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.leads4pass.com/md-101.html

100% Passing Guarantee
100% Money Back Assurance

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

QUESTION 1

Which devices are registered by using the Windows Autopilot deployment service?

A. Device1 only

B. Device3 only

C. Device1 and Device3 only

D. Device1, Device2, and Device3

Correct Answer: C

Scenario: Windows Autopilot Configuration

Assignments

Included groups: Group1

Excluded groups: Group2

Device1 is member of Group1.

Device2 is member of Group1 and member of Group2.

Device3 is member of Group1.

Group1 and Group2 have a Membership type of Assigned.

Exclusion takes precedence over inclusion in the following same group type scenarios.

Reference: https://learn.microsoft.com/en-us/mem/intune/apps/apps-inc-exl-assignments

QUESTION 2

Your network contains an Active Directory domain. The domain contains 100 computers that run Windows 10.

You need to prevent users and apps from accessing dangerous websites.

What should you configure?

A. Microsoft Defender Application Control

B. Microsoft Defender Exploit Guard

C. Microsoft Defender Application Guard

D. Microsoft Defender Firewall

Correct Answer: B

Network protection, a part of Microsoft Defender Exploit Guard, helps to prevent employees from using any application

to access dangerous domains that may host phishing scams, exploits, and other malicious content on the internet.

Reference: https://docs.microsoft.com/en-us/microsoft-365/security/defender-endpoint/enable-network-protection?view=o365-worldwide

QUESTION 3

HOTSPOT

A company named A.Datum Corporation uses Microsoft Endpoint Configuration Manager, Microsoft Intune, and Desktop Analytics.

A.Datum purchases a company named Contoso, Ltd. Contoso has devices that run the following operating systems:

1.

Windows 8.1

2.

Windows 10

3.

Android

4.

iOS

A.Datum plans to use Desktop Analytics to monitor the Contoso devices.

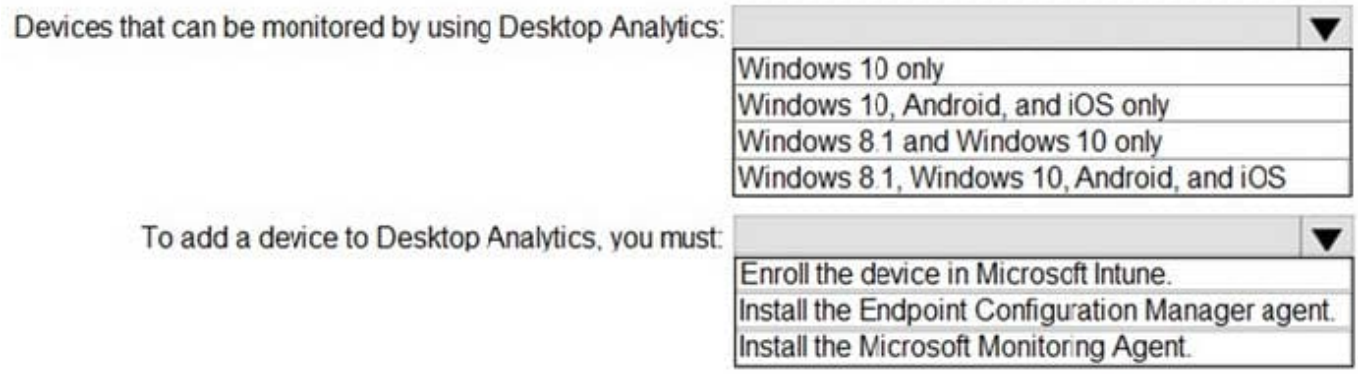
You need to identify which devices can be monitored by using Desktop Analytics and how to add the devices to Desktop Analytics.

What should you identify? To answer, select the appropriate options in the answer area.

NOTE: Each correct selection is worth one point.

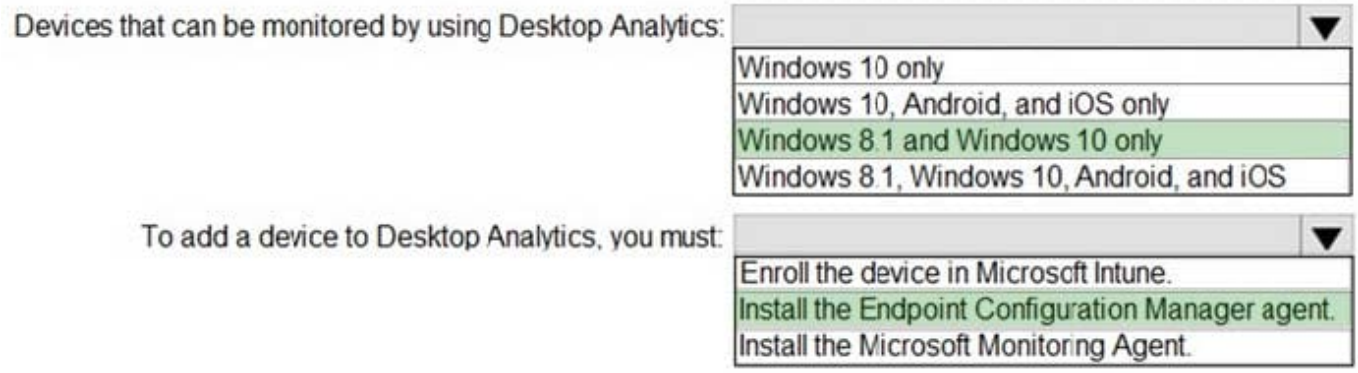
Hot Area:

Answer Area



Correct Answer:

Answer Area



Box 1: Windows 8.1 and Windows 10 only

Windows 7, Windows 8.1 and Windows 10 are supported.

Box 2: Install the Endpoint Configuration Manager agent.

Need to for the Windows 8.1 client.

Reference:

https://docs.microsoft.com/en-us/mem/configmgr/desktop-analytics/enroll-devices https://docs.microsoft.com/en-us/mem/configmgr/desktop-analytics/overview

---

QUESTION 4

You need a new conditional access policy that has an assignment for Office 365 Exchange Online.

