DUMPSQUEEN

Managing Modern Desktops

Microsoft MD-101

Version Demo

Total Demo Questions: 20

Total Premium Questions: 489

Buy Premium PDF

https://dumpsqueen.com

support@dumpsqueen.com

Topic Break Down

Topic	No. of Questions
Topic 1, New Update	170
Topic 2, Case Study 1	5
Topic 3, Case Study 2	4
Topic 4, Case Study 3	2
Topic 5, Case Study 4	3
Topic 6, Case Study 5	6
Topic 7, Case Study 6	5
Topic 8, Mixed Questions	294
Total	489

QUESTION NO: 1

You have a Microsoft 365 tenant that uses Microsoft Intune.

You use the Company Portal app to access and install published apps to enrolled devices.

From the Microsoft Endpoint Manager admin center, you add a Microsoft Store app.

Which two App information types are visible in the Company Portal?

Note: Each correct selection is worth one point.

A. information URL

B. Developer

C. Privacy URL

D. Owner

ANSWER: B C

QUESTION NO: 2

You have a Microsoft Azure Active Directory (Azure AD) tenant. All corporate devices are enrolled in Microsoft Intune.

You have a web-based application named App1 that uses Azure AD to authenticate.

You need to prompt all users of App1 to agree to the protection of corporate data when they access App1 from both corporate and noncorporate devices.

What should you configure?

A. Notifications in Device compliance

B. Terms and Conditions in Device enrollment

C. Terms of use in Conditional access

D. an Endpoint protection profile in Device configuration

ANSWER: C

Explanation:

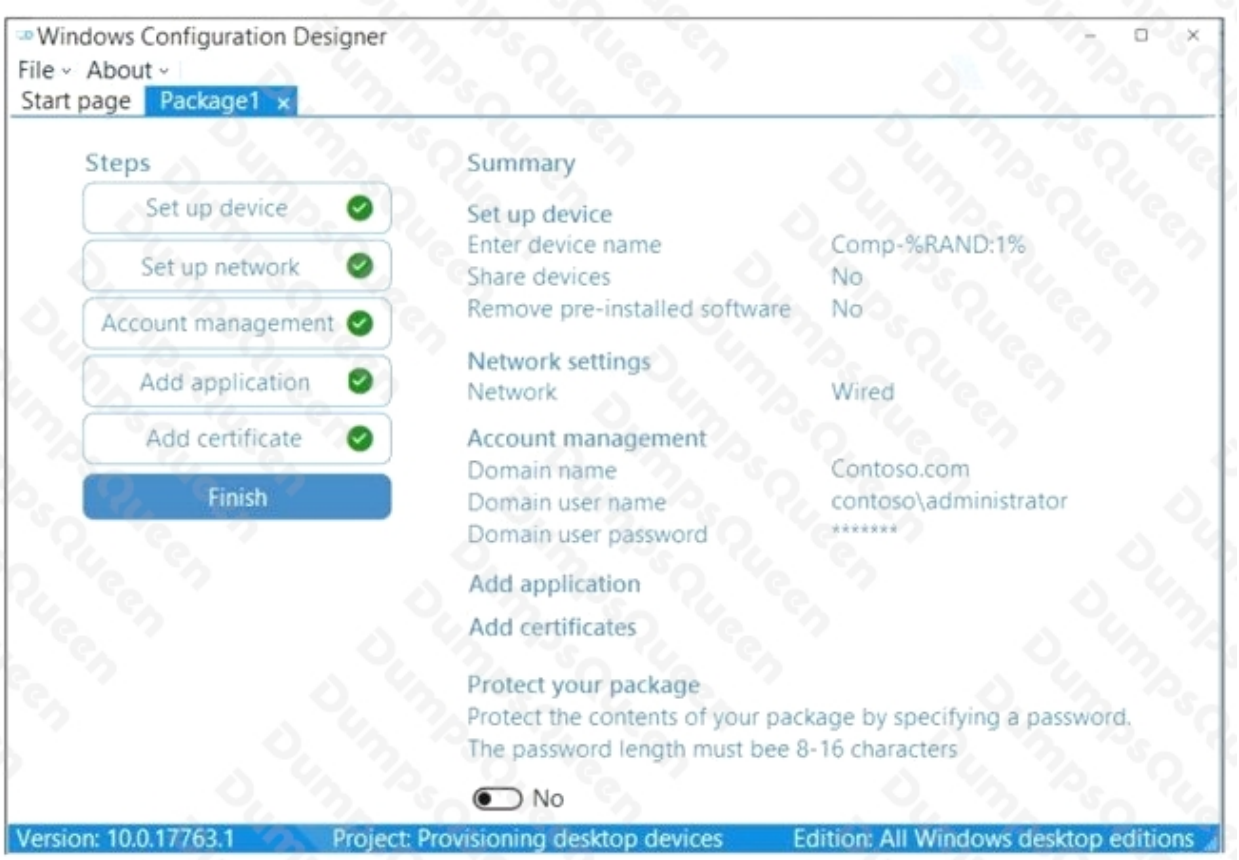
Reference:

https://docs.microsoft.com/en-us/azure/active-directory/conditional-access/terms-of-use

QUESTION NO: 3

Your network contains an Active Directory domain named contoso.com.

You create a provisioning package named Package1 as shown in the following exhibit.



What is the maximum number of devices on which you can run Package1 successfully?

A. 1

B. 10

C. 25

D. unlimited

ANSWER: B

Explanation:

The device name uses a single random number (applied by %RAND:1%). This allows for 10 unique values (0 – 9).

QUESTION NO: 4 - (HOTSPOT)

HOTSPOT

You have a Microsoft 365 subscription.

You plan to enroll devices in Microsoft Endpoint Manager that have the platforms and versions shown in the following table.

Platform	Version
Android	8, 9
iOS	11, 12

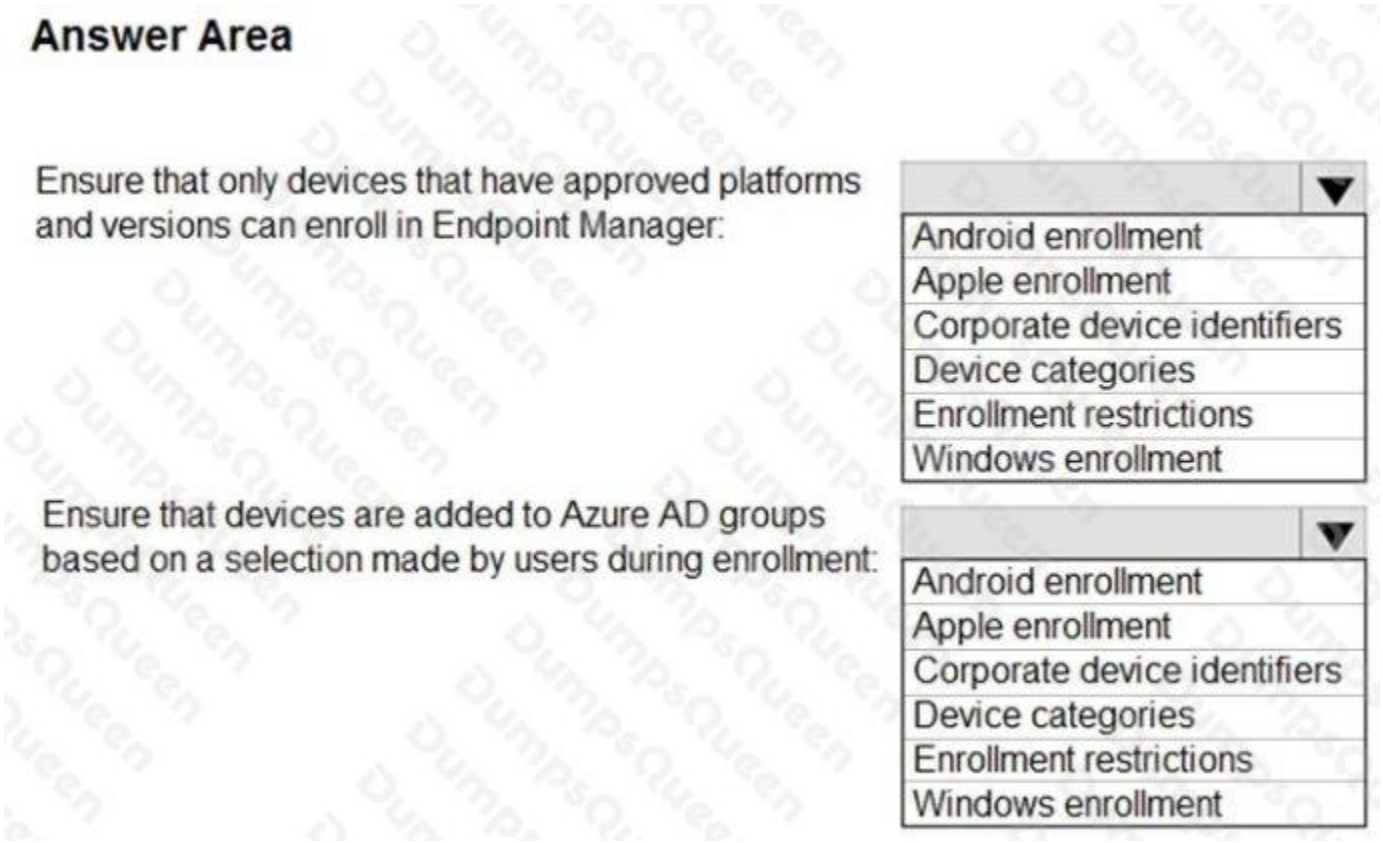
You need to configure device enrollment to meet the following requirements:

- Ensure that only devices that have approved platforms and versions can enroll in Endpoint Manager.
- Ensure that devices are added to Microsoft Azure Active Directory (Azure AD) groups based on a selection made by users during the enrollment.

Which device enrollment setting should you configure for each requirement? To answer, select the appropriate options in the answer area.

NOTE: Each correct selection is worth one point.

Hot Area:



ANSWER:

Answer Area

Ensure that only devices that have approved platforms and versions can enroll in Endpoint Manager:

- Android enrollment
- Apple enrollment
- Corporate device identifiers
- Device categories
- **Enrollment restrictions**
- Windows enrollment

Ensure that devices are added to Azure AD groups based on a selection made by users during enrollment:

- Android enrollment
- Apple enrollment
- Corporate device identifiers
- **Device categories**
- Enrollment restrictions
- Windows enrollment

Explanation:

Reference:

https://docs.microsoft.com/en-us/mem/intune/enrollment/enrollment-restrictions-set https://docs.microsoft.com/en-us/mem/intune/enrollment/device-group-mapping

QUESTION NO: 5 - (DRAG DROP)

DRAG DROP

You use the Antimalware Assessment solution in Microsoft Azure Log Analytics.

From the Protection Status dashboard, you discover the computers shown in the following table.

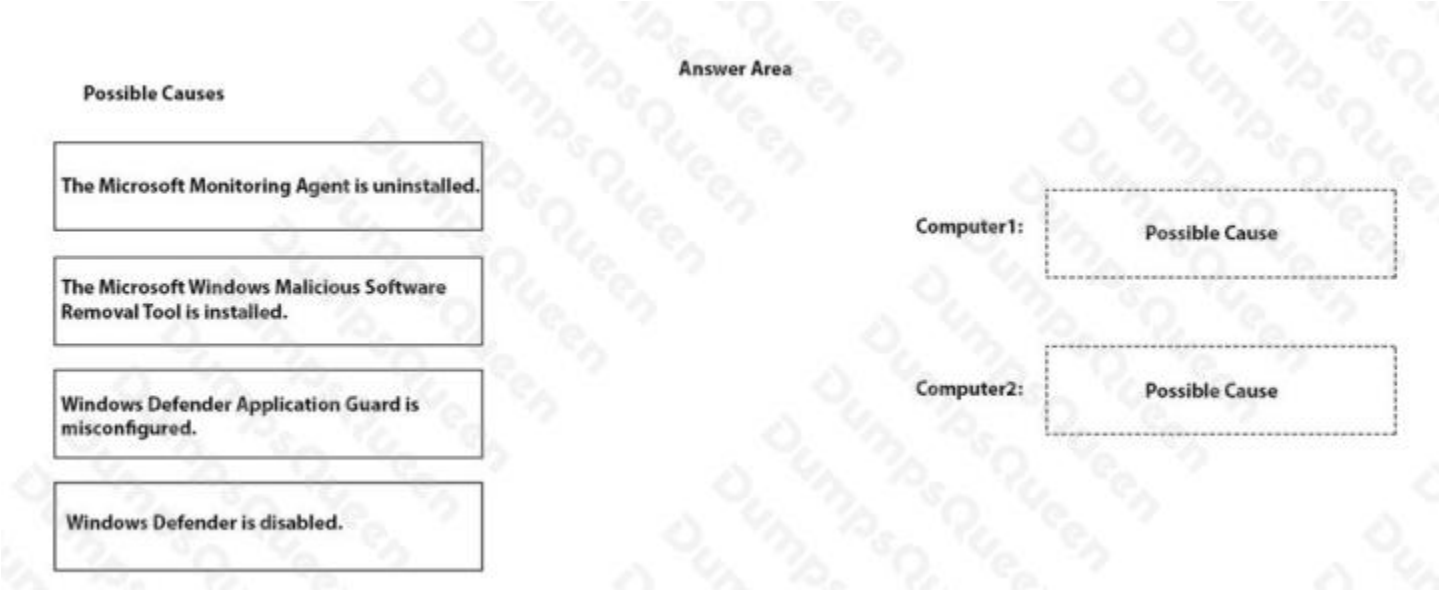
Name	Issue
Computer1	No real time protection
Computer2	Not reporting

You verify that both computers are connected to the network and running.

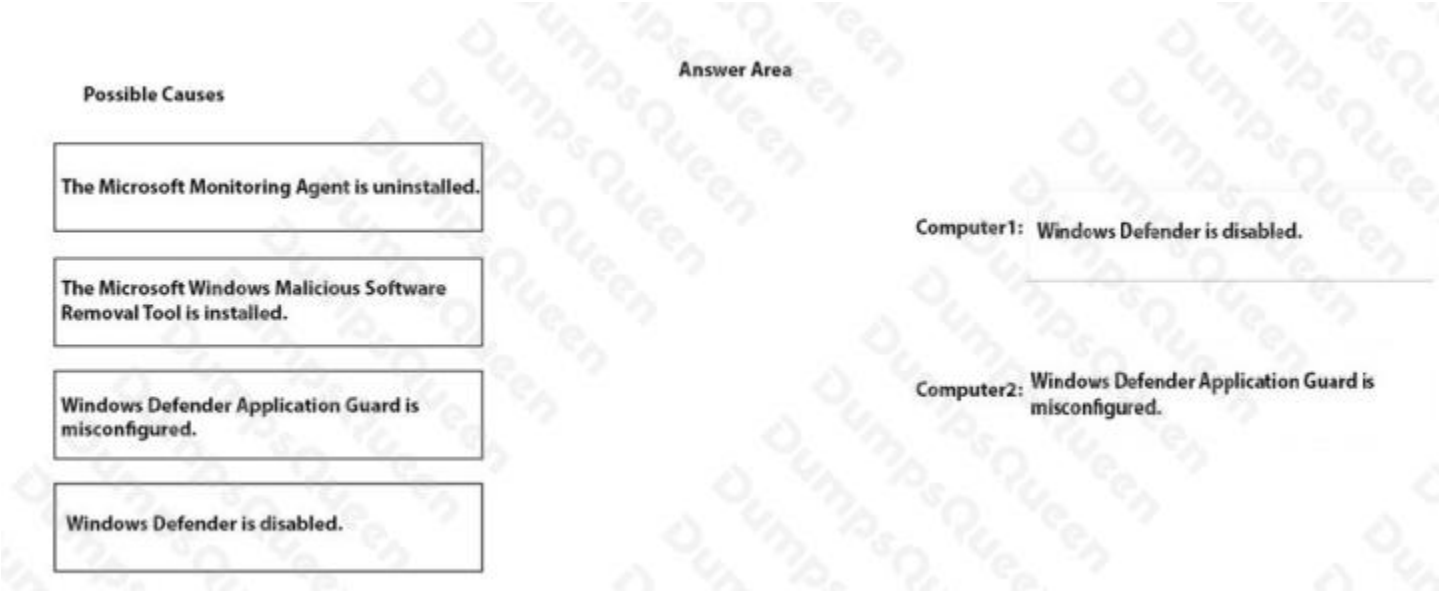
What is a possible cause of the issue on each computer? To answer, drag the appropriate causes to the correct computers. Each cause may be used once, more than once, or not at all. You may need to drag the split bar between panes or scroll to view content.

