

# Microsoft

## Exam Questions MD-102

Endpoint Administrator



### NEW QUESTION 1

- (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 2

- (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 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 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 Selected<sup>1</sup>.

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 devices<sup>2</sup>.
- 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 users<sup>3</sup>.
- 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 role<sup>4</sup>.

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 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 6**

- (Exam Topic 4)

You need to implement mobile device management (MDM) for personal devices that run Windows 11. The solution must meet the following requirements:

- Ensure that you can manage the personal devices by using Microsoft Intune.
- Ensure that users can access company data seamlessly from their personal devices.
- Ensure that users can only sign in to their personal devices by using their personal account What should you use to add the devices to Azure AD?

- A. Azure AD registered
- B. hybrid Azure AD join
- C. AD joined

**Answer:** A

**Explanation:**

To implement MDM for personal devices that run Windows 11, you should use Azure AD registered. Azure AD registered devices are devices that are connected to your organization’s resources using a personal device and a personal account. You can manage these devices by using Microsoft Intune and enable seamless access to company data. Users can only sign in to their personal devices by using their personal account, not their organizational account. Azure AD registered devices support Windows 10 or newer, iOS, Android, macOS, and Ubuntu 20.04/22.04 LTS1.

The other options are not suitable for this scenario because:

➤ Hybrid Azure AD join is for corporate-owned and managed devices that are joined to both on-premises Active Directory and Azure AD. Users can sign in to these devices by using their organizational account that exists in both directories2.

➤ AD joined is for devices that are joined only to on-premises Active Directory. These devices are not managed by Microsoft Intune and do not have access to cloud resources3.

References: What are Azure AD registered devices?, What are hybrid Azure AD joined devices?, What is Active Directory domain join?

**NEW QUESTION 7**

- (Exam Topic 4)

You have a Windows 11 capable device named Device1 that runs the 64-bit version of Windows 10 Enterprise and has Microsoft Office 2019 installed. You have the Windows 11 Enterprise images shown in the following table.

Name	Platform	Description
Image1	x64	Custom Windows 11 image that has Office 2021 installed
Image2	x64	Default Windows 11 image created by Microsoft

Which images can be used to perform an in-place upgrade of Device1?

- A. image1 only
- B. Image2only
- C. Image1 and Image2

**Answer:** B

**NEW QUESTION 8**

- (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 9

- (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 10

- (Exam Topic 4)

You have the devices shown in the following table.

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

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

#### Answer Area

Device1:

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

Device2:

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

- A. Mastered  
B. Not Mastered

Answer: A

Explanation:

#### Answer Area

Device1:

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

Device2:

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

#### NEW QUESTION 10

- (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 14**

- (Exam Topic 4)

You have an Azure AD group named Group1. Group1 contains two Windows 10 Enterprise devices named Device1 and Device2. You create a device configuration profile named Profile1. You assign Profile1 to Group1. You need to ensure that Profile1 applies to Device1 only. What should you modify in Profile1?

- A. Assignments
- B. Settings
- C. Scope (Tags)
- D. Applicability Rules

**Answer:** D

**Explanation:**

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

**NEW QUESTION 15**

- (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 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:

- User1 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 24

- (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 25

- (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 29

- (Exam Topic 4)

You have a computer named Computer5 that has Windows 10 installed. You create a Windows PowerShell script named config.ps1.

You need to ensure that config.ps1 runs after feature updates are installed on Computer5. Which file should you modify on Computer5?

- A. LiteTouch.wsf
- B. SetupConfig.ini
- C. Unattendb\*
- D. Unattend.xml

**Answer: B**

#### Explanation:

SetupConfig.ini is a file that can be used to customize the behavior of Windows Setup during feature updates. You can use this file to specify commands or scripts that run before or after the installation process. To run a PowerShell script after a feature update, you can use the PostOOBE parameter in SetupConfig.ini and specify the path to the script file. References: [SetupConfig.ini reference]

#### NEW QUESTION 33

- (Exam Topic 4)

You have following types of devices enrolled in Microsoft Intune:

- Windows 10
- Android
- iOS

For which types of devices can you create VPN profiles in Microsoft Intune admin center?

- A. Windows 10 only
- B. Windows 10 and Android only
- C. Windows 10 and iOS only
- D. Android and iOS only
- E. Windows 10, Android, and iOS

**Answer: E**

#### NEW QUESTION 35

- (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 36

- (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 40

- (Exam Topic 4)

You are creating a device configuration profile in Microsoft Intune. You need to configure specific OMA-URI settings in the profile. Which profile type template should you use?

- A. Device restrictions (Windows 10 Team)
- B. Identity protection
- C. Custom
- D. Device restrictions

**Answer:** C

**NEW QUESTION 43**

- (Exam Topic 4)

You have a Microsoft Deployment Toolkit (MDT) deployment share named Share1. You add Windows 10 images to Share1 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:

<input type="checkbox"/>	Image3 only
<input type="checkbox"/>	Image3, Image4, and Image5 only
<input type="checkbox"/>	Image1, Image2, and Image3 only
<input type="checkbox"/>	Image1, Image2, Image3, and Image4 only
<input type="checkbox"/>	Image1, Image2, Image3, Image4, and Image5

Standard Client Upgrade Task Sequence:

<input type="checkbox"/>	Image3 only
<input type="checkbox"/>	Image3, Image4, and Image5 only
<input type="checkbox"/>	Image1, Image2, and Image3 only
<input type="checkbox"/>	Image1, Image2, Image3, and Image4 only
<input type="checkbox"/>	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 45

- (Exam Topic 4)  
 Your company has devices enrolled in Microsoft Intune as shown in the following table.

