



# Microsoft

## Exam Questions MD-102

Endpoint Administrator

## About ExamBible

*[Your Partner of IT Exam](#)*

## Found in 1998

ExamBible is a company specialized on providing high quality IT exam practice study materials, especially Cisco CCNA, CCDA, CCNP, CCIE, Checkpoint CCSE, CompTIA A+, Network+ certification practice exams and so on. We guarantee that the candidates will not only pass any IT exam at the first attempt but also get profound understanding about the certificates they have got. There are so many alike companies in this industry, however, ExamBible has its unique advantages that other companies could not achieve.

## Our Advances

### \* 99.9% Uptime

All examinations will be up to date.

### \* 24/7 Quality Support

We will provide service round the clock.

### \* 100% Pass Rate

Our guarantee that you will pass the exam.

### \* Unique Gurantee

If you do not pass the exam at the first time, we will not only arrange FULL REFUND for you, but also provide you another exam of your claim, ABSOLUTELY FREE!

### NEW QUESTION 1

- (Exam Topic 4)

You have an Azure subscription.

You have an on-premises Windows 11 device named Device 1. You plan to monitor Device1 by using Azure Monitor.

You create a data collection rule (DCR) named DCR1 in the subscription. To what should you associate DCR1 ?

- A. Azure Network Watcher
- B. Device1
- C. a Log Analytics workspace
- D. a Monitored Object

**Answer: B**

#### Explanation:

To monitor Device1 by using Azure Monitor, you should associate DCR1 with Device1. A data collection rule (DCR) defines the data collection process in Azure Monitor, such as what data to collect, how to transform it, and where to send it. A DCR can be associated with multiple virtual machines and specify different data sources, such as Azure Monitor Agent, custom logs, or Azure Event Hubs1. To associate a DCR with a virtual machine, you need to install the Azure Monitor Agent on the machine and then select the DCR from the list of available rules2. You can also use Azure Policy to automatically install the agent and associate a DCR with any virtual machines or virtual machine scale sets as they are created in your subscription3.

The other options are not correct for this scenario because:

➤ Azure Network Watcher is a service that provides network performance monitoring and diagnostics for Azure resources. It is not related to data collection rules or Azure Monitor4.

➤ A Log Analytics workspace is a destination where you can send the data collected by a data collection rule. It is not an entity that you can associate a DCR with5.

➤ A Monitored Object is not a valid term in the context of Azure Monitor or data collection rules. References: Data collection rules in Azure Monitor, Configure data collection for Azure Monitor Agent, U

Azure Policy to install Azure Monitor Agent and associate with a DCR, What is Azure Network Watcher?, Log Analytics workspaces in Azure Monitor

### 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)

Your network contains an Active Directory domain named contoso.com. The domain contains two computers named Computer1 and Computer2 that run Windows 10. On Computer1, you need to run the

Invoke-Command cmdlet to execute several PowerShell commands on Computer2. What should you do first?

- A. On Computer2, run the Enable-PSRemoting cmdlet.
- B. On Computer2, add Computer1 to the Remote Management Users group.
- C. From Active Directory, configure the Trusted for Delegation setting for the computer account of Computer2.
- D. On Computer1, run the HcK-PSSession cmdlet.

**Answer: C**

### NEW QUESTION 5

- (Exam Topic 4)

You have an Azure AD tenant named contoso.com.

You need to ensure that users are not added automatically to the local Administrators group when they join their Windows 11 device to contoso.com. What should you configure?

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

**Answer: D**

#### Explanation:

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

The other options are not relevant for this scenario because:

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

- Provisioning packages for Windows are files that contain custom settings and policies that can be applied to Windows devices during the setup process. They do not affect the Azure AD join process or the local administrator role of the users3.
  - Security defaults in Azure AD are a set of basic identity security mechanisms that are enabled by default to protect your organization from common attacks. They do not include any settings related to device management or local administrator role4.
- References: Manage device identities using the Microsoft Entra admin center, Windows Autopilot, Provisioning packages for Windows 10, What are security defaults?

#### NEW QUESTION 6

- (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 7

- (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 8

- (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 9

- (Exam Topic 4)

You have a Microsoft 365 ES subscription that uses Microsoft Intune. Devices are enrolled in Intune as shown in the following table.

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

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

Name	Members
Group1	Device1, Device2, Device3
Group2	Device2

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



Create profile

iOS/iPadOS

✓ Basics

✓ Update policy settings

✓ Assignments

⬇ Review + create

Summary

Basics

Name

Profile1

Description

--

Update policy settings

Update to install

Install iOS/iPadOS Latest update

Schedule type

Update outside of scheduled time

Time zone

UTC±00

Time window

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

Assignments

Included groups

Group

Group Members ⌵

Group1

3 devices, 0 users

Excluded groups

Group

Group Members ⌵

Group2

1 devices, 0 users

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

Answer Area

Statements	Yes	No
If an iOS update becomes available on Tuesday at 5 AM, the update is installed on Device1 automatically on Wednesday.	<input type="radio"/>	<input type="radio"/>
If an iPadOS update becomes available on Thursday at 2 AM, the update is installed on Device2 automatically on Thursday.	<input type="radio"/>	<input type="radio"/>
If an iPadOS update becomes available on Friday at 10 PM, the update is installed on Device3 automatically on Sunday.	<input type="radio"/>	<input type="radio"/>