NOTE: Each correct selection is worth one point.

Select and Place:



ANSWER:



Explanation:

Reference:

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

QUESTION NO: 6

You install a feature update on a computer that runs Windows 10.

How many days do you have to roll back the update?

A. 5

B. 10

C. 14

D. 30

ANSWER: B

Explanation:

Microsoft has changed the time period associated with operating system rollbacks with Windows 10 version 1607, decreasing it to 10 days. Previously, Windows 10 had a 30-day rollback period.

Reference:

https://redmondmag.com/articles/2016/08/04/microsoft-shortens-windows-10-rollback-period.aspx

QUESTION NO: 7

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.

ANSWER: A

Explanation:

Reference:

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

QUESTION NO: 8

You have a Microsoft 365 subscription.

A remote user purchases a laptop from a retail store. The laptop is intended for company use and has Windows 10 Pro edition installed.

You need to configure the laptop to meet the following requirements:

What should you do?

A. Create a custom Windows image (.wim) file that contains an image of Windows 10 Enterprise and upload the file to a Microsoft

B. Create a provisioning package (.ppkg) file and email the file to the user

C. Create a Windows To Go workspace and ship the workspace to the user

D. Create a Sysprep Unattend (.xml) file and email the file to the user

ANSWER: B

Explanation:

Reference:

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

QUESTION NO: 9

You need to consider the underlined segment to establish whether it is accurate.

After installing a feature update on a Windows 10 computer, you have 7 days to roll back the update

Select “No adjustment required” if the underlined segment is accurate. If the underlined segment is inaccurate, select the accurate option.

A. No adjustment required.

B. 10

C. 90

D. 30

ANSWER: B

Explanation:

Microsoft has changed the time period associated with operating system rollbacks with Windows 10 version 1607, decreasing it to 10 days. Previously, Windows 10 had a 30-day rollback period.

