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

Note: The question is included in a number of questions that depicts the identical set-up. However, every question has a distinctive result. Establish if the solution satisfies the requirements.

Your company has a number of Windows 10 Microsoft Azure Active Directory (Azure AD) joined workstations. These workstations have been enrolled in Microsoft Intune.

You have been tasked with making sure that the workstations are only able to run applications that you have explicitly permitted.

Solution: You make use of Windows Defender Application Guard.

Does the solution meet the goal?

A. Yes

B. No

Correct Answer: A

Instead use Windows Defender Application Control (WDAC).

Windows Defender Application Control and virtualization-based protection of code integrity.

Using WDAC to restrict devices to only authorized apps has these advantages over other solutions:

1.

WDAC lets you set application control policy for code that runs in user mode, kernel mode hardware and software drivers, and even code that runs as part of Windows.

2.

WDAC policy is enforced by the Windows kernel itself, and the policy takes effect early in the boot sequence before nearly all other OS code and before traditional antivirus solutions run.

3.

Etc.

Note: Application Guard helps to isolate enterprise-defined untrusted sites, protecting your company while your employees browse the Internet. As an enterprise administrator, you define what is among trusted web sites, cloud resources, and

internal networks. Everything not on your list is considered untrusted. If an employee goes to an untrusted site through either Microsoft Edge or Internet Explorer, Microsoft Edge opens the site in an isolated Hyper-V-enabled container.

For Microsoft Office, Application Guard helps prevents untrusted Word, PowerPoint and Excel files from accessing trusted resources.

Reference:

https://docs.microsoft.com/en-us/windows/security/threat-protection/device-guard/introduction-to-device-guard-virtualization-based-security-and-windows-defender-application-control

QUESTION 2

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 user-driven deployment profile.

Does this meet the goal?

A. Yes

B. No

Correct Answer: A

Windows Autopilot user-driven mode lets you configure new Windows devices to automatically transform them from their factory state to a ready-to-use state. This process doesn\\'t require that IT personnel touch the device.

The process is very simple. Devices can be shipped or distributed to the end user directly with the following instructions:

Unbox the device, plug it in, and turn it on.

Choose a language (only required when multiple languages are installed), locale, and keyboard.

Connect it to a wireless or wired network with internet access. If using wireless, the user must establish the Wi-Fi link.

Specify your e-mail address and password for your organization account.

The rest of the process is automated. The device will:

Join the organization.

Enroll in Intune (or another MDM service)

Get configured as defined by the organization.

Reference:

https://docs.microsoft.com/en-us/windows/deployment/windows-autopilot/user-driven

QUESTION 3

You have 100 devices that run Windows 10 and are joined to Microsoft Azure Active Directory (Azure AD).

You need to prevent users from joining their home computer to Azure AD.

What should you do?

A. From the Device enrollment blade in the Intune admin center, modify the Enrollment restriction settings.

B. From the Devices blade in the Azure Active Directory admin center, modify the Device settings.

C. From the Device enrollment blade in the Intune admin center, modify the Device enrollment manages settings.

D. From the Mobility (MDM and MAM) blade in the Azure Active Directory admin center, modify the Microsoft Intune enrollment settings.

Correct Answer: A

As an Intune administrator, you can create and manage enrollment restrictions that define what devices can enroll into management with Intune, including the:

Number of devices.

Operating systems and versions.

You can create multiple restrictions and apply them to different user groups. You can set the priority order for your different restrictions.

Create a device type restriction

1.

Sign in to the Microsoft Endpoint Manager admin center > Devices > Enroll Devices > Enrollment restrictions > Create restriction > Device type restriction.

2.

Etc.

Reference: https://docs.microsoft.com/en-us/intune/enrollment-restrictions-set

QUESTION 4

Note: The question is included in a number of questions that depicts the identical set-up. However, every question has a distinctive result. Establish if the solution satisfies the requirements.

Your company has a number of Windows 10 Microsoft Azure Active Directory (Azure AD) joined workstations. These workstations have been enrolled in Microsoft Intune.