- A. Mastered
- B. Not Mastered

Answer: A

Explanation:

Answer Area

Statements	Yes	No
If an iOS update becomes available on Tuesday at 5 AM, the update is installed on Device1 automatically on Wednesday.	<input type="radio"/>	<input checked="" type="radio"/>
If an iPadOS update becomes available on Thursday at 2 AM, the update is installed on Device2 automatically on Thursday.	<input type="radio"/>	<input checked="" type="radio"/>
If an iPadOS update becomes available on Friday at 10 PM, the update is installed on Device3 automatically on Sunday.	<input type="radio"/>	<input checked="" type="radio"/>

You have a Microsoft 365 subscription that contains 1,000 Windows 11 devices enrolled in Microsoft Intune. You plan to create and monitor the results of a compliance policy used to validate the BIOS version of the devices.

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


Actions	Answer Area
Review the compliance dashboard for results.	1
Create and assign a compliance policy that has System Security settings configured.	2
Review the Conditional Access Insights and Reporting workbook for results.	3
Create a PowerShell discovery script and a JSON file.	4
Upload the PowerShell script to Intune.	
Upload the JSON file to Azure AD.	
Create and assign a custom compliance policy.	

- A. Mastered  
B. Not Mastered

**Answer:** A

**Explanation:**

Actions	Answer Area
Review the compliance dashboard for results.	
Create and assign a compliance policy that has System Security settings configured.	
Review the Conditional Access Insights and Reporting workbook for results.	
Create a PowerShell discovery script and a JSON file.	
Upload the PowerShell script to Intune.	
Upload the JSON file to Azure AD.	
Create and assign a custom compliance policy.	



#### NEW QUESTION 10

- (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 12

- (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 16

- (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 20

- (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 22

- (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 25

- (Exam Topic 4)

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

You have a Microsoft 365 subscription

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

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

- Devices must be joined to AD DS regardless of their current working location.
- Users in the marketing department must have a line-of-business (LOB) app installed during the deployment. The solution must minimize administrative effort.

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

#### Answer Area

Devices must be joined to AD DS regardless of their current working location:	<div>Install the Intune connector for Active Directory.</div> <div>Deploy Always On VPN.</div> <div><b>Install the Intune connector for Active Directory.</b></div> <div>Modify the Autopilot deployment profile.</div> <div>Edit the Co-management settings in Intune.</div>
The marketing department users must have an LOB app installed during the deployment:	<div>Modify the Autopilot deployment profile.</div> <div><b>Modify the Autopilot deployment profile.</b></div> <div>Create a Microsoft Intune app deployment.</div> <div>Create a device configuration profile in Intune.</div>

- A. Mastered  
 B. Not Mastered

**Answer: A**

**Explanation:**

#### Answer Area

Devices must be joined to AD DS regardless of their current working location:	<div>Install the Intune connector for Active Directory.</div> <div>Deploy Always On VPN.</div> <div><b>Install the Intune connector for Active Directory.</b></div> <div>Modify the Autopilot deployment profile.</div> <div>Edit the Co-management settings in Intune.</div>
The marketing department users must have an LOB app installed during the deployment:	<div>Modify the Autopilot deployment profile.</div> <div><b>Modify the Autopilot deployment profile.</b></div> <div>Create a Microsoft Intune app deployment.</div> <div>Create a device configuration profile in Intune.</div>

### NEW QUESTION 30

- (Exam Topic 4)

You have a Microsoft 365 E5 subscription that contains 1,000 Windows 11 devices. All the devices are enrolled in Microsoft Intune.

You plan to integrate Intune with Microsoft Defender for Endpoint.

You need to establish a service-to-service connection between Intune and Defender for Endpoint. Which settings should you configure in the Microsoft Endpoint Manager admin center?

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

**Answer: A**

**Explanation:**

Microsoft Defender for Endpoint – Important Service and Endpoint Settings You Should Configure Right Now.

As a prerequisite, however, head to tenant administration > connectors and tokens > Microsoft Defender for Endpoint and confirm the connection is enabled. You previously set this up in the advanced settings of Microsoft 365 Defender.

Reference: <https://petri.com/microsoft-defender-for-endpoint-which-settings-configure-right-now/>

### NEW QUESTION 34

- (Exam Topic 4)

You have a Microsoft Intune subscription.

You are creating a Windows Autopilot deployment profile named Profile1 as shown in the following exhibit.

