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.geekcert.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 network contains an Active Directory domain named contoso.com. The domain contains 25 computers that run Windows 11.

You have a Microsoft 365 subscription

You have an Azure AD tenant that syncs with contoso.com.

You configure hybrid Azure AD join and discover that some of the computers have a registered state of Pending.

You need to ensure that the computers complete the join successfully.

What should you ensure?

A. that Windows is activated on all the computers

B. that the users of the computers are assigned Microsoft 365 licenses

C. that each computer has a line of sight to a domain controller

D. that the computers contain the latest quality updates

Correct Answer: C

Pending devices in Azure Active Directory

How a device gets stuck in a pending state:

There are two scenarios in which a device can be stuck in a pending state.

Sync a new on-premises domain joined device to Azure AD

A new on-premises device can get stuck in a pending state if it can\\'t complete the device registration process. This problem can be caused by several factors, such as that the *device can\\'t connect to the registration service*.

To troubleshoot a device registration problem, see:

Troubleshooting hybrid Azure Active Directory joined devices

*-> Test Device Registration Connectivity

Note: Pending devices are devices that are synced to Azure Active Directory (Azure AD) from your on-premises Active Directory, but haven\\'t completed registration with the Azure AD device registration service. When the registered state of a

device is pending, the device can\\'t complete any authorization or authentication requests, such as requesting a Primary Refresh token for single sign-on, or applying device-based Conditional Access policies.

Reference:

https://learn.microsoft.com/en-us/troubleshoot/azure/active-directory/pending-devices

QUESTION 2

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

Correct Answer: DE

D: Microsoft Intune includes many built-in settings to control different features on a device. You can also create custom profiles, which are created similar to built-in profiles. Custom profiles are great when you want to use device settings and features that aren\\'t built in to Intune. These profiles include features and settings for you to control on devices in your organization. For example, you can create a custom profile that sets the same feature for every Windows device.

E Set up Insider Preview builds using Intune

1.

Log in to the Azure portal and select Intune.

2.

Go to Software Updates > Windows 10 Update Rings and select + Create to make an Update Ring policy. Add a name and select the Settings section to configure its settings.

3.

Etc.

Reference: https://docs.microsoft.com/en-us/windows-insider/business/manage-builds

QUESTION 3

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

Correct Answer: A

Manage regular users

By default, Microsoft Entra ID adds the user performing the Microsoft Entra join to the administrator group on the device. If you want to prevent regular users from becoming local administrators, you have the following options:

*-> Windows Autopilot - Windows Autopilot provides you with an option to prevent primary user performing the join from becoming a local administrator by creating an Autopilot profile.

* Bulk enrollment - a Microsoft Entra join that is performed in the context of a bulk enrollment happens in the context of an autocreated user. Users signing in after a device has been joined aren\\'t added to the administrators group.

Reference: https://learn.microsoft.com/en-us/azure/active-directory/devices/assign-local-admin

---

QUESTION 4

You have a Microsoft 365 Business Standard subscription and 100 Windows 10 Pro devices.

You purchase a Microsoft 365 E5 subscription.

You need to upgrade the Windows 10 Pro devices to Windows 10 Enterprise. The solution must minimize administrative effort.

Which upgrade method should you use?

A. Windows Autopilot

B. a Microsoft Deployment Toolkit (MDT) lite-touch deployment

C. Subscription Activation

D. an in-place upgrade by using Windows installation media

Correct Answer: C

Windows 10/11 Subscription Activation Windows 10 Pro supports the Subscription Activation feature, enabling users to “step-up” from Windows 10 Pro or Windows 11 Pro to Windows 10 Enterprise or Windows 11 Enterprise, respectively, if they are subscribed to Windows 10/11 Enterprise E3 or E5.

Reference: https://docs.microsoft.com/en-us/windows/deployment/windows-10-subscription-activation

---

QUESTION 5

You have a Microsoft 365 Subscription that uses Microsoft Intune. You add apps to Intune as shown in the following

table.

Name	App type
App1	Android store app
App2	Android line-of-business app
App3	Managed Google Play app

You need to create an app configuration policy named Policy1 for the Android Enterprise platform. Which apps can you manage by using Policy1?

A. App2 only

B. App3 only

C. App1 and App3 only

D. App2 and App3 only

E. App1, App2, and App3

Correct Answer: B

Add app configuration policies for managed Android Enterprise devices App configuration policies in Microsoft Intune supply settings to Managed Google Play apps on managed Android Enterprise devices. The app developer exposes Android-managed app configuration settings. Intune uses these exposed setting to let the admin configure features for the app. The app configuration policy is assigned to your user groups. The policy settings are used when the app checks for them, typically the first time the app runs.

Not every app supports app configuration. Check with the app developer to see if their app supports app configuration policies.

Use the configuration designer You can use the configuration designer for Managed Google Play apps when the app is designed to support configuration settings. Configuration applies to devices enrolled in Intune. The designer lets you configure specific configuration values for the settings exposed by the app.

Reference: https://learn.microsoft.com/en-us/mem/intune/apps/app-configuration-policies-use-android¨