Name	Platform
Device1	Windows 10
Device2	Android device administrator
Device3	iOS

In Microsoft Endpoint Manager, you define the company's network as a location named Location1. Which devices can use network location-based compliance policies?

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

Answer: E

Explanation:

Intune supported operating systems  
 Intune supports devices running the following operating systems (OS): iOS  
 Android Windows macOS  
 Note: View the device compliance settings for the different device platforms: Android device administrator  
 Android Enterprise iOS  
 macOS  
 Windows Holographic for Business Windows 8.1 and later  
 Windows 10/11  
 Reference: <https://docs.microsoft.com/en-us/mem/intune/fundamentals/supported-devices-browsers> <https://docs.microsoft.com/en-us/mem/intune/protect/device-compliance-get-started>

NEW QUESTION 46

- (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 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 48**

- (Exam Topic 4)

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

- A. From the Microsoft Endpoint Manager admin center, create a configuration profile.
- B. From the Microsoft Endpoint Manager admin center, create a security baseline.
- C. Onboard the macOS devices to the Microsoft 365 compliance center.
- D. Install Defender for Endpoint on the macOS devices.

**Answer: D**

**Explanation:**

Just install, and use Defender for Endpoint on Mac. Reference:

<https://docs.microsoft.com/en-us/microsoft-365/security/defender-endpoint/microsoft-defender-endpoint-mac>

**NEW QUESTION 49**

- (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 51**

- (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](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 56**

- (Exam Topic 4)  
Your network contains an Active Directory domain.  
You install the Microsoft Deployment Toolkit (MDT) on a server. You have a custom image of Windows 11.  
You need to deploy the image to 100 devices by using MDT.  
Which three actions should you perform in sequence? To answer, move answer area and arrange them in the correct order.

**Actions**

Enable multicast.

Install Windows Deployment Services (WDS).

Create a deployment share.

Add the Windows 11 image.

Create a task sequence.

**Answer Area**

>

<

- A. Mastered
- B. Not Mastered

**Answer:** A

**Explanation:**

To deploy the Windows 11 image to 100 devices by using MDT, you should perform the following three actions in sequence:

- > Install Windows Deployment Services (WDS) on the server. WDS is a role that enables you to deploy Windows operating systems over the network by using PXE boot and multicast technologies. You need to install WDS before you can enable multicast and configure the boot images for MDT. You can install WDS by using the Server Manager or PowerShell1.
- > Create a deployment share on the server. A deployment share is a folder that contains the MDT files, scripts, applications, drivers, operating systems, and task sequences that you use to deploy Windows. You need to create a deployment share by using the MDT Deployment Workbench2.
- > Add the Windows 11 image and create a task sequence in the deployment share. An image is a file that contains a snapshot of a Windows installation. A task sequence is a set of steps that MDT executes to install Windows and configure the settings. You need to add the Windows 11 image by importing it from a source folder or a WIM file, and create a task sequence by using a template or customizing your own3.

These are the basic steps to prepare for deploying Windows 11 with MDT. For more details and guidance, you can refer to the web search results I found for you by using search\_web("deploy Windows 11 image with MDT").

**NEW QUESTION 61**

- (Exam Topic 4)  
You have a Microsoft 365 tenant that uses Microsoft Intune and contains the devices shown in the following table.

Name	Platform
Device1	Windows 10
Device2	macOS

In Microsoft Intune Endpoint security, you need to configure a disk encryption policy for each device. Which encryption type should you use for each device, and which role-based access control (RBAQ role in Intune should you use to manage the encryption keys? To answer, select the appropriate options m the answer area.  
NOTE: Each correct selection is worth one point.

**Answer Area**

Device1:

FileVault  
Cryptsetup  
Encrypting File System (EFS)  
BitLocker Drive Encryption (BitLocker)

Device2:

FileVault  
Cryptsetup  
Encrypting File System (EFS)  
BitLocker Drive Encryption (BitLocker)

RBAC role:

Help Desk Operator  
Application Manager  
Intune Role Administrator  
Policy and Profile Manager

- A. Mastered
- B. Not Mastered

**Answer:** A

**Explanation:**  
Graphical user interface, text, application Description automatically generated

**NEW QUESTION 62**

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

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

**Answer:** CE

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

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

The other options are not correct for this scenario because:

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

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

**NEW QUESTION 65**

- (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:

Setting

Device2:

Setting

Device3:

Setting

- 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 69**

- (Exam Topic 4)  
Your network contains an Active Directory domain. The domain contains a user named Admin1. All computers run Windows 10.  
You enable Windows PowerShell remoting on the computers.  
You need to ensure that Admin1 can establish remote PowerShell connections to the computers. The solution must use the principle of least privilege.  
To which group should you add Admin1?

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

Answer: B

**NEW QUESTION 70**

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

Name	Platform
Device1	Windows 10
Device2	Windows 11
Device3	Android
Device4	iOS

On which devices can you apply app configuration policies?

- A. Device2 only
- B. Device1 and Device2 only

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

**Answer:** D

**Explanation:**

The correct answer is D because app configuration policies can be applied to managed devices and managed apps1. Managed devices are enrolled and managed by Intune, while managed apps are integrated with Intune App SDK or wrapped using the Intune Wrapping Tool1. Device2, Device3, and Device4 are either enrolled in Intune or have managed apps installed, so they can receive app configuration policies2. Device1 is not enrolled in any MDM solution and does not have any managed apps installed, so it cannot receive app configuration policies2. References: 1: App configuration policies for Microsoft Intune | Microsoft Learn <https://learn.microsoft.com/en-us/mem/intune/apps/app-configuration-policies-overview> 2: Policy sets - Microsoft Intune | Microsoft Learn <https://learn.microsoft.com/en-us/mem/intune/fundamentals/policy-sets>

**NEW QUESTION 74**

- (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 75**

- (Exam Topic 4)

Your company uses Microsoft Intune to manage devices.