### Create profile

Windows PC

1 Basics
2 Out-of-box experience (OOBE)
3 Scope tags
4 Assignments
5 Review + create

Configure the out-of-box experience for your Autopilot devices

\* Deployment mode ⓘ

User-Driven

\* Join to Azure AD as ⓘ

Azure AD joined

Microsoft Software License Terms ⓘ

Show Hide

Important information about hiding license terms

Privacy settings ⓘ

Show Hide

The default value for diagnostic data collection has changed for devices running Windows 10, version 1903 and later. [Learn more](#)

Hide change account options ⓘ

Show Hide

User account type ⓘ

Administrator Standard

Allow White Glove OOBE ⓘ

No Yes

Language (Region) ⓘ

Operating system default

Automatically configure keyboard ⓘ

No Yes

Apply device name template ⓘ

No Yes

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

## Answer Area

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

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

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

computer name  
 Cortana settings  
 keyboard layout

- A. Mastered  
 B. Not Mastered

Answer: A

Explanation:

## Answer Area

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

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

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

computer name  
 Cortana settings  
 keyboard layout

NEW QUESTION 39

- (Exam Topic 4)

You have a Microsoft 365 subscription that contains two security groups named Group1 and Group2. Microsoft 365 uses Microsoft Intune Suite.

You use Microsoft Intune to manage devices.

You need to assign roles in Intune to meet the following requirements:

- The members of Group1 must manage Intune roles and assignments.
- The members of Group2 must assign existing apps and policies to users and devices.

The solution must follow the principle of least privilege.

Which role should you assign to each group? To answer, select the appropriate options in the answer area. NOTE: Each correct selection is worth one point.

### Answer Area



Group1: Intune Service Administrator  
Help Desk Operator  
Intune Role Administrator  
Intune Service Administrator  
Policy and Profile Manager

Group2: Policy and Profile Manager  
Help Desk Operator  
Intune Role Administrator  
Intune Service Administrator  
Policy and Profile Manager

- A. Mastered  
B. Not Mastered

**Answer:** A

#### Explanation:

To assign roles in Intune to meet the requirements, you should assign the following roles to each group: Group1: Intune Role Administrator Group2: Help Desk Operator

- The Intune Role Administrator role is the only Intune role that can manage custom Intune roles and add assignments for built-in Intune roles<sup>1</sup>. This role meets the requirement for Group1 to manage Intune roles and assignments.
- The Help Desk Operator role can perform remote tasks on users and devices, and can assign applications or policies to users or devices<sup>1</sup>. This role meets the requirement for Group2 to assign existing apps and policies to users and devices.

### NEW QUESTION 42

- (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 44

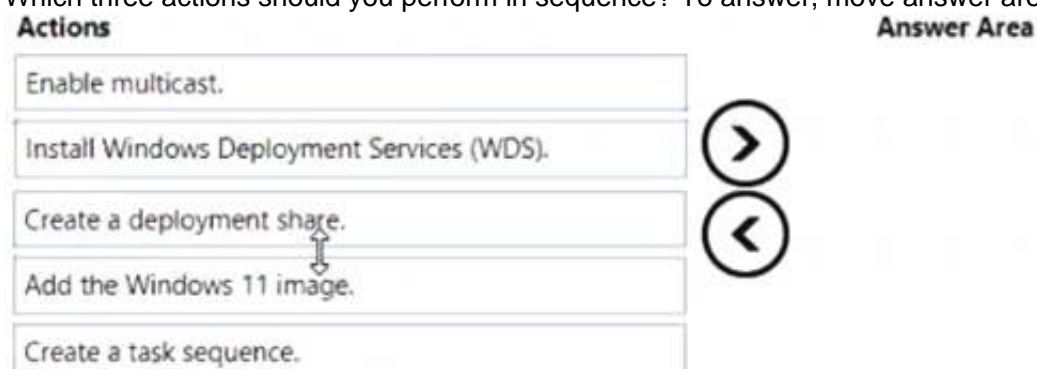
- (Exam Topic 4)

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 47

- (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 49

- (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 52

- (Exam Topic 4)

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

You use Windows Autopilot to deploy Windows 11 to devices.

A support engineer reports that when a deployment fails, they cannot collect deployment logs from failed device.

You need to ensure that when a deployment fails, the deployment logs can be collected.

What should you configure?

- A. the automatic enrollment settings
- B. the Windows Autopilot deployment profile
- C. the enrollment status page (ESP) profile
- D. the device configuration profile

**Answer: B**

## NEW QUESTION 57

- (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:
Import the Deployment Image Servicing and Management (DISM) PowerShell module.
Import the WindowsAutopilotIntune Windows PowerShell module.
Install the Windows Assessment and Deployment Kit (Windows ADK).
Install the Windows Deployment Services server role.

Add to the MDT deployment share:
Windows 10 image and package only
Windows 10 image and task sequence only
Windows 10 image only
Windows 10 image, task sequence, and package

- 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 58

- (Exam Topic 4)

You have a Microsoft 365 subscription.

You plan to use Windows Autopilot to provision 25 Windows 11 devices. You need to configure the Out-of-box experience (OOBE) settings.

What should you create in the Microsoft Intune admin center?

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

**Answer:** B

#### NEW QUESTION 60

- (Exam Topic 4)

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

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

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

[Settings]

Priority=DefaultGateway, Default

[DefaultGateway]

10.1.1.1=NewYork

10.5.5.1=London

[NewYork]

DeployRoot=\\MDT1\Production\$

[London]

DeployRoot=\\MDT2\Production\$

KeyboardLocale=en-gb -

[Default]

DeployRoot=\\MDT3\Production\$

KeyboardLocale=en-us -

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

Name	IP address
LT1	10.1.1.240
DT1	10.5.5.115
TB1	10.2.2.193

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

NOTE: Each correct selection is worth one point.

