

MD-102^{Q&As}

Endpoint Administrator

Pass Microsoft MD-102 Exam with 100% Guarantee

Free Download Real Questions & Answers **PDF** and **VCE** file from:

<https://www.certbus.com/md-102.html>

100% Passing Guarantee
100% Money Back Assurance

Following Questions and Answers are all new published by Microsoft
Official Exam Center

-  **Instant Download** After Purchase
-  **100% Money Back** Guarantee
-  **365 Days** Free Update
-  **800,000+** Satisfied Customers



QUESTION 1

Your company uses Microsoft Intune.

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

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

You need to ensure that the policies can target the devices based on their version of Android or iOS.

What should you configure first?

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

Correct Answer: A

We can create dynamic groups by using the deviceOSVersion or deviceOSType properties, and then apply Intune configuration policies to those groups.

Reference: <https://docs.microsoft.com/en-us/archive/blogs/pauljones/dynamic-group-membership-in-azure-active-directory-part-2> <https://docs.microsoft.com/en-ie/mem/intune/enrollment/device-group-mapping>

QUESTION 2

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

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

Which devices can be activated by using subscription activation?

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

Correct Answer: C

Windows subscription activation The subscription activation feature enables you to "step-up" from Windows Pro edition to Enterprise or Education editions. You can use this feature if you're subscribed to Windows Enterprise E3 or E5 licenses. Subscription activation also supports step-up from Windows Pro Education edition to Education edition.

Devices must be Azure AD-joined or hybrid Azure AD joined. Workgroup-joined or Azure AD registered devices aren't supported.

Reference: <https://learn.microsoft.com/en-us/windows/deployment/windows-10-subscription-activation>

QUESTION 3

HOTSPOT

You have a Microsoft 365 E5 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
- ✔ Configuration settings
- ✔ Scope tags
- ✔ Assignments
- 5 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.

Hot Area:

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"/>

Correct Answer:

Answer Area

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

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

Correct Answer: D

Android Enterprise device settings list to allow or restrict features on corporate-owned devices using Intune

Device experience Use these settings to configure a kiosk-style experience on your dedicated devices, or to customize the home screen experiences on your fully managed devices. You can configure devices to run one app, or run many apps. When a device is set with kiosk mode, only the apps you add are available.

Note: You can control and restrict on Android Enterprise devices owned by your organization. As part of your mobile device management (MDM) solution, use these settings to allow or disable features, run apps on dedicated devices, control security, and more.

This feature applies to:

1.

Android Enterprise corporate-owned work profile (COPE)

2.

Android Enterprise corporate owned fully managed (COBO)

3.

Android Enterprise corporate owned dedicated devices (COSU)

Reference: <https://learn.microsoft.com/en-us/mem/intune/configuration/device-restrictions-android-for-work>

QUESTION 5

DRAG DROP

Your company has a Microsoft 365 E5 tenant.

All the devices of the company are enrolled in Microsoft Intune.

You need to create advanced reports by using custom queries and visualizations from raw Microsoft Intune data.

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.

Select and Place:

Actions

- Create a Microsoft SharePoint Online site.
- Purchase an Azure subscription.
- Add diagnostic settings.
- Install Microsoft Power BI Desktop.
- Create a Log Analytics workspace.
- Add a certificate connector to Microsoft Intune.

Answer Area



Correct Answer:

Actions

- Create a Microsoft SharePoint Online site.
-
-
- Install Microsoft Power BI Desktop.
-
- Add a certificate connector to Microsoft Intune.

Answer Area

- Purchase an Azure subscription.
- Create a Log Analytics workspace.
- Add diagnostic settings.



Step 1: Purchase an Azure subscription.

Complex reporting functionality require an Azure subscription.

Step 2: Create a Log Analytics workspace.

Each Azure resource requires its own diagnostic setting. The diagnostic setting defines the following for a resource:

*

One or more destinations to send the logs. Current destinations include Log Analytics workspace, Event Hubs, and Azure Storage.

