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.passapply.com/md-102.html

100% Passing Guarantee
100% Money Back Assurance

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

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 an Azure AD tenant named contoso.com.

You plan to purchase 25 computers that run Windows 11. You plan to deliver the computers directly to users.

You need to ensure that during the out-of-box experience (OBE), users are prompted to sign in, and then the computers are configured to use Microsoft Intune.

Which two components should you configure? Each correct answer presents part of the solution.

NOTE: Each correct selection is worth one point.

A. a provisioning package

B. automatic enrollment

C. an unattend.xml answer file

D. a Windows Autopilot deployment profile for self-deploying mode

E. a Windows Autopilot deployment profile for user-driven mode

Correct Answer: BE

Reference: https://learn.microsoft.com/en-us/windows/client-management/azure-ad-and-microsoft-intune-automatic-mdm-enrollment-in-the-new-portal https://learn.microsoft.com/en-us/autopilot/user-driven

QUESTION 3

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 4

Your company uses Microsoft Intune to manage devices.

You need to ensure that only Android devices that use Android work profiles can enroll in Intune.

Which two configurations should you perform in the device enrollment restrictions? Each correct answer presents part of the solution.

NOTE: Each correct selection is worth one point.

A. From Platform Settings, set Android device administrator Personally Owned to Block.

B. From Platform Settings, set Android Enterprise (work profile) to Allow.

C. From Platform Settings, set Android device administrator Personally Owned to Allow.

D. From Platform Settings, set Android device administrator to Block.

Correct Answer: BD

Set up enrollment of Android Enterprise personally-owned work profile devices

Set up enrollment for bring-your-own-device (BYOD) and personal device scenarios using the Android Enterprise personally-owned work profile management solution. During enrollment, a work profile is created on the device to house work

apps and work data. The work profile can be managed by Microsoft Intune policies. Personal apps and data stay separate in another part of the device and remain unaffected by Intune.

Set up enrollment

Complete these steps to set up enrollment for Android Enterprise devices in BYOD scenarios.

1.

Sign in to the Microsoft Intune admin center.

2.

Go to Devices > Enrollment device platform restrictions to set up enrollment restrictions. By default, Android Enterprise work profile is marked as allowed for personal devices enrolling in Intune. You can allow or block enrollment in device platform restrictions. Your options:

Block: Personal devices that enroll will use the Android device administrator management solution, unless device administrator enrollment is also blocked.

Allow (set by default): Personal devices that support the work profile management solution will enroll with a work profile. Android devices that don\\'t support Android Enterprise are enrolled using the Android device administrator solution, unless device administrator enrollment is blocked.

Any device that supports Android Enterprise personal work profiles also supports the Android device administrator management solution, so if you don\\'t want Android device administrator to be a part of enrollments, make sure to block the platform.

Reference: https://learn.microsoft.com/en-us/mem/intune/enrollment/android-work-profile-enroll

QUESTION 5

Your company implements Azure AD, Microsoft 365, Microsoft Intune, and Azure Information Protection.

The company\\'s security policy states the following:

1.

Personal devices do not need to be enrolled in Intune.

2.

Users must authenticate by using a PIN before they can access corporate email data.

3.

Users can use their personal iOS and Android devices to access corporate cloud services.

4.

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

Correct Answer: D

By implementing app-level policies, you can restrict access to company resources and keep data within the purview of your IT department.

Note: The important benefits of using App protection policies are the following:

Protecting your company data at the app level. Because mobile app management doesn\\'t require device management, you can protect company data on both managed and unmanaged devices. The management is centered on the user identity, which removes the requirement for device management.

End-user productivity isn\\'t affected and policies don\\'t apply when using the app in a personal context. The policies are applied only in a work context, which gives you the ability to protect company data without touching personal data.

App protection policies makes sure that the app-layer protections are in place. For example, you can:

Require a PIN to open an app in a work context Control the sharing of data between apps Prevent the saving of company app data to a personal storage location MDM, in addition to MAM, makes sure that the device is protected. For example, you can require a PIN to access the device, or you can deploy managed apps to the device. You can also deploy apps to devices through your MDM solution, to give you more control over app management.

Reference: https://docs.microsoft.com/en-us/intune/app-protection-policy