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

HOTSPOT

You have a Microsoft Deployment Toolkit (MDT) deployment share named Share1.

You add Windows 10 images to Share1 as shown in the following table.

Name	In WIM file	Description
Image1	Install1.wim	Default Windows 10 Pro image from the Windows 10 installation media
Image2	Install1.wim	Default Windows 10 Enterprise image from the Windows 10 installation media
Image3	Install2.wim	Default Windows 10 Pro for Workstations image from the Windows 10 installation media
Image4	Custom1.wim	Custom Windows 10 Enterprise image without any additional applications
Image5	Custom2.wim	Custom Windows 10 Enterprise image that includes custom applications

Which images can be used in the Standard Client Task Sequence, and which images can be used in the Standard Client Upgrade Task Sequence? NOTE: Each correct selection is worth one point.

Hot Area:

Answer Area

Standard Client Task Sequence:

Image3 only
Image3, Image4, and Image5 only
Image1, Image2, and Image3 only
Image1, Image2, Image3, and Image4 only
Image1, Image2, Image3, Image4, and Image5

Standard Client Upgrade Task Sequence:

Image3 only
Image3, Image4, and Image5 only
Image1, Image2, and Image3 only
Image1, Image2, Image3, and Image4 only
Image1, Image2, Image3, Image4, and Image5

Correct Answer:

Answer Area

Standard Client Task Sequence:

Image3 only
Image3, Image4, and Image5 only
Image1, Image2, and Image3 only
Image1, Image2, Image3, and Image4 only
Image1, Image2, Image3, Image4, and Image5

Standard Client Upgrade Task Sequence:

Image3 only
Image3, Image4, and Image5 only
Image1, Image2, and Image3 only
Image1, Image2, Image3, and Image4 only
Image1, Image2, Image3, Image4, and Image5

Box 1: Image1, Image2, Image3, Image4, and Image5.

All images.

Standard Client Task Sequence Standard Client task sequence. The most frequently used task sequence. Used for creating reference images and for deploying clients in production.

Box 2: Image1, Image2, Image3, and Image4 only.

Exclude image5 with applications.

Standard Client Upgrade Task Sequence

Standard Client Upgrade task sequence. A simple task sequence template used to perform an in-place upgrade from Windows 7, Windows 8, or Windows 8.1 directly to Windows 10, automatically preserving existing data, settings,

applications, and drivers.

Reference:

https://docs.microsoft.com/en-us/windows/deployment/deploy-windows-mdt/get-started-with-the-microsoft-deployment-toolkit

QUESTION 2

HOTSPOT

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

Name	Member of
User1	Group1
User2	Group2

Contoso.com contains the devices shown in the following table.

Name	Platform	Member of	Microsoft Intune managed
Device1	Windows 10	GroupA	Yes
Device2	Windows 10	GroupB	No

In Intune, you create the app protection policies shown in the following table.

Name	Platform	Enrollment state	Assigned to
Policy1	Windows 10	With enrollment	Group1
Policy2	Windows 10	Without enrollment	Group2
Policy3	Windows 10	With enrollment	GroupA
Policy4	Windows 10	Without enrollment	GroupB

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:

Statements	Yes	No
When User1 signs in to Device1, Policy1 applies.	○	○
When User2 signs in to Device1, Policy2 applies.	○	○
When User2 signs in to Device2, Policy2 applies.	○	○

Correct Answer:

Statements	Yes	No
When User1 signs in to Device1, Policy1 applies.	○	○
When User2 signs in to Device1, Policy2 applies.	○	○
When User2 signs in to Device2, Policy2 applies.	○	○

Box 1: Yes - User1 is a member of Group1, Device1 is Intune managed, Policy1 is enrolled and assigned to Group1. Box 2: No - User2 is a member of Group2, Device1 is Intune managed, Policy2 is not enrolled and is assigned to Group2. Box 3: Yes - User2 is a member of Group2,Device2 is not Intune managed, Policy2 is assigned to Group2

Reference: https://docs.microsoft.com/en-us/mem/intune/apps/app-protection-policy

QUESTION 3

Your company has computers that run Windows 10. The company uses Microsoft Intune to manage the computers.

You have an app protection policy for Microsoft Edge. You assign the policy to a group.

On a computer named Computer1, you open Microsoft Edge.

You need to verify whether Microsoft Edge on Computer1 is protected by the app protection policy.

Which column should you add in Task Manager?

A. Operating system context

B. UAC virtualization

C. Enterprise Context

D. Data Execution Prevention

Correct Answer: C

Use Task Manager to check the context of your apps while running in Windows Information Protection (WIP) to make sure that your organization\\'s policies are applied and running correctly.

Viewing the Enterprise Context column in Task Manager

You need to add the Enterprise Context column to the Details tab of the Task Manager.

Make sure that you have an active WIP policy deployed and turned on in your organization.

Open the Task Manager (taskmgr.exe), click the Details tab, right-click in the column heading area, and click Select Columns.

The Select columns box appears.

Scroll down and check the Enterprise Context option, and then click OK to close the box.