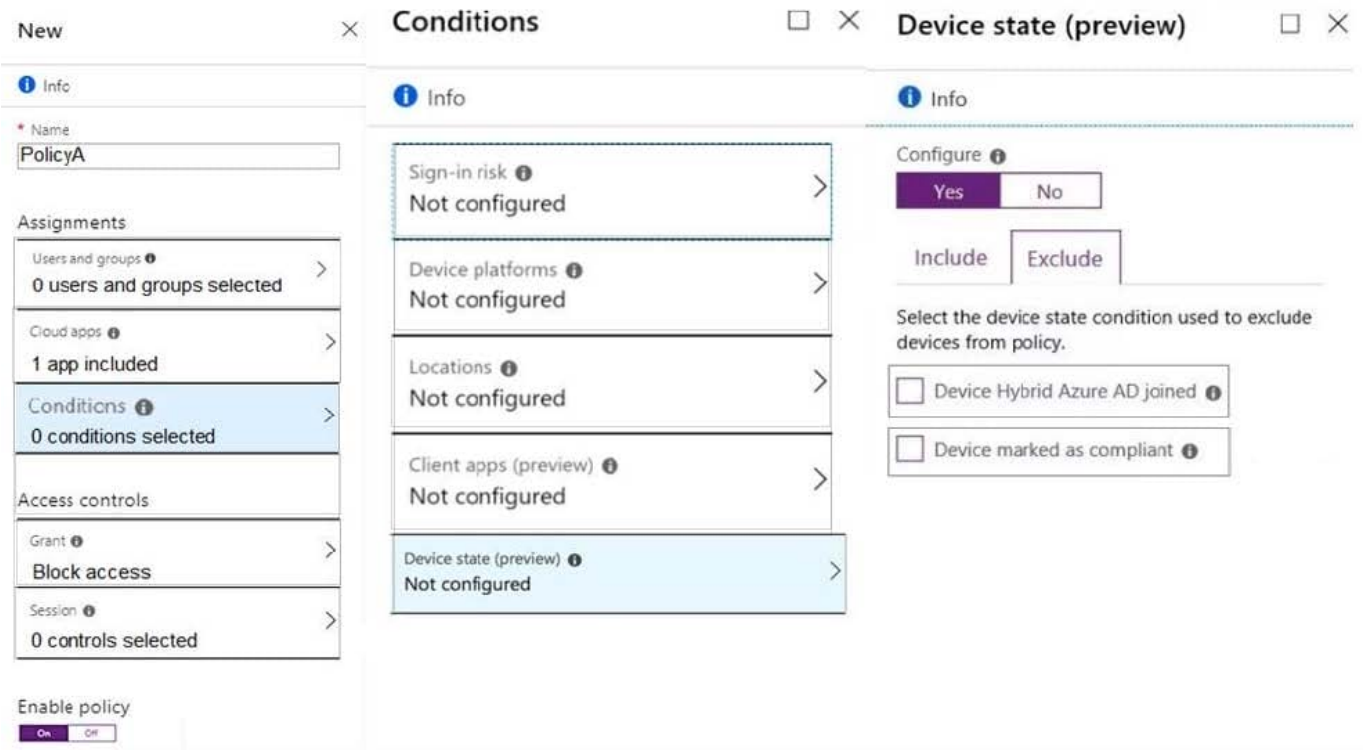
You need to configure the policy to meet the technical requirements for Group4.

Which two settings should you configure in the policy? To answer, select the appropriate settings in the answer area.

NOTE: Each correct selection is worth one point.

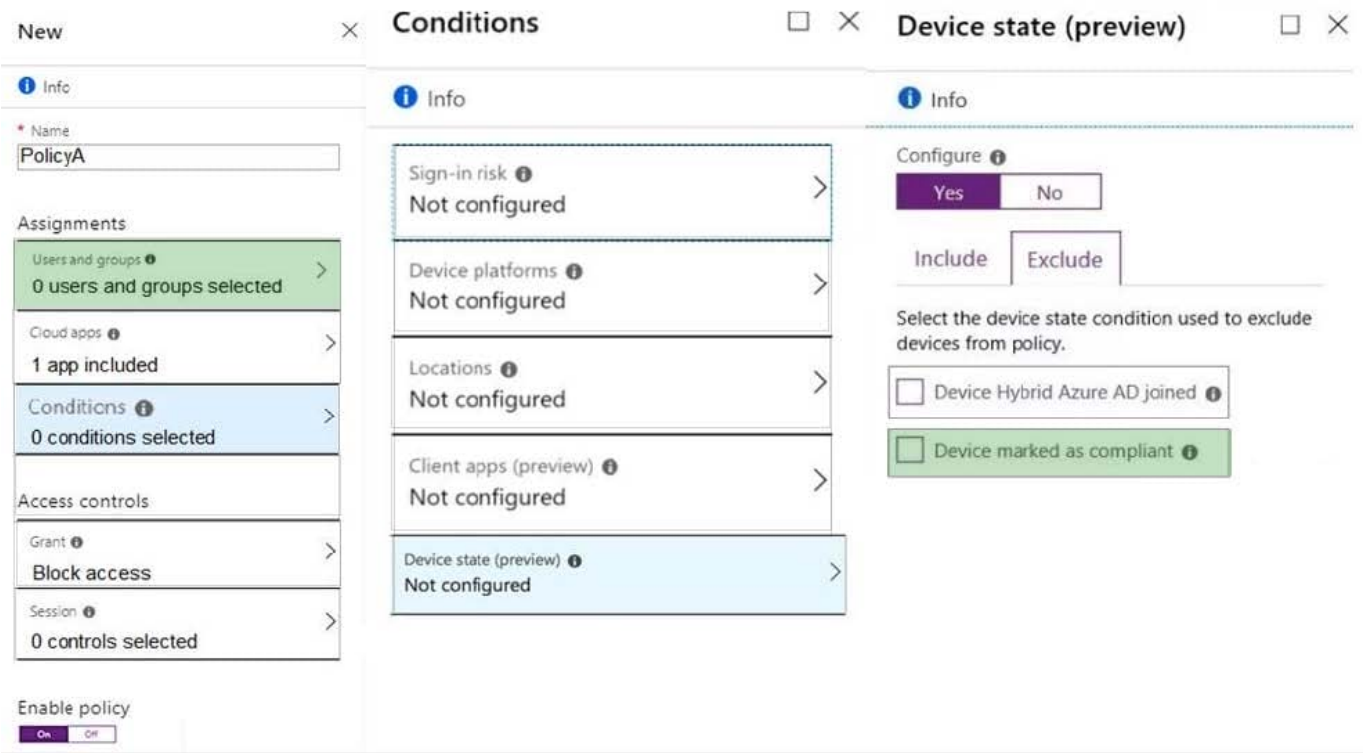
Hot Area:

Answer Area



Correct Answer:

Answer Area



The policy needs to be applied to Group4 so we need to configure Users and Groups. The Access controls are set to Block access

We therefore need to exclude compliant devices.

From the scenario:

Ensure that the users in a group named Group4 can only access Microsoft Exchange Online from devices that are enrolled in Intune.

Note: When a device enrolls in Intune, the device information is updated in Azure AD to include the device compliance status. This compliance status is used by conditional access policies to block or allow access to e-mail and other

organization resources.

References:

https://docs.microsoft.com/en-us/azure/active-directory/conditional-access/overview

https://docs.microsoft.com/en-us/azure/active-directory/conditional-access/conditions

https://docs.microsoft.com/en-us/intune/device-compliance-get-started

QUESTION 5

You have the 64-bit computers shown in the following table.

Name	Operating system	Memory	BitLocker Drive Encryption (BitLocker)
Computer1	32-bit version of Windows 7 Service Pack 1 (SP1)	1 GB	Enabled
Computer2	64-bit version of Windows 7 Service Pack 1 (SP1)	4 GB	Enabled
Computer3	32- bit version of Windows 8.1	2 GB	Enabled
Computer4	64-bit version of Windows 8.1	4 GB	Disabled

You plan to perform an in-place upgrade to the 64-bit version of Windows 10.

Which computers can you upgrade to the 64-bit version of Windows 10 in their current state?

A. Computer2 and Computer4 only

B. Computer4 only

C. Computer3 and Computer4 only

D. Computer1, Computer2, Computer3 and Computer4

E. Computer2, Computer3, and Computer4 only

Correct Answer: A

Note: Once the Windows 10 upgrade is complete the key in plain text is removed, and then BitLocker will enable again automatically. This means that the Windows 10 upgrade process on a device using BitLocker is the same to a device

without using the security feature

Incorrect:

Not Computer1 or Computer3:

Changing from Windows 7, Windows 8, or Windows 8.1 x86 to Windows 10 x64. The upgrade process cannot change from a 32-bit operating system to a 64-bit operating system, because of possible complications with installed applications

and drivers.

Reference:

https://docs.microsoft.com/en-us/windows/deployment/windows-10-deployment-scenarios
https://pureinfotech.com/upgrade-windows-10-bitlocker-enabled/

QUESTION 6

Reference: https://danielchronlund.com/2018/11/27/how-to-replace-your-old-gpos-with-intune-configuration-profiles/

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 has an Azure Active Directory (Azure AD) tenant named contoso.com that contains several Windows 10 devices. When you join new Windows 10 devices to contoso.com, users are prompted to set up a four-digit pin.

You need to ensure that the users are prompted to set up a six-digit pin when they join the Windows 10 devices to contoso.com.

Solution: From the Azure Active Directory admin center, you configure automatic mobile device management (MDM) enrollment. From the Endpoint Management admin center, you create and assign a device restrictions profile.

Does this meet the goal?

A. Yes

B. No

Correct Answer: B

Instead, from the Azure Active Directory admin center, you configure automatic mobile device management (MDM) enrollment. From the Endpoint Management admin center, you configure the Windows Hello for Business enrollment options.

References: https://docs.microsoft.com/en-us/intune/protect/windows-hello

QUESTION 7

HOTSPOT

Your network contains an Active Directory domain. The domain contains the users shown in the following table.

Name	Member of
User1	Group1
User2	Group2

You have a server named Server that runs Windows Server 2019 and has the Windows Deployment Services role installed. Server1 contains an x86 boot image and three Windows 10 install images. The install images are shown in the following table.

Name	Architecture	User permission
Image1	x64	Full control: Administrators, WDSServer
Image2	x64	Full control: Administrators Read: Group1
Image3	x86	Full control: Administrators, WDSServer Read: Group2

You purchase a computer named Computer1 that is compatible with the 64-bit version of Windows 10.

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
User1 can install Image1 on Computer1 by using Windows Deployment Services (WDS).	○	○
User1 can install Image2 on Computer1 by using Windows Deployment Services (WDS).	○	○
User2 can install Image3 on Computer1 by using Windows Deployment Services (WDS).	○	○

Correct Answer:

Answer Area

Statements	Yes	No
User1 can install Image1 on Computer1 by using Windows Deployment Services (WDS).	○	●
User1 can install Image2 on Computer1 by using Windows Deployment Services (WDS).	●	○
User2 can install Image3 on Computer1 by using Windows Deployment Services (WDS).	●	○

Box 1: No

User1 is a member of Group1. User1 does not have any permission to Image1.

Box 2: Yes

User1 has read permissions to Image2 through Group1.

Box 3: Yes

User2 has read permissions to Image3 through Group2.

QUESTION 8

You have a Microsoft 365 subscription.

You are assigned the User administrator role.

An Azure AD security group named Group1 was deleted five days ago.

You need to restore Group1.

What should you do?

A. Modify the group expiration policy.

B. From Deleted groups, restore Group1.

C. Manually recreate Group1.

D. Ask a global administrator to restore Group1.

Correct Answer: B

QUESTION 9

You have a Microsoft Azure subscription that contains an Azure Log Analytics workspace.