You need to ensure that only Android devices that use Android work profiles can enroll in intune. Which two configurations should you perform in the device enrollment restrictions? Each correct answer presents part of the solution.

NOTE Each correct selection is worth one point.

- A. From Platform Settings, set Android device administrator Personally Owned to Block.
- B. From Platform Settings, set Android Enterprise (work profile) to Allow.
- C. From Platform Settings, set Android device administrator Personally Owned to Allow
- D. From Platform Settings, set Android device administrator to Block.

**Answer:** AB

**Explanation:**

To ensure that only Android devices that use Android work profiles can enroll in Intune, you need to perform two configurations in the device enrollment restrictions. First, you need to set Android device administrator Personally Owned to Block. This prevents users from enrolling personal Android devices that use device administrator mode. Second, you need to set Android Enterprise (work profile) to Allow. This allows users to enroll corporate-owned or personal Android devices that use work profiles. References: <https://docs.microsoft.com/en-us/mem/intune/enrollment/enrollment-restrictions-set>

**NEW QUESTION 78**

- (Exam Topic 4)

You have a server named Server1 and computers that run Windows 8.1. Server1 has the Microsoft Deployment Toolkit (MDT) installed.

You plan to upgrade the Windows 8.1 computers to Windows 10 by using the MDT deployment wizard. You need to create a deployment share on Server1.

What should you do on Server1, and what are the minimum components you should add to the MDT deployment share? To answer, select the appropriate options in the answer area.

NOTE: Each correct selection is worth one point.

**Answer Area**

On Server1:	<div><div>Import the Deployment Image Servicing and Management (DISM) PowerShell module.</div><div>Import the WindowsAutopilotIntune Windows PowerShell module.</div><div>Install the Windows Assessment and Deployment Kit (Windows ADK).</div><div>Install the Windows Deployment Services server role.</div></div>
Add to the MDT deployment share:	<div><div>Windows 10 image and package only</div><div>Windows 10 image and task sequence only</div><div>Windows 10 image only</div><div>Windows 10 image, task sequence, and package</div></div>

- A. Mastered
- B. Not Mastered

**Answer:** A

#### Explanation:

Box 1: Install the Windows Deployment Services role. Install and initialize Windows Deployment Services (WDS) On the server:  
 Open an elevated Windows PowerShell prompt and enter the following command: Install-WindowsFeature -Name WDS -IncludeManagementTools  
 WDSUTIL /Verbose /Progress /Initialize-Server /Server:MDT01 /RemInst:"D:\RemoteInstall" WDSUTIL /Set-Server /AnswerClients:All  
 Box 2: Windows 10 image and task sequence only Create the reference image task sequence  
 In order to build and capture your Windows 10 reference image for deployment using MDT, you will create a task sequence.  
 Reference:  
<https://docs.microsoft.com/en-us/windows/deployment/deploy-windows-mdt/prepare-for-windows-deployment>  
<https://docs.microsoft.com/en-us/windows/deployment/deploy-windows-mdt/create-a-windows-10-reference-im>

#### NEW QUESTION 81

- (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
<a href="#">ConfigurationProfile1</a>	Windows 10 and later	Device restrictions

Device compliance policies (1)

Name	Platform	Profile Type
<a href="#">CompliancePolicy1</a>	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 83

- (Exam Topic 4)