You have been tasked with making sure that the workstations are only able to run applications that you have explicitly permitted.

Solution: You make use of Windows Defender SmartScreen.

Does the solution meet the goal?

A. Yes

B. No

Correct Answer: B

Instead use Windows Defender Application Control (WDAC).

Windows Defender Application Control and virtualization-based protection of code integrity.

Using WDAC to restrict devices to only authorized apps has these advantages over other solutions:

1.

WDAC lets you set application control policy for code that runs in user mode, kernel mode hardware and software drivers, and even code that runs as part of Windows.

2.

WDAC policy is enforced by the Windows kernel itself, and the policy takes effect early in the boot sequence before nearly all other OS code and before traditional antivirus solutions run.

3.

Etc.

Reference: https://docs.microsoft.com/en-us/windows/security/threat-protection/device-guard/introduction-to-device-guard-virtualization-based-security-and-windows-defender-application-control

QUESTION 5

You manage a Microsoft 365 environment that has co-management enabled.

All computers run Windows 10 and are deployed by using the Microsoft Deployment Toolkit (MDT).

You need to recommend a solution to deploy Microsoft Office 365 ProPlus to new computers. The latest version must always be installed. The solution must minimize administrative effort.

What is the best tool to use for the deployment? More than one answer choice may achieve the goal. Select the BEST answer.

A. Microsoft Intune

B. Microsoft Deployment Toolkit

C. Office Deployment Tool (ODT)

D. a Group Policy object (GPO)

E. Microsoft System Center Configuration Manager

Correct Answer: A

Intune --> Create device group --> Select o365 app --> deploy to group

ODT --> Download files -> create XML --> how to trigger install (manual install/MDT Task seq/powershell script/logon script etc)

SCCM --> create new package via ODT or via wizard --> select DPs to distribute -->deploy to collection

MDT --> requires ODT to have latest version, but is fastest with install as O365 is installed during TS, so at the end I would use this in production, but is not wat MS asks.

In the question it states the machines are in co-management, which indicates the presence of ConfigMgr and Intune otherwise machines cannot be co-managed. In configMgr there is a co-management workload you can move to Intune

specifically for Office 365 management. Office deployment and management from intune is by far the most simple way to deploy the Office apps (MS 365 Apps for business) .

https://docs.microsoft.com/en-us/mem/configmgr/comanage/workloads#office-click-to-run-apps

https://docs.microsoft.com/en-us/mem/intune/apps/apps-add-office365#select-microsoft-365-apps

QUESTION 6

Your network contains an Active Directory forest. The forest contains a single domain and three sites named Site1, Site2, and Site3. Each site is associated to two subnets. Site1 contains two subnets named SubnetA and SubnetB.

All the client computers in the forest run Windows 10. Delivery Optimization is enabled.

You have a computer named Computer1 that is in SubnetA.

From which hosts will Computer1 download updates?

A. the computers in Site1 only

B. any computer in the domain

C. the computers in SubnetA only

D. any computer on the network

Correct Answer: C

Download mode option : LAN (1=Default)

This default operating mode for Delivery Optimization enables peer sharing on the same network. The Delivery Optimization cloud service finds other clients that connect to the Internet using the same public IP as the target client. These

clients then try to connect to other peers on the same network by using their private subnet IP.

https://docs.microsoft.com/en-us/windows/deployment/update/waas-delivery-optimization-reference

https://docs.microsoft.com/en-us/windows/deployment/do/waas-delivery-optimization-reference#download-mode

https://techcommunity.microsoft.com/t5/windows-it-pro-blog/delivery-optimization-scenarios-and-configuration-options/ba-p/280195

QUESTION 7

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 network contains an Active Directory domain. The domain contains a computer named Computer1 that runs Windows 8.1.

Computer1 has apps that are compatible with Windows 10.

You need to perform a Windows 10 in-place upgrade on Computer1.

Solution: You add Windows 10 startup and install images to a Windows Deployment Services (WDS) server. You start Computer1 by using WDS and PXE, and then you initiate the Windows 10 installation.

