MD-101 Q&As

Managing Modern Desktops

Pass Microsoft MD-101 Exam with 100% Guarantee

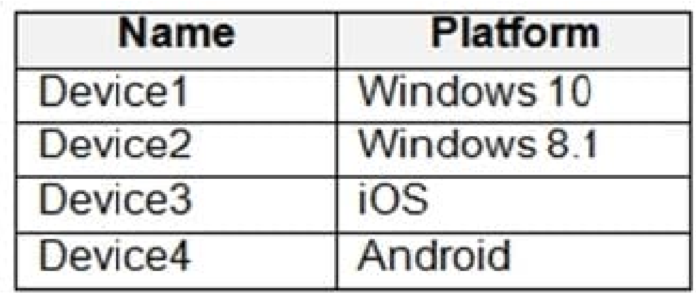
Following Questions and Answers are all new published by Microsoft Official Exam Center

QUESTION 1

HOTSPOT

You have a Microsoft 365 E5 tenant that connects to Microsoft Defender for Endpoint.

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



Name	Platform
Device1	Windows 10
Device2	Windows 8.1
Device3	iOS
Device4	Android

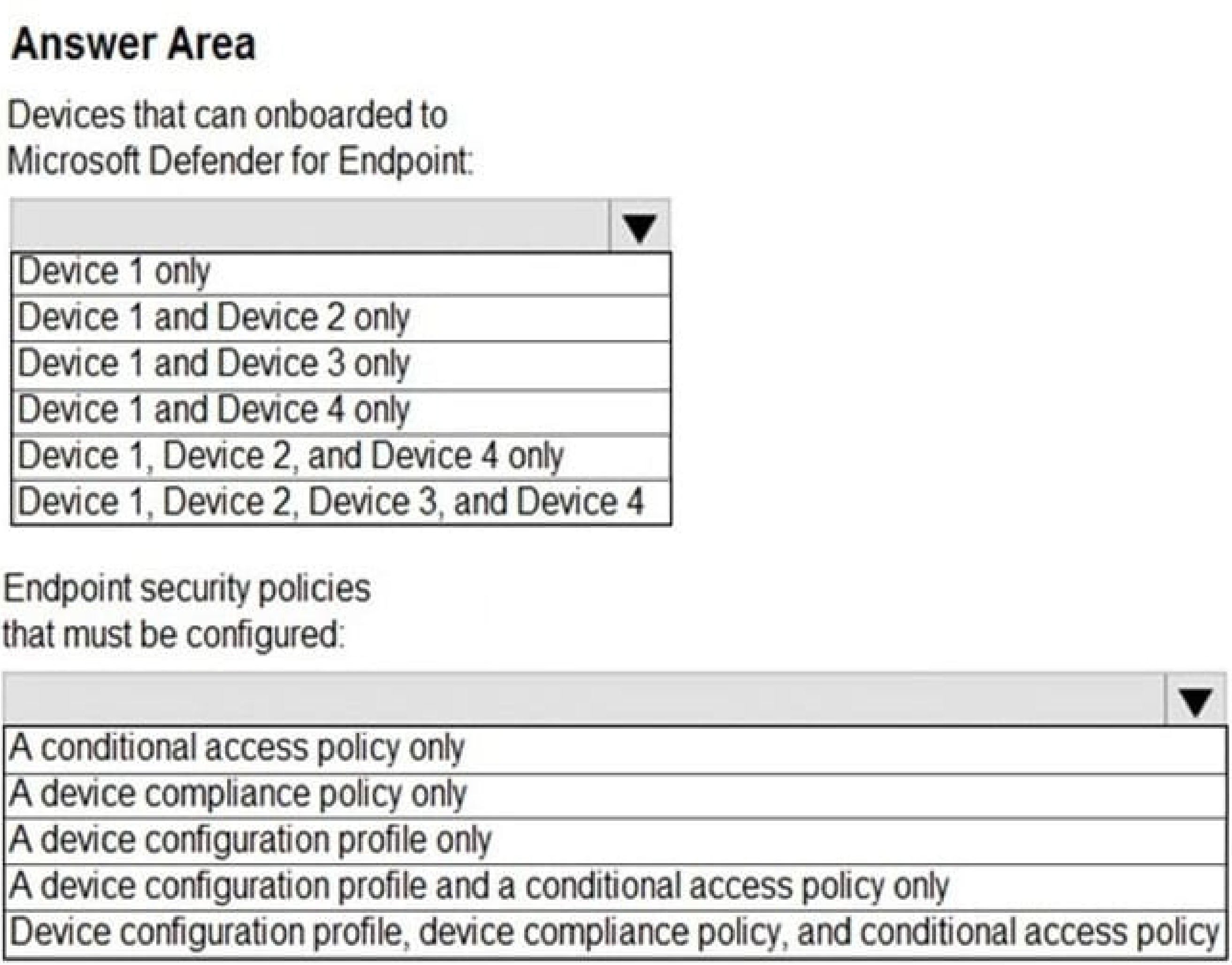
You plan to use risk levels in Microsoft Defender for Endpoint to identify whether a device is compliant. Noncompliant devices must be blocked from accessing corporate resources.