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

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

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

```
[Settings]
Priority=DefaultGateway, Default
[DefaultGateway]
10.1.1.1=NewYork
10.5.5.1=London
[NewYork]
DeployRoot=\\MDT1\Production$
[London]
DeployRoot=\\MDT2\Production$

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

KeyboardLocale=en-us -

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

Name	IP address
LT1	10.1.1.240
DT1	10.5.5.115
TB1	10.2.2.193

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

NOTE: Each correct selection is worth one point.

Statements	Yes	No
TB1 will download the image from MDT3.	<input type="radio"/>	<input type="radio"/>
DT1 will have a KeyboardLocale of en-gb.	<input type="radio"/>	<input type="radio"/>
LT1 will download the image from MDT1.	<input type="radio"/>	<input type="radio"/>

- A. Mastered  
B. Not Mastered

Answer: A

Explanation:

Statements	Yes	No
TB1 will download the image from MDT3.	<input type="radio"/>	<input checked="" type="radio"/>
DT1 will have a KeyboardLocale of en-gb.	<input checked="" type="radio"/>	<input type="radio"/>
LT1 will download the image from MDT1.	<input checked="" type="radio"/>	<input type="radio"/>

NEW QUESTION 87

- (Exam Topic 3)

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

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

Answer: A

Explanation:

Reference:

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

NEW QUESTION 89

- (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 91

- (Exam Topic 3)

You need a new conditional access policy that has an assignment for Office 365 Exchange Online. You need to configure the policy to meet the technical requirements for Group4.

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

NOTE: Each correct selection is worth one point.

New

Conditions

Device state (preview)

Info

Name

PolicyA

Assignments

Users and groups

0 users and groups selected

Cloud apps

1 app included

Conditions

0 conditions selected

Access controls

Grant

Block access

Session

0 controls selected

Info

Sign-in risk

Not configured

Device platforms

Not configured

Locations

Not configured

Client apps (preview)

Not configured

Device state (preview)

Not configured

Info

Configure

Yes

No

Include

Exclude

Select the device state condition used to exclude devices from policy.

☐

Device Hybrid Azure AD joined

☐

Device marked as compliant

- A. Mastered
- B. Not Mastered

**Answer:** A

**Explanation:**

The policy needs to be applied to Group4 so we need to configure Users and Groups. The Access controls are set to Block access

A screenshot of a computer Description automatically generated

We therefore need to exclude compliant devices. From the scenario:

➤ Ensure that the users in a group named Group4 can only access Microsoft Exchange Online from devices that are enrolled in Intune.

Note: When a device enrolls in Intune, the device information is updated in Azure AD to include the device compliance status. This compliance status is used by conditional access policies to block or allow access to e-mail and other organization resources.

References:

<https://docs.microsoft.com/en-us/azure/active-directory/conditional-access/overview> [https://docs.microsoft.com/en-us/active-directory/conditional-access/conditions](https://docs.microsoft.com/en-us/azure/active-directory/conditional-access/conditions) <https://docs.microsoft.com/en-us/intune/device-compliance-get-started>

**NEW QUESTION 96**

- (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:**

Device1 only

Device2 only

Device3 only

Device4 only

Device2 and Device3 only

Device1 and Device3 only

Device1, Device2, and Device 3

**Policy2:**

Device1 only

Device2 only

Device3 only

Device4 only

Device2 and Device3 only

Device1 and Device3 only

Device1, Device2, and Device 3

- A. Mastered
- B. Not Mastered

**Answer:** A

**Explanation:**

Reference:

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

Passing Certification Exams Made Easy

visit - <https://www.surepassexam.com>



NEW QUESTION 99

- (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 102

- (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 105

- (Exam Topic 2)

You need to meet the OOBЕ requirements for Windows AutoPilot.  
Which two settings should you configure from the Azure Active Directory blade? To answer, select the appropriate settings in the answer area.  
NOTE: Each correct selection is worth one point.

**Overview**

Getting started

**Manage**

Users
Groups
Organizational relationships
Roles and administrators
Enterprise applications
Devices
App registrations
App registrations (Preview)
Application proxy
Licenses
Azure AD Connect
Custom domain names
Mobility (MDM and MAM)
Password reset
Company branding
User settings
Properties
Notifications settings

- A. Mastered
- B. Not Mastered

Answer: A

**Explanation:**

Reference:  
<https://blogs.msdn.microsoft.com/sgern/2018/10/11/intune-intune-and-autopilot-part-3-preparing-your-envirom>  
<https://blogs.msdn.microsoft.com/sgern/2018/11/27/intune-intune-and-autopilot-part-4-enroll-your-first-device/>

**NEW QUESTION 107**

- (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
An app protection policy
Azure information Protection
iOS app provisioning profiles

For the Sales department employees:

<input checked="" type="checkbox"/>
An app configuration policy
An app protection policy
Azure information Protection
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 111**

- (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 116**

- (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 120**

- (Exam Topic 1)  
Which user can enroll Device6 in Intune?

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

**Answer:** B

**NEW QUESTION 123**

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

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

- A. Mastered
- B. Not Mastered

**Answer:** A

**Explanation:**



A screenshot of a computer Description automatically generated with medium confidence

NEW QUESTION 126

- (Exam Topic 1)

You implement Boundary1 based on the planned changes.

Which devices have a network boundary of 192.168.1.0/24 applied?