Does this meet the goal?

A. Yes

B. No

Correct Answer: A

Reference: https://docs.microsoft.com/en-us/windows/deployment/windows-deployment-scenarios-and-tools

QUESTION 8

You have a Microsoft 365 subscription that uses Microsoft Intune.

You need to ensure that you can deploy apps to Android Enterprise devices.

What should you do first?

A. Add a certificate connector.

B. Link your managed Google Play account to Intune.

C. Configure the Partner device management settings

D. Create a configuration profile.

Correct Answer: B

Connect your Intune account to your Managed Google Play account.

Managed Google Play is Google\\'s enterprise app store and sole source of applications for Android Enterprise in Intune. You can use Intune to orchestrate app deployment through Managed Google Play for any Android Enterprise scenario

(including personally-owned work profile, dedicated, fully managed, and corporate- owned work profile enrollments).

Reference:

https://docs.microsoft.com/en-us/mem/intune/apps/apps-add-android-for-work

https://docs.microsoft.com/en-us/mem/intune/enrollment/connect-intune-android-enterprise

QUESTION 9

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 perform a local Windows Autopilot Reset.

Does this meet the goal?

A. Yes

B. No

Correct Answer: B

Instead:

Windows Autopilot user-driven mode lets you configure new Windows devices to automatically transform them from their factory state to a ready-to-use state. This process doesn\\'t require that IT personnel touch the device.

The process is very simple. Devices can be shipped or distributed to the end user directly with the following instructions:

Unbox the device, plug it in, and turn it on.

Choose a language (only required when multiple languages are installed), locale, and keyboard.

Connect it to a wireless or wired network with internet access. If using wireless, the user must establish the Wi-Fi link.

Specify your e-mail address and password for your organization account.

The rest of the process is automated. The device will:

Join the organization.

Enroll in Intune (or another MDM service)

Get configured as defined by the organization.

Reference:

https://docs.microsoft.com/en-us/windows/deployment/windows-autopilot/windows-autopilot-reset

QUESTION 10

HOTSPOT

You have a workgroup computer named Computer1 that runs Windows 10 and has the users shown in the following table.

Name	Member of
User1	Group1
User2	Group2
User3	Group3

Group1 is a member of Group3.

You are creating a file named Kiosk.xml that specifies a lockdown profile for a multi-app kiosk.

Kiosk.xml contains the following section.

```
<Configs>
  <Config>
    <UserGroup Type="LocalGroup" Name="Group3" />
    <DefaultProfile Id="{9A2A490F-10F6-4764-974A-43B19E722C23}"/>
  </Config>
</Configs>
```

You apply Kiosk.xml to Computer1.

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
The lockdown profile applies to User1.	○	○
The lockdown profile applies to User2.	○	○
The lockdown profile applies to User3.	○	○

Correct Answer:

Answer Area

Statements	Yes	No
The lockdown profile applies to User1.	○	○
The lockdown profile applies to User2.	○	○
The lockdown profile applies to User3.	○	○

Box 1: No The lockdown profile only applies to the specified group, not to the nested group. Box 2: No

Box 3: Yes Reference: https://docs.microsoft.com/en-us/windows/configuration/lock-down-windows-10-to-specific-apps#config-for-group-accounts

QUESTION 11

You have 100 computers that run Windows 8.1.

You need to identify which computers can be upgraded to Windows 10.

What should you use?

A. Microsoft Deployment Toolkit (MDT)

B. Update Compliance Azure

C. Windows Assessment Toolkit

D. Microsoft Assessment and Planning (MAP) Toolkit.

Correct Answer: D

Reference: https://www.techielass.com/using-maps-azure-readiness/

QUESTION 12

You have configured the use of Windows Defender Advanced Threat Protection (Windows Defender ATP) to protect your company\\'s Windows 10 devices. You have been tasked with checking how the configuration of Windows Defender ATP compares to the Microsoft-recommended configuration baseline. Which of the following should you use to achieve your goal?

