

Microsoft

Exam Questions MD-102

Endpoint Administrator



NEW QUESTION 1

- (Exam Topic 4)

You have computers that run Windows 11 Pro. The computers are joined to Azure AD and enrolled in Microsoft Intune. You need to upgrade the computers to Windows 11 Enterprise. What should you configure in Intune?

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

Answer: D

NEW QUESTION 2

- (Exam Topic 4)

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

Name	Multi-factor authentication (MFA) status
User1	Disabled
User2	Enabled

You have the devices shown in the following table.

Name	Platform
Device1	Android
Device2	iOS

You have a Conditional Access policy named CAPolicy1 that has the following settings:

- Assignments
 - o Users or workload identities: User 1. User1
 - o Cloud apps or actions: Office 365 Exchange Online
 - o Conditions: Device platforms: Windows, iOS
- Access controls
 - o Grant Require multi-factor authentication

You have a Conditional Access policy named CAPolicy2 that has the following settings:

- Assignments
 - o Users or workload identities: User2
 - o Cloud apps or actions: Office 365 Exchange Online
 - o Conditions
 - Device platforms: Android, iOS
 - Filter for devices
 - Device matching the rule: Exclude filtered devices from policy
 - Rule syntax: device.displayName- contains "1"
- Access controls Grant Block access

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

Answer Area

Statements	Yes	No
If User1 connects to Microsoft Exchange Online from Device1, the user is prompted for MFA.	<input type="radio"/>	<input type="radio"/>
If User2 connects to Microsoft Exchange Online from Device1, the user is prompted for MFA.	<input type="radio"/>	<input type="radio"/>
User2 can access Microsoft Exchange Online from Device2.	<input type="radio"/>	<input type="radio"/>

- A. Mastered
- B. Not Mastered

Answer: A

Explanation:

A screen shot of a computer Description automatically generated with low confidence

NEW QUESTION 3

- (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 BI

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 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.

Features	Answer Area
A device restriction policy	Enforces compliance: <input type="text"/>
A security baseline	Prevents suspicious scripts: <input type="text"/>
An attack surface reduction (ASR) rule	
An Intune connection	

- 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)

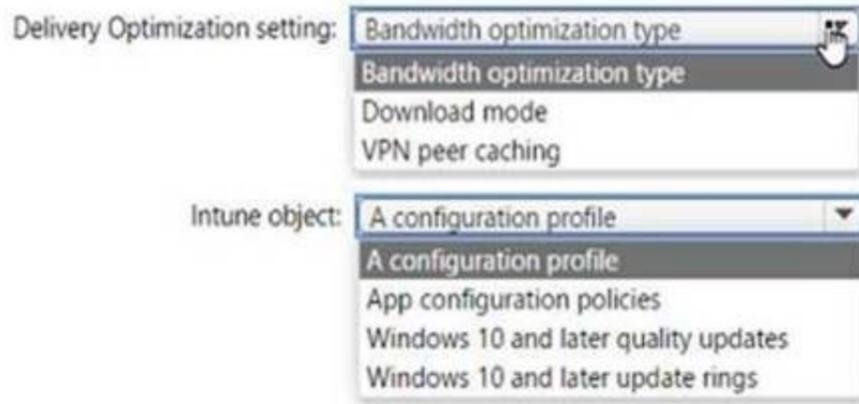
You have 100 Windows 10 devices enrolled in Microsoft Intune.

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 contains the devices shown in the following table.

Name	Platform
Device1	Windows 10
Device2	iOS

You plan to enroll the devices in Microsoft Intune.

How often will the compliance policy check-ins run after each device is enrolled in Intune? To answer, select the appropriate options in the answer area.

NOTE: Each correct selection is worth one point.

Device1:

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

Device2:

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

- A. Mastered
- B. Not Mastered

Answer: A

Explanation:

Box 1: Every three minutes for 15 minutes, then every 15 minutes for two hours, and then around every eight hours

If devices recently enroll, then the compliance, non-compliance, and configuration check-in runs more frequently. The check-ins are estimated at:

Windows 10: Every 3 minutes for 15 minutes, then every 15 minutes for 2 hours, and then around every 8 hours

Graphical user interface, text, application, email Description automatically generated

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

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

NEW QUESTION 7

- (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:

Configure a:

- 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 restrict 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 8

- (Exam Topic 4)

You have a computer that runs Windows 10 and contains two local users named User1 and User2. You need to ensure that the users can perform the following actions:

- 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 9

- (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 iOS/iPadOS update profile as shown in the following exhibit.