#### Statements

Yes

No

TB1 will download the image from MDT3.

☐
☐

DT1 will have a KeyboardLocale of en-gb.

☐
☐

LT1 will download the image from MDT1.

☐
☐

- A. Mastered
- B. Not Mastered

**Answer:** A

**Explanation:**

Statements	Yes	No
TB1 will download the image from MDT3.	<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 62**  
- (Exam Topic 3)  
You need to meet the technical requirements for the LEG department computers.  
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

Configure the commercial ID on the LEG department computers.

Create an Azure Machine Learning service workspace.

Create an Azure Log Analytics workspace.

Install the Microsoft Monitoring Agent on the LEG department computers.

Add a solution to a workspace.

Answer Area

A. Mastered

B. Not Mastered

**Answer:** A  
**Explanation:**  
A screenshot of a white box Description automatically generated  
Reference:  
<https://docs.microsoft.com/en-us/windows/deployment/update/windows-analytics-azure-portal>

**NEW QUESTION 66**  
- (Exam Topic 3)  
You need to prepare for the deployment of the Phoenix office computers. What should you do first?

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

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

**NEW QUESTION 68**  
- (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/azure/active-directory/conditional-access/conditions> <https://docs.microsoft.com/en-us/intune/device-compliance-get-started>

NEW QUESTION 70

- (Exam Topic 3)

You are evaluating which devices are compliant.

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 compliant	<input type="radio"/>	<input type="radio"/>
Device3 is compliant	<input type="radio"/>	<input type="radio"/>
Device4 is compliant	<input type="radio"/>	<input type="radio"/>

- A. Mastered
- B. Not Mastered

Answer: A

Explanation:



Statements	Yes	No
Device1 is compliant	<input type="radio"/>	<input checked="" type="radio"/>
Device3 is compliant	<input checked="" type="radio"/>	<input type="radio"/>
Device4 is compliant	<input checked="" type="radio"/>	<input type="radio"/>

#### NEW QUESTION 74

- (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 75

- (Exam Topic 3)

You need to meet the technical requirements for the new HR department computers.

How should you configure the provisioning package? To answer, select the appropriate options in the answer area.

NOTE: Each correct selection is worth one point.

**Specify ComputerName as:**

<input checked="" type="checkbox"/>
"HR" + RAND(4)
"HumanResources-" + RAND(????)
HR-%RAND:4%
HR-????
HumanResources-%RAND:4%

**Specify AccountOU as:**

<input checked="" type="checkbox"/>
CN=Computers, CN=HR, DC=Contoso, DC=com
Computers/HumanResources/Contoso.com
Contoso.com/HR/Computers
OU=Computers, OU=HR, DC=Contoso, DC=com

- A. Mastered
- B. Not Mastered

**Answer:** A

#### Explanation:

Reference:

<https://docs.microsoft.com/en-us/windows/configuration/wcd/wcd-accounts>

#### NEW QUESTION 80

- (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 type="checkbox"/>
An app configuration policy
An app protection policy
Azure information Protection
iOS app provisioning profiles

For the Sales department employees:

<input 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 84

- (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 89

- (Exam Topic 1)

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

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

**Answer:** C

**Explanation:**

Scenario: Windows Autopilot Configuration Assignments

Included groups: Group1

Excluded groups: Group2 Device1 is member of Group1.

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

Group1 and Group2 have a Membership type of Assigned.

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

#### NEW QUESTION 90

- (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.

☐☐

Device4 is marked as compliant.

☐☐

Device5 is marked as compliant.

☐☐

- A. Mastered  
B. Not Mastered

Answer: A

Explanation:  
Text Description automatically generated

NEW QUESTION 95

- (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 97

- (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.

Answer Area

Statements	Yes	No
If User1 adds a shortcut to the desktop of Device1, when User1 signs in to Device3, the same shortcut will appear on the desktop.	<input type="radio"/>	<input type="radio"/>
If User1 sets the desktop background to blue on Device2, when User1 signs in to Device4, the desktop background will be blue.	<input type="radio"/>	<input type="radio"/>
If User2 increases the size of the font in the command prompt of Device2, when User2 signs in to Device3, the command prompt will show the increased font size.	<input type="radio"/>	<input type="radio"/>

- A. Mastered  
B. Not Mastered

Answer: A

Explanation:  
Text, letter Description automatically generated

NEW QUESTION 99

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

- A. Yes  
B. No

Answer: B

NEW QUESTION 101

- (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 105**

- (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 110**

- (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 112**

- (Exam Topic 4)

You have a Microsoft 365 E5 subscription that contains a user named User1 and a web app named Appl. App1 must only accept modern authentication requests.

You plan to create a Conditional Access policy named CAPolicy1 that will have the following settings:

- Assignments
  - Users or workload identities: User1
  - Cloud apps or actions: App1
- Access controls
  - Grant: Block access

You need to block only legacy authentication requests to Appl. Which condition should you add to CAPolicy1?