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

Answer: D

Explanation:

Reference:

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

NEW QUESTION 130

- (Exam Topic 1)

You implement the planned changes for Connection1 and Connection2

How many VPN connections will there be for User1 when the user signs in to Device 1 and Devke2? To answer select the appropriate options in the answer area.

NOTE; Each correct selection is worth one point.

Answer Area

Device1:

1

2

3

4

5

Device2:

1

2

3

4

5

- A. Mastered
- B. Not Mastered

Answer: A

Explanation:

Answer Area

Device1:

1

2

3

4

5

Device2:

1

2

3

4

5

NEW QUESTION 135

- (Exam Topic 1)

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

NOTE: Each correct selection is worth one point.

Statements	Yes	No
Device1 is marked as compliant.	<input type="radio"/>	<input type="radio"/>
Device4 is marked as compliant.	<input type="radio"/>	<input type="radio"/>
Device5 is marked as compliant.	<input type="radio"/>	<input type="radio"/>

- A. Mastered
- B. Not Mastered

**Answer:** A

**Explanation:**

Text Description automatically generated

**NEW QUESTION 136**

- (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 140**

- (Exam Topic 4)

You have a Microsoft 365 E5 subscription that contains 100 iOS devices enrolled in Microsoft Intune. You need to ensure that notifications of iOS updates are deferred for 30 days after the updates are released. What should you create?

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

**Answer:** C

**Explanation:**

Manage iOS/iPadOS software update policies in Intune, delay visibility of software updates.

When you use update policies for iOS, you might have need to delay visibility of an iOS software update. Reasons to delay visibility include:

Prevent users from updating the OS manually

To deploy an older update while preventing users from installing a more recent one

To delay visibility, deploy a device restriction template that configures the following settings: Defer software updates = Yes

This doesn't affect any scheduled updates. It represents days before software updates are visible to end users after release.

Delay default visibility of software updates = 1 to 90 90 days is the maximum delay that Apple supports.

Reference: <https://docs.microsoft.com/en-us/mem/intune/protect/software-updates-ios>

**NEW QUESTION 144**

- (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 149**

- (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

<div style="background-color: #f0f0f0; padding: 2px;">net accounts</div> <div style="background-color: #f0f0f0; padding: 2px;">net localgroup</div> <div style="background-color: #f0f0f0; padding: 2px;">net user</div>	Administrators /add "	<div style="background-color: #f0f0f0; padding: 2px;">AzureAD</div> <div style="background-color: #f0f0f0; padding: 2px;">CONTOSO</div> <div style="background-color: #f0f0f0; padding: 2px;">UPN</div>	\user1@contoso.com"
--	-----------------------	---	---------------------

- A. Mastered
- B. Not Mastered

**Answer:** A

**Explanation:**

### Answer Area

<div style="background-color: #f0f0f0; padding: 2px;">net accounts</div> <div style="border: 2px solid red; background-color: #f0f0f0; padding: 2px;">net localgroup</div> <div style="background-color: #f0f0f0; padding: 2px;">net user</div>	Administrators /add "	<div style="border: 2px solid red; background-color: #f0f0f0; padding: 2px;">AzureAD</div> <div style="border: 2px solid red; background-color: #f0f0f0; padding: 2px;">CONTOSO</div> <div style="background-color: #f0f0f0; padding: 2px;">UPN</div>	\user1@contoso.com"
---	-----------------------	---	---------------------

### NEW QUESTION 151

- (Exam Topic 4)

You have a Microsoft 365 E5 subscription that contains 10 Android Enterprise devices. Each device has a corporate-owned work profile and is enrolled in Microsoft Intune.

You need to configure the devices to run a single app in kiosk mode.

Which Configuration settings should you modify in the device restrictions profile?

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

**Answer:** D

**Explanation:**

To configure the devices to run a single app in kiosk mode, you need to modify the Device experience settings in the device restrictions profile. You can specify the app package name and activity name for the app that you want to run in kiosk mode. References:

<https://docs.microsoft.com/en-us/mem/intune/configuration/device-restrictions-android-for-work#device-experie>

### NEW QUESTION 154

- (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 159

- (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 160**

- (Exam Topic 4)

You have a Microsoft 365 tenant that uses Microsoft Intune to manage personal and corporate devices. The tenant contains three Windows 10 devices as shown in the following exhibit.

Name	Enabled	OS	Version	Join Type	Owner	MDM	Compliant
 LON-CL2	✔ Yes	Windows	10.0.17763.615	Azure AD registered	User2	Microsoft Intune	✔ Yes
 LON-CL4	✔ Yes	Windows	10.0.17763.107	Azure AD joined	User1	Microsoft Intune	✔ Yes

How will Intune classify each device after the devices are enrolled in Intune automatically? To answer, select the appropriate options in the answer area.

NOTE: Each correct selection is worth one point.

**Answer Area**

Identified by Intune as a personal device:

LON-CL2 only

LON-CL4 only

Both LON-CL2 and LON-CL4

Neither LON-CL2 or LON-CL4

Identified by Intune as a corporate device:

LON-CL2 only

LON-CL4 only

Both LON-CL2 and LON-CL4

Neither LON-CL2 or LON-CL4

- A. Mastered
- B. Not Mastered

**Answer:** A

**Explanation:**

Table Description automatically generated

Reference:

<https://docs.microsoft.com/en-us/azure/active-directory/devices/concept-azure-ad-join> <https://docs.microsoft.com/en-us/azure/active-directory/devices/concept-azure-ad-register>

**NEW QUESTION 164**

- (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 167**

- (Exam Topic 4)

You have a Microsoft 365 subscription that uses Microsoft Intune Suite. You use Microsoft Intune to manage devices. Azure AD joined Windows devices enroll automatically in Intune. You have the devices shown in the following table.

Name	Operating system	Azure AD joined	Line-of-business (LOB) apps installed