You deploy a new computer named Computer1 that runs Windows 10. Computer1 is in a workgroup.

You need to ensure that you can use Log Analytics to query events from Computer1.

What should you do on Computer1?

A. Configure the commercial ID

B. Join Azure Active Directory (Azure AD)

C. Create an event subscription

D. Install the Microsoft Monitoring Agent

Correct Answer: D

Verify agent connectivity to Azure Monitor.

From the computer in Control Panel, find the item Microsoft Monitoring Agent. Select it and on the Azure Log Analytics tab, the agent should display a message stating: The Microsoft Monitoring Agent has successfully connected to the

Microsoft Operations Management Suite service.

Reference:

https://docs.microsoft.com/en-us/azure/azure-monitor/platform/agent-windows

QUESTION 10

DRAG DROP

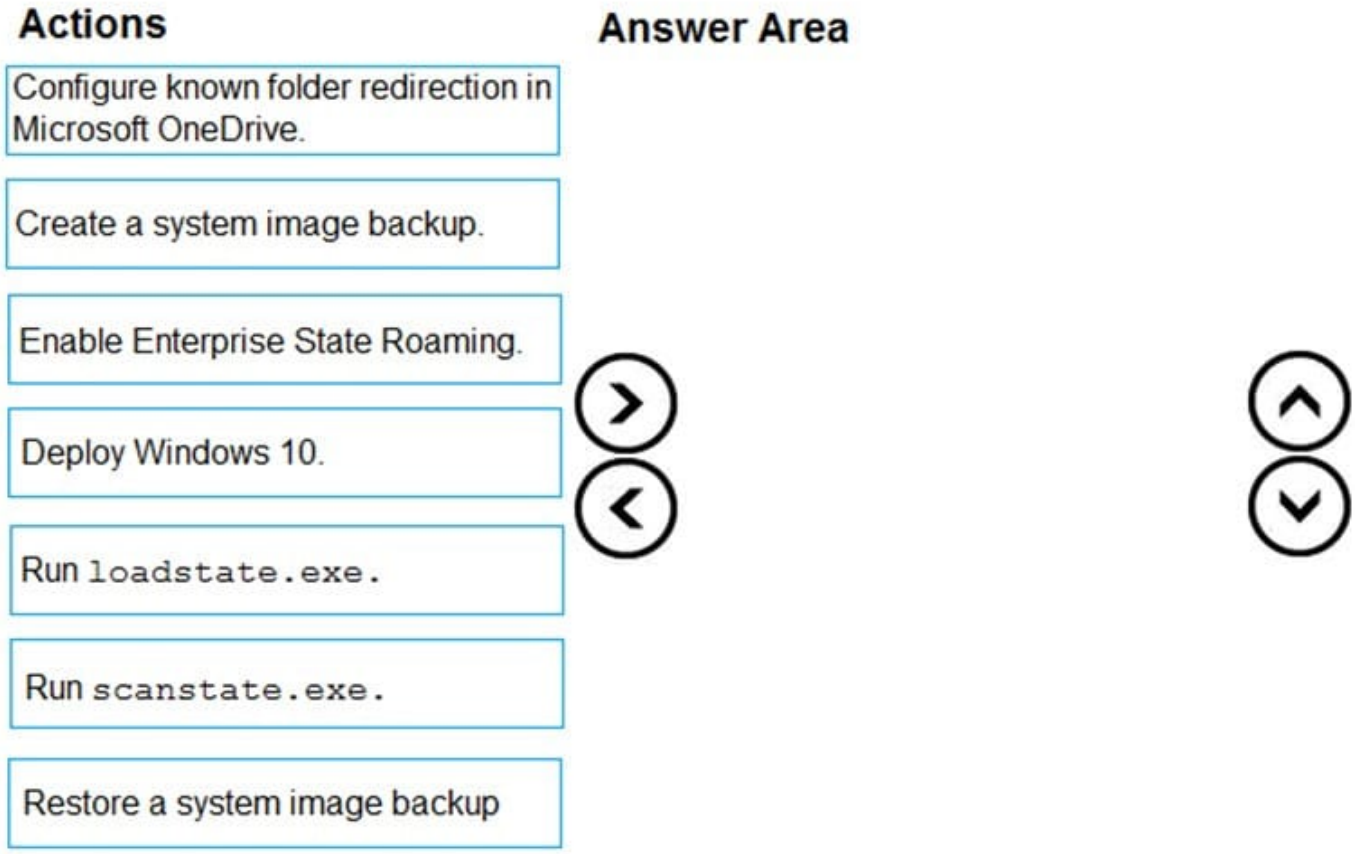
You have 100 computers that run Windows 8.1.

You plan to deploy Windows 10 to the computers by performing a wipe and load installation.