*

Categories of logs and metric data sent to the destinations defined in the setting. The available categories will vary for different resource types.

*

Retention policy for data stored in Azure Storage.

Step 3: Add diagnostic settings.

You can create and view custom reports using the following steps:

1.

Sign in to the Microsoft Endpoint Manager admin center.

2.

Select Reports > Diagnostic settings add a diagnostic setting.

3.

Etc.

Reference: <https://docs.microsoft.com/en-us/mem/intune/fundamentals/reports>

QUESTION 6

HOTSPOT


You need to meet the technical requirements for Windows AutoPilot.

Which two settings should you configure from the Azure Active Directory blade? To answer, select the appropriate settings in the answer area.

NOTE: Each correct selection is worth one point.

Hot Area:


 Overview


 Getting started


Manage

 Users


 Groups

 Organizational relationships

 Roles and administrators

 Enterprise applications

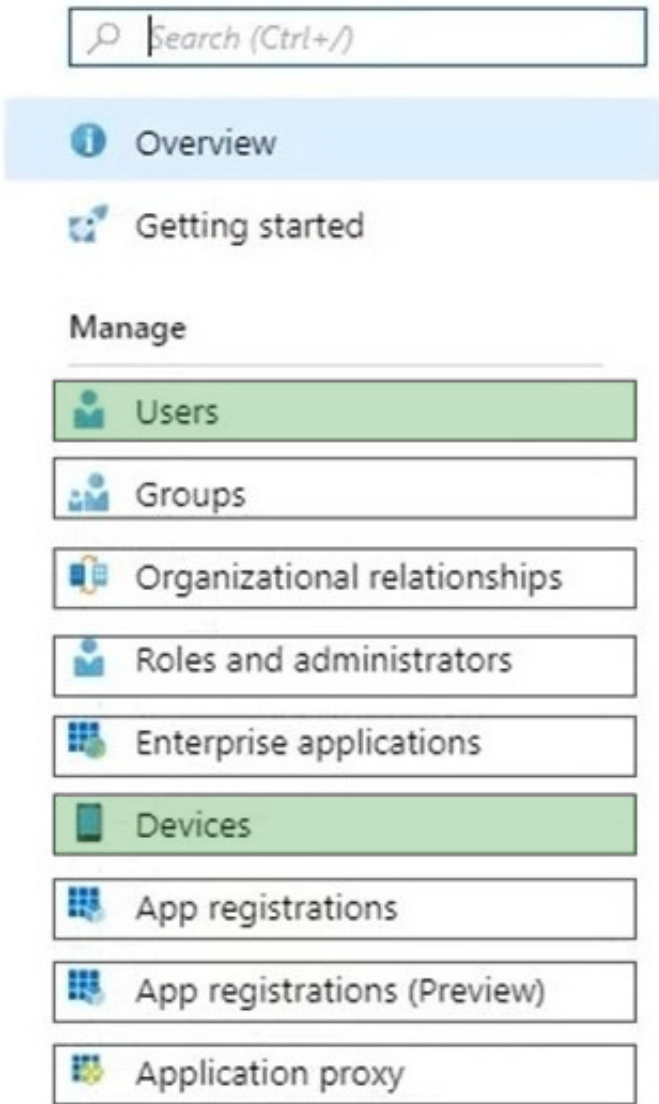
 Devices

 App registrations

 App registrations (Preview)

 Application proxy

Correct Answer:



References:

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

QUESTION 7

HOTSPOT

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

Name	Member of
User1	Group1
User2	None
User3	None

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

Device management [Edit](#)

Device configuration profiles (1)

Name	Platform	Profile Type
ConfigurationProfile1	Windows 10 and later	Device restrictions

Device compliance policies (1)

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

Device enrollment [Edit](#)

Windows autopilot deployment profiles

No results

Enrollment status pages

No results.

Assignments [Edit](#)

Included groups	All Users
Excluded groups	Group1

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

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

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

Hot Area:

Answer Area

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

Correct Answer:

Answer Area

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

QUESTION 8

You have a Microsoft 365 E5 subscription that contains 100 iOS devices enrolled in Microsoft Intune.