You need to identify which devices can be onboarded to Microsoft Defender for Endpoint, and which Endpoint security policies must be configured.

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

Devices that can onboarded to
Microsoft Defender for Endpoint:

▼

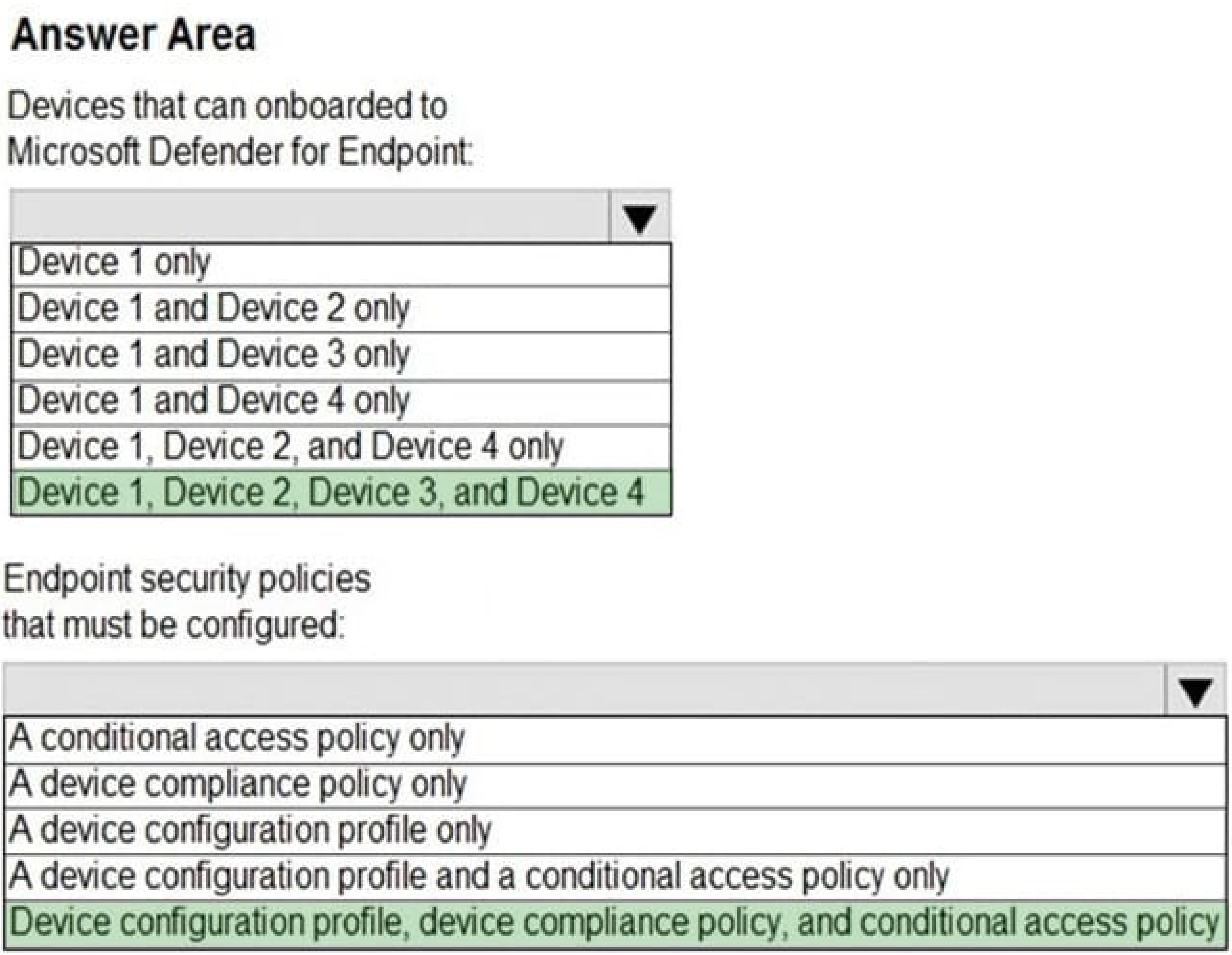
Device 1 only
Device 1 and Device 2 only
Device 1 and Device 3 only
Device 1 and Device 4 only
Device 1, Device 2, and Device 4 only
Device 1, Device 2, Device 3, and Device 4

Endpoint security policies
that must be configured:

▼

A conditional access policy only
A device compliance policy only
A device configuration profile only
A device configuration profile and a conditional access policy only
Device configuration profile, device compliance policy, and conditional access policy

Correct Answer:



Answer Area

Devices that can onboarded to Microsoft Defender for Endpoint:

- Device 1 only
- Device 1 and Device 2 only
- Device 1 and Device 3 only
- Device 1 and Device 4 only
- Device 1, Device 2, and Device 4 only
- [✓ Device 1, Device 2, Device 3, and Device 4]

Endpoint security policies that must be configured:

- A conditional access policy only
- A device compliance policy only
- A device configuration profile only
- A device configuration profile and a conditional access policy only
- [✓ Device configuration profile, device compliance policy, and conditional access policy]