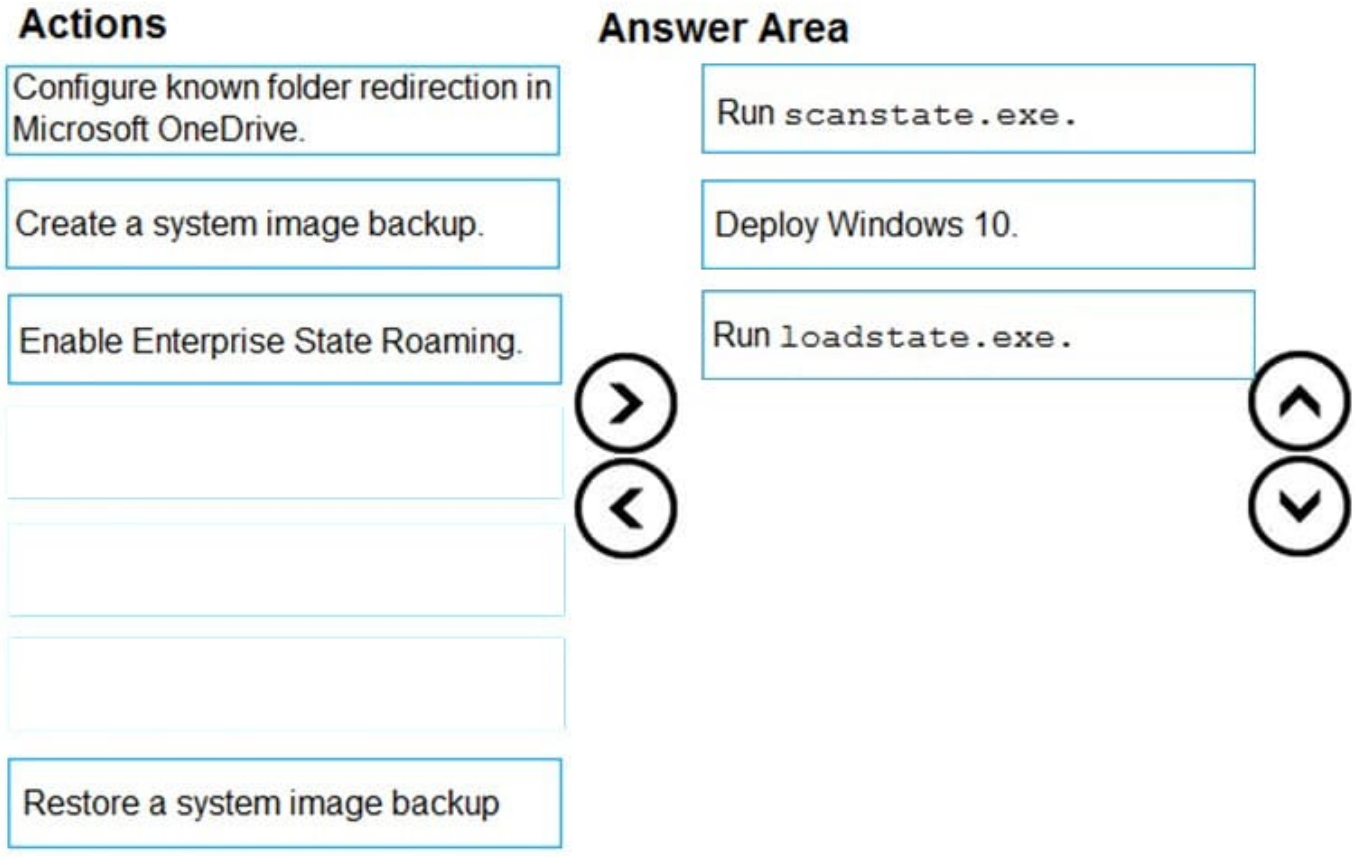
You need to recommend a method to retain the user settings and the user data.

Which three actions should you recommend be performed in sequence? To answer, move the appropriate actions from the list of actions to the answer area and arrange them in the correct order.

Select and Place:



Correct Answer:



Step 1: Run scanstate.exe

1.

Collect files and settings from the source computer.

2.

Back up the source computer.

3.

Close all applications.

4.

Run the ScanState command on the source computer to collect files and settings.

5.

Etc.

Step 2: Deploy Windows 10 Prepare the destination computer and restore files and settings.

Install the operating system on the destination computer.

Install all applications that were on the source computer. Although it is not always required, we recommend installing all applications on the destination computer before you restore the user state. This makes sure that migrated settings are

preserved.

Step 3: Run loadstate.exe Run the LoadState command on the destination computer. Specify the same set of .xml files that you specified when you used the ScanState command.

Reference:

https://docs.microsoft.com/en-us/windows/deployment/usmt/getting-started-with-the-user-state-migration-tool

---

QUESTION 11

You have a shared computer that runs Windows 10.

The computer is infected with a virus.

You discover that a malicious TTF font was used to compromise the computer.

You need to prevent this type of threat from affecting the computer in the future.

What should you use?

A. Windows Defender Exploit Guard

B. Windows Defender Application Guard

C. Windows Defender Credential Guard

D. Windows Defender System Guard

E. Windows Defender SmartScreen

Correct Answer: A

Reference: https://docs.microsoft.com/en-us/windows/security/threat-protection/windows-defender-exploit-guard/windows-defender-exploit-guard

---

QUESTION 12

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.

You have an Azure Directory group named Group1 that contains Windows 10 Enterprise devices and Windows 10 Pro devices.

From Microsoft Intune, you create a device configuration profile named Profile1.

You need to ensure that Profile1 applies to only the Windows 10 Enterprise devices in Group1.

Solution: You create a scope tag, and then you add the scope tag to the Windows 10 Enterprise devices and Profile1.

Does this meet the goal?

A. Yes

B. No

Correct Answer: B

Instead: You configure an applicability rule for Profile1. You assign Profile1 to Group1.

Note: Applicability rules allow administrators to target devices in a group that meet specific criteria. For example, you create a device restrictions profile that applies to the All Windows 10/11 devices group. And, you only want the profile

assigned to devices running Windows Enterprise.

To do this task, create an applicability rule.

Reference:

https://docs.microsoft.com/en-us/mem/intune/configuration/device-profile-create

---

QUESTION 13

HOTSPOT

Your company has computers that run Windows 10. The employees at the company use the computers.

You plan to monitor the computers by using the Update Compliance solution.

