 164
- (Exam Topic 4)
You have computers that run Windows 10 and are managed by using Microsoft Intune. Users store their files in a folder named D:\Folder1.
You need to ensure that only a trusted list of applications is granted write access to D:\Folder1. What should you configure in the device configuration profile?

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

Answer: A

NEW QUESTION 169
- (Exam Topic 4)
You have a Microsoft 365 subscription.
Users have iOS devices that are not enrolled in Microsoft 365 Device Management.
You create an app protection policy for the Microsoft Outlook app as shown in the exhibit. (Click the Exhibit tab.)
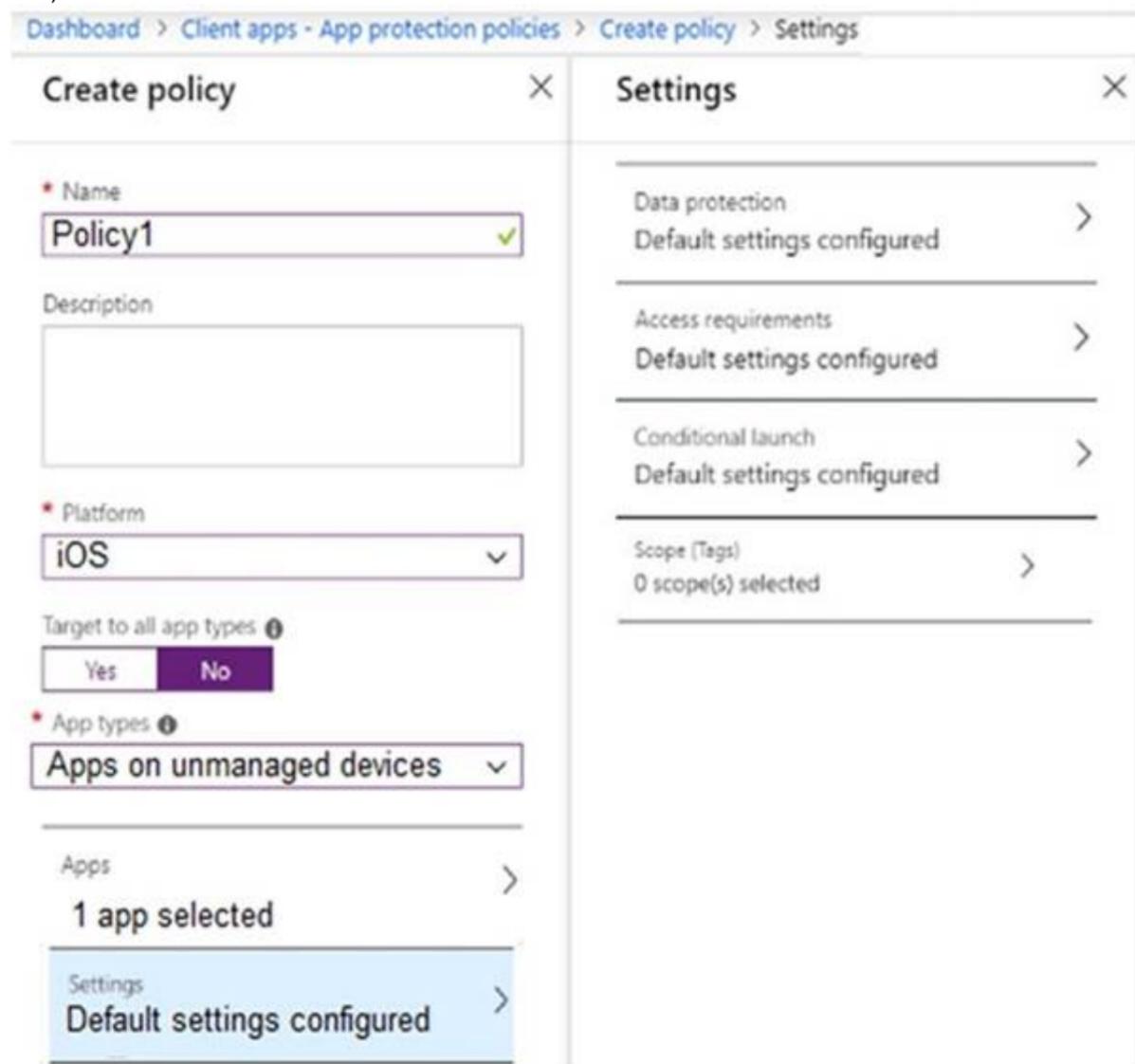
You need to configure the policy to meet the following requirements:

> Prevent the users from using the Outlook app if the operating system version is less than 12.0.0.

> Require the users to use an alphanumeric passcode to access the Outlook app.

What should you configure in an app protection policy for each requirement? To answer, select the appropriate options in the answer area.
NOTE: Each correct selection is worth one point.

Answer Area

Prevent the users from using Outlook if the operating system version is less than 12.0.0:

▼
Access requirements
Conditional launch
Data protection
Scope

Require the users to use an alphanumeric passcode to access Outlook:

▼
Access requirements
Conditional launch
Data protection
Scope

A. Mastered
B. Not Mastered

Answer: A

Explanation:
References:
https://docs.microsoft.com/en-us/intune/app-protection-policy-settings-ios

NEW QUESTION 171
- (Exam Topic 4)
You have a Microsoft Deployment Toolkit (MDT) deployment share named DS1.
in the Out-of-Box Drivers node, you create folders that contain drivers for different hardware models.
You need to configure the Inject Drivers MDT task to use PnP detection to install the drivers for one of the hardware models.
What should you do first?

A. Import an OS package.
B. Create a selection profile.
C. Add a Gather task to the task sequence.
D. Add a Validate task to the task sequence.

Answer: B

NEW QUESTION 175
- (Exam Topic 4)
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.

Answer: B

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. References: [Enable tamper protection]

NEW QUESTION 179
- (Exam Topic 4)
Your network contains an on-premises Active Directory Domain Services (AD DS) domain that syncs with an Azure AD tenant. The tenant contains the users shown in the following table.

Name	Member of	On-premises sync
User1	Group1	Disabled
User2	Group2	Enabled

You assign Windows 10/11 Enterprise E5 licenses to Gtoup1 and Uset2. You deploy the devices shown in the following table.

Name	Operating system	Joined to
Device1	Windows 11 Pro	Azure AD
Device2	Windows 11 Pro	AD DS
Device3	Windows 10 Pro	Azure AD

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

Answer Area

Statements	Yes	No
If User1 signs in to Device1, Device1 is upgraded to Windows 11 Enterprise automatically.		
If User2 signs in to Device2, Device2 is upgraded to Windows 11 Enterprise automatically.		
If User2 signs in to Device3, Device3 is upgraded to Windows 11 Enterprise automatically.		

A. Mastered
B. Not Mastered

Answer: A

Explanation:

Answer Area

Statements	Yes	No
If User1 signs in to Device1, Device1 is upgraded to Windows 11 Enterprise automatically.		☐
If User2 signs in to Device2, Device2 is upgraded to Windows 11 Enterprise automatically.	☐	
If User2 signs in to Device3, Device3 is upgraded to Windows 11 Enterprise automatically.		☐

NEW QUESTION 183
......

THANKS FOR TRYING THE DEMO OF OUR PRODUCT

Visit Our Site to Purchase the Full Set of Actual MD-102 Exam Questions With Answers.

We Also Provide Practice Exam Software That Simulates Real Exam Environment And Has Many Self-Assessment Features. Order the MD-102 Product From:

https://www.2passeasy.com/dumps/MD-102/

Money Back Guarantee

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