Device1	64-bit version of Windows 10 Pro	Yes	No
Device2	32-bit version of Windows 10 Pro	No	Yes
Device3	64-bit version of Windows 10 Pro	No	Yes

You are preparing to upgrade the devices to Windows 11. All the devices are compatible with Windows 11. You need to evaluate Windows Autopilot and in-place upgrade as deployment methods to implement Windows 11 Pro on the devices, while retaining all user settings and applications.

Which devices can be upgraded by using each method? To answer, select the appropriate options in the answer area.

NOTE: Each correct selection is worth one point.

**Answer Area**

Windows Autopilot:

In-place upgrade:

- A. Mastered
- B. Not Mastered

**Answer:** A

**Explanation:**

**Answer Area**

Windows Autopilot:

In-place upgrade:

**NEW QUESTION 169**

- (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.	<input type="radio"/>	<input type="radio"/>
Admin1@contoso.com can configure the firewall and Microsoft Defender on Computer1.	<input type="radio"/>	<input type="radio"/>
Admin2@contoso.com can install software on Computer1.	<input type="radio"/>	<input type="radio"/>

- 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.	<input type="radio"/>	<input checked="" type="radio"/>
Admin1@contoso.com can configure the firewall and Microsoft Defender on Computer1.	<input type="radio"/>	<input checked="" type="radio"/>
Admin2@contoso.com can install software on Computer1.	<input type="radio"/>	<input checked="" type="radio"/>

NEW QUESTION 174

- (Exam Topic 4)  
You have a Microsoft 365 subscription that uses Microsoft Intune Suite. You use Microsoft Intune to manage devices. You need to configure an update ring that meets the following requirements:

- Fixes and improvements to existing Windows functionality can be deferred for 14 days but will install automatically seven days after that date.
- The installation of new Windows features can be deferred for 90 days but will install automatically 10 days after that date.
- Devices must restart automatically three days after an update is installed.

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

Answer Area

Feature update deferral period (days):

90

3

7

10

14

90

Quality update deferral period (days):

14

3

7

10

14

90

7

3

7

10

14

90

Grace period:

3

3

7

10

14

90

- A. Mastered
- B. Not Mastered

Answer: A

Explanation:



Answer Area

Feature update deferral period (days):  

90  
3  
7  
10  
14  
90

Quality update deferral period (days):  

14  
3  
7  
10  
14  
90

7  
3  
7  
10  
14  
90

Grace period:  

3  
7  
10  
14  
90

NEW QUESTION 179

- (Exam Topic 4)

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

Answer Area

Azure service to provision:

An Azure Storage account

Azure Cosmos DB

Azure SQL Database

Log Analytics

Action to perform on the computers:

Create a collector-initiated subscription

Install the Microsoft Monitoring Agent

Enroll in Microsoft Intune

Register to Azure Active Directory (Azure AD)

- A. Mastered
- B. Not Mastered

Answer: A

Explanation:

Answer Area

Azure service to provision:

An Azure Storage account

Azure Cosmos DB

Azure SQL Database

Log Analytics

Action to perform on the computers:

Create a collector-initiated subscription

Install the Microsoft Monitoring Agent

Enroll in Microsoft Intune

Register to Azure Active Directory (Azure AD)

NEW QUESTION 183

- (Exam Topic 4)  
 You have a Microsoft 365 tenant and an internal certification authority (CA).  
 You need to use Microsoft Intune to deploy the root CA certificate to managed devices.  
 Which type of Intune policy and profile should you use? To answer, select the appropriate options in the answer area.  
 NOTE: Each correct selection is worth one point.

Answer Area

Policy type:

App configuration policy

App protection policy

Compliance policy

Configuration profile

Profile:

Imported public key pair (PKCS) certificate

Public key pair (PKCS) certificate

Simple Certificate Enrollment Protocol (SCEP) certificate

Trusted certificate

- A. Mastered
- B. Not Mastered

Answer: A

Explanation:

Box 1: Configuration profile Create a trusted certificate profile. Box 2: Trusted certificate  
 When using Intune to provision devices with certificates to access your corporate resources and network, use a trusted certificate profile to deploy the trusted root certificate to those devices. Trusted root certificates establish a trust from the device to your root or intermediate (issuing) CA from which the other certificates are issued.  
 Reference: <https://docs.microsoft.com/en-us/mem/intune/protect/certificates-trusted-root>

NEW QUESTION 185

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

- A. Mastered
- B. Not Mastered

Answer: A

Explanation:

Answer Area

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

NEW QUESTION 187

- (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 191

- (Exam Topic 4)

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

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

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



Name	Platform	Encryption	Secure Boot
Policy1	Windows 10	Not configured	Not configured
Policy2	Windows 10	Not configured	Required
Policy3	Windows 10	Required	Required
Policy4	Android	Not configured	<i>Not applicable</i>

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

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

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

Answer Area

Statements	Yes	No
Device1 is marked as compliant.	<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 comp = No

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

NEW QUESTION 195

- (Exam Topic 4)

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

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

Answer: C

Explanation:

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

NEW QUESTION 198

- (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 200

- (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 201

- (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 205

- (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 207

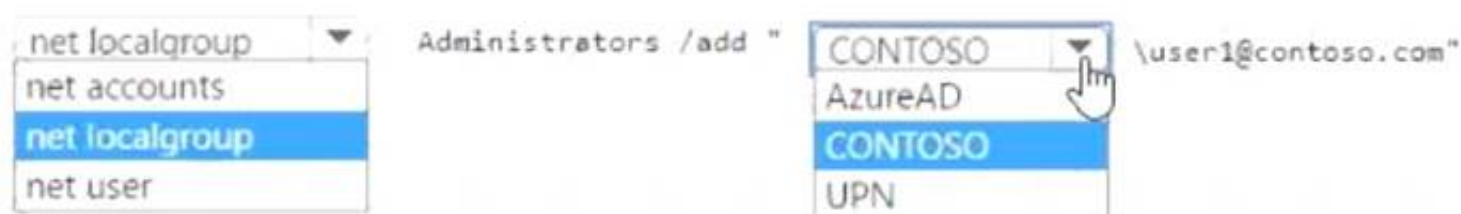
- (Exam Topic 4)