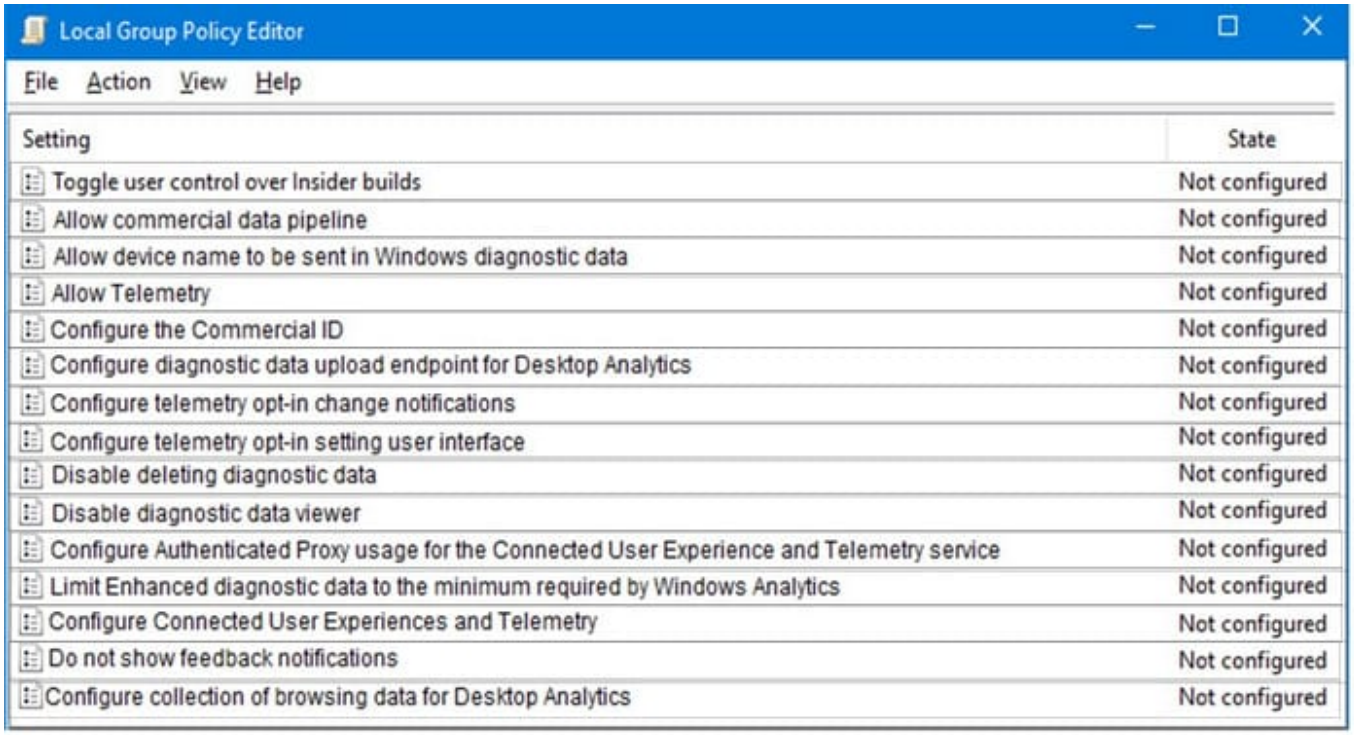
You create the required resources in Azure.

You need to configure the computers to send enhanced Update Compliance data.

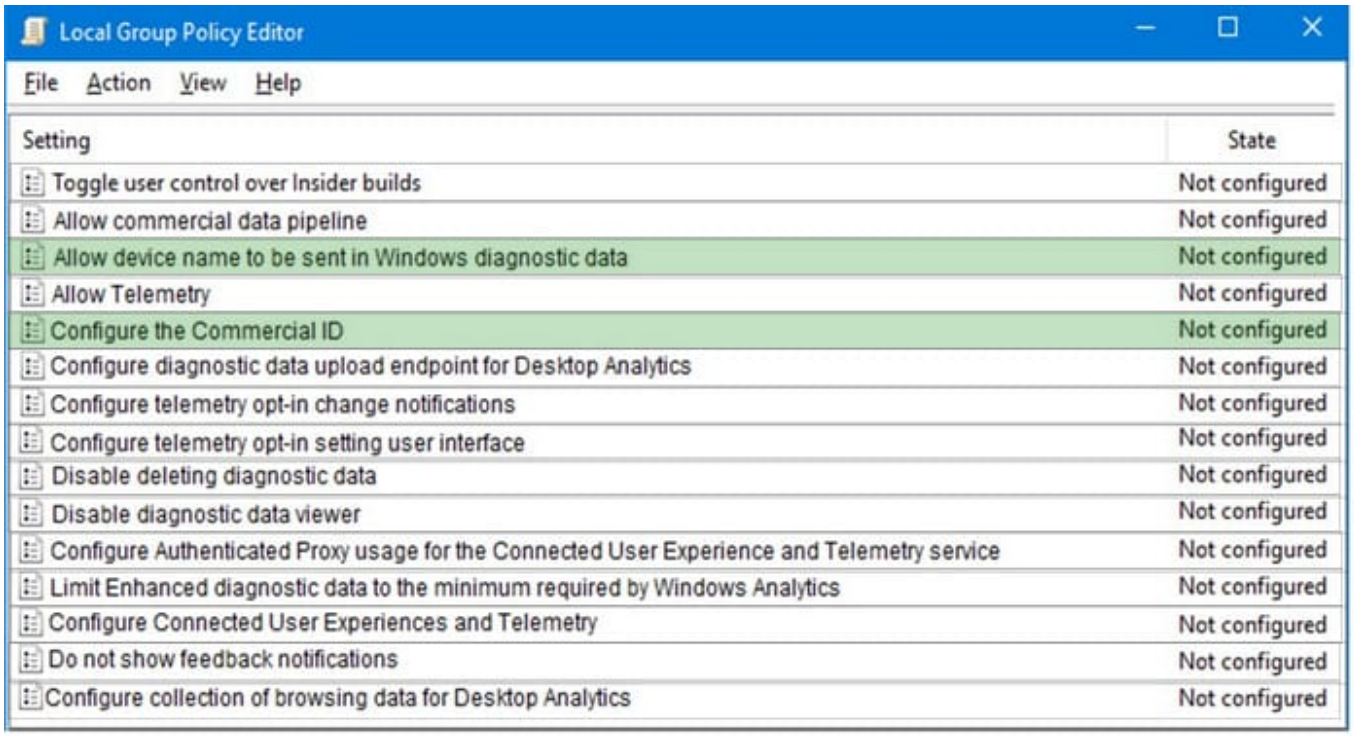
Which two Group Policy settings should you configure? To answer, select the appropriate settings in the answer area.

NOTE: Each correct selection is worth one point.