The Enterprise Context column should now be available in Task Manager

Use Task Manager to check the context of your apps while running in Windows Information Protection (WIP) to make sure that your organization\\'s policies are applied and running correctly.

Viewing the Enterprise Context column in Task Manager.

You need to add the Enterprise Context column to the Details tab of the Task Manager.

Reference:

https://docs.microsoft.com/en-us/windows/security/information-protection/windows-information-protection/wip-app-enterprise-context https://www.itpromentor.com/win10-mam-wip/

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.

Reference: https://docs.microsoft.com/en-us/windows-insider/business/manage-builds

Your company has a hybrid configuration of Microsoft Azure Active Directory (Azure AD). Your company also has a Microsoft 365 subscription.

After creating a conditional access policy for Microsoft Exchange Online, you are tasked with configuring the policy to block access to Exchange Online. However, the policy should allow access for hybrid Azure AD-joined devices

Solution: You should configure the Device platforms settings.

Does the solution meet the goal?

A. Yes

B. No

Correct Answer: B

Within a Conditional Access policy, an administrator can make use of signals from conditions like risk, device platform, or location to enhance their policy decisions.

Client apps By default, all newly created Conditional Access policies will apply to all client app types even if the client apps condition isn\\'t configured.

These conditions are commonly used when requiring a managed device, blocking legacy authentication, and blocking web applications but allowing mobile or desktop apps.

Reference:

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

QUESTION 5

HOTSPOT

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 create a file named D:\Folder1\file1.txt on Device4 by using Notepad.	○	○
User2 can remove D:\Folder1 from the list of protected folders on Device2.	○	○
User3 can create a file named C:\Users\User3\Desktop\file1.txt on Device2 by running a custom Windows PowerShell script.	○	○

Correct Answer:

Answer Area

Statements	Yes	No
User1 can create a file named D:\Folder1\file1.txt on Device4 by using Notepad.	○	○
User2 can remove D:\Folder1 from the list of protected folders on Device2.	○	○
User3 can create a file named C:\Users\User3\Desktop\file1.txt on Device2 by running a custom Windows PowerShell script.	○	○

QUESTION 6

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 need to ensure that feature and quality updates install automatically during a maintenance window.

Solution: In Group policy, from the Windows Update settings, you enable Configure Automatic Updates, select 3 ?Auto download and notify for Install, and then enter a time.

Does this meet the goal?

A. Yes

B. No

Correct Answer: B

Instead: In Group policy, from the Windows Update settings, you enable Configure Automatic Updates, select 4-Auto download and schedule the install, and then enter a time.

Reference: https://docs.microsoft.com/en-us/sccm/sum/deploy-use/automatically-deploy-software-updates

QUESTION 7

Your network contains an Active Directory domain named contoso.com. The domain contains 500 computers that run Windows 7. Some of the computers are used by multiple users.

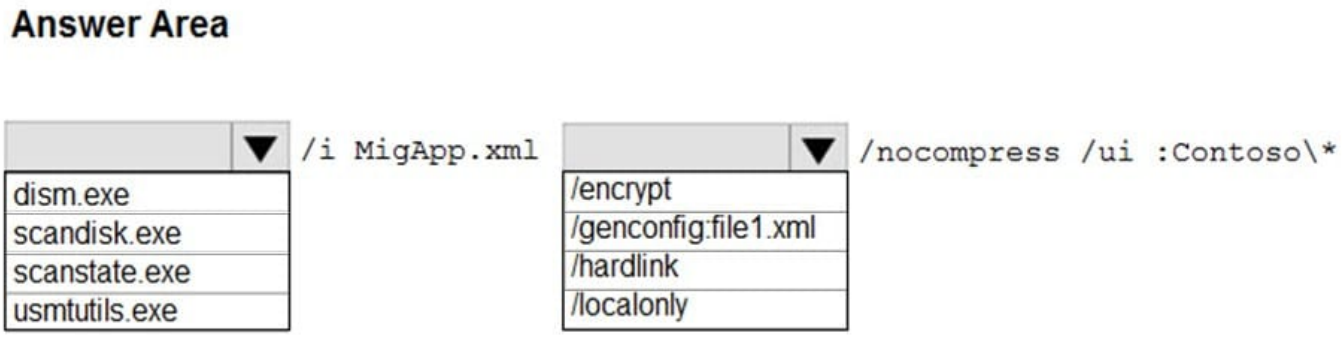
You plan to refresh the operating system of the computers to Windows 10.

You need to retain the personalization settings to applications before you refresh the computers. The solution must minimize network bandwidth and network storage space.

