MD-101$^{\text{Q\&As}}$

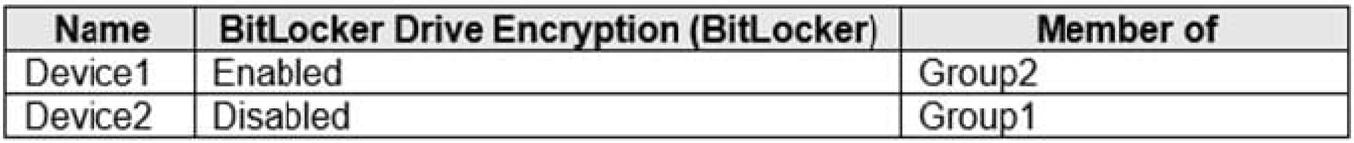
Managing Modern Desktops

Pass Microsoft MD-101 Exam with 100% Guarantee

QUESTION 1

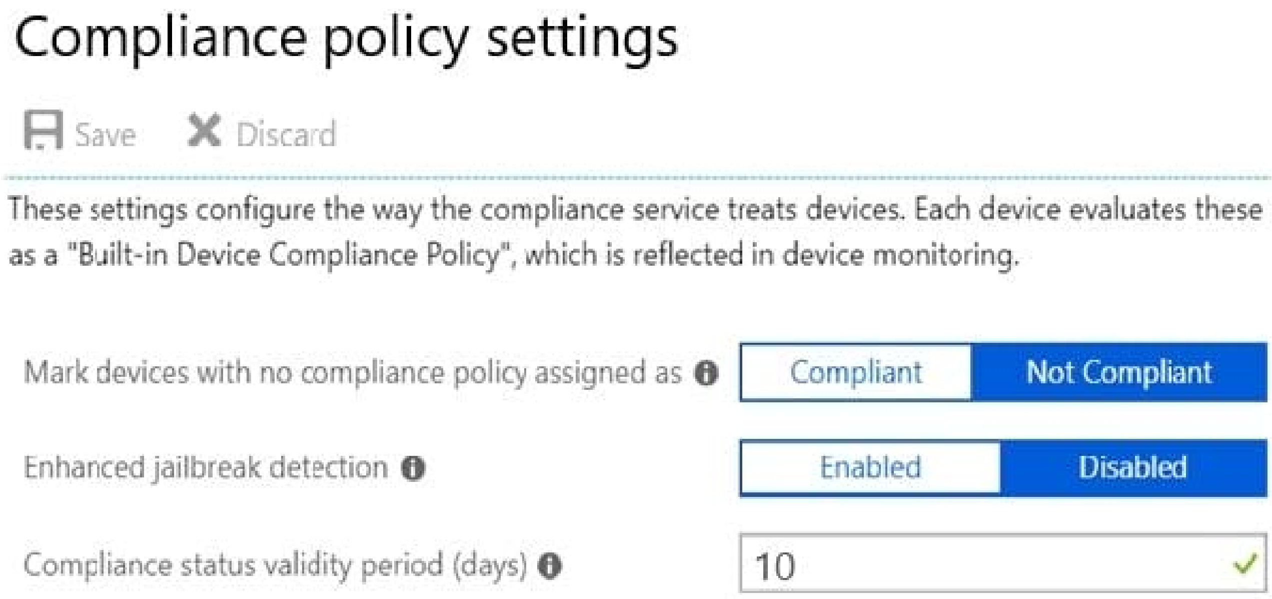
HOTSPOT

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.