- A. Filter for devices
- B. Device platforms
- C. User risk
- D. Sign-in risk
- E. Client apps

**Answer:** E

**Explanation:**

you can use the client apps condition to block legacy authentication requests to App11. Legacy authentication is a term that refers to authentication protocols that do not support modern authentication features such as multi-factor authentication or conditional access2. Examples of legacy authentication protocols include Basic Authentication, Digest Authentication, NTLM, and Kerberos2. To block legacy authentication requests, you need to configure the client apps condition to include Other clients, which covers any client that uses legacy authentication protocols13. References: 1: Conditional Access: Block legacy authentication |

Microsoft Learn <https://learn.microsoft.com/en-us/mem/identity-protection/conditional-access/block-legacy-authentication> 2:

What is legacy authentication? | Microsoft Learn

<https://learn.microsoft.com/en-us/mem/identity-protection/conditional-access/legacy-authentication> 3: Client apps condition in Azure Active Directory Conditional Access | Microsoft Learn <https://learn.microsoft.com/en-us/mem/identity-protection/conditional-access/client-apps-condition>

**NEW QUESTION 113**

- (Exam Topic 4)

You have a Microsoft 365 E5 subscription.

You create an app protection policy for Android devices named Policy1 as shown in the following exhibit.



Home > Apps >

## Create policy ...



- 1 Basics 2 **Apps** 3 Data protection 4 Access requirements ...

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

Target to apps on all device types ⓘ ☐ Yes ☒ No

Device types \* ⓘ

Target policy to

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

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

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

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

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

- users only
- devices only
- users and devices

- A. Mastered
- B. Not Mastered

**Answer:** A

### Explanation:

Box 1: Install the Intune Company Portal app on the device

On Android, Android devices will prompt to install the Intune Company Portal app regardless of which Device type is chosen.

Box 2: Devices only

For Android devices, unmanaged devices are devices where Intune MDM management has not been detected. This includes devices managed by third-party MDM vendors.

Reference:

<https://docs.microsoft.com/en-us/mem/intune/apps/app-protection-policies#app-protection-policies-for-iosipado>

### NEW QUESTION 116

- (Exam Topic 4)

You have a Microsoft 365 tenant that uses Microsoft Intune.

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

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

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

**Answer:** AC

### NEW QUESTION 120

- (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 122

- (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: Device1 and Device3 only

In-place upgrade: Device1 and Device3 only

- A. Mastered
- B. Not Mastered

Answer: A

Explanation:

Answer Area

Windows Autopilot: Device1 and Device3 only

In-place upgrade: Device1 and Device3 only

NEW QUESTION 127

- (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 132

- (Exam Topic 4)  
You have a Microsoft 365 E5 subscription that contains 150 hybrid Azure AD joined Windows devices. All the devices are enrolled in Microsoft Intune. You need to configure Delivery Optimization on the devices to meet the following requirements:

- Allow downloads from the internet and from other computers on the local network.
- Limit the percentage of used bandwidth to 50. What should you use?

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

Answer: A

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

- > Windows 10 Delivery Optimization settings for Intune - Microsoft Intune | Microsoft Learn
- > Delivery Optimization settings in Microsoft Intune

NEW QUESTION 136

- (Exam Topic 4)  
You have a Microsoft 365 E5 subscription that contains 100 Windows 10 devices enrolled in Microsoft Intune. You plan to use Endpoint analytics. You need to create baseline metrics. What should you do first?

- A. Create an Azure Monitor workbook.

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

**Answer:** C

**Explanation:**

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

**NEW QUESTION 137**

- (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

Quality update deferral period (days): 14

Grace period: 3

- A. Mastered
- B. Not Mastered

**Answer:** A

**Explanation:**



### Answer Area

Feature update deferral period (days): 90

Quality update deferral period (days): 14

Grace period: 3

### NEW QUESTION 140

- (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:

<input checked="" type="checkbox"/>
An Azure Storage account
Azure Cosmos DB
Azure SQL Database
Log Analytics

Action to perform on the computers:

<input checked="" type="checkbox"/>
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:

<input type="checkbox"/>	An Azure Storage account
<input type="checkbox"/>	Azure Cosmos DB
<input type="checkbox"/>	Azure SQL Database
<input checked="" type="checkbox"/>	Log Analytics

Action to perform on the computers:

<input type="checkbox"/>	Create a collector-initiated subscription
<input checked="" type="checkbox"/>	Install the Microsoft Monitoring Agent
<input type="checkbox"/>	Enroll in Microsoft Intune
<input type="checkbox"/>	Register to Azure Active Directory (Azure AD)

### NEW QUESTION 145

- (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 148

- (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	<i>Not applicable</i>	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 149

- (Exam Topic 4)

You have a Microsoft 365 E5 subscription that contains a group named Group1.

You create a Conditional Access policy named CAPolicy1 and assign CAPolicy1 to Group1.

You need to configure CAPolicy1 to require the members of Group1 to reauthenticate every eight hours when they connect to Microsoft Exchange Online.

What should you configure?

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

**Answer:** A

### Explanation:

User sign-in frequency

Sign-in frequency defines the time period before a user is asked to sign in again when attempting to access a resource.

The Azure Active Directory (Azure AD) default configuration for user sign-in frequency is a rolling window of 90 days.

Sign-in frequency control

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

Select Sign-in frequency.