Create profile

iOS/iPadOS

- Basics
- Update policy settings
- Assignments
- Review + create

Summary

Basics

Name Profile1
 Description --

Update policy settings

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

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

Assignments

Included groups

Group	Group Members
Group1	3 devices, 0 users

Excluded groups

Group	Group Members
Group2	1 devices, 0 users

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

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.	<input checked="" type="radio"/>	<input type="radio"/>
If an iPadOS update becomes available on Thursday at 2 AM, the update is installed on Device2 automatically on Thursday.	<input checked="" type="radio"/>	<input type="radio"/>
If an iPadOS update becomes available on Friday at 10 PM, the update is installed on Device3 automatically on Sunday.	<input checked="" type="radio"/>	<input type="radio"/>

- 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.	<input checked="" type="radio"/>	<input type="radio"/>
If an iPadOS update becomes available on Thursday at 2 AM, the update is installed on Device2 automatically on Thursday.	<input checked="" type="radio"/>	<input type="radio"/>
If an iPadOS update becomes available on Friday at 10 PM, the update is installed on Device3 automatically on Sunday.	<input checked="" type="radio"/>	<input type="radio"/>

NEW QUESTION 10
 - (Exam Topic 4)

Your company has 200 computers that run Windows 10. The computers are managed by using Microsoft Intune. Currently, Windows updates are downloaded without using Delivery Optimization. You need to configure the computers to use Delivery Optimization. What should you create in Intune?

- A. a device compliance policy
- B. a Windows 10 update ring
- C. a device configuration profile
- D. an app protection policy

Answer: C

NEW QUESTION 10

- (Exam Topic 4)

Your network contains an on-premises Active Directory Domain Services (AD DS) domain that syncs with an Azure AD tenant.

You have a Microsoft 365 subscription

You plan to use Windows Autopilot to deploy new Windows devices. You plan to create a deployment profile.

You need to ensure that The deployment meets the following requirements:

- Devices must be joined to AD DS regardless of their current working location.
 - Users in the marketing department must have a line-of-business (LOB) app installed during the deployment. The solution must minimize administrative effort.
- What should you do for each requirement? To answer, select the appropriate options in the answer area. NOTE: Each correct selection is worth one point.

Answer Area

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

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

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

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

- A. Mastered
- B. Not Mastered

Answer: A

Explanation:

Answer Area

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

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

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

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

NEW QUESTION 15

- (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 20

- (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, and VM3

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 and 2 cores.
- A system firmware that supports UEFI and Secure Boot.
- A Trusted Platform Module (TPM) version 2.0 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 25

- (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 modify the User settings and the Device settings. Does this meet the goal?

- A. Yes
- B. No

Answer: B

NEW QUESTION 26

- (Exam Topic 4)

You have a Microsoft 365 subscription.

You plan to enroll devices in Microsoft Endpoint Manager that have the platforms and versions shown in the following table.

Platform	Version
Android	8, 9
iOS	11, 12

You need to configure device enrollment to meet the following requirements:

- Ensure that only devices that have approved platforms and versions can enroll in Endpoint Manager.
- Ensure that devices are added to Microsoft Azure Active Directory (Azure AD) groups based on a selection made by users during the enrollment.

Which device enrollment setting should you configure for each requirement? To answer, select the appropriate options in the answer area.

NOTE: Each correct selection is worth one point.

Answer Area

Ensure that only devices that have approved platforms and versions can enroll in Endpoint Manager:

▼
Android enrollment
Apple enrollment
Corporate device identifiers
Device categories
Enrollment restrictions
Windows enrollment

Ensure that devices are added to Azure AD groups based on a selection made by users during enrollment:

▼
Android enrollment
Apple enrollment
Corporate device identifiers
Device categories
Enrollment restrictions
Windows enrollment

- A. Mastered
- B. Not Mastered

Answer: A

Explanation:

A screenshot of a computer Description automatically generated

Reference:

<https://docs.microsoft.com/en-us/mem/intune/enrollment/enrollment-restrictions-set> <https://docs.microsoft.com/en-us/mem/intune/enrollment/device-group-mapping>

NEW QUESTION 28

- (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 ⓘ

Block Office applications from creating executable content ⓘ

Block all Office applications from creating child processes ⓘ

Block Win32 API calls from Office macro ⓘ

Block execution of potentially obfuscated scripts (js/vbs/ps) ⓘ

Edit profile

Attack Surface Reduction Rules

- Block credential stealing from the Windows local security authority subsystem (lsass.exe) ⓘ
- Block Adobe Reader from creating child processes ⓘ
- Block Office applications from injecting code into other processes ⓘ
- Block Office applications from creating executable content ⓘ
- Block all Office applications from creating child processes ⓘ
- Block Win32 API calls from Office macro ⓘ

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

Block Office applications from creating executable content:

Audit mode

Block

Disable

Warn

Block Win32 API calls from Office macro:

Audit mode

Block

Disable

Warn

- A. Mastered
- B. Not Mastered

Answer: A

Explanation:

Answer Area

Block Office applications from creating executable content:

Audit mode

Block

Disable

Warn

Block Win32 API calls from Office macro:

Audit mode

Block

Disable

Warn

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 31

- (Exam Topic 4)

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

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

Answer: D

NEW QUESTION 34

- (Exam Topic 4)

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

Name	Type
Device1	Windows 10
Device2	iOS
Device3	Android Enterprise

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

Settings

- Require BitLocker.
- Prevent jailbroken devices from having corporate access.
- Prevent rooted devices from having corporate access.
- Require Secure Boot to be enabled on the device.

