MD-101 Q&As

Managing Modern Desktops

Pass Microsoft MD-101 Exam with 100% Guarantee

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

https://www.pass4itsure.com/md-101.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 an on-premises server named Server1 that hosts a Microsoft Deployment Toolkit (MDT) deployment share named MDT1.

You need to ensure that MDT1 supports multicast deployments.

What should you install on Server1?

A. Windows Server Update Services (WSUS)

B. Multipath I/O (MPIO)

C. Windows Deployment Services (WDS)

D. Multipoint Connector

Correct Answer: C

QUESTION 2

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 Endpoint Manager admin center, add an app.

B. From Microsoft Azure Active Directory (Azure AD), add an app registration.

C. From Microsoft Azure Active Directory (Azure AD), add an enterprise application.

D. From the Endpoint Manager admin center, create a Windows 10 device profile.

Correct Answer: A

Before you can assign, monitor, configure, or protect apps, you must add them to Intune. Select Microsoft 365 Apps.

1.

Sign in to the Microsoft Endpoint Manager admin center.

2.

Select Apps > All apps > Add.

3.

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

4.

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

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

QUESTION 3

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

B. Modify the enrollment restrictions.

C. Configure an Apple MDM push certificate.

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

Correct Answer: C

An Apple MDM Push certificate is required for Intune to manage iOS/iPadOS and macOS devices. After you add the certificate to Intune, your users can enroll their devices.

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

QUESTION 4

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 uses Windows Autopilot to configure the computer settings of computers issued to users.

A user named User1 has a computer named Computer1 that runs Windows 10. User1 leaves the company.

You plan to transfer the computer to a user named User2.

You need to ensure that when User2 first starts the computer, User2 is prompted to select the language setting and to agree to the license agreement.

Solution: You create a new Windows AutoPilot self-deploying deployment profile.

Does this meet the goal?

A. Yes

B. No

Correct Answer: A

In Group Policy, within Configure Automatic Updates, you can configure a forced restart after a specified installation time.

To set the time, you need to go to Configure Automatic Updates, select option 4 - Auto download and schedule the install, and then enter a time in the Scheduled install time dropdown. Alternatively, you can specify that installation will occur

during the automatic maintenance time.

1) Automatic Maintenance Random Delay has NOTHING to do with us achieving our goal of automatically installing updates during a maintenance window

2) Automatic Maintenance Activation Boundary made me take a deeper dive into these specific GPOs. From my understanding, configuring Activation Boundary will install updates on devices that are not in use. If a user is currently signed in,

the updates will not install.

3) "Auto download and schedule the install" does what our question asks. We can decide NOT to check the option for "Automatic Maintenance", which includes Activation Boundary and Random Delay. This question is once again quite nonspecific. Activation Boundary seems to do more than what the question is asking. If we just need to auto install updates during a maintenance window, answer B achieves that goal.

Reference:

https://docs.microsoft.com/en-us/windows/deployment/update/waas-restart

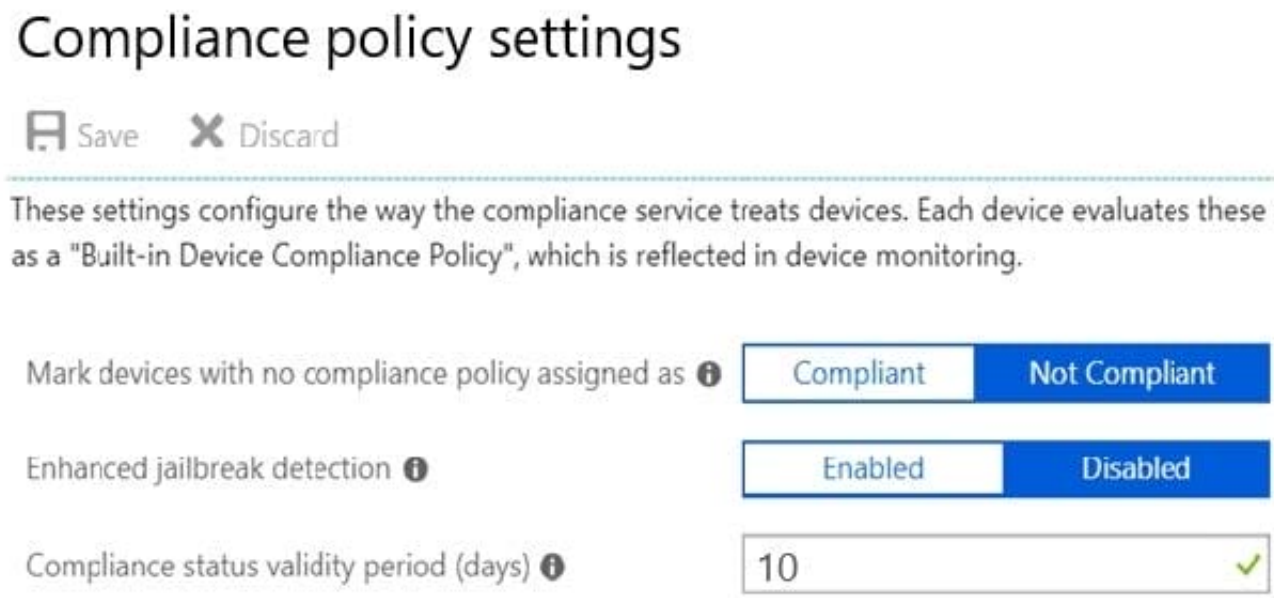
QUESTION 5

HOTSPOT

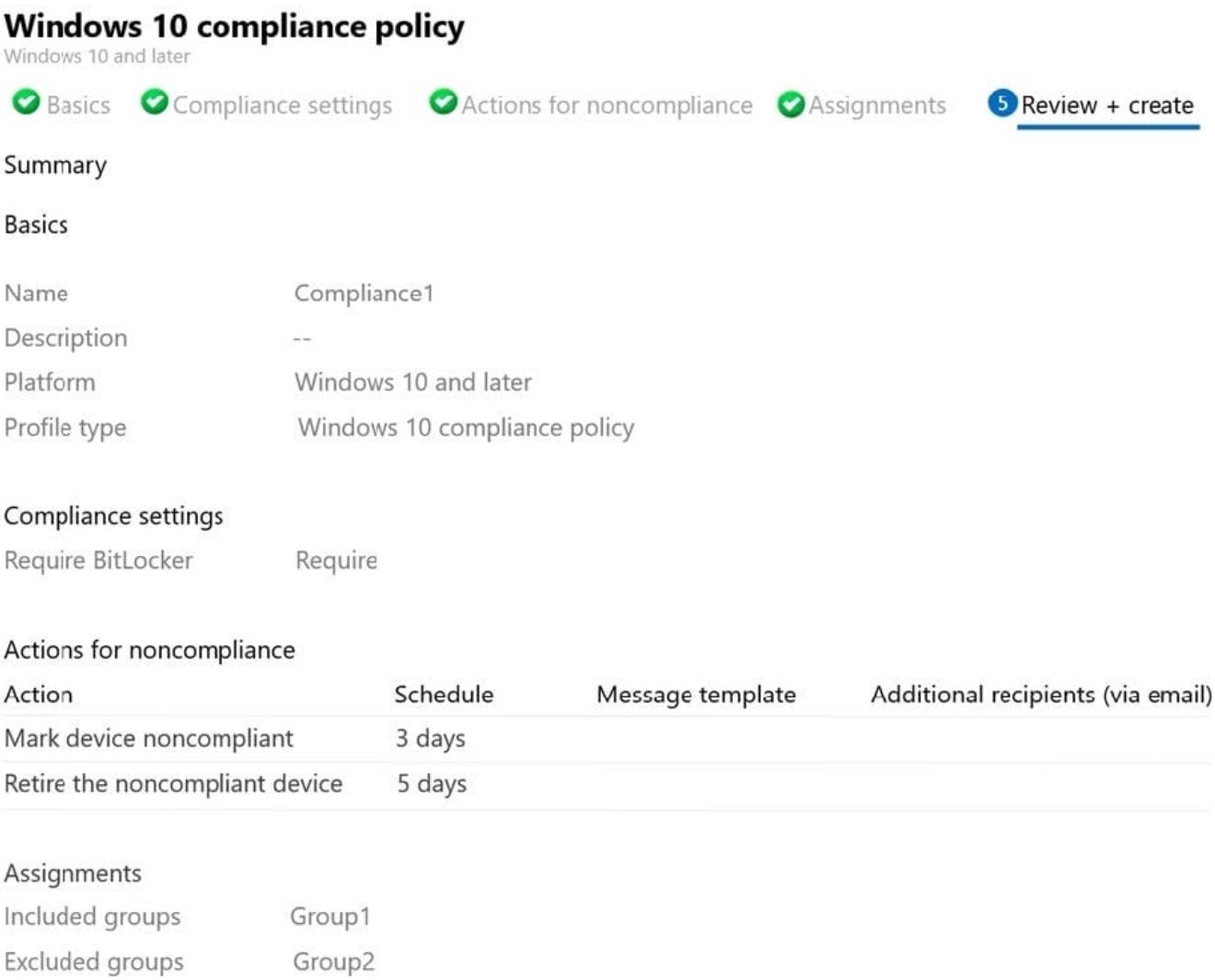
You have two Windows 10 devices enrolled in Microsoft Intune as shown in the following table.

Name	BitLocker Drive Encryption (BitLocker)	Member of
Device1	Enabled	Group2
Device2	Disabled	Group1

The Compliance policy settings are configured as shown in the following exhibit.



On August 1, you create a compliance policy as shown in the following exhibit.



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:

Correct Answer:

Box 1: No

Device1 belongs to Group2. Group2 has not been assigned a compliance policy. Devices with no compliance policy assigned as Not Compliant. Device1 gets a 3 day grace period, but at August 4 is it marked as Non-compliant.

Box 2: Yes

Device1 belongs to Group2. Group2 has not been assigned a compliance policy. Devices with no compliance policy assigned as Not Compliant. Device1 gets a 3 day grace period, so at August 2 it is compliant.

Box 3: No

Device2 has BitLocker Disabled. The Windows 10 compliance policy applies to Group1 which includes Device1. At August 4 Device is marked noncompliant. 5 days later, at August 9th it is retired.

Note:

*

Retire the noncompliant device: This action removes all company data off the device and removes the device from Intune management.

*

By default, each compliance policy includes the action for noncompliance of Mark device noncompliant with a schedule of zero days (0). The result of this default is when Intune detects a device isn\\'t compliant, Intune immediately marks the

device as noncompliant.

By configuring Actions for noncompliance you gain flexibility to decide what to do about noncompliant devices, and when to do it. For example, you might choose to not block the device immediately, and give the user a grace period to become

compliant.

Compliance status validity period (days):

Specify a period in which devices must successfully report on all their received compliance policies. If a device fails to report its compliance status for a policy before the validity period expires, the device is treated as noncompliant.

Reference: https://docs.microsoft.com/en-us/mem/intune/protect/device-compliance-get-started
https://docs.microsoft.com/en-us/mem/intune/protect/actions-for-noncompliance