Choose Periodic reauthentication and enter a value of hours or days or select Every time.

- Save your policy. Reference:

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

### NEW QUESTION 151

- (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 152

- (Exam Topic 4)

You have an Azure AD tenant and 100 Windows 10 devices that are Azure AD joined and managed by using Microsoft Intune. You need to configure Microsoft Defender Firewall and Microsoft Defender Antivirus on the devices. The solution must minimize administrative effort. Which two actions should you perform? Each correct answer presents part of the solution. NOTE: Each correct selection is worth one point.

- A. To configure Microsoft Defender Antivirus, create a Group Policy Object (GPO) and configure the Windows Defender Antivirus settings.
- B. To configure Microsoft Defender Firewall, create a device configuration profile and configure the Device restrictions settings.
- C. To configure Microsoft Defender Antivirus, create a device configuration profile and configure the Endpoint protection settings.
- D. To configure Microsoft Defender Antivirus, create a device configuration profile and configure the Device restrictions settings.
- E. To configure Microsoft Defender Firewall, create a device configuration profile and configure the Endpoint protection settings.
- F. To configure Microsoft Defender Firewall, create a Group Policy Object (GPO) and configure Windows Defender Firewall with Advanced Security.

**Answer:** CE

**Explanation:**

To configure Microsoft Defender Firewall and Microsoft Defender Antivirus on Azure AD joined devices that are managed by Intune, you need to create a device configuration profile and configure the Endpoint protection settings. You can use this profile to configure various settings for firewall and antivirus protection on the devices. References:

<https://docs.microsoft.com/en-us/mem/intune/protect/endpoint-protection-windows-10>

**NEW QUESTION 155**

- (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 157**

- (Exam Topic 4)

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

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

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

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

**Answer:** B

**Explanation:**

\* Admin1

An application admin has full access to enterprise applications, applications registrations, and application proxy settings.

\* Admin2

Mark your app as publisher verified.

In Azure AD this user must be a member of one of the following roles: Application Admin, Cloud Application Admin, or Global Admin.

\* Admin3

Office Apps admin - Assign the Office Apps admin role to users who need to do the following:

- Use the Office cloud policy service to create and manage cloud-based policies for Office
- Create and manage service requests
- Manage the What's New content that users see in their Office apps
- Monitor service health Reference:

Office Apps admin - Assign the Office Apps admin role to users who need to do the following <https://docs.microsoft.com/en-us/azure/active-directory/develop/mark-app-as-publisher-verified>

**NEW QUESTION 159**

- (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 161

- (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:

Device restriction

Delivery optimization

Device restriction

Endpoint protection

Identity protection

Rename the local Administrator account:

Identity protection

Delivery optimization

Device restriction

Endpoint protection

Identity protection

- A. Mastered
- B. Not Mastered

Answer: A

Explanation:

Answer Area

Deploy a custom Start layout:

Device restriction

Delivery optimization

Device restriction

Endpoint protection

Identity protection

Rename the local Administrator account:

Identity protection

Delivery optimization

Device restriction

Endpoint protection

Identity protection

NEW QUESTION 166

- (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	<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 170**  
- (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 172**

- (Exam Topic 4)

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

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

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

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

**Answer:** B

**NEW QUESTION 175**

- (Exam Topic 4)

Your company has computers that run Windows 10 and are Microsoft Azure Active Directory (Azure AD)-joined.

The company purchases an Azure subscription.

You need to collect Windows events from the Windows 10 computers in Azure. The solution must enable you to create alerts based on the collected events.

What should you create in Azure and what should you configure on the computers? To answer, select the appropriate options in the answer area.

NOTE: Each correct selection is worth one point.

**Answer Area**

Resource to create in Azure:	<div><div></div><div>An Azure event hub</div><div>An Azure Log Analytics workspace</div><div>An Azure SQL database</div><div>An Azure Storage account</div></div>
Configuration to perform on the computers:	<div><div></div><div>Configure the Event Collector service</div><div>Create an event subscription</div><div>Install the Microsoft Monitoring Agent</div></div>

- A. Mastered
- B. Not Mastered

**Answer:** A

**Explanation:**

A screenshot of a computer Description automatically generated

Reference:

<https://docs.microsoft.com/en-us/azure/azure-monitor/platform/log-analytics-agent>

**NEW QUESTION 179**

- (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 181

- (Exam Topic 4)

You have a Microsoft 365 subscription.

You have devices enrolled in Microsoft Intune as shown in the following table. To which devices can you deploy apps by using Intune?

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

Answer: E

NEW QUESTION 186

- (Exam Topic 4)

Your network contains an Active Directory domain. The domain contains 2,000 computers that run Windows 10. You implement hybrid Azure AD and Microsoft Intune.

You need to automatically register all the existing computers to Azure AD and enroll the computers in Intune. The solution must minimize administrative effort. What should you use?

- A. an Autodiscover address record
- B. a Group Policy object (GPO)
- C. an Autodiscover service connection point (SCP)
- D. a Windows Autopilot deployment profile

Answer: D

NEW QUESTION 189

- (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 190

- (Exam Topic 4)

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

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

You purchase the devices shown in the following table.