Answer Area

Device1:

Device2:

Device3:

- 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-ios>

NEW QUESTION 37

- (Exam Topic 4)

You have a Microsoft Deployment Toolkit (MDT) solution that is used to manage Windows 11 deployment tasks.

MDT contains the operating system images shown in the following table.

Name	Description
Image1.wim	Custom-built Windows 10 image that has preinstalled custom apps
Image2.wim	Custom-built Windows 10 image without apps
Install.wim	Default Windows 10 image

You need to perform a Windows 11 in-place upgrade on several computers that run Windows 10. From the Deployment Workbench, you open the New Task Sequence Wizard.

You need to identify which task sequence template and which operating system image to use for the task sequence. The solution must minimize administrative effort.

What should you identify? To answer, select the appropriate options in the answer area.

NOTE: Each correct selection is worth one point.

Answer Area

Task sequence template:

Standard Client Task Sequence

Standard Client Replace Task Sequence

Standard Client Upgrade Task Sequence

Operating system image:

Image1.wim

Image2.wim

Install.wim

- A. Mastered
- B. Not Mastered

Answer: A

Explanation:

Box 1: Standard Client Upgrade Task Sequence

Use Template: Standard Client Upgrade Task Sequence

In-place upgrade is the preferred method to use when migrating from Windows 10 to a later release of Windows 10, and is also a preferred method for upgrading from Windows 7 or 8.1 if you do not plan to significantly change the device's configuration or applications. MDT includes an in-place upgrade task sequence template that makes the process really simple.

Box 2: Install.wim

In-place upgrade differs from computer refresh in that you cannot use a custom image to perform the in-place upgrade. I

Reference:

<https://docs.microsoft.com/en-us/windows/deployment/deploy-windows-mdt/upgrade-to-windows-10-with-the>

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 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

- Require BitLocker.
- Prevent jailbroken devices from having corporate access.
- Prevent rooted devices from having corporate access.
- Require Secure Boot to be enabled on the device.

Answer Area

Device1:

Device2:

Device3:

- A. Mastered
- B. Not Mastered

Answer: A

Explanation:

Settings

- Require BitLocker.
- Prevent jailbroken devices from having corporate access.
- Prevent rooted devices from having corporate access.
- Require Secure Boot to be enabled on the device.

Answer Area

Device1:

Device2:

Device3:

NEW QUESTION 43

- (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 44

- (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
User1	Group1
User2	None
User3	None

You create a policy set named Set1 as shown in the exhibit. (Click the Exhibit tab.)

Device management [Edit](#)

Device configuration profiles (1)

Name	Platform	Profile Type
ConfigurationProfile1	Windows 10 and later	Device restrictions

Device compliance policies (1)

Name	Platform	Profile Type
CompliancePolicy1	Windows 10 and later	Windows 10 and later co...

Device enrollment [Edit](#)

Windows autopilot deployment profiles

No results

Enrollment status pages

No results.

Assignments [Edit](#)

Included groups

Excluded groups

All Users

Group1

You enroll devices in Intune as shown in the following table.

Name	Operating system	User
Device1	Windows 10	User1
Device2	Windows 11	User2
Device3	Android	User3

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 will have both ConfigurationProfile1 and CompliancePolicy1 assigned.	<input type="radio"/>	<input type="radio"/>
If User2 signs in to Device2, Device2 will have both ConfigurationProfile1 and CompliancePolicy1 assigned.	<input type="radio"/>	<input type="radio"/>
If User3 signs in to Device3, Device3 will have both ConfigurationProfile1 and CompliancePolicy1 assigned.	<input type="radio"/>	<input type="radio"/>

- A. Mastered
- B. Not Mastered

Answer: A

Explanation:

Answer Area

Statements	Yes	No
If User1 signs in to Device1, Device1 will have both ConfigurationProfile1 and CompliancePolicy1 assigned.	<input type="radio"/>	<input checked="" type="radio"/>
If User2 signs in to Device2, Device2 will have both ConfigurationProfile1 and CompliancePolicy1 assigned.	<input type="radio"/>	<input checked="" type="radio"/>
If User3 signs in to Device3, Device3 will have both ConfigurationProfile1 and CompliancePolicy1 assigned.	<input type="radio"/>	<input checked="" type="radio"/>

NEW QUESTION 49

- (Exam Topic 3)

You need to prepare for the deployment of the Phoenix office computers. What should you do first?