A. Windows Defender Security Center

B. Device Health

C. Device compliance

D. Microsoft Secure Score

Correct Answer: D

References: https://docs.microsoft.com/en-us/windows/security/threat-protection/microsoft-defender-atp/overview-secure-score

QUESTION 13

HOTSPOT

You have a Microsoft 365 E5 subscription that contains the users shown in the following table.

Name	Member of	Multi-factor authentication (MFA) status
User1	Group1	Disabled
User2	Group1, Group2	Enforced

You have the devices shown in the following table.

Name	Platform
Device1	Windows 11
Device2	Android

You have a Conditional Access policy named CAPolicy1 that has the following settings: Assignments

-Users or workload identities: Group1

-Cloud apps or actions: All cloud apps

Conditions

-Device platforms: include: Windows, Android

-Grant access controls: Require multi-factor authentication

You have a Conditional Access named CAPolicy2 that has the following settings:

Assignments

-Users or workload identities: Group2

-Cloud apps or actions: All cloud apps

Conditions

-Device platforms: Android

-Access controls: Block access

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 access Microsoft Exchange Online from Device2.	○	○
User2 can access Microsoft Exchange Online from Device1.	○	○
User2 can access Microsoft Exchange Online from Device2.	○	○

Correct Answer:

Answer Area

Statements	Yes	No
User1 can access Microsoft Exchange Online from Device2.	○	◉
User2 can access Microsoft Exchange Online from Device1.	◉	○
User2 can access Microsoft Exchange Online from Device2.	◉	○

QUESTION 14

Your network contains an on-premises Active Directory domain and an Azure Active Directory (Azure AD) tenant. The Default Domain Policy Group Policy Object (GPO) contains the settings shown in the following table.

Name	GPO value
LockoutBadCount	0
MaximumPasswordAge	42
MinimumPasswordAge	1
MinimumPasswordLength	7
PasswordComplexity	True
PasswordHistorySize	24

You need to migrate the existing Default Domain Policy GPO settings to a device configuration profile.

Which type of device configuration profile should you create?

