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.pass4itsure.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

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 365 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 AD, add an enterprise application.

D. From the Microsoft Intune admin center, add an app.

Correct Answer: D

Add Microsoft 365 Apps to Windows 10/11 devices with Microsoft Intune

Before you can assign, monitor, configure, or protect apps, you must add them to Intune. One of the available app types is Microsoft 365 apps for Windows 10 devices. By selecting this app type in Intune, you can assign and install Microsoft

365 apps to devices you manage that run Windows 10.

Select Microsoft 365 Apps

Sign in to the Microsoft Intune admin center.

Select Apps > All apps > Add.

Select Windows 10 in the Microsoft 365 Apps section of the Select app type pane.

Click Select. The Add Microsoft 365 Apps steps are displayed.

Reference:

https://learn.microsoft.com/en-us/mem/intune/apps/apps-add-office365

QUESTION 2

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

You use Microsoft Intune to manage Windows 11 devices.

You create a new policy set named Set and add five device configuration profiles for Windows 10 and later.

You create a device compliance policy named Policy1.

You need to ensure that when users are assigned the device configuration profiles in Set1, they are always assigned Policy1 also.

What should you configure?

A. the assignments of Policy1

B. the Policy1 configurations

C. the assignments of Set1

D. the Set1 configurations

Correct Answer: C

Creating a policy set enables you to select many different objects at once, and assign them from a single place.

You can include the following management objects in a policy set:

Apps

App configuration policies

App protection policies *-> Device configuration profiles *-> Device compliance policies Windows autopilot deployment profiles Enrollment status page Settings catalog policies

Note: Use policy sets to group collections of management objects Policy sets allow you to create a bundle of references to already existing management entities that need to be identified, targeted, and monitored as a single conceptual unit. A policy set is an assignable collection of apps, policies, and other management objects you\\'ve created. Creating a policy set enables you to select many different objects at once, and assign them from a single place. As your organization changes, you can revisit a policy set to add or remove its objects and assignments. You can use a policy set to associate and assign existing objects, such as apps, policies, and VPNs in a single package.

Policy sets don\\'t replace existing concepts or objects. You can continue to assign individual objects and you can also reference individual objects as part of a policy set. Therefore, any changes to those individual objects will be reflected in the policy set.

You can use policy sets to:

Group objects that need to be assigned together Assign your organization\\'s minimum configuration requirements on all managed devices Assign commonly used or relevant apps to all users

Reference: https://learn.microsoft.com/en-us/mem/intune/fundamentals/policy-sets

QUESTION 3

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 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 Intune admin center, you define the company\\'s network as a location named Location1. Which devices can use network location-based compliance policies?

A. Device1 only

B. Device2 only

C. Device1 and Device2 only

D. Device2 and Device3 only

E. Device1, Device2, and Device3

Correct Answer: E

Intune supported operating systems

Intune supports devices running the following operating systems (OS):

1.

iOS

2.

Android

3.

Windows

4.

macOS

Note: View the device compliance settings for the different device platforms:

1.

Android device administrator

2.

Android Enterprise

3.

iOS

4.

macOS

5.

Windows Holographic for Business

6.

Windows 8.1 and later

7.

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

QUESTION 5

You have a Microsoft 365 E5 subscription.

You need to download a report that lists all the devices that are NOT enrolled in Microsoft Intune and are assigned an app protection policy.

What should you select in the Microsoft Intune admin center?

A. Reports, and then Device compliance

B. Apps, and then App protection policies

C. Devices, and then Monitor

D. Apps, and then Monitor

Correct Answer: D

https://learn.microsoft.com/en-us/mem/intune/apps/app-protection-policies-monitor#view-the-app-protection-status-report