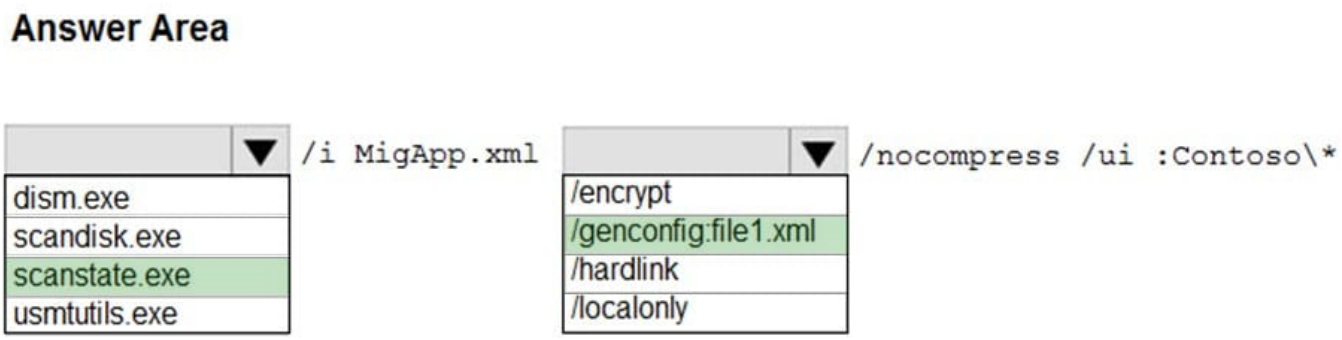
Which command should you run on the computer? To answer, select the appropriate options in the answer area.

NOTE: Each correct selection is worth one point.

Hot Area:



Correct Answer:



Box 1: scanstate.exe The ScanState command is used with the User State Migration Tool (USMT) 10.0 to scan the source computer, collect the files and settings, and create a store. For example, to create a Config.xml file in the current directory, use: scanstate /i:migapp.xml /i:migdocs.xml /genconfig:config.xml /v:13

Box 2: genconfig:file.xml

Reference: https://docs.microsoft.com/en-us/windows/deployment/usmt/usmt-scanstate-syntax#how-to-use-ui-and-ue

QUESTION 8

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 Windows 10 computers that are enrolled in Microsoft Intune. You make use of Intune to manage the servicing channel settings of all company computers.

You receive an enquiry regarding the servicing status of a specific computer.

You need to review the necessary policy report.

Solution: You navigate to device status via Device configuration.

Does the solution meet the goal?

A. Yes

B. No

Correct Answer: B

Note 1: Intune offers integrated report views for the Windows update ring policies you deploy. These views display details about the update ring deployment and status:

1.

Sign in to Microsoft Endpoint Manager admin center.

2.

Select Devices > Monitor. Then under Software updates select Per update ring deployment state and choose the deployment ring to review.

Note 2: Use the Windows 10 and later feature updates (Organizational) report

To open the Windows 10 and later feature updates report and view device details for a specific feature updates profile:

In the admin center, go to Reports > Windows updates > select the Reports tab > select Windows Feature Update Report.

Note 3: To help you monitor and troubleshoot update deployments, Intune supports the following reporting options:

Reports in Intune:

Windows 10 and later update rings Use a built-in report that\\'s ready by default when you deploy update rings to your devices.

Windows 10 and later feature updates In public preview Use two built-in reports that work together to gain a deep picture of update status and issues.

Reference: https://docs.microsoft.com/en-us/intune/windows-update-compliance-reports

QUESTION 9

You have a Microsoft 365 E5 subscription that contains 10 Android Enterprise devices. Each device has a corporate-owned work profile and is enrolled in Microsoft Intune.

You need to configure the devices to run a single app in kiosk mode.

Which Configuration settings should you modify in the device restrictions profile?

A. General

B. Users and Accounts

C. System security

D. Device experience

Correct Answer: D

Device experience Use these settings to configure a kiosk-style experience on your dedicated devices, or to customize the home screen experiences on your fully managed devices. You can configure devices to run one app, or run many apps. When a device is set with kiosk mode, only the apps you add are available. Device experience, Enrollment profile type: Select an enrollment profile type to start configuring Microsoft Launcher or the Microsoft Managed Home Screen on your devices. Your options:

*

Dedicated device, Kiosk mode, Single App

*

etc.

Reference: https://docs.microsoft.com/en-us/mem/intune/configuration/device-restrictions-android-for-work

QUESTION 10

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 Windows Update settings in a Group Policy object (GPO), you enable Do not include drivers with Windows Updates.

Does this meet the goal?

A. Yes

B. No

Correct Answer: A

Do not include drivers with Windows Updates.

Allows admins to exclude Windows Update drivers during updates.

To configure this setting in Group Policy, use Computer Configuration\Administrative Templates\Windows Components\Windows update\Do not include drivers with Windows Updates. Enable this policy to not include drivers with Windows

quality updates. If you disable or do not configure this policy, Windows Update will include updates that have a Driver classification.

Reference:

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

QUESTION 11

You are currently making use of the Antimalware Assessment solution in Microsoft Azure Log Analytics.

You have accessed the Protection Status dashboard and find that there is a device that has no real time protection.

Which of the following could be a reason for this occurring?