- A. Extract the hardware ID information of each computer to a CSV file and upload the file from the Devices settings in Microsoft Store for Business.
- B. Generalize the computers and configure the Mobility (MDM and MAM) settings from the Azure Active Directory blade in the Azure portal.
- C. Generalize the computers and configure the Device settings from the Azure Active Directory blade in the Azure portal.
- D. Extract the hardware ID information of each computer to an XLSX file and upload the file from the Devices settings in Microsoft Store for Business.

Answer: A

Explanation:

References:

<https://docs.microsoft.com/en-us/microsoft-store/add-profile-to-devices#manage-autopilot-deployment-profiles>

NEW QUESTION 50

- (Exam Topic 3)

To which devices do Policy1 and Policy2 apply? To answer, select the appropriate options in the answer area. NOTE: Each correct selection is worth one point.

Policy1:

<input type="checkbox"/>	Device1 only
<input type="checkbox"/>	Device2 only
<input type="checkbox"/>	Device3 only
<input type="checkbox"/>	Device4 only
<input type="checkbox"/>	Device2 and Device3 only
<input type="checkbox"/>	Device1 and Device3 only
<input type="checkbox"/>	Device1, Device2, and Device 3

Policy2:

<input type="checkbox"/>	Device1 only
<input type="checkbox"/>	Device2 only
<input type="checkbox"/>	Device3 only
<input type="checkbox"/>	Device4 only
<input type="checkbox"/>	Device2 and Device3 only
<input type="checkbox"/>	Device1 and Device3 only
<input type="checkbox"/>	Device1, Device2, and Device 3

- A. Mastered
- B. Not Mastered

Answer: A

Explanation:

Reference:

<https://docs.microsoft.com/en-us/intune/device-profile-assign>

NEW QUESTION 55

- (Exam Topic 3)

You need to meet the technical requirements for the IT department. What should you do first?

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

D. From the Microsoft Intune blade in the Azure portal, configure the Windows enrollment settings.

Answer: C

Explanation:

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

NEW QUESTION 58

- (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 63

- (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 67

- (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 72

- (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.

For the Research department employees:

<input checked="" type="checkbox"/>	An app configuration policy
<input checked="" type="checkbox"/>	An app protection policy
<input checked="" type="checkbox"/>	Azure information Protection
<input checked="" type="checkbox"/>	iOS app provisioning profiles

For the Sales department employees:

<input checked="" type="checkbox"/>	An app configuration policy
<input checked="" type="checkbox"/>	An app protection policy
<input checked="" type="checkbox"/>	Azure information Protection
<input checked="" type="checkbox"/>	iOS app provisioning profiles

- 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 75

- (Exam Topic 2)

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

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

Answer: B

Explanation:

References:

<https://docs.microsoft.com/en-us/windows/deployment/windows-autopilot/existing-devices>

"This topic describes how to convert Windows 7 or Windows 8.1 domain-joined computers to Windows 10 devices joined to either Azure Active Directory or Active Directory (Hybrid Azure AD Join) by using Windows Autopilot"

NEW QUESTION 79

- (Exam Topic 2)

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

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

Answer: B

Explanation:

Litware identifies the following device management requirements:

➤ Ensure that Microsoft Edge Favorites are accessible from all computers to which the developers sign in. Enterprise State Roaming allows for the synchronization of Microsoft Edge browser setting, including favorites and reading list, across devices.

Reference:

<https://docs.microsoft.com/en-us/azure/active-directory/devices/enterprise-state-roaming-windows-settings-refer>

NEW QUESTION 82

- (Exam Topic 1)

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

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

Answer: C

Explanation:

Scenario: Windows Autopilot Configuration Assignments

Included groups: Group1

Excluded groups: Group2 Device1 is member of Group1.

Device2 is member of Group1 and member of Group2. Device3 is member of Group1.

Group1 and Group2 have a Membership type of Assigned.

Exclusion takes precedence over inclusion in the following same group type scenarios. Reference: <https://learn.microsoft.com/en-us/mem/intune/apps/apps-inc-exl-assignments>

NEW QUESTION 85

- (Exam Topic 1)

Which users can purchase and assign App1?