Box 1: Device 1, Device2, Device 3, and Device 4 Supported Windows versions include Windows 8.1 and Windows 10 Other supported operating systems Android iOS Linux macOS Box 2: Device configuration profile, device compliance policy, and conditional access policy We need all three policies. Establish a service-to-service connection between Intune and Microsoft Defender for Endpoint. This connection lets Microsoft Defender for Endpoint collect data about machine risk from supported devices you manage with Intune. Use a device configuration profile to onboard devices with Microsoft Defender for Endpoint. You onboard devices to configure them to communicate with Microsoft Defender for Endpoint and to provide data that helps assess their risk level. Use a device compliance policy to set the level of risk you want to allow. Risk levels are reported by Microsoft Defender for Endpoint. Devices that exceed the allowed risk level are identified as noncompliant. Use a conditional access policy to block users from accessing corporate resources from devices that are noncompliant.

Reference: https://docs.microsoft.com/en-us/microsoft-365/security/defender-endpoint/minimum-requirements https://docs.microsoft.com/en-us/mem/intune/protect/advanced-threat-protection#onboard-devices-by-using-a-configuration-profile

QUESTION 2

You have a Microsoft 365 E5 subscription and 150 Windows 10 devices.

All the devices are enrolled in Microsoft Intune.

You need to use Intune to apply Windows updates to the devices.

What should you do first?

A. From the Microsoft Endpoint Manager admin center, configure scope tags.

B. Create a device restriction policy that has telemetry set to the minimum setting of Required.

C. From the Microsoft Endpoint Manager admin center, configure a security baseline.

D. Create a device restriction policy that has telemetry set to Security (Enterprise Only).

Correct Answer: A

QUESTION 3

Your company plans to deploy tablets to 50 meeting rooms.

The tablets run Windows 10 and are managed by using Microsoft Intune. The tablets have an application named App1.

You need to configure the tablets so that any user can use App1 without having to sign in. Users must be prevented from using other applications on the tablets.

Which device configuration profile type should you use?

A. Kiosk

B. Endpoint protection

C. Identity protection

D. Device restrictions

Correct Answer: A

References: https://docs.microsoft.com/en-us/windows/configuration/kiosk-single-app

QUESTION 4

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).

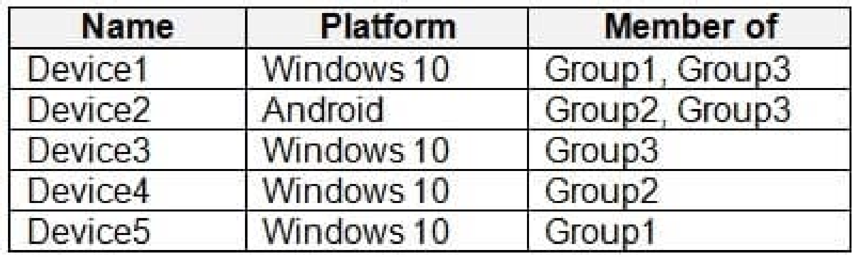
Correct Answer: C

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 5

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



Name	Platform	Member of
Device1	Windows 10	Group1, Group3
Device2	Android	Group2, Group3
Device3	Windows 10	Group3
Device4	Windows 10	Group2
Device5	Windows 10	Group1

You create an app protection policy named Policy1 that has the following settings:

1.

Platform: Windows 10

2.

Protected apps: App1

3.

Exempt apps: App2

4.

Network boundary: Cloud resources, IPv4 ranges

You assign Policy1 to Group1 and Group2. You exclude Group3 from Policy1.

Which devices will apply Policy1?

A. Device1, Device2, Device4, and Device5

B. Device1, Device4, and Device5 only

C. Device4 and Device5 only

D. Device1, Device3, Device4 and Device5

Correct Answer: C

Intune device configuration profiles let you include and exclude groups from profile assignment. Exclusion takes precedence over inclusion in same group types.

Policy1 excludes Group3 and Group3 includes Device1, Device2, and Device3.

Incorrect Answers:

A, B, D: Device1, Device2, and Device3 are members of Group3. Policy1 excludes Group3. Exclusion takes precedence over inclusion.

Reference:

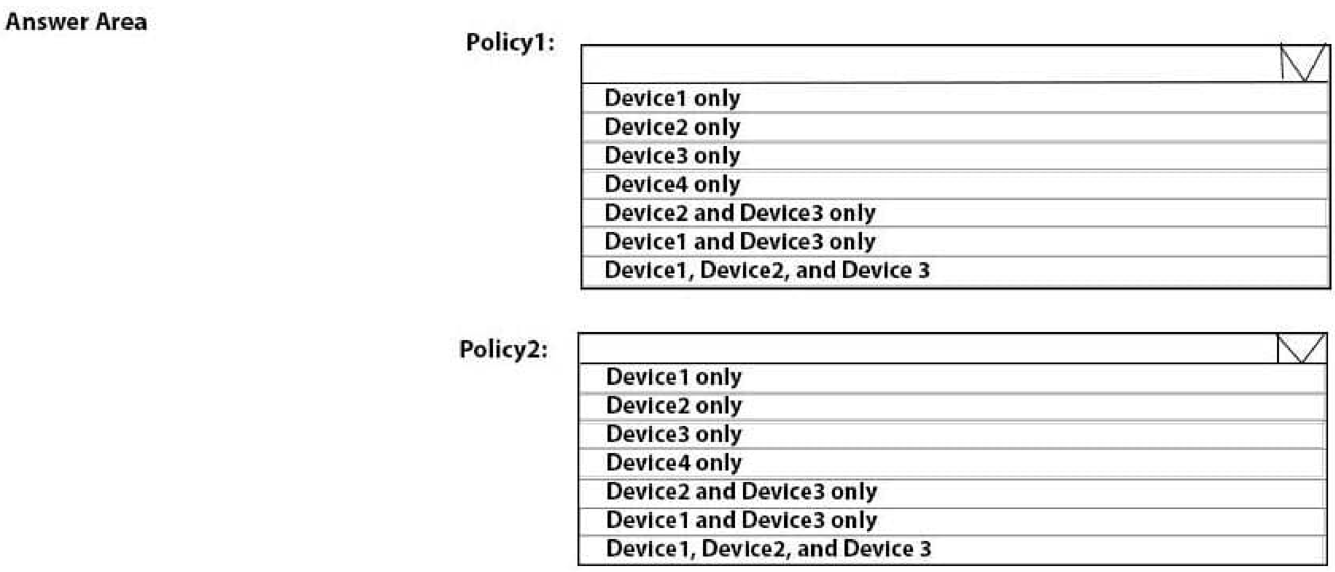
https://docs.microsoft.com/en-us/mem/intune/configuration/device-profile-assign#exclude-groups-from-a-profile-assignment

https://docs.microsoft.com/en-us/intune/app-protection-policies

QUESTION 6

To which devices do Policy1 and Policy2 apply? To answer, select the appropriate options in the answer area. NOTE: Each correct selection is worth one point.

Hot Area:



Answer Area

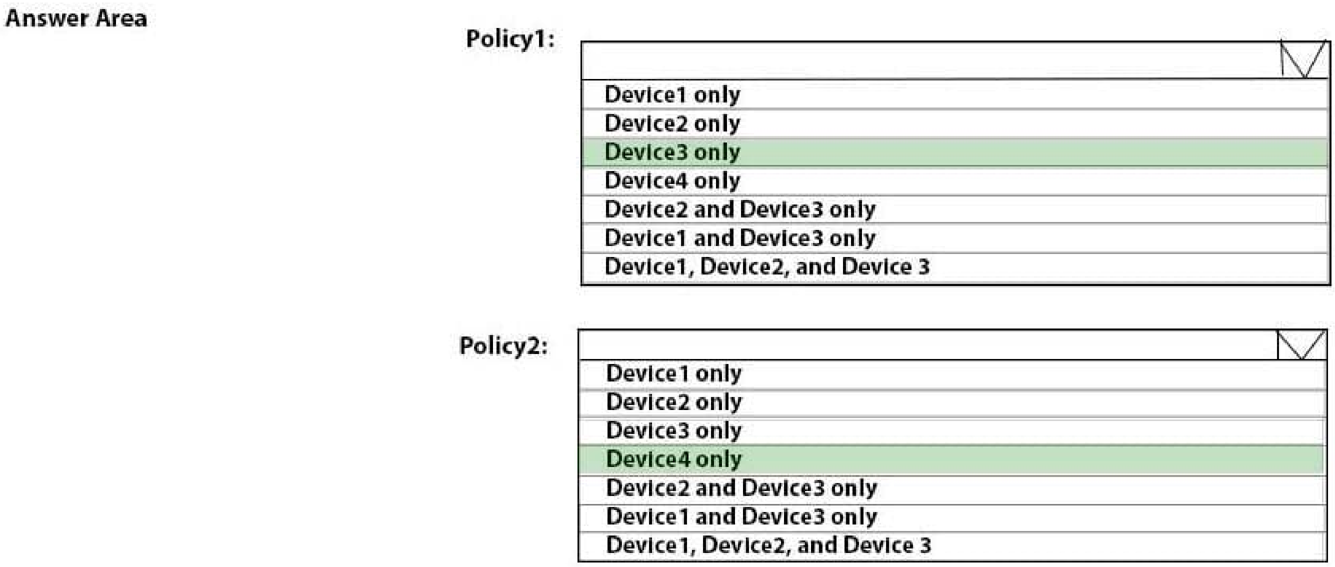
Policy1:

- Device1 only
- Device2 only
- Device3 only
- Device4 only
- Device2 and Device3 only
- Device1 and Device3 only
- Device1, Device2, and Device 3

Policy2:

- Device1 only
- Device2 only
- Device3 only
- Device4 only
- Device2 and Device3 only
- Device1 and Device3 only
- Device1, Device2, and Device 3

Correct Answer:



Answer Area

Policy1:

- Device1 only
- Device2 only
- [✓ Device3 only]
- Device4 only
- Device2 and Device3 only
- Device1 and Device3 only
- Device1, Device2, and Device 3

Policy2:

- Device1 only
- Device2 only
- Device3 only
- [✓ Device4 only]
- Device2 and Device3 only
- Device1 and Device3 only
- Device1, Device2, and Device 3

Box 1: Device 3 only Policy1 applies to Device3 (Android)

Box 2: Device 4 only Policy2 applies to Device4 (iOS)

Reference:

https://docs.microsoft.com/en-us/intune/device-profile-assign

QUESTION 7

HOTSPOT

You use the Microsoft Deployment Toolkit (MDT) to deploy Windows 10.