A. Windows Defender has been disabled.

B. You need to install the Azure Diagnostic extension.

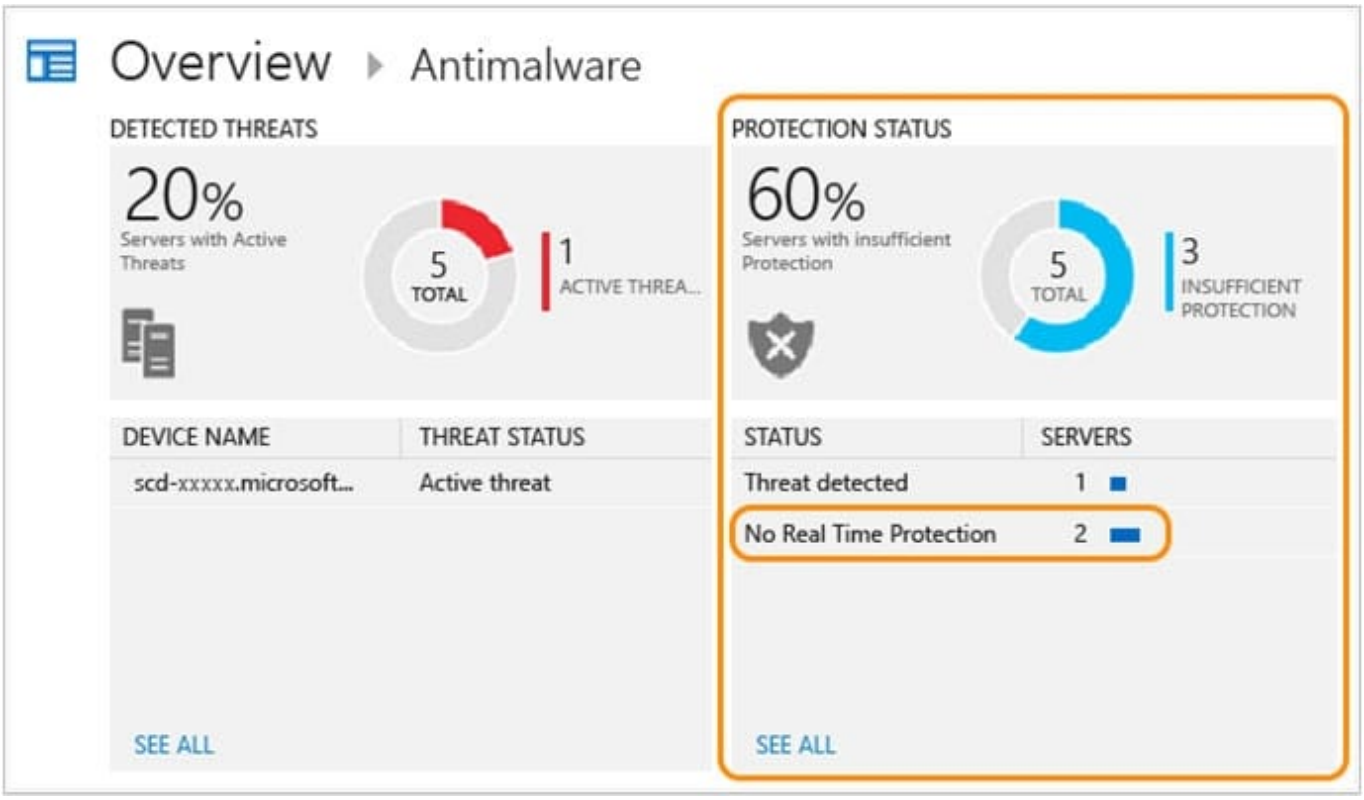
C. Windows Defender Credential Guard is incorrectly configured.