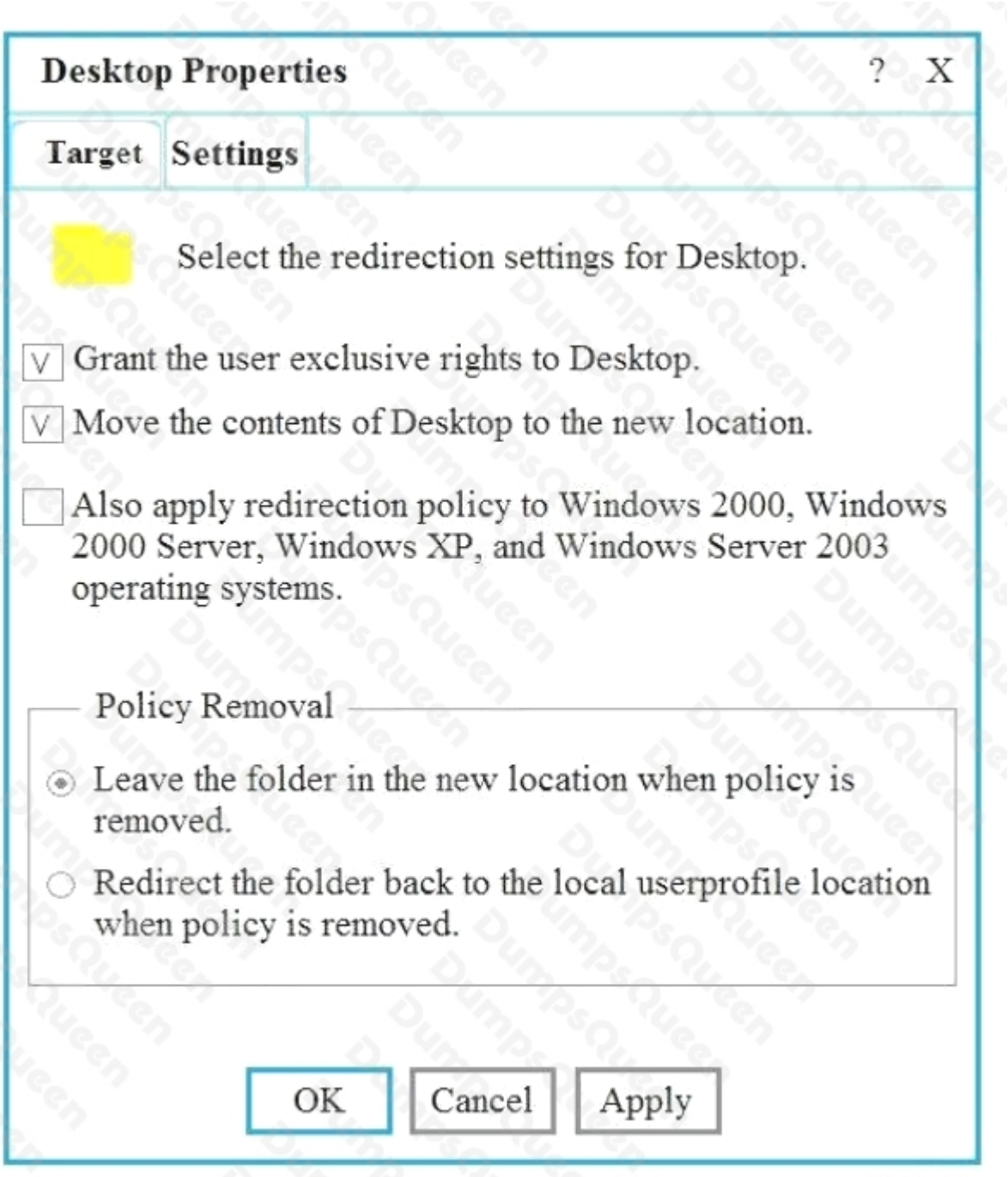
Reference:

https://redmondmag.com/articles/2016/08/04/microsoft-shortens-windows-10-rollback-period.aspx

QUESTION NO: 10

Your network contains an Active Directory domain named contoso.com. The domain contains 200 computers that run Windows 10.

Folder Redirection for the Desktop folder is configured as shown in the following exhibit.



The target is set to Server1.

You plan to use known folder redirection in Microsoft OneDrive for Business.

You need to ensure that the desktop content of users remains on their desktop when you implement known folder redirection.

Which two actions should you perform? Each correct answer presents part of the solution.

NOTE: Each correct selection is worth one point.

A. Clear the Grant the user exclusive rights to Desktop check box.

B. Change the Policy Removal setting.

C. Disable Folder Redirection.

D. Clear the Move the contents of Desktop to the new location check box.

ANSWER: A B

Explanation:

Reference: https://docs.microsoft.com/en-us/onedrive/redirect-known-folders

QUESTION NO: 11

You have an Azure Active Directory (Azure AD) tenant and 100 Windows 10 devices that are Azure AD joined and managed by using Microsoft Intune.

You need to configure Microsoft Defender Firewall and Microsoft Defender Antivirus on the devices. The solution must minimize administrative effort.

Which two actions should you perform? Each correct answer presents part of the solution.

NOTE: Each correct selection is worth one point.

A. To configure Microsoft Defender Antivirus, create a device configuration profile and configure the Endpoint protection settings.

B. To configure Microsoft Defender Firewall, crate a device configuration profile and configure the Device restrictions settings.