You need to modify the deployment share to meet the following requirements:

1.

Ensure that the user who performs the installation is prompted to set the local Administrator password.

2.

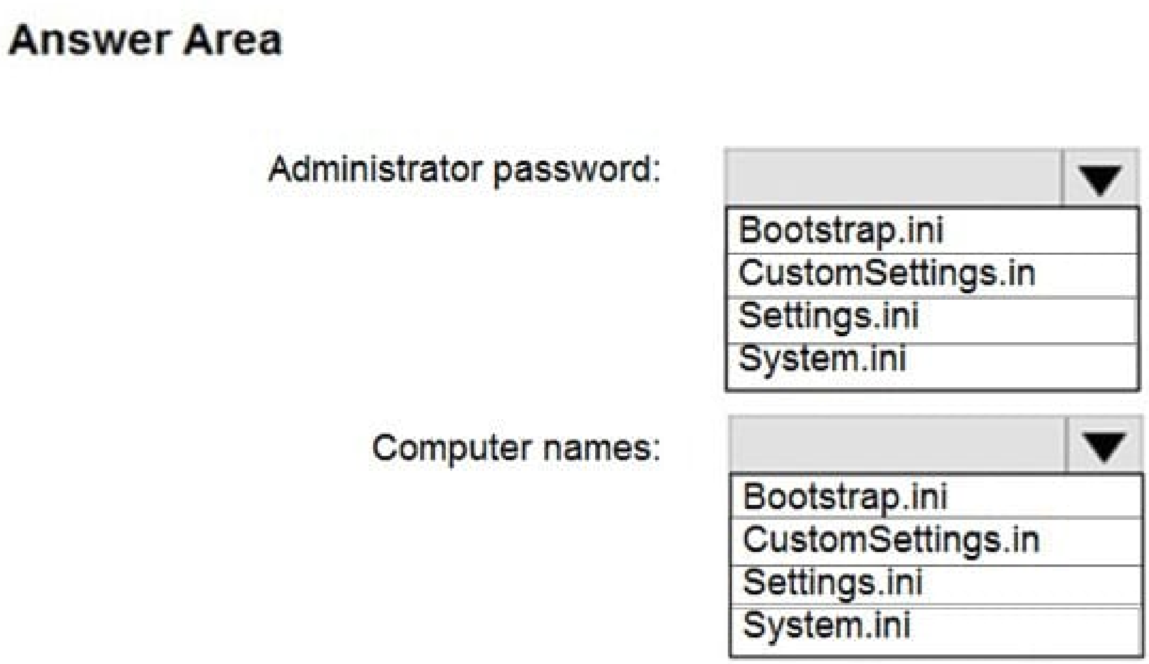
Define a rule for how to name computers during the deployment.

The solution must NOT replace the existing WinPE image.

Which file should you modify for each requirement? To answer, select the appropriate options in the answer area.

NOTE: Each correct selection is worth one point.

Hot Area:

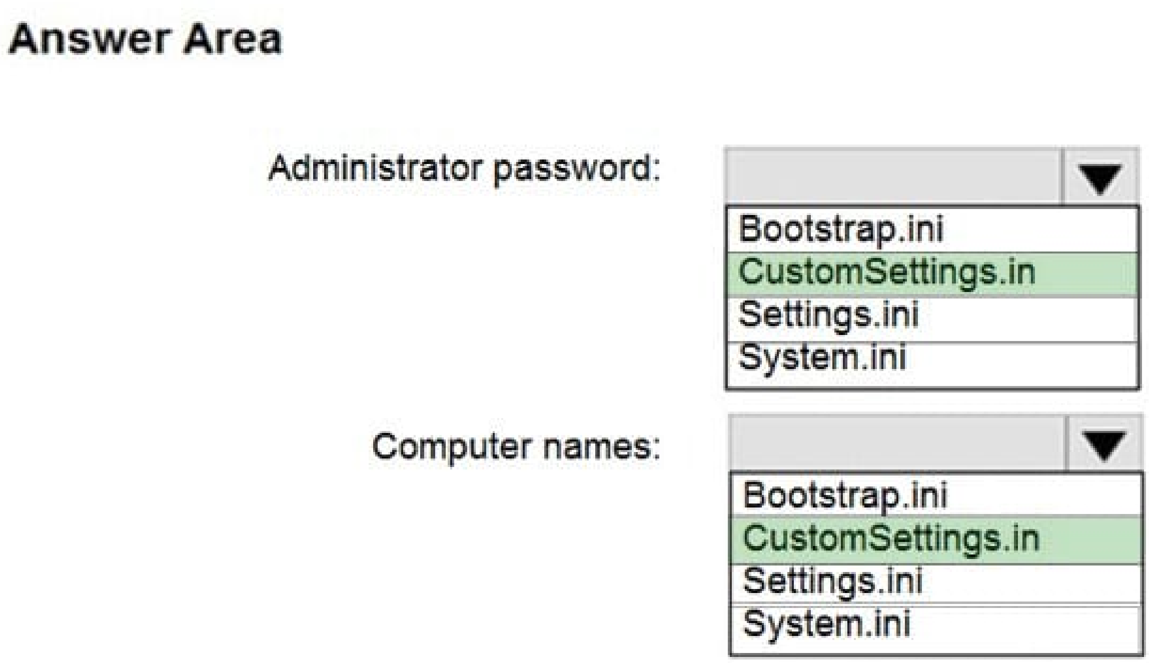


Answer Area

Administrator password: ▼
- Bootstrap.ini
- CustomSettings.in
- Settings.ini
- System.ini

Computer names: ▼
- Bootstrap.ini
- CustomSettings.in
- Settings.ini
- System.ini

Correct Answer:



Answer Area

Administrator password: ▼
- Bootstrap.ini
- [✓ CustomSettings.in]
- Settings.ini
- System.ini

Computer names: ▼
- Bootstrap.ini
- [✓ CustomSettings.in]
- Settings.ini
- System.ini

Box 1: CustomSettings.ini You can skip the entire Windows Deployment Wizard by specifying the SkipWizard property in CustomSettings.ini. To skip individual wizard pages, use the following properties:

SkipAdminPassword Etc.

Note: The CustomSettings.ini file includes for example:

AdminPassword=pass@word1

DomainAdmin=CONTOSO\MDT_JD

DomainAdminPassword=pass@word1 Some properties to use in the MDT Production rules file are as follows:

DomainAdmin. The account to use when joining the machine to the domain.

DomainAdminDomain. The domain for the join domain account.

DomainAdminPassword. The password for the join domain account.

Box 2: CustomSettings.ini Example of content in the CustomSettings.ini file:

SkipComputerName=YES OSDComputerName=%ComputerName%

Reference:

https://docs.microsoft.com/en-us/windows/deployment/deploy-windows-mdt/deploy-a-windows-10-image-using-mdt
https://docs.microsoft.com/en-us/mem/configmgr/mdt/samples-guide

---

QUESTION 8

You need to meet the requirements for the MKG department users.

What should you do?

A. Assign the MKG department users the Purchaser role in Microsoft Store for Business

B. Download the APPX file for App1 from Microsoft Store for Business

C. Add App1 to the private store

D. Assign the MKG department users the Basic Purchaser role in Microsoft Store for Business

E. Acquire App1 from Microsoft Store for Business

Correct Answer: E

Enable the users in the MKG department to use App1.

The private store is a feature in Microsoft Store for Business and Education that organizations receive during the signup process. When admins add apps to the private store, all employees in the organization can view and download the apps.

Your private store is available as a tab in Microsoft Store app, and is usually named for your company or organization. Only apps with online licenses can be added to the private store.

Reference:

https://docs.microsoft.com/en-us/microsoft-store/distribute-apps-from-your-private-store

---

QUESTION 9

You have a Microsoft 365 E5 subscription that contains 100 Windows 10 devices enrolled in Microsoft Intune.

You plan to use Endpoint analytics.

You need to create baseline metrics.

What should you do first?

A. Create an Azure Monitor workbook.

B. Onboard 10 devices to Endpoint analytics.

C. Create a Log Analytics workspace.

D. Modify the Baseline regression threshold.

Correct Answer: B

Onboarding from the Endpoint analytics portal is required for Intune managed devices. Reference: https://docs.microsoft.com/en-us/mem/analytics/enroll-intune

QUESTION 10

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 a computer named Computer1 that runs Windows 10.

You save a provisioning package named Package1 to a folder named C:\Folder1.

You need to apply Package1 to Computer1.

Solution: From the Settings app, you select Access work or school, and then you select Add or remove a provisioning package. Does this meet the goal?

A. Yes

B. No

Correct Answer: B

B is the correct Answer. To apply a provisioning package, this can be done from a USB frive. not from settings.

Answer is no - since .ppkg is stored at C.