Compliance policy settings

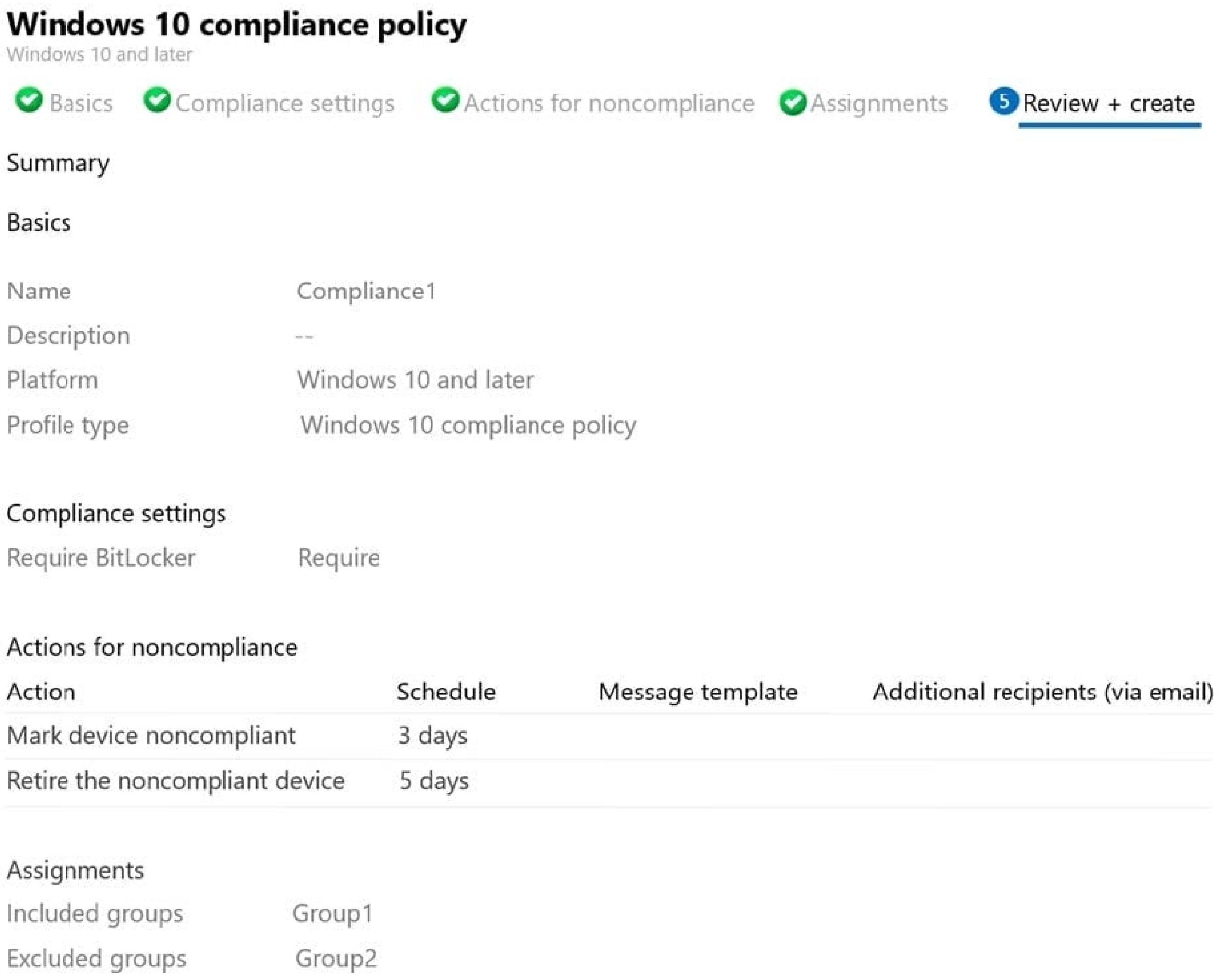
These settings configure the way the compliance service treats devices. Each device evaluates these as a "Built-in Device Compliance Policy", which is reflected in device monitoring.

Mark devices with no compliance policy assigned as: Compliant [✓ Not Compliant]

Enhanced jailbreak detection: Enabled [✓ Disabled]

Compliance status validity period (days): 10 ✓

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



Windows 10 compliance policy

Windows 10 and later

Summary

Basics

Name	Compliance1
Description	--
Platform	Windows 10 and later
Profile type	Windows 10 compliance policy