You need to ensure that notifications of iOS updates are deferred for 30 days after the updates are released.

What should you create?

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

Correct Answer: D

<https://learn.microsoft.com/en-us/mem/intune/protect/software-updates-ios> <https://learn.microsoft.com/en-us/mem/intune/protect/software-updates-ios#delay-visibility-of-software-updates>

QUESTION 9

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

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

Correct Answer: C

Windows client custom profiles use Open Mobile Alliance Uniform Resource Identifier (OMA-URI) settings to configure different features. These settings are typically used by mobile device manufacturers to control features on the device.

Reference: <https://docs.microsoft.com/en-us/mem/intune/configuration/custom-settings-windows-10>

QUESTION 10

HOTSPOT

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

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

All devices contain an app named App1 and are enrolled in Microsoft Intune.

You need to prevent users from copying data from App1 and pasting the data into other apps.

Which type of policy and how many policies should you create in Intune? To answer, select the appropriate options in the answer area.

NOTE: Each correct selection is worth one point.

Hot Area:

Answer Area

Policy type: ▼

App configuration policy
App protection policy
Conditional access policy
Device compliance policy

Minimum number of policies: ▼

1
2
3
4
5

Correct Answer:

Answer Area

Policy type: ▼

App configuration policy
App protection policy
Conditional access policy
Device compliance policy

Minimum number of policies: ▼

1
2
3
4
5

QUESTION 11

You need to meet the technical requirements for the iOS devices. Which object should you create in Intune?

- A. a deployment profile
- B. an app protection policy

- C. a device configuration profile
- D. a compliance policy

Correct Answer: C

Scenario: Technical requirements include: Block iOS devices from sending diagnostic and usage telemetry data.

Create a device configuration profile.

Note: Intune includes device restriction policies that help administrators control Android, iOS, macOS, and Windows devices. These restrictions let you control a wide range of settings and features to protect your organization's resources. For example, administrators can:

Allow or block the device camera Control access to Google Play, app stores, viewing documents, and gaming Block built-in apps, or create a list of apps that allowed or prohibited Allow or prevent backing up files to cloud and storage accounts Set a minimum password length, and block simple passwords

Reference: <https://docs.microsoft.com/en-us/intune/device-restrictions-configure>

QUESTION 12

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.

Correct Answer: C

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

QUESTION 13

HOTSPOT

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

NOTE: Each correct selection is worth one point.

Hot Area:

Answer Area

Statements	Yes	No
If User1 joins a Windows 10 device to Azure AD, the device will be enrolled in Intune automatically.	<input type="radio"/>	<input type="radio"/>
If User2 joins a Windows 10 device to Azure AD, the device will be enrolled in Intune automatically.	<input type="radio"/>	<input type="radio"/>
If User3 joins a Windows 10 device to Azure AD, the device will be enrolled in Intune automatically.	<input type="radio"/>	<input type="radio"/>

Correct Answer:

Answer Area

Statements	Yes	No
If User1 joins a Windows 10 device to Azure AD, the device will be enrolled in Intune automatically.	<input type="radio"/>	<input checked="" type="radio"/>
If User2 joins a Windows 10 device to Azure AD, the device will be enrolled in Intune automatically.	<input checked="" type="radio"/>	<input type="radio"/>
If User3 joins a Windows 10 device to Azure AD, the device will be enrolled in Intune automatically.	<input type="radio"/>	<input checked="" type="radio"/>

Box 1: No

User1 is a Cloud device administrator.

Local administrative privileges are required when enrolling an already configured Windows 10 device in Intune.

Cloud Device Administrator

Users in this role can enable, disable, and delete devices in Azure AD and read Windows 10 BitLocker keys (if present) in the Azure portal. The role does not grant permissions to manage any other properties on the device.

Note: The Windows 10 devices are joined to Azure AD and enrolled in Microsoft Intune.