You have an 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 11 device named Client1 to contoso.com. You need to add User1 to the local Administrators group of Client1.

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

#### Answer Area



- A. Mastered
- B. Not Mastered

**Answer:** A

#### Explanation:

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 208

- (Exam Topic 4)

You have an Azure AD tenant named contoso.com.

You have a workgroup computer named Computer1 that runs Windows 11. You need to add Computer1 to contoso.com. What should you use?

- A. dsreecmd.exe
- B. Computer Management
- C. netdom.exe
- D. the Settings app

**Answer:** A

#### NEW QUESTION 210

- (Exam Topic 4)

You have a hybrid deployment of Azure AD that contains 50 Windows 10 devices. All the devices are enrolled in Microsoft Intune.

You discover that Group Policy settings override the settings configured in Microsoft Intune policies. You need to ensure that the settings configured in Microsoft Intune override the Group Policy settings. What should you do?

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

**Answer:** C

#### NEW QUESTION 214

- (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 215

- (Exam Topic 4)

You have a Microsoft 365 subscription that uses Microsoft Intune and contains 100 Windows 10 devices. You need to create Intune configuration profiles to perform the following actions on the devices:

- Deploy a custom Start layout.
- Rename the local Administrator account.

Which profile type template should you use for each action? To answer, select the appropriate options in the answer area. NOTE: Each correct selection is worth one point.

#### Answer Area

Deploy a custom Start layout:	<div>Device restriction</div> <div>Delivery optimization</div> <div style="background-color: #0070c0; color: white;">Device restriction</div> <div>Endpoint protection</div> <div>Identity protection</div>
Rename the local Administrator account:	<div>Identity protection</div> <div style="background-color: #0070c0; color: white;">Delivery optimization</div> <div>Device restriction</div> <div>Endpoint protection</div> <div style="background-color: #0070c0; color: white;">Identity protection</div>

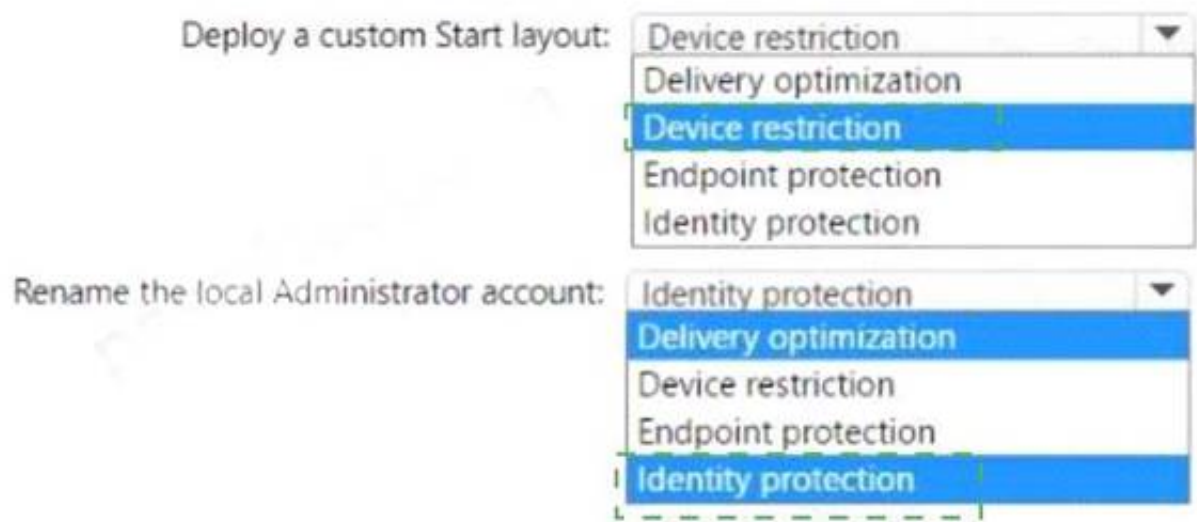
- A. Mastered
- B. Not Mastered

**Answer:** A

#### Explanation:



**Answer Area**



**NEW QUESTION 218**

- (Exam Topic 4)

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

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

**Answer: C**

**Explanation:**

To apply Microsoft Defender for Endpoint antivirus policies to the macOS devices, you need to install Defender for Endpoint on the devices. You can use Intune to deploy a script that installs Defender for Endpoint on macOS devices. After installation, you can use Intune to create and assign antivirus policies to the devices. References:

<https://docs.microsoft.com/en-us/windows/security/threat-protection/microsoft-defender-atp/mac-install-with-int>

**NEW QUESTION 221**

- (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 223**  
- (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 228**

- (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 231**

- (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 233

- (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 235

- (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 236

- (Exam Topic 4)

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

You use Microsoft Intune to manage devices. All devices are in the same time zone. You create an update rings policy and assign the policy to all Windows devices.

On the November 1, you pause the update rings policy. All devices remain online.

Without further modification to the policy, on which date will the devices next attempt to update?

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

**Answer:** C

#### NEW QUESTION 239

- (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 242

- (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:

System Security

Requires a minimum operating system version:

Device Properties

NEW QUESTION 245

- (Exam Topic 4)

Your network contains an on-premises Active Directory domain named contoso.com that syncs to Azure AD. A user named User1 uses the domain-joined devices shown in the following table.

Name	Operating system
Device1	Windows 10 Pro
Device2	Windows 11 Pro

In the Microsoft Entra admin center, you assign a Windows 11 Enterprise E5 license to User1. You need to identify what will occur when User1 next signs in to the devices.

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

Answer Area

Device1:

Will activate as Windows 11 Enterprise

Will activate as Windows 11 Enterprise

Will not upgrade to Windows 11 Enterprise

Will perform a clean installation of Windows 11 Enterprise

Will perform an in-place upgrade to Windows 11 Enterprise

Device2:

Will not upgrade to Windows 11 Enterprise

Will activate as Windows 11 Enterprise

Will not upgrade to Windows 11 Enterprise

Will perform a clean installation of Windows 11 Enterprise

Will perform an in-place upgrade to Windows 11 Enterprise

- A. Mastered
- B. Not Mastered

Answer: A

Explanation:

Device 1:

- > Will activate as Windows 11 Enterprise. According to Deploy Windows Enterprise licenses, Windo 11 Enterprise E5 license is a subscription license that can be assigned to users who have a supported and licensed version of Windows 10 Pro or Windows 11 Pro. Device 1 has Windows 11 Pro, so it meets the requirement. When User1 signs in to Device 1 with their Azure AD account, the device will automatically activate as Windows 11 Enterprise without changing the edition.
- > Will not activate as Windows 11 Enterprise. According to Deploy Windows Enterprise licenses, Windows 11 Enterprise E5 license is a subscription license that can be assigned to users who have a supported and licensed version of Windows 10 Pro or Windows 11 Pro. Device 2 has Windows 10 Home, so it does not meet the requirement. When User1 signs in to Device 2 with their Azure AD account, the device will not activate as Windows 11 Enterprise by subscription.

NEW QUESTION 249



- (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 250**

- (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 251**