D. Windows Defender System Guard is incorrectly configured.

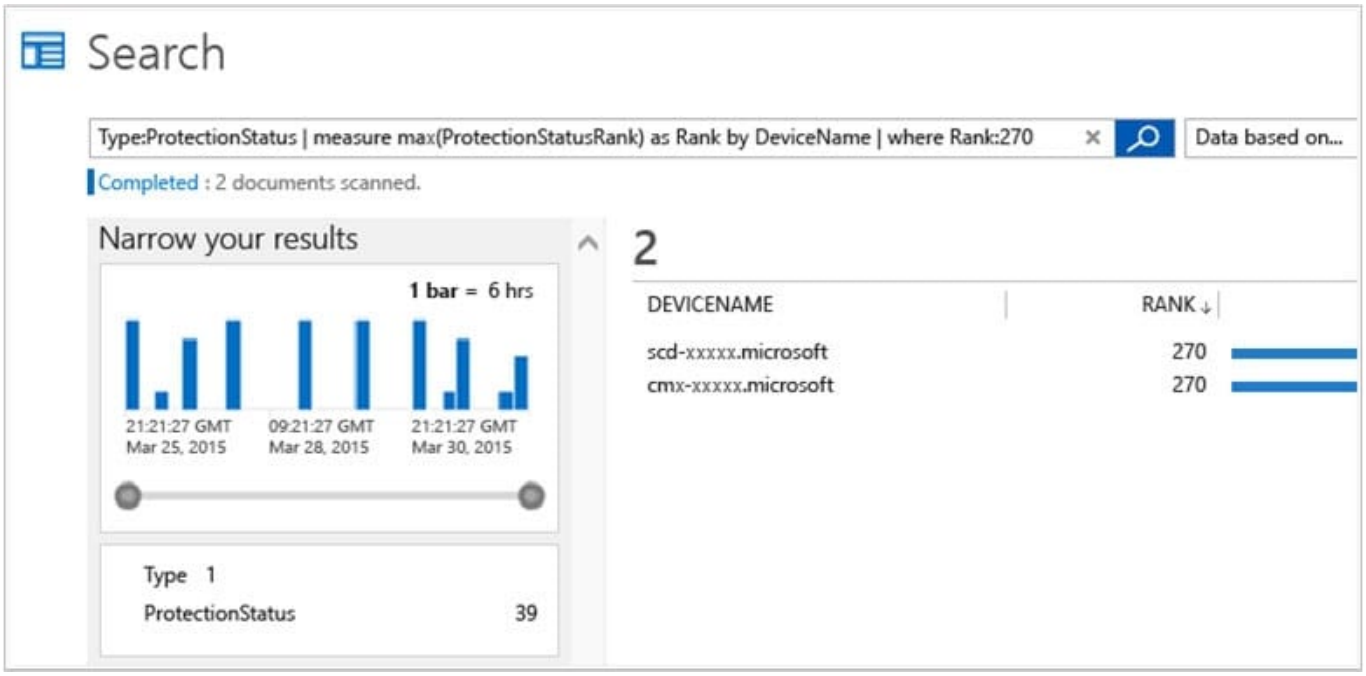
Correct Answer: A

Microsoft Defender Antivirus is usually the primary antivirus/antimalware product on your device. To review protection status

1. On the Antimalware dashboard, you will review the Protection Status blade and click no real time protection.



2. Search shows a list of servers without protection.



3. At this point you now know what servers do not have realtime protection.

Computers that do not have System Center Endpoint Protection installed (or if SCEP is not detected) will be reported as no real time protection.

Reference: https://docs.microsoft.com/ga-ie/azure/security-center/security-center-install-endpoint-protection

---

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.

Your company has several Windows 10 devices that are enrolled in Microsoft Intune.

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

You need to enroll Computer1 in Intune.

Solution: From the Settings app on Computer1, you use the Connect to work or school account settings. Does this meet the goal?

A. Yes

B. No

Correct Answer: B

Use MDM enrolment.

MDM only enrollment lets users enroll an existing Workgroup, Active Directory, or Azure Active directory joined PC into Intune. Users enroll from Settings on the existing Windows PC.

References:

https://docs.microsoft.com/en-us/mem/intune/enrollment/windows-enrollment-methods

QUESTION 13

DRAG DROP

You have a Microsoft Deployment Toolkit (MDT) deployment share named DS1.

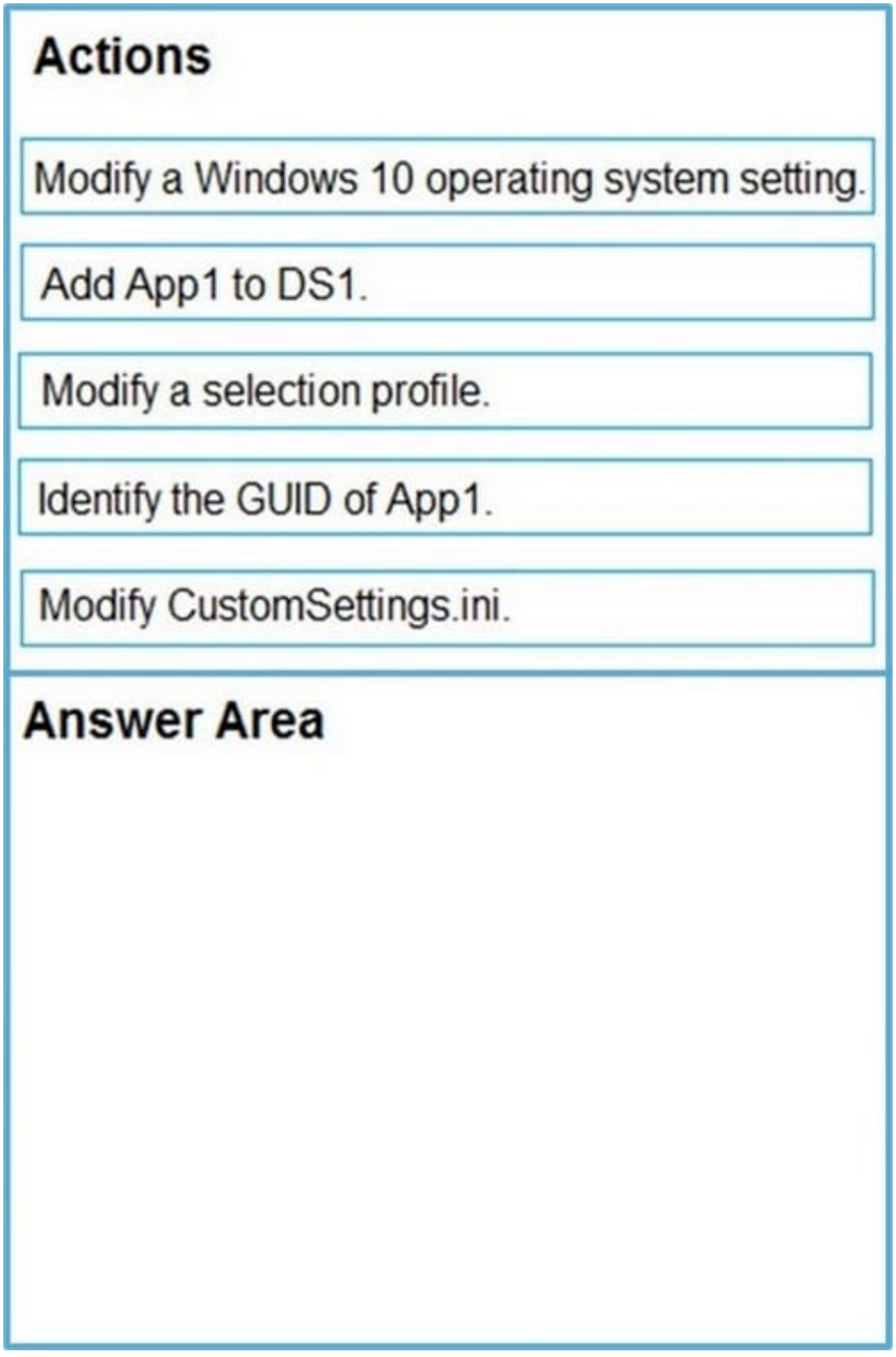
You import a Windows 10 image to DS1.