- A. User3 only
- B. User1 and User3 only
- C. User1, User2, User3, and User4
- D. User1, User3, and User4 only
- E. User3 and User4 only

Answer: B

Explanation:

Reference:

<https://docs.microsoft.com/en-us/microsoft-store/acquire-apps-microsoft-store-for-business> <https://docs.microsoft.com/en-us/microsoft-store/assign-apps-to-employees>

NEW QUESTION 89

- (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 91

- (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

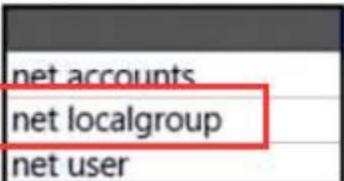
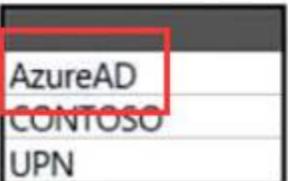
Administrators /add "  \user1@contoso.com" 

- A. Mastered
- B. Not Mastered

Answer: A

Explanation:

Answer Area

Administrators /add "  \user1@contoso.com" 

NEW QUESTION 92

- (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 97

- (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 98

- (Exam Topic 4)

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

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

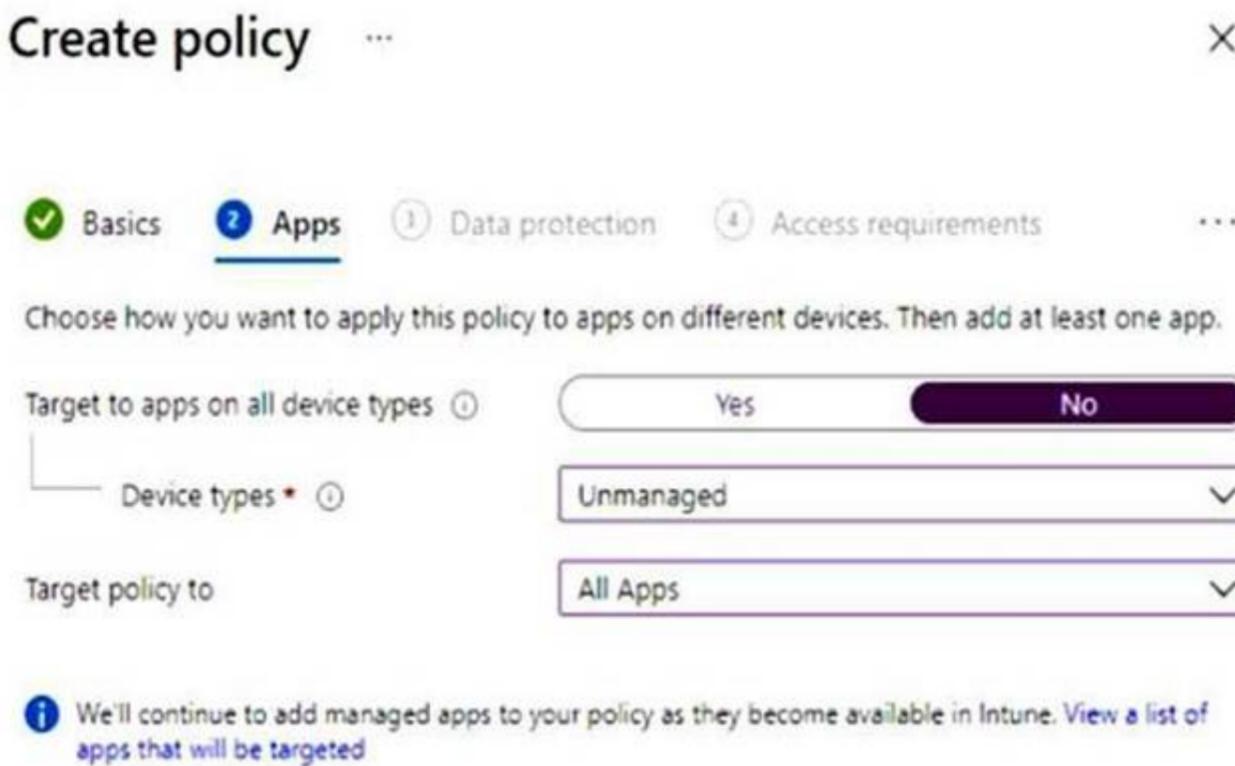
Answer: D

NEW QUESTION 102

- (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 [Close]

Basics
 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 * [v]

Target policy to [v]

i 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.

Box 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 103

- (Exam Topic 4)

You have a Microsoft 365 tenant that uses Microsoft Intune.

You use the Company Portal app to access and install published apps to enrolled devices. From the Microsoft Intune admin center, you add a Microsoft Store app.

Which two App information types are visible in the Company Portal? NOTE: Each correct selection is worth one point.

- A. Privacy URL
- B. Information URL
- C. Developer
- D. Owner

Answer: AC

NEW QUESTION 106

- (Exam Topic 4)

You have a Microsoft 365 E5 subscription that contains 100 Windows 10 devices enrolled in Microsoft Intune. You plan to use Endpoint analytics.

You need to create baseline metrics.

What should you do first?

- A. Create an Azure Monitor workbook.
- B. Onboard 10 devices to Endpoint analytics.
- C. Create a Log Analytics workspace.
- D. Modify the Baseline regression threshold.