A. Custom

B. Endpoint protection

C. Administrative Templates

D. Device restrictions

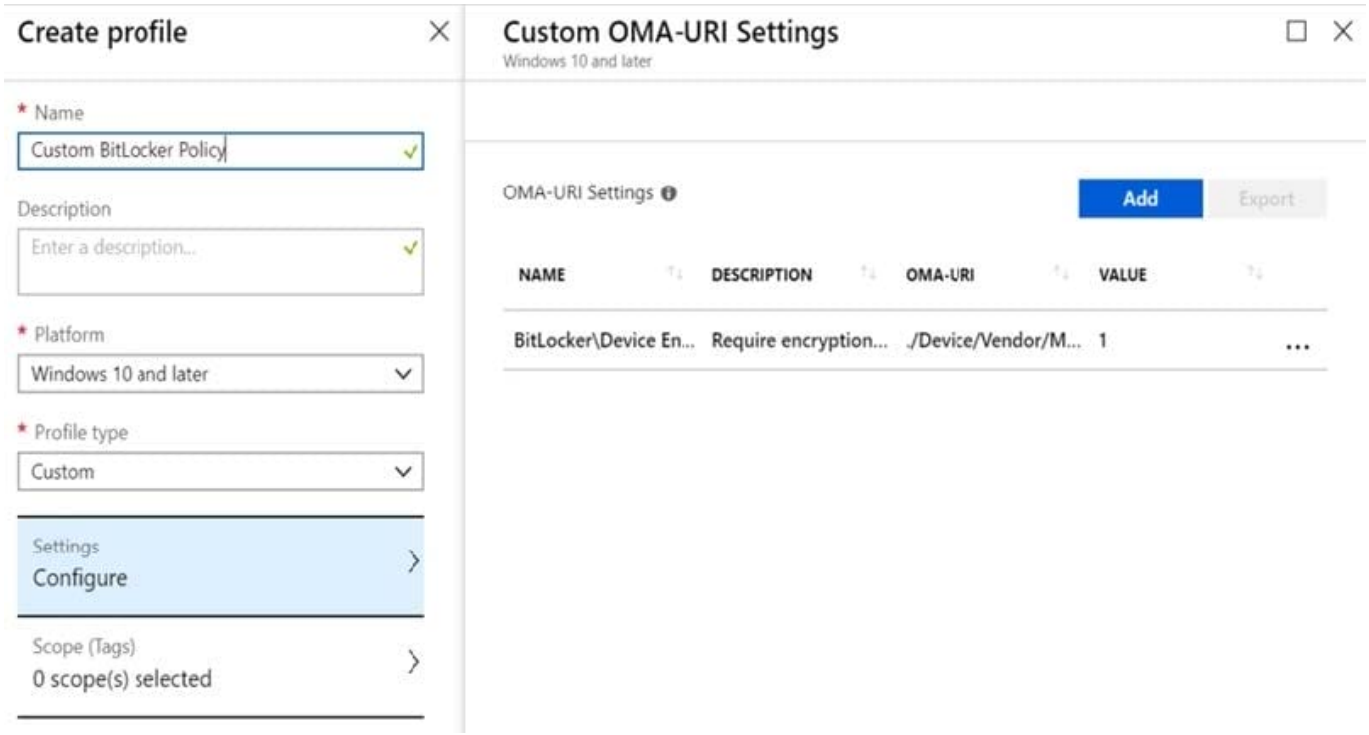
Correct Answer: A

Intune (and other MDM solutions) build there policy configurations and user interfaces on top of CSPs(Configuration Service Providers) . However, some CSPs and its settings might not be exposed in the interface directly but such a setting

can be set anyway by entering its OMA-URI manually. Think of an OMA-URI as sort of a registry key that you can set to make the underlying configuration setting happen.

In Intune this is called a Custom Policy.

Example:



QUESTION 15

HOTSPOT

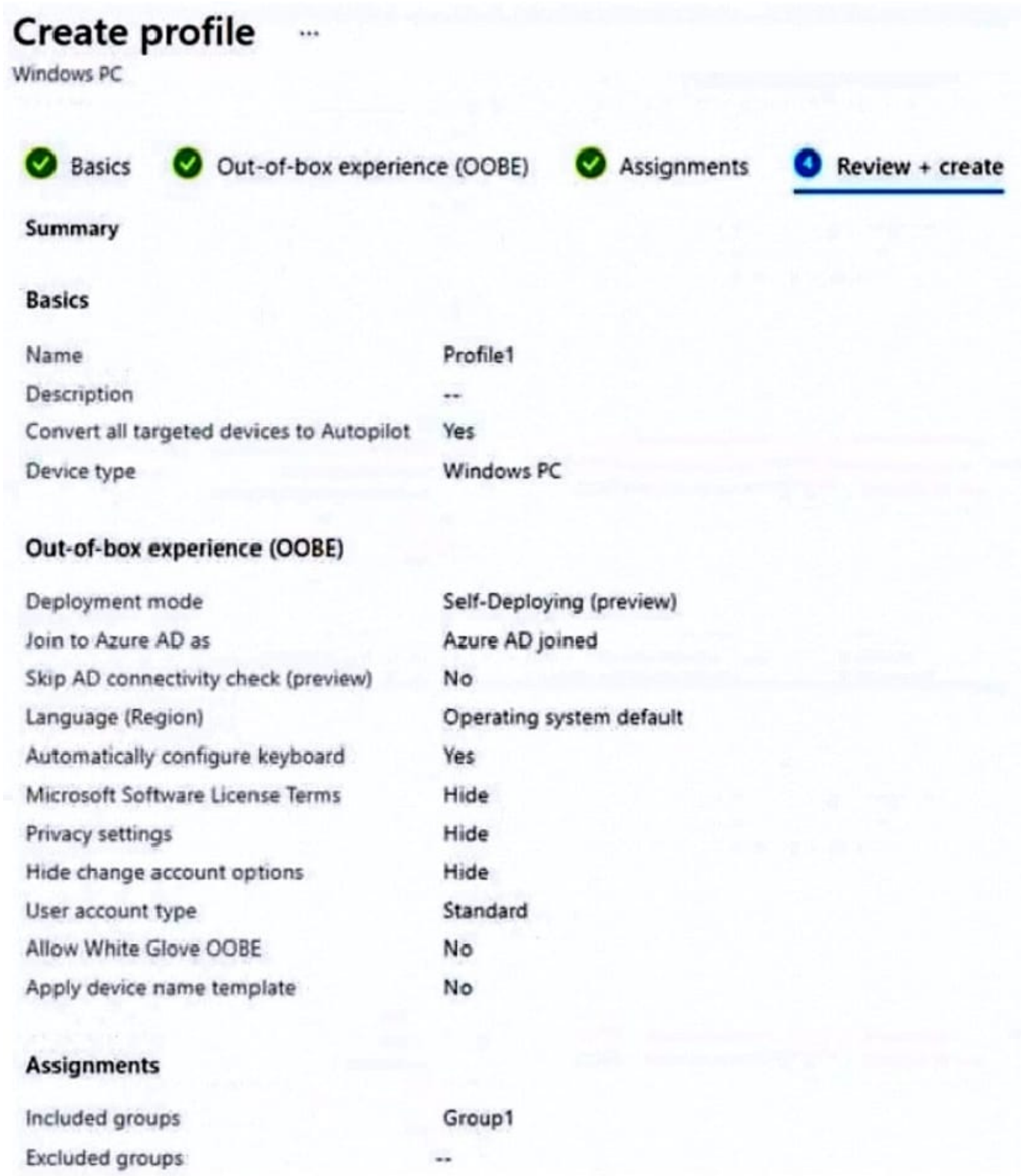
You have an Azure Active Directory (Azure AD) tenant named contoso.com that contains the devices shown in the following table.