You have an executable installer for an application named App1.

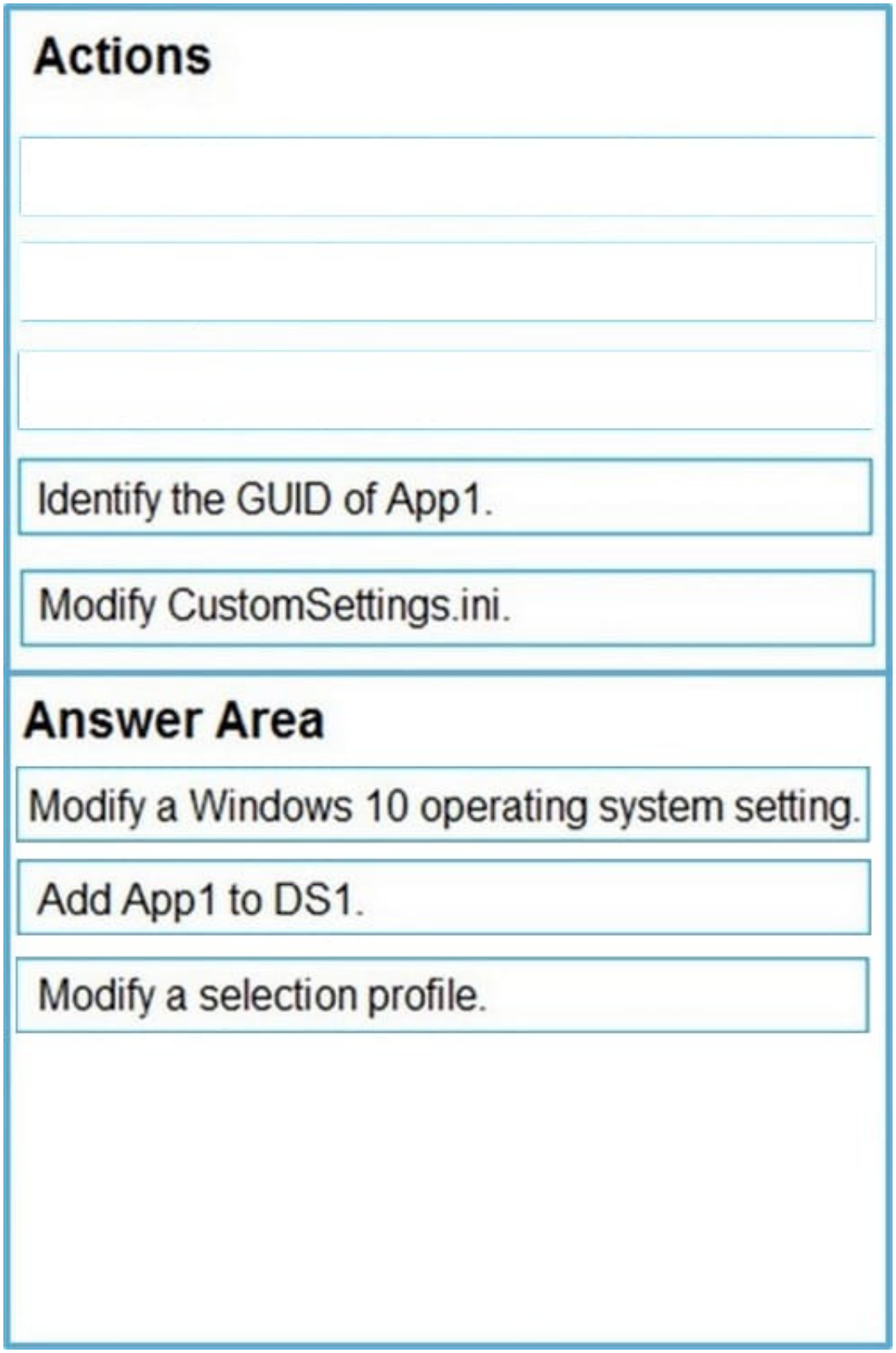
You need to ensure that App1 will be installed for all the task sequences that deploy the image.