Answer: C

Explanation:

Onboarding from the Endpoint analytics portal is required for Intune managed devices. Reference: <https://docs.microsoft.com/en-us/mem/analytics/enroll-intune>

NEW QUESTION 107

- (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 112

- (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.	<input type="checkbox"/>	<input type="checkbox"/>
User2 can complete the Autopilot process on Device1.	<input type="checkbox"/>	<input type="checkbox"/>
User3 can view device setup information during the enrollment phase of Device1.	<input type="checkbox"/>	<input type="checkbox"/>

- A. Mastered
- B. Not Mastered

Answer: A

Explanation:

Answer Area

Statements	Yes	No
User1 can complete the Autopilot process on Device1.	<input type="checkbox"/>	<input checked="" type="checkbox"/>
User2 can complete the Autopilot process on Device1.	<input checked="" type="checkbox"/>	<input type="checkbox"/>
User3 can view device setup information during the enrollment phase of Device1.	<input type="checkbox"/>	<input checked="" type="checkbox"/>

NEW QUESTION 115

- (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 118

- (Exam Topic 4)

You are replacing 100 company-owned Windows devices.

You need to use the Microsoft Deployment Toolkit (MDT) to securely wipe and decommission the devices. The solution must meet the following requirements:

- Back up the user state.
- Minimize administrative effort.

Which task sequence template should you use?

- A. Standard Client Task Sequence
- B. Standard Client Replace Task Sequence
- C. Litetouch OEM Task Sequence
- D. Sysprep and Capture

Answer: B

NEW QUESTION 123

- (Exam Topic 4)

Your company uses Microsoft Intune.

More than 500 Android and iOS devices are enrolled in the Intune tenant.

You plan to deploy new Intune policies. Different policies will apply depending on the version of Android or iOS installed on the device.

You need to ensure that the policies can target the devices based on their version of Android or iOS. What should you configure first?

- A. groups that have dynamic membership rules in Azure AD
- B. Device categories in Intune
- C. Corporate device identifiers in Intune
- D. Device settings in Azure AD

Answer: B

NEW QUESTION 124

- (Exam Topic 4)

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

You use Microsoft Intune to manage devices.

You need to ensure that the startup performance of managed Windows 11 devices is captured and available for review in the Intune admin center.

What should you configure?

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

Answer: D

NEW QUESTION 129

- (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 131

- (Exam Topic 4)

In Microsoft Intune, you have the device compliance policies shown in the following table.

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

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

Save Discard

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

Mark devices with no compliance policy assigned as Compliant Not Compliant

Enhanced jailbreak detection Enabled Disabled

Compliance status validity period (days) ✓

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

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

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

Answer Area

Statements	Yes	No
On June 4, Device1 is marked as compliant.	<input type="radio"/>	<input type="radio"/>
On June 6, Device1 is marked as compliant.	<input type="radio"/>	<input type="radio"/>
On June 9, Device2 is marked as compliant.	<input type="radio"/>	<input type="radio"/>

- A. Mastered
- B. Not Mastered

Answer: A

Explanation:

Device 1 is Windows 10 - and policy 1 is for Windows 8. Default compliance for devices without a policy is not compliant so first 2 questions are NO. Then the third device has 2 policies, the first one is compliant and the second policy is not compliant but the device is not marked as non-compliant due to the fact that mark device as non-compliant is set to 10 days. This means that the machine will be compliant until June 10th.

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

NEW QUESTION 133

- (Exam Topic 4)

You have a Microsoft 365 E5 subscription that contains a user named User1 and uses Microsoft Intune Suite. You use Microsoft Intune to manage devices. You have a device named Device1 that is enrolled in Intune.

You need to ensure that User1 can use Remote Help from the Intune admin center for Device1. Which three actions should you perform? Each correct answer presents part of the solution.

NOTE: Each correct selection is worth one point.

- A. Deploy the Remote Help app to Device1.
- B. Assign the Help Desk Operator role to User1.
- C. Assign the Intune Administrator role to User1.
- D. Assign a Microsoft 365 E5 license to User1.
- E. Rerun device onboarding on Device1.
- F. Assign the Remote Help add-on license to User1.

Answer: ABF

NEW QUESTION 138

- (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 139

- (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 142

- (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.

Create profile ...

Windows PC

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

Summary

Basics

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

Out-of-box experience (OOBE)

Deployment mode	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	Yes
Microsoft Software License Terms	Hide
Privacy settings	Hide
Hide change account options	Hide
User account type	Standard
Allow White Glove OOBE	No
Apply device name template	No

Assignments

Included groups	Group1
Excluded groups	--

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.	<input type="radio"/>	<input type="radio"/>
If Device2 starts in Out of Box Experience (OOBE) mode, the device will be deployed by using Autopilot.	<input type="radio"/>	<input type="radio"/>
If Device3 starts in Out of Box Experience (OOBE) mode, the device will be deployed by using Autopilot.	<input type="radio"/>	<input type="radio"/>

- 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 144

- (Exam Topic 4)

Your company implements Azure AD, Microsoft 365, Microsoft Intune, and Azure Information Protection. The company's security policy states the following:

- Personal devices do not need to be enrolled in Intune.
- Users must authenticate by using a PIN before they can access corporate email data.
- Users can use their personal iOS and Android devices to access corporate cloud services.
- Users must be prevented from copying corporate email data to a cloud storage service other than Microsoft OneDrive for Business.

