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.pass2lead.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

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. Configure an Apply MDM push certificate.

B. Add your user account as a device enrollment manager (DEM).

C. Modify the enrollment restrictions.

D. Upload a file that has the device identifiers for each iPad.

Correct Answer: A

Set up iOS/iPadOS device enrollment with Apple Configurator

Prerequisites

Physical access to iOS/iPadOS devices

Set MDM authority

An Apple MDM push certificate

Device serial numbers (Setup Assistant enrollment only)

USB connection cables

macOS computer running Apple Configurator 2.0

Note:

Upload and renew your Apple MDM push certificates in Microsoft Intune. An Apple MDM Push certificate is required to manage iOS/iPadOS and macOS devices in Microsoft Intune, and enables devices to enroll via:

The Intune Company Portal app.

Apple bulk enrollment methods, such as the Device Enrollment Program, Apple School Manager, and Apple Configurator.

Certificates must be renewed annually.

Reference:

https://learn.microsoft.com/en-us/mem/intune/enrollment/apple-mdm-push-certificate-get

QUESTION 2

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

You use Microsoft Intune to manage Windows 11 devices.

You need to implement passwordless authentication that requires users to use number matching.

Which authentication method should you use?

A. Microsoft Authenticator

B. voice calls

C. FIDO2 security keys

D. text messages

Correct Answer: A

How number matching works in multifactor authentication (MFA) push notifications for Authenticator - Authentication methods policy This topic covers how number matching in Microsoft Authenticator push notifications improves user sign-in security. Number matching is a key security upgrade to traditional second factor notifications in Authenticator. Beginning May 8, 2023, number matching is enabled for all Authenticator push notifications. As relevant services deploy, users worldwide who are enabled for Authenticator push notifications will begin to see number matching in their

approval requests. Users can be enabled for Authenticator push notifications either in the Authentication methods policy or the legacy multifactor authentication policy if Notifications through mobile app is enabled.

Reference:

https://learn.microsoft.com/en-us/azure/active-directory/authentication/how-to-mfa-number-match

---

QUESTION 3

You have a Microsoft 365 subscription that includes Microsoft Intune.

You plan to use Windows Autopilot to deploy Windows 11 devices.

You need to meet the following requirements during Autopilot provisioning:

1.

Display the app and profile configuration progress.

2.

Block users from using the devices until all apps and profiles are installed What should you configure?

A. an app configuration policy

B. an app protection policy

C. an enrollment device platform restriction

D. an enrollment status page

Correct Answer: D

https://learn.microsoft.com/en-us/mem/intune/enrollment/windows-enrollment-status

QUESTION 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. Image2 only

C. Image1 and Image2

Correct Answer: B

How to Perform an In-Place Upgrade on Windows 11.

To perform an in-place upgrade, you need to do two things. Firstly, you need to download the latest Windows 11 ISO file. Then, you need to run the setup from the ISO file, pick the appropriate in-place upgrade option, and proceed.

1.

Download the Windows 11 ISO Image File

First of all, you need to grab the Windows 11 ISO image file. If you don\\'t already have one on hand, check out how to download a Windows ISO without the Media Creation tool for some easy methods.

2.

Perform an In-Place Upgrade Using the Windows11 ISO Image File

Etc.

Reference:

https://www.makeuseof.com/in-place-upgrade-windows-11/

QUESTION 5

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