For a provisioning package stored on a network folder or on a SharePoint site, navigate to the provisioning package and double-click it to begin installation.

https://docs.microsoft.com/en-us/windows/configuration/provisioning-packages/provisioning-apply-package

QUESTION 11

HOTSPOT

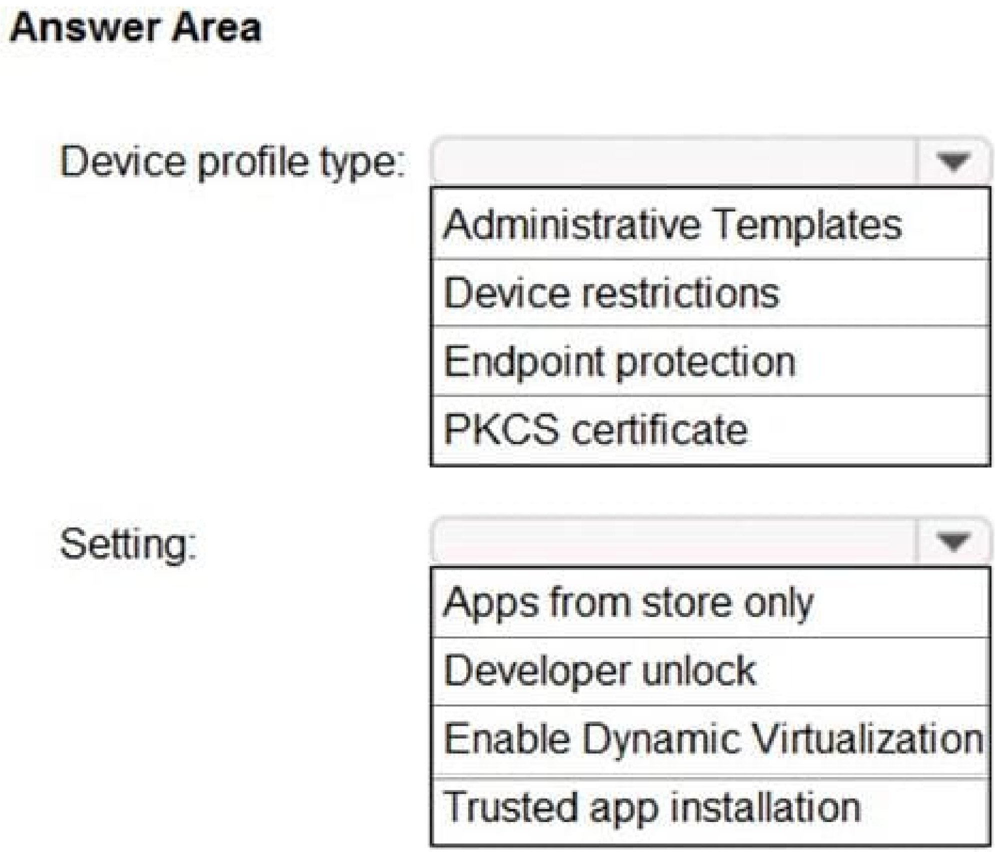
You have 100 Windows 10 devices that are managed by using Microsoft Endpoint Manager.

You plan to sideload an app to the devices.

You need to configure Microsoft Endpoint Manager to enable sideloading.

Which device profile type and setting should you configure? To answer, select the appropriate options in the answer area. NOTE: Each correct selection is worth one point.

Hot Area:



Answer Area

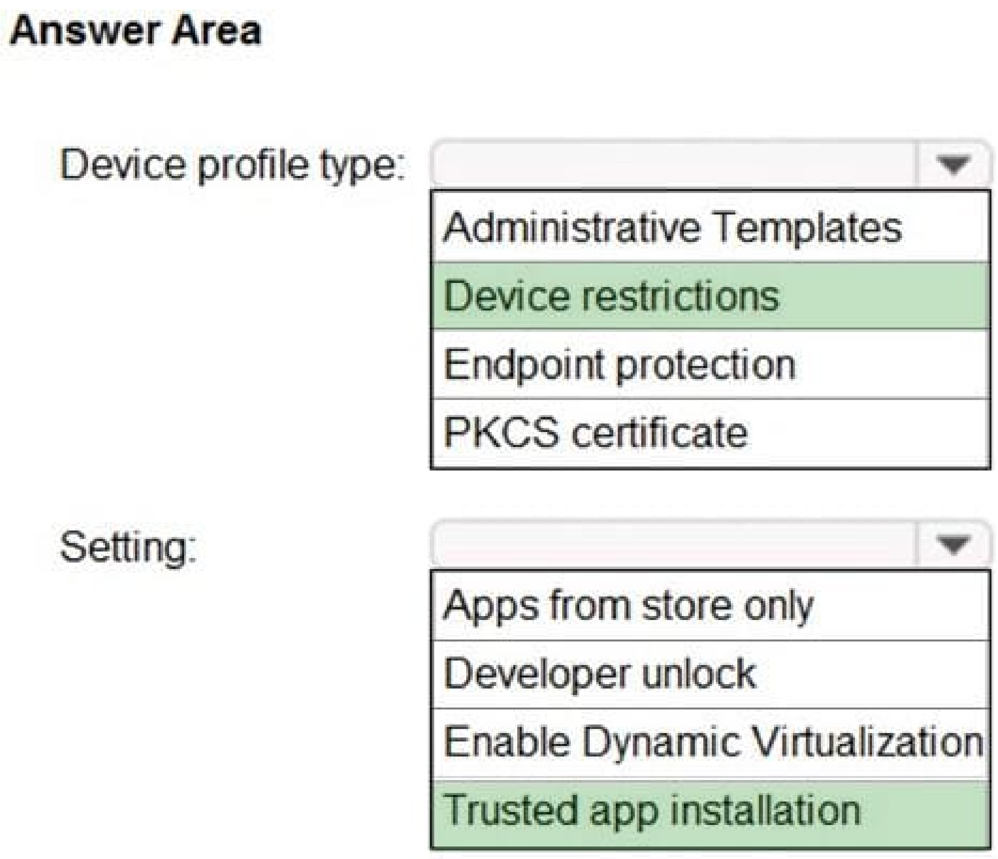
Device profile type:

- Administrative Templates
- Device restrictions
- Endpoint protection
- PKCS certificate

Setting:

- Apps from store only
- Developer unlock
- Enable Dynamic Virtualization
- Trusted app installation

Correct Answer:



Answer Area

Device profile type:

- Administrative Templates
- [✓ Device restrictions]
- Endpoint protection
- PKCS certificate

Setting:

- Apps from store only
- Developer unlock
- Enable Dynamic Virtualization
- [✓ Trusted app installation]

Box 1: Device restrictions In a Windows 10/11 device restrictions profile, most configurable settings are deployed at the device level using device groups. Policies deployed to user groups apply to targeted users. The policies also apply to users who have an Intune license, and users that sign in to that device.

Box 2: Trusted app installation Trusted app installation: Choose if non-Microsoft Store apps can be installed, also known as sideloading. Sideloading is installing, and then running or testing an app that isn\\'t certified by the Microsoft Store. For example, an app that is internal to your company only.

Reference: https://docs.microsoft.com/en-us/mem/intune/configuration/device-restrictions-windows-10

QUESTION 12

Your company has a Microsoft Azure Active Directory (Azure AD) tenant. All users in the company are licensed for Microsoft Intune.

You need to ensure that the users enroll their iOS device in Intune.

What should you configure first?

A. A Device Enrollment Program (DEP) token.

B. An Intune device configuration profile.

C. A Device enrollment manager (DEM) account.

D. An Apple MDM Push certificate.

Correct Answer: D

Prerequisites for iOS enrollment Before you can enable iOS devices, complete the following steps: Make sure your device is eligible for Apple device enrollment. Set up Intune - These steps set up your Intune infrastructure. In particular, device enrollment requires that you set your MDM authority. Get an Apple MDM Push certificate - Apple requires a certificate to enable management of iOS and macOS devices.

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

QUESTION 13

You need to enable Microsoft Defender Credential Guard on computers that run Windows 10.

What should you install on the computers?

A. Hyper-V

B. Microsoft Defender Application Guard

C. a guarded host

D. containers

Correct Answer: A

Microsoft Defender Credential Guard software requirements.

The Virtualization-based security requires:

64-bit CPU

CPU virtualization extensions plus extended page tables

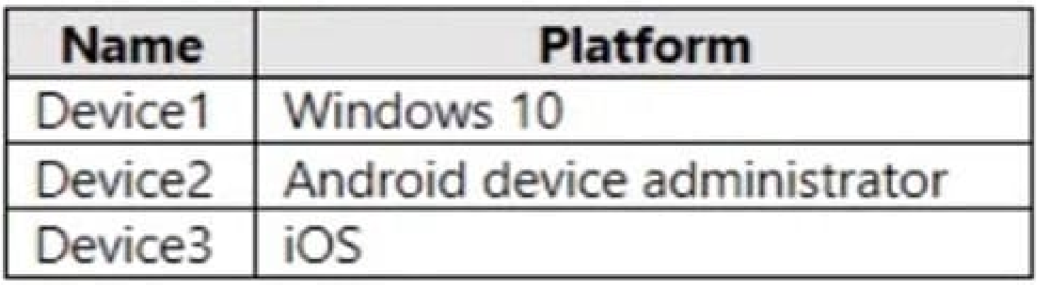
Windows hypervisor (does not require Hyper-V Windows Feature to be installed)

Reference:

https://docs.microsoft.com/en-us/windows/security/identity-protection/credential-guard/credential-guard-requirements

QUESTION 14

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

A. Device2 and Device3 only

B. Device2 only

C. Device1 and Device2 only

D. Device1 only

E. Device1, Device2, and Device3

Correct Answer: E

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

Android

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

Android device administrator Android Enterprise iOS macOS Windows Holographic for Business

Windows 8.1 and later

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 15

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 Update for Business.

The research department has several computers that have specialized hardware and software installed.

You need to prevent the video drivers from being updated automatically by using Windows Update.

Solution: From the Device Installation settings in a Group Policy object (GPO), you enable Specify search order for device driver source locations, and then you select Do not search Windows Update.

Does this meet the goal?

A. Yes

B. No

Correct Answer: A

Device driver searches using Windows Update must be prevented.

Configure the policy value for Computer Configuration -> Administrative Templates -> System -> Device Installation -> "Specify search order for device driver source locations" to "Enabled: Do not search Windows Update".

Reference:

https://www.stigviewer.com/stig/microsoft_windows_server_2012_member_server/2013-07-25/finding/WN12-CC-000024