Hot Area:



Correct Answer:



Box 1: Configure the Commercial ID All Group policies that need to be configured for Update Compliance are under Computer Configuration>Administrative Templates>Windows Components\Data Collection and Preview Builds. All of these policies must be in the Enabled state and set to the defined Value below.

*

Configure the Commercial ID Identifies the device as belonging to your organization. Box 2: Allow device name to be

sent in Windows diagnostic data

*

Allow device name to be sent in Windows diagnostic data Allows device name to be sent for Windows Diagnostic Data. If this policy is Not Configured or Disabled, Device Name will not be sent and will not be visible in Update Compliance, showing # instead.

Reference: https://docs.microsoft.com/en-us/windows/deployment/update/update-compliance-configuration-manual

QUESTION 14

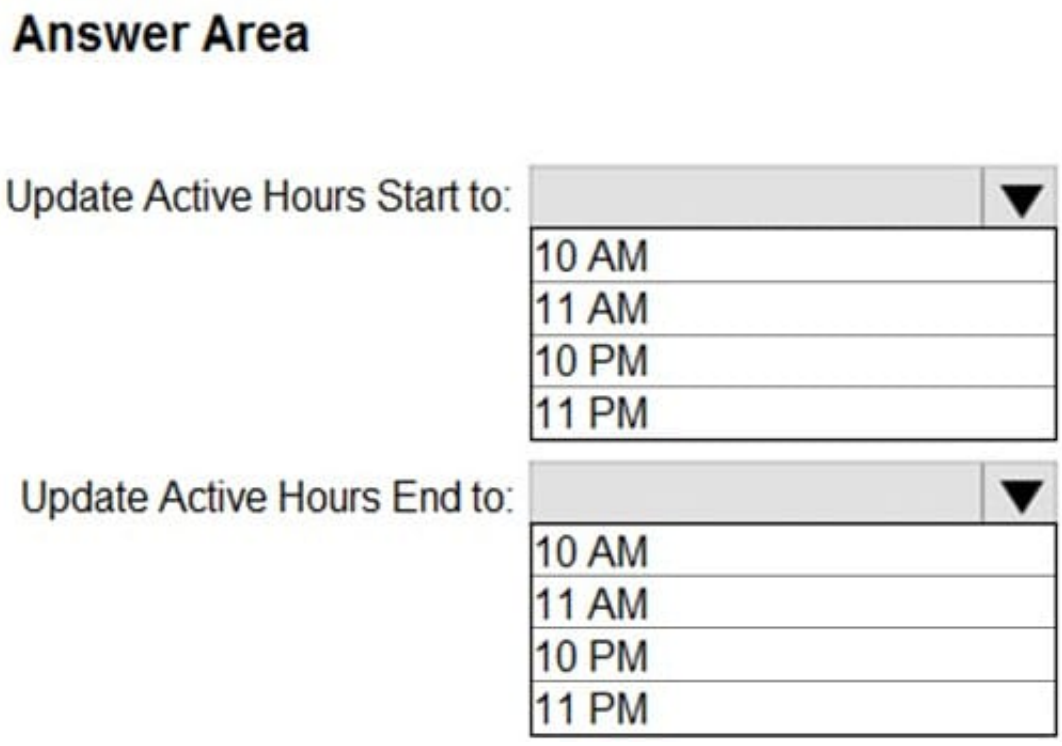
HOTSPOT

You need to resolve the performance issues in the Los Angeles office.

How should you configure the update settings? To answer, select the appropriate options in the answer area.

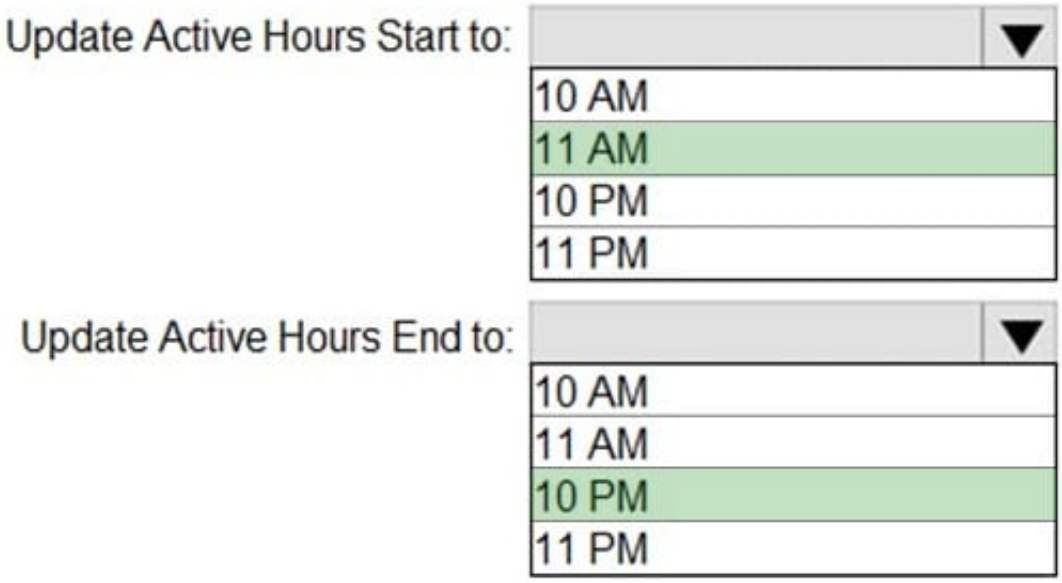
NOTE: Each correct selection is worth one point.

Hot Area:



Correct Answer:

Answer Area



The Los Angeles office has 500 developers. The developers work flexible hours ranging from 11 AM to 10 PM.