Which three actions should you perform 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: Add App1 to DS1 Add an application in the MDT console.

Step 2: Identify the GUID of App1.

Step 3: Modify the CustomSettings.ini

It is possible in the CustomSettings.ini file, to check the default program to add the following line:

ApplicationsXXX ={GUID-APPLICATION}

or to force the installation of the application box checked and grayed out:

MandatoryApplicationsXXX ={GUID-APPLICATION}

Reference:

https://rdr-it.com/en/mdt-installation-of-applications-when-deploying-windows/

QUESTION 14

HOTSPOT

Name	Platform
Device1	Windows 10
Device2	macOS

You have a Microsoft 365 tenant that uses Microsoft Intune and contains the devices shown in the following table.

In Endpoint security, you need to configure a disk encryption policy for each device.

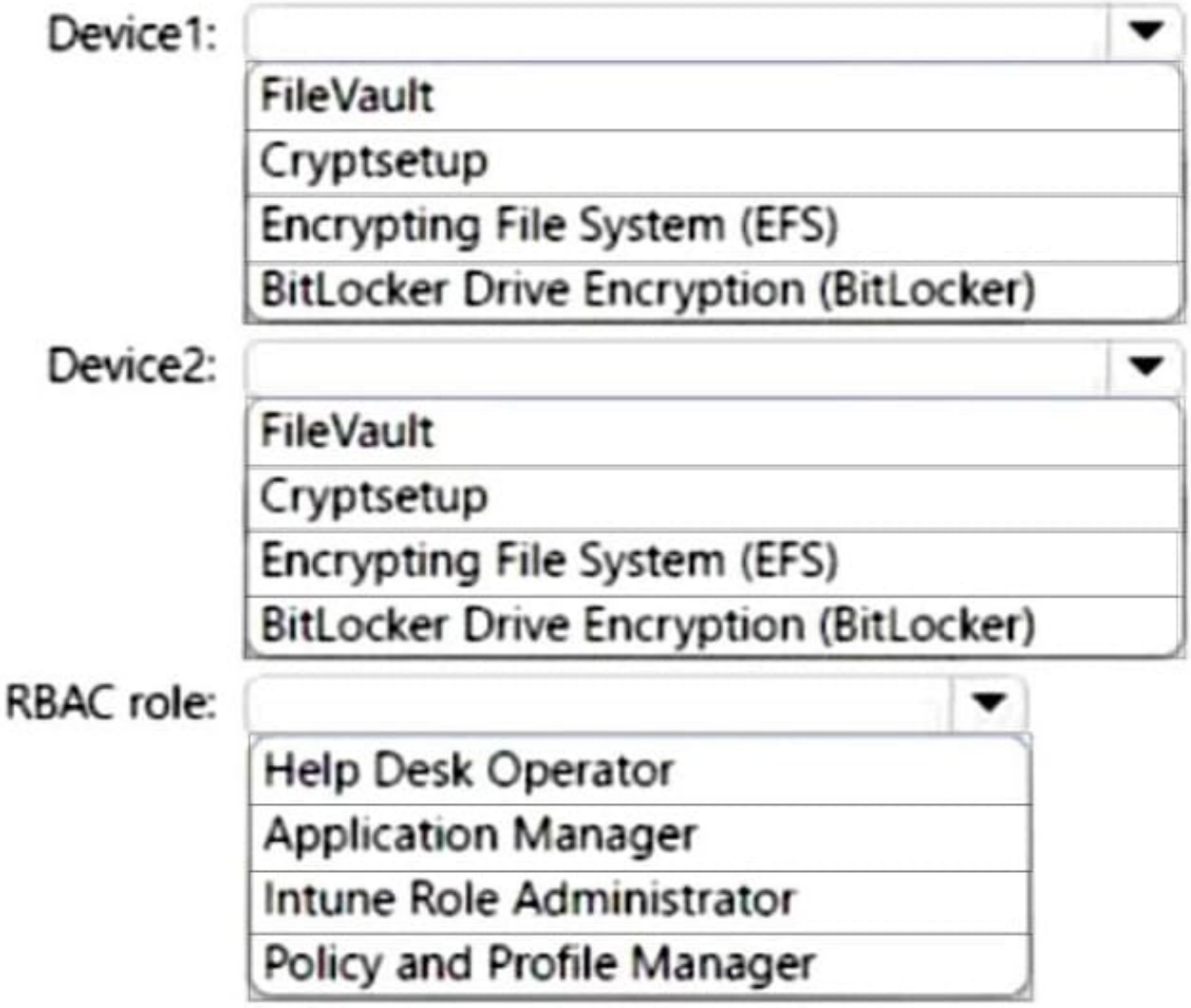
Which encryption type should you use for each device, and which role-based access control (RBAC) role in Intune should you use to manage the encryption keys?