Name	Type
Device1	Windows 10
Device2	Android

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

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

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

NOTE: Each correct selection is worth one point.

Answer Area

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

- A. Mastered
- B. Not Mastered

Answer: A

Explanation:

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

#### NEW QUESTION 194

- (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 197**

- (Exam Topic 4)

Your company has a computer named Computer1 that runs Windows 10. Computer1 was used by a user who left the company.

You plan to repurpose Computer1 and assign the computer to a new user. You need to redeploy Computer1 by using Windows Autopilot.

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

Actions	Answer Area
Upload the file by using Microsoft Intune.	
Generate a CSV file that contains the computer information.	
Reset the computer.	
Generate a JSON file that contains the computer information.	
Upload the file by running azcopy.exe.	

- A. Mastered
- B. Not Mastered

**Answer:** A

**Explanation:**

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

- Generate a JSON file that contains the computer information. This file specifies the Autopilot profile to be applied during the deployment. You can use the Get-AutopilotProfilesForExistingDevices PowerShell script to generate this file1.
- Reset the computer. You can use the Windows Automatic Redeployment feature to trigger a reset from the login screen by pressing Ctrl + R and providing an administrator account2. Alternatively, you can use the Windows Autopilot Reset feature to remotely reset the device from Intune1.
- Upload the file by running azcopy.exe. This step copies the JSON file to a blob storage account in Azure, where it can be accessed by the device during the deployment. You need to specify the storage account name, access key, and container name as parameters for azcopy.exe1.

**NEW QUESTION 198**

- (Exam Topic 4)

You have a Microsoft 365 E5 subscription that contains a user named User1. You need to perform the following tasks for User1:

- Set the Usage location to Canada.
  - Configure the Phone and Email authentication contact info for self-service password reset (SSPR). Which two settings should you configure in the Azure Active Directory admin center? To answer, select the appropriate settings in the answer area.
- NOTE: Each correct selection is worth one point.

## Manage

	Profile
	Custom security attributes (Preview)
	Assigned roles
	Administrative units
	Groups
	Applications
	Licenses
	Devices
	Azure role assignments
	Authentication methods

- A. Mastered
- B. Not Mastered

**Answer:** A

**Explanation:**

Graphical user interface, application Description automatically generated

### NEW QUESTION 201

- (Exam Topic 4)

You have a Microsoft 365 subscription that uses Microsoft Intune. You have five new Windows 11 Pro devices.

You need to prepare the devices for corporate use. The solution must meet the following requirements:

- Install Windows 11 Enterprise on each device.
- Install a Windows Installer (MSI) package named App1 on each device.
- Add a certificate named Certificate1 that is required by App1.
- Join each device to Azure AD.

Which three provisioning options can you use? Each correct answer presents a complete solution. NOTE: Each correct selection is worth one point.

- A. subscription activation
- B. a custom Windows image
- C. an in-place upgrade
- D. Windows Autopilot
- E. provisioning packages

**Answer:** BDE

### NEW QUESTION 202

- (Exam Topic 4)

You have a Microsoft 365 subscription that includes Microsoft Intune.

You have an update ring named UpdateRing1 that contains the following settings:

- Automatic update behavior: Auto install and restart at a scheduled time
- Automatic behavior frequency: First week of the month
- Scheduled install day: Tuesday
- Scheduled install time: 3 AM

From the Microsoft Intune admin center, you select Uninstall for the feature updates of UpdateRing1. When will devices start to remove the feature updates?

- A. when a user approves the uninstall
- B. as soon as the policy is received
- C. next Tuesday
- D. the first Tuesday of the next month

**Answer:** C



#### NEW QUESTION 207

- (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 210

- (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 212

- (Exam Topic 4)

You have a Microsoft 365 subscription that contains 500 Android Enterprise devices. All the devices are enrolled in Microsoft Intune.

You need to deliver bookmarks to the Chrome browser on the devices What should you create?

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

**Answer:** D

#### NEW QUESTION 213

- (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 218

- (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



**NEW QUESTION 222**

- (Exam Topic 4)

You have a Microsoft Intune subscription that has the following device compliance policy settings: Mark devices with no compliance policy assigned as: Compliant  
 Compliance status validity period (days): 14

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

Name	BitLocker Drive Encryption (BitLocker)	Firewall	Scope (Tags)	Member of
Device1	Enabled	Off	Tag1	Group1
Device2	Disabled	On	Tag2	Group2

On January 4, you create the following two device compliance policies:

- > Name: Policy1
- > Platform: Windows 10 and later
- > Require BitLocker: Require
- > Mark device noncompliant: 5 days after noncompliance
- > Scope (Tags): Tag1
- > Name: Policy2
- > Platform: Windows 10 and later
- > Firewall: Require
- > Mark device noncompliant: Immediately
- > Scope (Tags): Tag2

On January 5, you assign Policy1 and Policy2 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
On January 7, Device1 is marked as compliant.	<input type="radio"/>	<input type="radio"/>
On January 8, Device1 is marked as compliant.	<input type="radio"/>	<input type="radio"/>
On January 8, Device2 is marked as compliant.	<input type="radio"/>	<input type="radio"/>

- A. Mastered
- B. Not Mastered

**Answer:** A

**Explanation:**

Box 1: No.