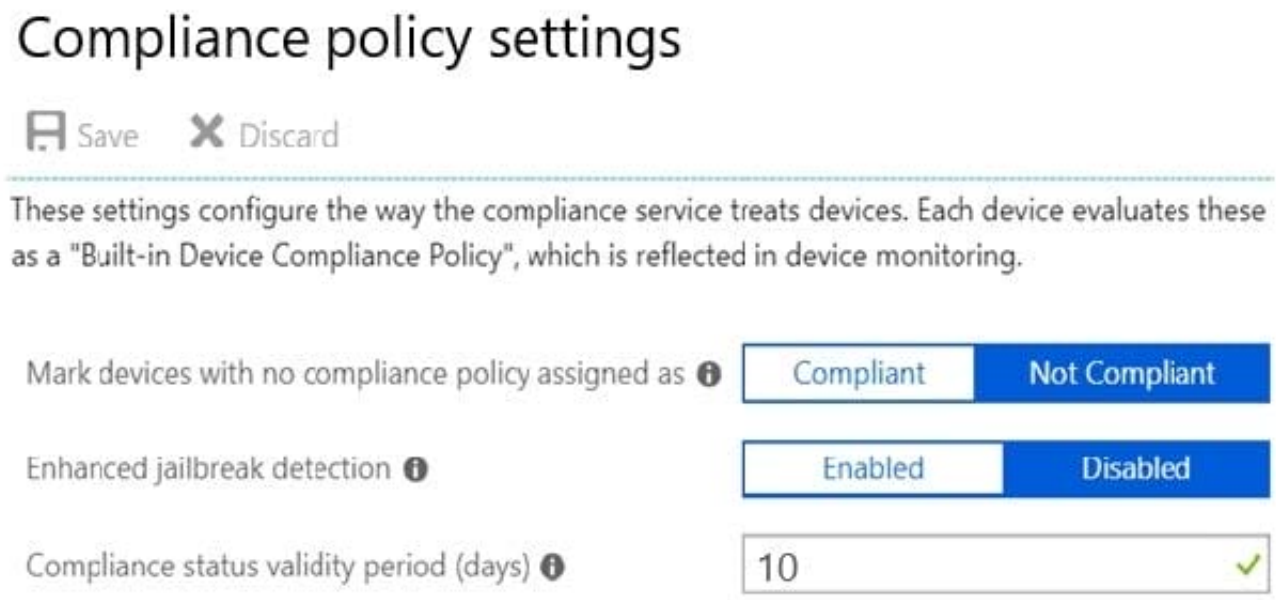
QUESTION 15

HOTSPOT

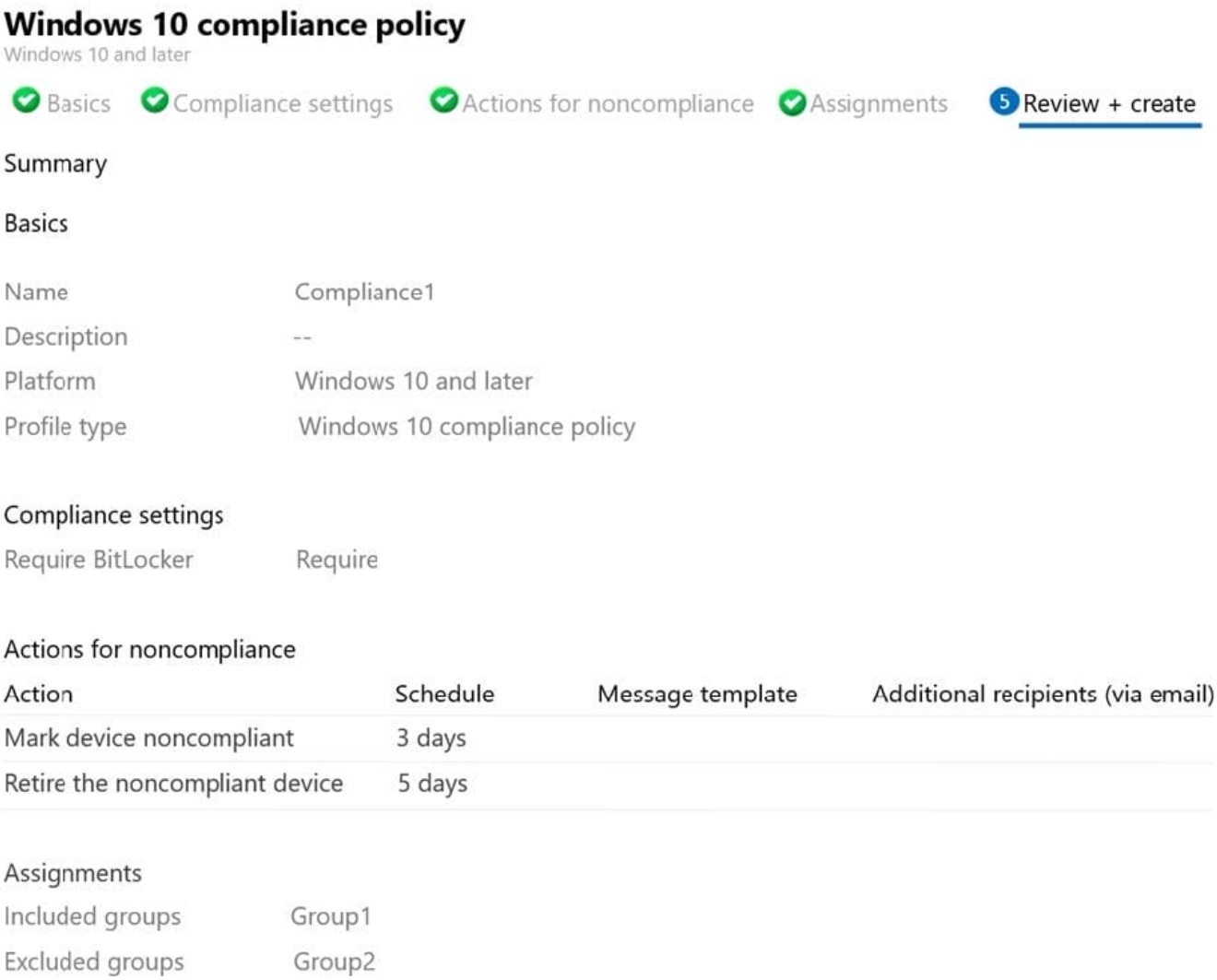
You have two Windows 10 devices enrolled in Microsoft Intune as shown in the following table.

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