You need to configure a solution to enforce the security policy. What should you create?

- A. a device configuration profile from the Microsoft Intune admin center
- B. a data loss prevention (DIP) policy from the Microsoft Purview compliance portal
- C. an insider risk management policy from the Microsoft Purview compliance portal
- D. an app protection policy from the Microsoft Intune admin center

Answer: B

NEW QUESTION 145

- (Exam Topic 4)

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

Name	Operating system	Azure AD join type
Device1	Windows 11 Pro	Joined
Device2	Windows 11 Pro	Registered
Device3	Windows 10 Pro	Joined
Device4	Windows 10 Pro	Registered

Which devices can be activated by using subscription activation?

- A. Device 1 only
- B. Device1 and Device2 only
- C. Device1 and Device3 only
- D. Device1, Device2, Device3, and Device4

Answer: C

NEW QUESTION 146

- (Exam Topic 4)

You have a Microsoft 365 subscription that contains 1,000 Windows 11 devices enrolled in Microsoft Intune. You plan to use Intune to deploy an application named App1 that contains multiple installation files.

What should you do first?

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

Answer: A

NEW QUESTION 150

- (Exam Topic 4)

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

Name	Member of
User1	Group1, Group2
User2	Group2
User3	Group3

Group2 and Group3 are members of Group1. All the users use Microsoft Excel.

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

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

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

Answer Area

Statements	Yes	No
When User1 saves a new spreadsheet, the .ods format is used.	<input type="radio"/>	<input type="radio"/>
When User2 saves a new spreadsheet, the .xlsb format is used.	<input type="radio"/>	<input type="radio"/>
When User3 saves a new spreadsheet, the .xlsx format is used.	<input type="radio"/>	<input type="radio"/>

- A. Mastered
- B. Not Mastered

Answer: A

Explanation:

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

NEW QUESTION 154

- (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 158

- (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, and Group4

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 163

- (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 165

- (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 170

- (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 173

- (Exam Topic 4)

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

- Requires BitLocker Drive Encryption (BitLocker) on each device
- Requires a minimum operating system version

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

NOTE: Each correct selection is worth one point.

Settings

Device Health

Device Properties

Microsoft Defender for Endpoint

System Security

Answer Area

Requires BitLocker:

Requires a minimum operating system version:

- A. Mastered
- B. Not Mastered

Answer: A

Explanation:

Settings

Device Health

Device Properties

Microsoft Defender for Endpoint

System Security

Answer Area

Requires BitLocker:

Requires a minimum operating system version:

NEW QUESTION 175

- (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 177

- (Exam Topic 4)

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

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

You purchase the devices shown in the following table.

Name	Type
Device1	Windows 10
Device2	Android

You configure automatic mobile device management (MDM) and mobile application management (MAM) enrollment by using the following settings:

- > MDM user scope: Group1
- > MAM user scope: Group2

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

NOTE: Each correct selection is worth one point.

Answer Area

Statements	Yes	No
If User1 registers Device1 in contoso.com, Device1 is enrolled automatically in Microsoft Intune.	<input type="radio"/>	<input type="radio"/>
If User1 joins Device1 to contoso.com, Device2 is enrolled automatically in Microsoft Intune.	<input type="radio"/>	<input type="radio"/>
If User2 registers Device3 in contoso.com, Device3 is enrolled automatically in Microsoft Intune.	<input type="radio"/>	<input type="radio"/>

- A. Mastered
- B. Not Mastered

Answer: A

Explanation:

Reference: <https://docs.microsoft.com/en-us/mem/intune/enrollment/android-enroll> <https://powerautomate.microsoft.com/fr-fr/blog/mam-flow-mobile/>

NEW QUESTION 181

- (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.	<input type="radio"/>	<input type="radio"/>
Device2 is marked as compliant.	<input type="radio"/>	<input type="radio"/>
Device3 is marked as compliant.	<input type="radio"/>	<input type="radio"/>

- 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 184

- (Exam Topic 4)

You use the Microsoft Deployment Toolkit (MDT) to manage Windows 11 deployments. From Deployment Workbench, you modify the WinPE settings and add PowerShell support. You need to generate a new set of WinPE boot image files that contain the updated settings. What should you do?

- A. From the Deployment Shares node, update the deployment share.
- B. From the Advanced Configuration node, create new media.
- C. From the Packages node, import a new operating system package
- D. From the Operating Systems node, import a new operating system.