Compliance settings

Require BitLocker	Require

Actions for noncompliance

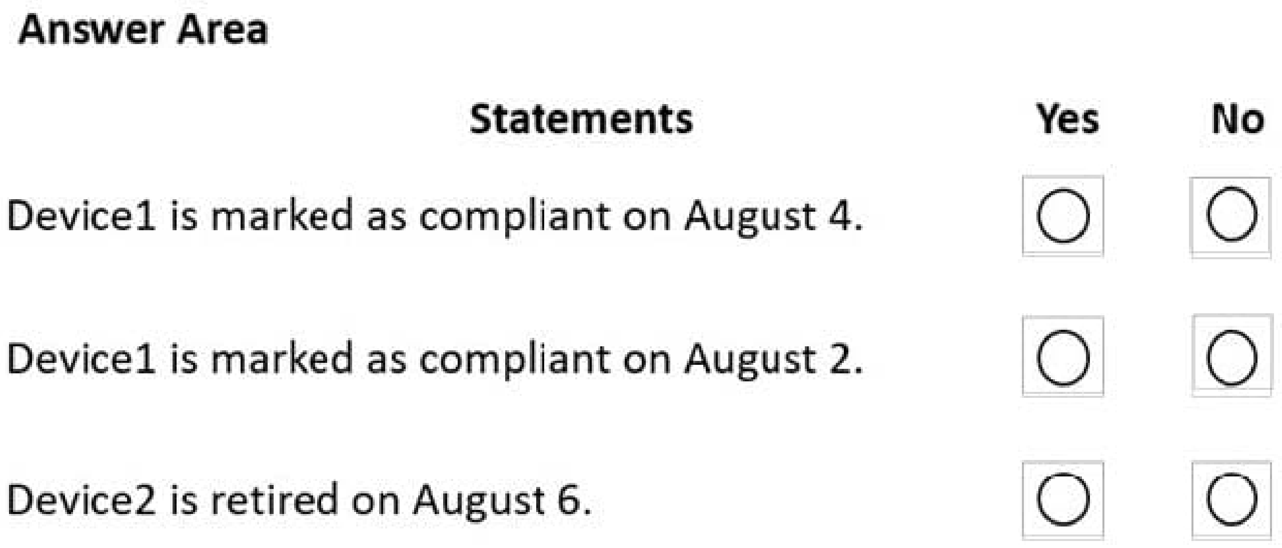
Action	Schedule	Message template	Additional recipients (via email)
Mark device noncompliant	3 days		
Retire the noncompliant device	5 days		

Assignments

Included groups	Group1
Excluded groups	Group2

For each of the following statements, select Yes if the statement is true. Otherwise, select No. NOTE: Each correct selection is worth one point.

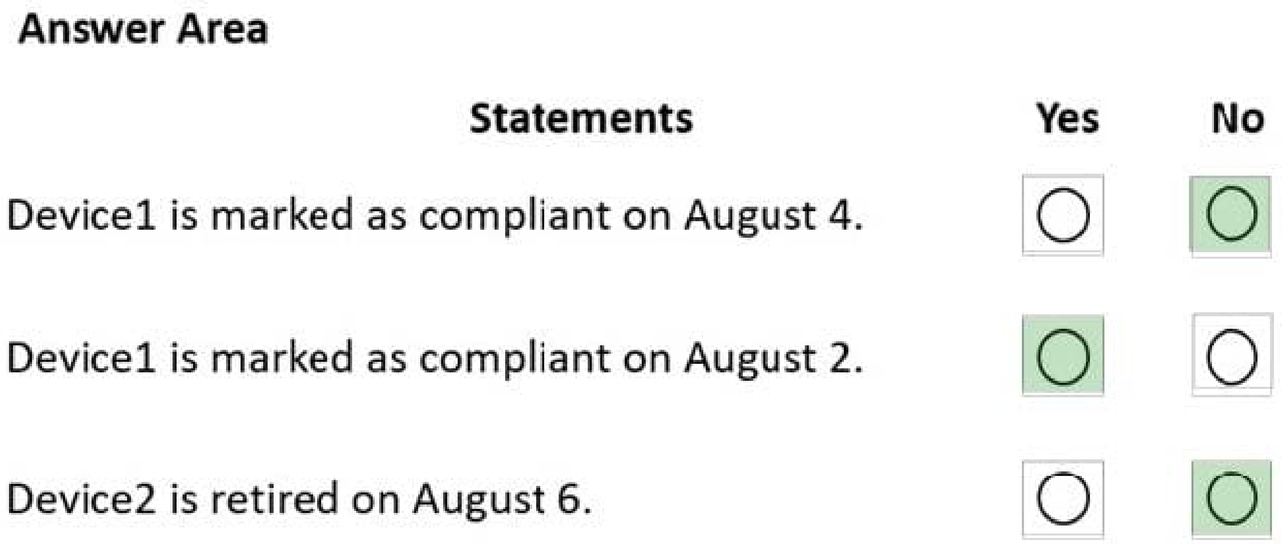
Hot Area:



Answer Area

Statements	Yes	No
Device1 is marked as compliant on August 4.	○	○
Device1 is marked as compliant on August 2.	○	○
Device2 is retired on August 6.	○	○

Correct Answer:



Answer Area

Statements	Yes	No
Device1 is marked as compliant on August 4.	○	[✓ ○]
Device1 is marked as compliant on August 2.	[✓ ○]	○
Device2 is retired on August 6.	○	[✓ ○]

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

QUESTION 2

HOTSPOT

You have an Azure Active Directory (Azure AD) tenant named contoso.com that contains a user named User1. User1 has a user principal name (UPN) of user1 @contoso.com.

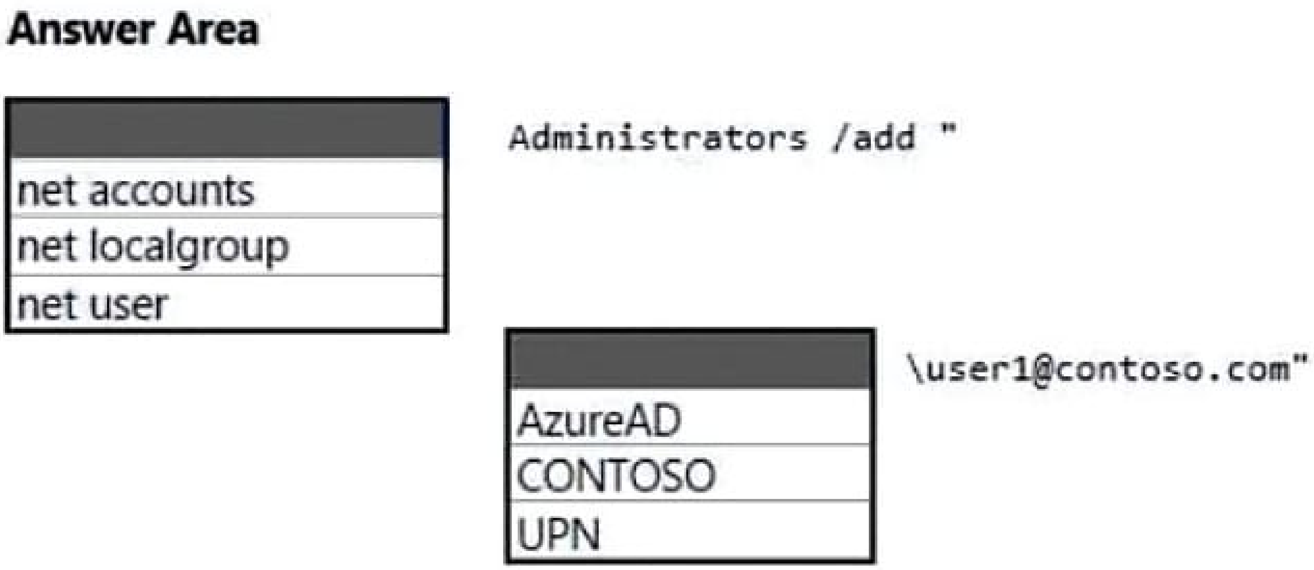
You join a Windows 10 device named Client1 to contoso.com.

You need to add User1 to the local Administrators group of Client1.

How should you complete the command? To answer, select the appropriate options in the answer area.

NOTE: Each correct selection is worth one point.

Hot Area:



Answer Area

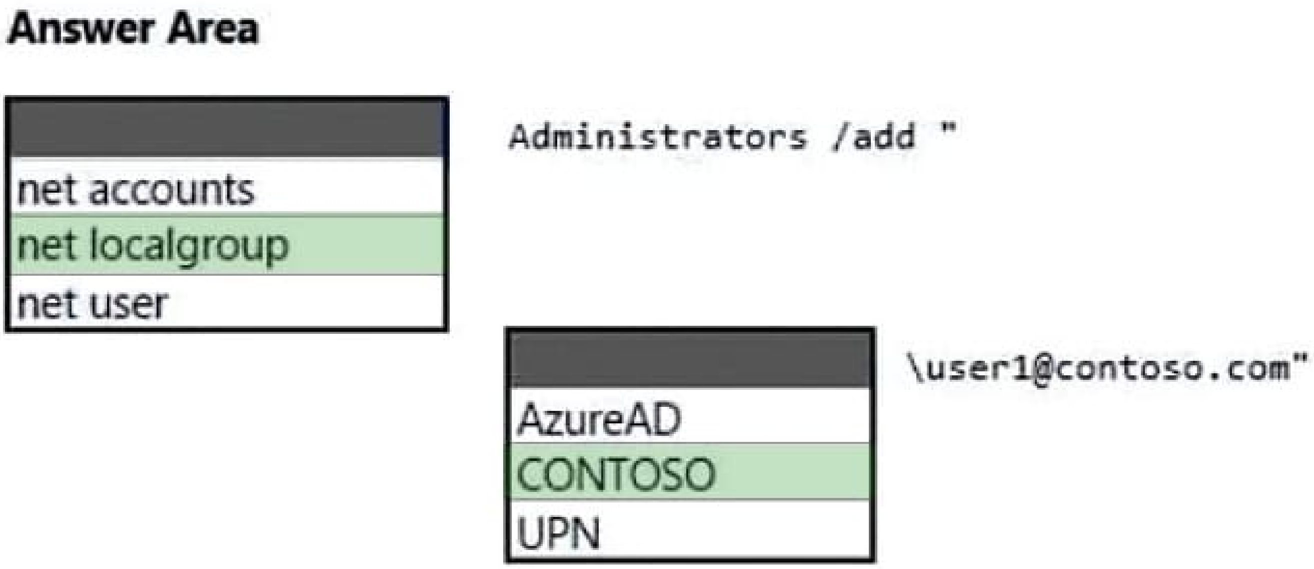
- net accounts
- net localgroup
- net user

`Administrators /add "`

- AzureAD
- CONTOSO
- UPN

`\user1@contoso.com"`

Correct Answer:



Answer Area

- net accounts
- [✓ net localgroup]
- net user

`Administrators /add "`

- AzureAD
- [✓ CONTOSO]
- UPN

`\user1@contoso.com"`

Box 1: net localgroup

Add user to group from command line (CMD)

Windows provides command line utilities to manager user groups. In this post, learn how to use the command net localgroup to add user to a group from command prompt\\'

For example to add a user \\'John\\' to administrators group, we can run the below command. net localgroup administrators John /add

Box 2: Contoso

The domain of the user is Contoso.

Reference:

https://www.windows-commandline.com/add-user-to-group-from-command-line/

QUESTION 3

Your company has a Microsoft Azure Active Directory (Azure AD) tenant named contoso.com. All users have computers that run Windows 10. The computers are joined to Azure AD and managed by using Microsoft Intune.

You need to ensure that you can centrally monitor the computers by using Windows Analytics.

What should you create in Intune?

A. a device configuration profile

B. a conditional access policy

C. a device compliance policy

D. an update policy

Correct Answer: A

To use Update Compliane (iclude in Desktop analytics solution), Commercial ID and telemetry must be enable. Device configuration (cith custom OMA-URI settings) allow to do that. https://docs.microsoft.com/en-us/windows/deployment/

update/update-compliance-configuration-mem

With CommercialID in hand, you\\'re ready to go to the MEM admin center portal and start putting your keyboard to work making a custom OMA-URI device configuration profile to enable Update Compliance settings. You\\'re going to need a

total of four custom policy settings to configure devices to play nice with

Update Compliance Reference:

https://www.jeffgilb.com/update-compliance-with-intune/

QUESTION 4

Your company implements Microsoft Azure Active Directory (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 data loss prevention (DLP) policy from the Microsoft 365 Compliance admin center

B. an insider risk management policy from the Microsoft 365 Compliance admin center

C. an app protection policy from the Endpoint Manager admin center

D. a device configuration profile from the Endpoint Manager admin center

Correct Answer: C

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

QUESTION 5

What should you use to meet the technical requirements for Azure DevOps?

A. An app protection policy

B. Windows Information Protection (WIP)

C. Conditional access

D. A device configuration profile

Correct Answer: C

Ensure that the projects in Azure DevOps can be accessed from the corporate network only.

Reference:

https://docs.microsoft.com/en-us/azure/devops/organizations/accounts/manage-conditional-access?view=azure-devops

MD-101 Practice Test MD-101 Study Guide MD-101 Exam Questions