- (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.	<input type="radio"/>	<input type="radio"/>
User2 receives Notification1 on Device2.	<input type="radio"/>	<input type="radio"/>
User1 receives Notification1 on Device3.	<input type="radio"/>	<input type="radio"/>

- 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 255**  
 - (Exam Topic 4)  
 Your network contains an on-premises Active Directory domain and an Azure AD tenant.  
 The Default Domain Policy Group Policy Object (GPO) contains the settings shown in the following table.

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

Which device configuration profile type template should you use?

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

Answer: A

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

**NEW QUESTION 257**  
 - (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 261**

- (Exam Topic 4)

You have 200 computers that run Windows 10. The computers are joined to Azure AD and enrolled in Microsoft Intune. You need to set a custom image as the wallpaper and sign-in screen.

Which two settings should you configure in the Device restrictions configuration profile? To answer, select the appropriate settings in the answer area.

NOTE: Each correct selection is worth one point.

**Answer Area**

## Device restrictions

Windows 10 and later

✓ Basics   2 Configuration settings   3 Assignments   4 Applicability Rules   5 Review + create

App Store

Cellular and connectivity

Cloud and Storage

Cloud Printer

Control Panel and Settings

Display

General

Locked Screen Experience ✓

Messaging

Microsoft Edge Browser

Network proxy

Password

Per-app privacy exceptions

Personalization ✓

Printer

Privacy

Projection

Previous   Next

- A. Mastered
- B. Not Mastered

**Answer: A**

**Explanation:**



**Answer Area**

## Device restrictions

Windows 10 and later

✓ Basics   **2 Configuration settings**   3 Assignments   4 Applicability Rules   5 Review + create

- App Store
- Cellular and connectivity
- Cloud and Storage
- Cloud Printer
- Control Panel and Settings
- Display
- General
- Locked Screen Experience** ✓
- Messaging
- Microsoft Edge Browser
- Network proxy
- Password
- Per-app privacy exceptions
- Personalization** ✓
- Printer
- Privacy
- Projection

Previous   **Next**

**NEW QUESTION 262**

- (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 263

- (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

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.

Answer Area

- A. Mastered
- B. Not Mastered

Answer: A

Explanation:

Actions

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.

Answer Area

Create a system image backup.

Deploy Windows 11.

Restore a system image backup.

NEW QUESTION 265

- (Exam Topic 4)

Your network contains an Active Directory domain. The domain contains a computer named Computer1 that runs Windows 11. You need to enable the Windows Remote Management (WinRM) service on Computer1 and perform the following configurations:

- For the WinRM service, set Startup type to Automatic.
- Create a listener that accepts requests from any IP address.
- Enable a firewall exception for WS-Management communications. Which PowerShell cmdlet should you use?

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

Answer: B

NEW QUESTION 269

- (Exam Topic 4)

You have a Microsoft 365 subscription that includes Microsoft Intune. You have computers that run Windows 11 as shown in the following table.

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

You have the groups shown in the following table.

Name	Members
Group1	Computer1, Computer2
Group2	Computer3

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

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

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

Answer Area

Statements

Yes

No

The compliance status of Computer1 is In grace period.

The compliance status of Computer2 is Compliant.

The compliance status of Computer3 is Not compliant.

- A. Mastered
- B. Not Mastered

Answer: A

Explanation:

Answer Area

Statements

Yes

No

The compliance status of Computer1 is In grace period.

☒

The compliance status of Computer2 is Compliant.

☒

The compliance status of Computer3 is Not compliant.

☒

**NEW QUESTION 272**

- (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 276**

- (Exam Topic 4)  
 You have 25 computers that run Windows 10 Pro.  
 You have a Microsoft 365 E5 subscription that uses Microsoft Intune.  
 You need to upgrade the computers to Windows 11 Enterprise by using an in-place upgrade. The solution must minimize administrative effort.  
 What should you use?

- A. Microsoft Deployment Toolkit (MDT) and a default image of Windows 11 Enterprise
- B. Microsoft Configuration Manager and a custom image of Windows 11 Enterprise
- C. Windows Autopilot
- D. Subscription Activation

Answer: C

**NEW QUESTION 281**

- (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 283**

- (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.)

Dashboard > Client apps - App protection policies > Create policy > Settings

Create policy

Name

Policy1

Description

Platform

iOS

Target to all app types

YesNo

App types

Apps on unmanaged devices

Apps

1 app selected

Settings

Default settings configured

Settings

Data protection

Default settings configured

Access requirements

Default settings configured

Conditional launch

Default settings configured

Scope (Tags)

0 scope(s) selected

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 284

- (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 285

- (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 286**

- (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 Pro

Windows 11 Enterprise

Windows 11 Pro

Windows 11 Pro for Workstations

Research: 

Windows 11 Enterprise

Windows 11 Enterprise

Windows 11 Pro

Windows 11 Pro for Workstations

- A. Mastered  
B. Not Mastered

**Answer:** A

**Explanation:**

**Answer Area**

Marketing: 

Windows 11 Pro

Windows 11 Enterprise

Windows 11 Pro

Windows 11 Pro for Workstations

Research: 

Windows 11 Enterprise

Windows 11 Enterprise

Windows 11 Pro

Windows 11 Pro for Workstations

**NEW QUESTION 287**

.....

## 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](#)**