Answer: A

NEW QUESTION 187

- (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.

Yes No

User2 receives Notification1 on Device2.

Yes No

User1 receives Notification1 on Device3.

Yes No

- 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 192

- (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 194

- (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



- A. Mastered
- B. Not Mastered

Answer: A

Explanation:

Answer Area



NEW QUESTION 199

- (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.

Actions	Answer Area
Configure known folder redirection in Microsoft OneDrive.	
Run scanstate.exe.	
Run loadstate.exe.	
Enable Enterprise State Roaming.	
Create a system image backup.	
Deploy Windows 11.	
Restore a system image backup.	

- A. Mastered
- B. Not Mastered

Answer: A

Explanation:

Actions	Answer Area
Configure known folder redirection in Microsoft OneDrive.	
Run scanstate.exe.	
Run loadstate.exe.	
Enable Enterprise State Roaming.	
Create a system image backup.	Create a system image backup.
Deploy Windows 11.	Deploy Windows 11.
Restore a system image backup.	Restore a system image backup.

NEW QUESTION 201

- (Exam Topic 4)

You use Microsoft Defender for Endpoint to protect computers that run Windows 10.

You need to assess the differences between the configuration of Microsoft Defender for Endpoint and the Microsoft-recommended configuration baseline.

Which tool should you use?

- A. Microsoft Defender for Endpoint Power 81 app
- B. Microsoft Secure Score
- C. Endpoint Analytics
- D. Microsoft 365 Defender portal

Answer: B

NEW QUESTION 203

- (Exam Topic 4)

You have a Microsoft Deployment Toolkit (MDT) deployment share named DS1. You import a Windows 11 image to DS1.

You have an executable installer for an application named App1.

You need to ensure that App1 will be installed for all the task sequences that deploy the image.

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

Actions	Answer Area
Modify a Windows 11 operating system setting.	
Modify a selection profile.	
Add App1 to DS1.	1 Add App1 to DS1.
Identify the GUID of App1.	2 Identify the GUID of App1.
Modify CustomSettings.ini.	3 Modify CustomSettings.ini.

- A. Mastered
- B. Not Mastered

Answer: A

Explanation:

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

- > Add App1 to DS1. You can use the Deployment Workbench to import the executable installer of App1 to a folder in your deployment share. This will create an application entry with a unique GUID that identifies App1.
- > Identify the GUID of App1. You can find the GUID of App1 by opening the application properties in the Deployment Workbench and looking at the Application GUID field. You can copy the GUID to use it later.
- > Modify CustomSettings.ini. You can edit the CustomSettings.ini file in your deployment share to specify which applications to install for each task sequence. You can use the Applications property to list the GUIDs of the applications you want to install, separated by commas. For example, if you want to install App1 and another application with GUID {1234-5678-90AB-CDEF}, you can use this line:
 Applications={GUID of App1},{1234-5678-90AB-CDEF}

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

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

- > [How to deploy applications with the Microsoft Deployment Toolkit](#)

NEW QUESTION 205

- (Exam Topic 4)

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

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

Answer: B

NEW QUESTION 206

- (Exam Topic 4)

You use Microsoft Endpoint Manager to manage Windows 10 devices. You are designing a reporting solution that will provide reports on the following:

- > Compliance policy trends
- > Trends in device and user enrolment
- > App and operating system version breakdowns of mobile devices

You need to recommend a data source and a data visualization tool for the design.

What should you recommend? To answer, select the appropriate options in the answer area. NOTE: Each correct selection is worth one point.

Answer Area

Data source:

Data visualization tool:

- A. Mastered
- B. Not Mastered

Answer: A

Explanation:

A screenshot of a computer Description automatically generated

Reference:

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

NEW QUESTION 210

- (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 212

- (Exam Topic 4)

You have a Microsoft 365 subscription that contains a user named User1. User1 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 215

- (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 217

- (Exam Topic 4)

You have a Microsoft 365 subscription that uses Microsoft Intune Suite. You use Microsoft Intune to manage devices.

You plan to create Windows 11 device builds for the marketing and research departments. The solution must meet the following requirements:

- Marketing department devices must support Windows Update for Business.
- Research department devices must have support for feature update versions for up to 36 months from release. What is the minimum Windows 11 edition required for each department? To answer, select the appropriate options in the answer area.

NOTE: Each correct selection is worth one point

Answer Area

Marketing:

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

Research:

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

- A. Mastered
- B. Not Mastered

Answer: A

Explanation:

Answer Area



NEW QUESTION 218

.....

Thank You for Trying Our Product

We offer two products:

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

2nd - Questions 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 First Try
- * MD-102 Practice Test Questions in Multiple Choice Formats and Updates for 1 Year

100% Actual & Verified — Instant Download, Please Click
[Order The MD-102 Practice Test Here](#)