Box 2: Yes

User2 is an Azure AD joined device local administrator.

Azure AD Joined Device Local Administrator

This role is available for assignment only as an additional local administrator in Device settings. Users with this role become local machine administrators on all Windows 10 devices that are joined to Azure Active Directory. They do not have

the ability to manage devices objects in Azure Active Directory.

Box 3: No

User3 is a Global reader.

Global Reader

Users in this role can read settings and administrative information across Microsoft 365 services but can't take management actions.

Reference:

<https://docs.microsoft.com/en-us/troubleshoot/mem/intune/no-permission-to-enroll-windows-devices>

<https://learn.microsoft.com/en-us/azure/active-directory/roles/permissions-reference>

QUESTION 14

Note: This question is part of a series of questions that present the same scenario. Each question in the series contains a unique solution that might meet the stated goals. Some question sets might have more than one correct solution, while

others might not have a correct solution.

After you answer a question in this section, you will NOT be able to return to it. As a result, these questions will not appear in the review screen.

Your company has an Azure AD tenant named contoso.com that contains several Windows 10 devices.

When you join new Windows 10 devices to contoso.com, users are prompted to set up a four-digit pin.

You need to ensure that the users are prompted to set up a six-digit pin when they join the Windows 10 devices to contoso.com.

Solution: From the Microsoft Entra admin center, you modify the User settings and the Device settings.

Does this meet the goal?

A. Yes

B. No

Correct Answer: B

Instead, from the Azure Active Directory admin center, you configure automatic mobile device management (MDM) enrollment. From the Endpoint Management admin center, you configure the Windows Hello for Business enrollment options.

Reference: <https://docs.microsoft.com/en-us/intune/protect/windows-hello>

QUESTION 15

HOTSPOT

You have a Microsoft 365 E5 subscription that contains a computer named Computer1 that runs Windows 11. Computer1 is enrolled in Microsoft Intune.

You need to deploy an app named App1 to Computer1. The App1 installation will use multiple files.

What should you use to package App1, and which file format will be used? To answer, select the appropriate options in the answer area.

NOTE: Each correct selection is worth one point.

Hot Area:

Answer Area

Use:

	▼
Deployment Image Servicing and Management (DISM)	
Microsoft Application Virtualization (App-V) Sequencer	
Win32 Content Prep Tool	
Windows Package Manager	

File format:

	▼
.apk	
.appv	
.intunewin	
.ipa	

Correct Answer:

Answer Area

Use: ▼

Deployment Image Servicing and Management (DISM)
Microsoft Application Virtualization (App-V) Sequencer
Win32 Content Prep Tool
Windows Package Manager

File format: ▼

.apk
.appv
.intunewin
.ipa

Box 1: Win32 Content Prep Tool Use:

In Microsoft Intune, there isn't a direct way to deploy .exe files. Instead, you need to package the .exe file using one of the supported formats, such as .intunewin or .msi, before deploying it. Here are two common methods to deploy .exe files via Intune:

Wrap the .exe file in a .intunewin package:

*

Create an application package by using the Microsoft Win32 Content Prep Tool (IntuneWinAppUtil.exe). This tool allows you to convert a .exe file into a .intunewin package.

*

Download the IntuneWinAppUtil.exe tool from the Microsoft Download Center.

Open a command prompt and run the following command to convert the .exe file into a .intunewin package:

*

```
IntuneWinAppUtil.exe -c -s -o
```

Replace with the path to the .exe file, with the path to the setup file or installation script, and with the desired output folder for the .intunewin package.

Box 2: . intunewin

File format:

Does Intune support .exe files?

In Microsoft Intune, there isn't a direct way to deploy .exe files. Instead, you need to package the .exe file using one of the supported formats, such as . intunewin or . msi, before deploying it.

Reference: <https://learn.microsoft.com/en-us/answers/questions/1312151/how-to-deploy-apps-with-exe-file-extension->

via-int

[Latest MD-102 Dumps](#)

[MD-102 Study Guide](#)

[MD-102 Exam Questions](#)