To answer, select the appropriate options in the answer area.

NOTE: Each correct selection is worth one point.

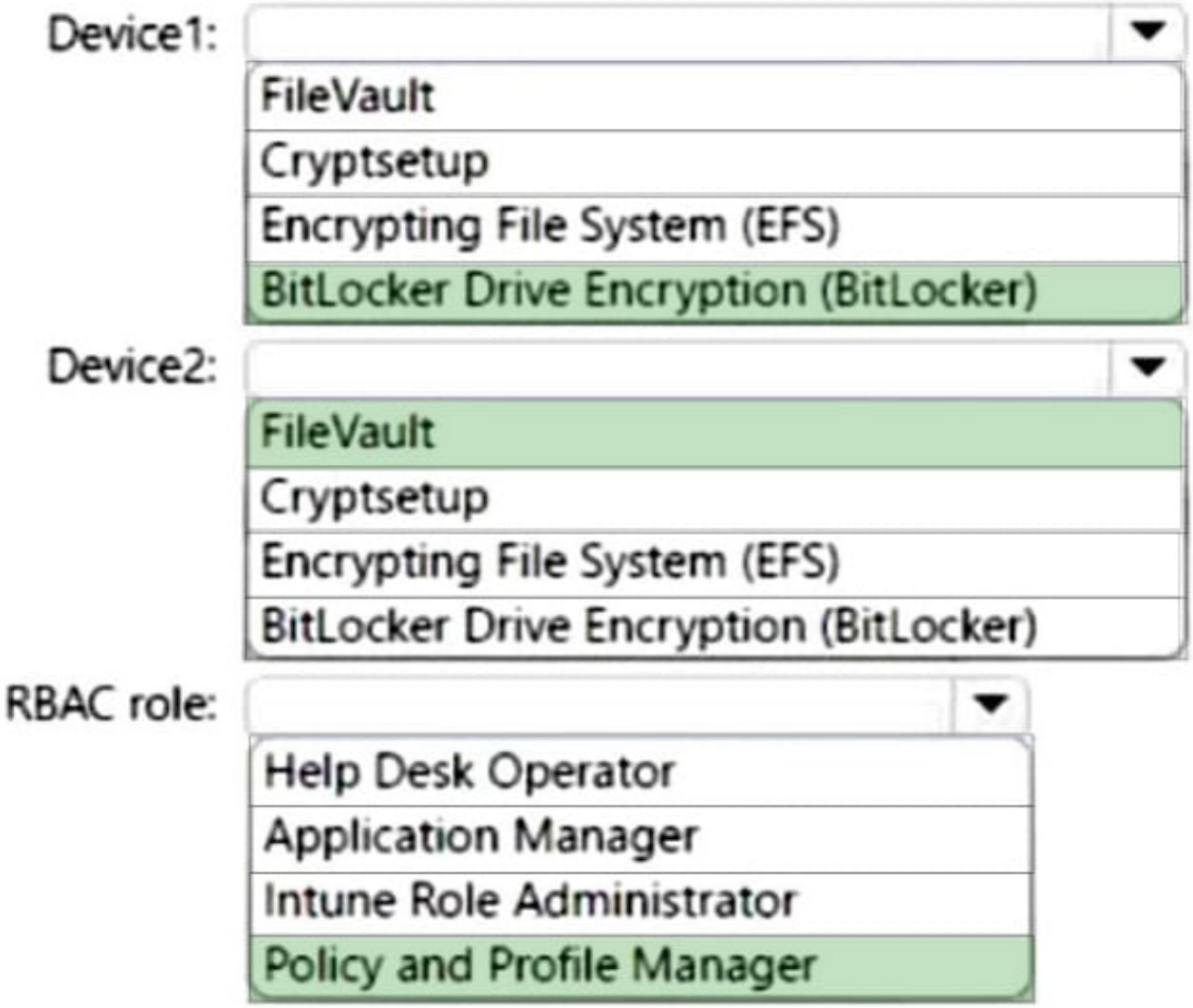
Hot Area:

Answer Area



Correct Answer:

Answer Area



QUESTION 15

You need to capture the required information for the sales department computers to meet the technical requirements.

Which Windows PowerShell command should you run first?

A. Install-Module WindowsAutoPilotIntune

B. Install-Script Get-WindowsAutoPilotInfo

C. Import-AutoPilotCSV

D. Get-WindowsAutoPilotInfo

Correct Answer: A

Re-provision the sales department computers by using Windows AutoPilot. Windows Autopilot Deployment for existing devices, install required modules:

1.

Install-PackageProvider -Name NuGet -MinimumVersion 2.8.5.201 -Force

2.

Install-Module AzureAD -Force

3.

Install-Module WindowsAutopilotIntune -Force

4.

Install-Module Microsoft.Graph.Intune -Force Reference: https://docs.microsoft.com/en-us/windows/deployment/windows-autopilot/existing-devices