Name	Operating system	Azure AD status	Mobile device management (MDM)
Device1	Windows 8.1	Registered	None
Device2	Windows 10	Joined	None
Device3	Windows 10	Joined	Microsoft Intune

Contoso.com contains the Azure Active Directory groups shown in the following table.

Name	Members
Group1	Group2, Device1, Device3
Group2	Device2

You add a Windows Autopilot deployment profile. The profile is configured 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:

Answer Area

Statements	Yes	No
If Device1 starts in Out of Box Experience (OOBE) mode, the device will be deployed by using Autopilot.	○	○
If Device2 starts in Out of Box Experience (OOBE) mode, the device will be deployed by using Autopilot.	○	○
If Device3 starts in Out of Box Experience (OOBE) mode, the device will be deployed by using	○	○

Correct Answer:

Answer Area

Statements	Yes	No
If Device1 starts in Out of Box Experience (OOBE) mode, the device will be deployed by using Autopilot.	○	●
If Device2 starts in Out of Box Experience (OOBE) mode, the device will be deployed by using Autopilot.	○	●
If Device3 starts in Out of Box Experience (OOBE) mode, the device will be deployed by using	●	○

Box 1: No

Device1 has no Mobile device Management (MDM) configured.

Note: Device1 is running Windows 8.1, and is registered, but not joined.

Device1 is in Group1.

Profile1 is assigned to Group1.

Box 2: No

Device2 has no Mobile device Management (MDM) configured.

Note: Device2 is running Windows 10, and is joined.

Device2 is in Group2.

Group2 is in Group1.

Profile1 is assigned to Group1.

Box 3: Yes

Device3 has Mobile device Management (MDM) configured.

Device3 is running Windows 10, and is joined

Device1 is in Group1.

Profile1 is assigned to Group1.

Mobile device management (MDM) enrollment: Once your Windows 10 device joins Azure AD, Autopilot ensures your device is automatically enrolled with MDMs such as Microsoft Intune. This program can automatically push configurations,

policies and settings to the device, and install Office 365 and other business apps without you having to get IT admins to manually sort the device. Intune can also apply the latest updates from Windows Update for Business.

Reference:

https://xo.xello.com.au/blog/windows-autopilot