Policy1 and Policy2 apply to Group1 which Device1 is a member of. Device1 does not meet the firewall requirement in Policy2 so the device will immediately be marked as non-compliant.

Box 2: No

For the same reason as Box1. Box 3: Yes

Policy1 and Policy2 apply to Group1. Device2 is not a member of Group1 so the policies don't apply.

The Scope (tags) have nothing to do with whether the policy is applied or not. The tags are used in RBAC.

**NEW QUESTION 226**

- (Exam Topic 4)

You have a Microsoft 365 E5 subscription and a computer that runs Windows 11. You need to create a customized installation of Microsoft 365 Apps for enterprise.

Which four actions should you perform in sequence? To answer, move the appropriate cmdlets from the list of cmdlets to the answer area and arrange them in the



correct order.

Actions	Answer Area
Run setup.exe and specify the /packager switch.	
Download the Microsoft Office Deployment Tool (ODT) and run the self-extracting executable (.exe) file.	
Edit the XML configuration file.	
Run setup.exe and specify the /download switch.	
Run setup.exe and specify the /configure switch.	

Navigation arrows: > and <

Answer navigation: ^ and v

- A. Mastered
- B. Not Mastered

**Answer:** A

**Explanation:**

- \* 1. Download ODT application
  - \* 2. Create a configuration file (XML)
  - \* 3. setup.exe /download to download the installation files
  - \* 4. setup.exe /configure to deploy the application
- <https://learn.microsoft.com/en-us/deployoffice/deploy-microsoft-365-apps-local-source>

**NEW QUESTION 227**

- (Exam Topic 4)

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

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

**Answer:** A

**NEW QUESTION 231**

- (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 234**

- (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 237**

- (Exam Topic 4)

You have SOO Windows 10 devices enrolled in Microsoft Intune. You plan to use Exploit protection in Microsoft Intune to enable the following system settings on the devices:

- Data Execution Prevention (DEP)
- Force randomization for images (Mandatory ASIR)

You need to configure a Windows 10 device that will be used to create a template file. Which protection areas on the device should you configure in the Windows Security app before you create the template file? To answer, drag the appropriate protection areas to the correct settings. Each protection area 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.

Protection areas	Answer Area
Account protection	DEP: <input type="text"/>
App & browser control	Mandatory ASLR: <input type="text"/>
Device security	
Virus & threat protection	

- A. Mastered
- B. Not Mastered

**Answer:** A

**Explanation:**

Exploit protection is a feature that helps protect against malware that uses exploits to infect devices and spread. Exploit protection consists of many mitigations that can be applied to either the operating system or individual apps1.

To configure a Windows 10 device that will be used to create a template file for Exploit protection, you need to configure the following protection areas on the device in the Windows Security app:

- DEP: Device security. Data Execution Prevention (DEP) is a mitigation that prevents code from running in memory regions marked as non-executable. You can enable DEP system-wide or for specific apps in the Device security section of the Windows Security app1.
- Mandatory ASLR: App & browser control. Force randomization for images (Mandatory ASLR) is a mitigation that randomizes the location of executable images in memory, making it harder for attackers to predict where to inject code. You can enable Mandatory ASLR system-wide or for specific apps in the App & browser control section of the Windows Security app1.

**NEW QUESTION 241**

- (Exam Topic 4)

You have a Microsoft Deployment Toolkit (MDT) deployment share named DS1.

in the Out-of-Box Drivers node, you create folders that contain drivers for different hardware models.

You need to configure the Inject Drivers MDT task to use PnP detection to install the drivers for one of the hardware models.

What should you do first?

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

**Answer:** B

**NEW QUESTION 245**

- (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 247**

- (Exam Topic 4)

Your company standardizes on Windows 10 Enterprise for all users.

Some users purchase their own computer from a retail store. The computers run Windows 10 Pro.

You need to recommend a solution to upgrade the computers to Windows 10 Enterprise, join the computers to Azure AD, and install several Microsoft Store apps.

The solution must meet the following

requirements:

- Ensure that any applications installed by the users are retained.
- Minimize user intervention.

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

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

D. Windows Deployment Services (WDS)

**Answer:** A

#### NEW QUESTION 252

- (Exam Topic 4)

You have a Microsoft 365 subscription.

You need provide a user the ability to disable Security defaults and principle of least privilege. Which role should you assign to the user?

- A. Global Administrator
- B. Conditional Access Administrator
- C. Security Administrator
- D. Intune Administrator

**Answer:** B

#### Explanation:

To enable or disable security defaults in your directory, sign in to the Azure portal as a security administrator, Conditional Access administrator, or global administrator.

Note: Conditional Access Administrator

Users with this role have the ability to manage Azure Active Directory Conditional Access settings.

Reference:

<https://docs.microsoft.com/en-us/azure/active-directory/fundamentals/concept-fundamentals-security-defaults>

#### NEW QUESTION 254

.....

## Relate Links

**100% Pass Your MD-102 Exam with ExamBible Prep Materials**

<https://www.exambible.com/MD-102-exam/>

## Contact us

We are proud of our high-quality customer service, which serves you around the clock 24/7.

Viste - <https://www.exambible.com/>