C. To configure Microsoft Defender Firewall, create a Group Policy Object (GPO) and configure Windows Defender Firewall with Advanced Security.

D. To configure Microsoft Defender Antivirus, create a Group Policy Object (GPO) and configure Windows Defender Antivirus settings.

E. To configure Microsoft Defender Antivirus, create a device configuration profile and configure the Device restrictions settings.

F. To configure Microsoft Defender Firewall, create a device configuration profile and configure the Endpoint protection settings.

ANSWER: A F

Explanation:

F: With Intune, you can use device configuration profiles to manage common endpoint protection security features on devices, including:

Reference:

https://docs.microsoft.com/en-us/mem/intune/protect/endpoint-protection-configure

https://docs.microsoft.com/en-us/mem/intune/protect/endpoint-security-policy#create-an-endpoint-security-policy

QUESTION NO: 12 - (DRAG DROP)

DRAG DROP

Your network contains an Active Directory domain that is synced to Microsoft Azure Active Directory (Azure AD). All computers are joined to the domain and registered to Azure AD.

The network contains a Microsoft Endpoint Configuration Manager deployment that is configured for co-management with Microsoft Intune.

All the computers in the finance department are managed by using Endpoint Configuration Manager. All the computers in the marketing department are managed by using Intune.

You install new computers for the users in the marketing department by using the Microsoft Deployment Toolkit (MDT).

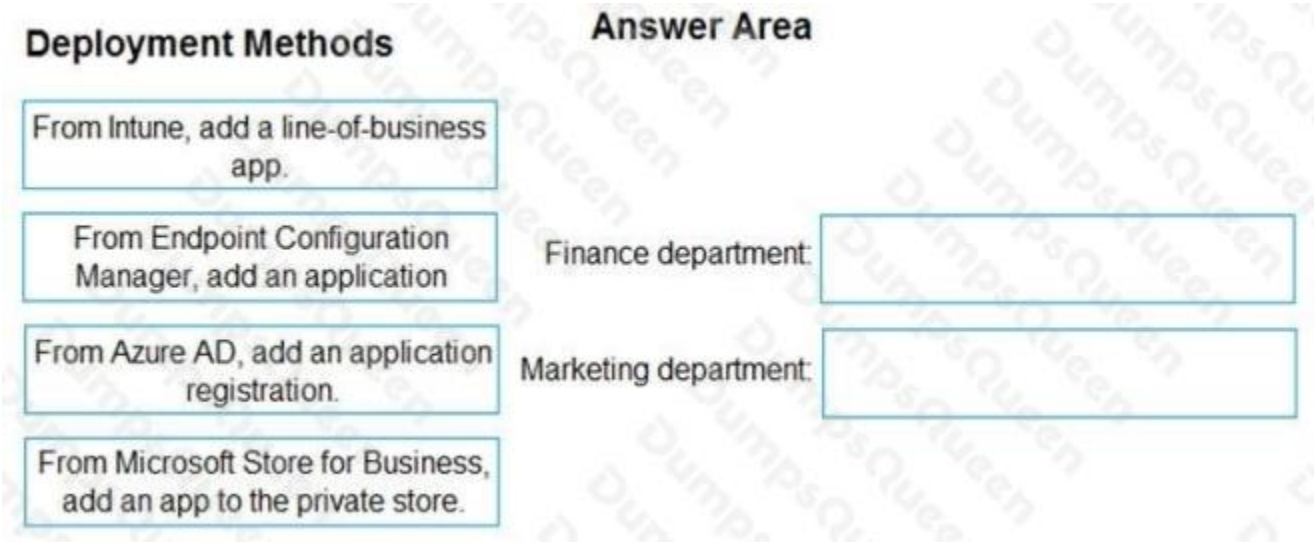
You purchase an application named App1 that uses an MSI package.

You need to install App1 on the finance department computers and the marketing department computers.

How should you deploy App1 to each department? To answer, drag the appropriate deployment methods to the correct departments. Each deployment method may be used once, more than once, or not at all. You may need to drag the split bat between panes or scroll to view content.

NOTE: Each correct selection is worth one point.

Select and Place:



ANSWER:

Explanation:

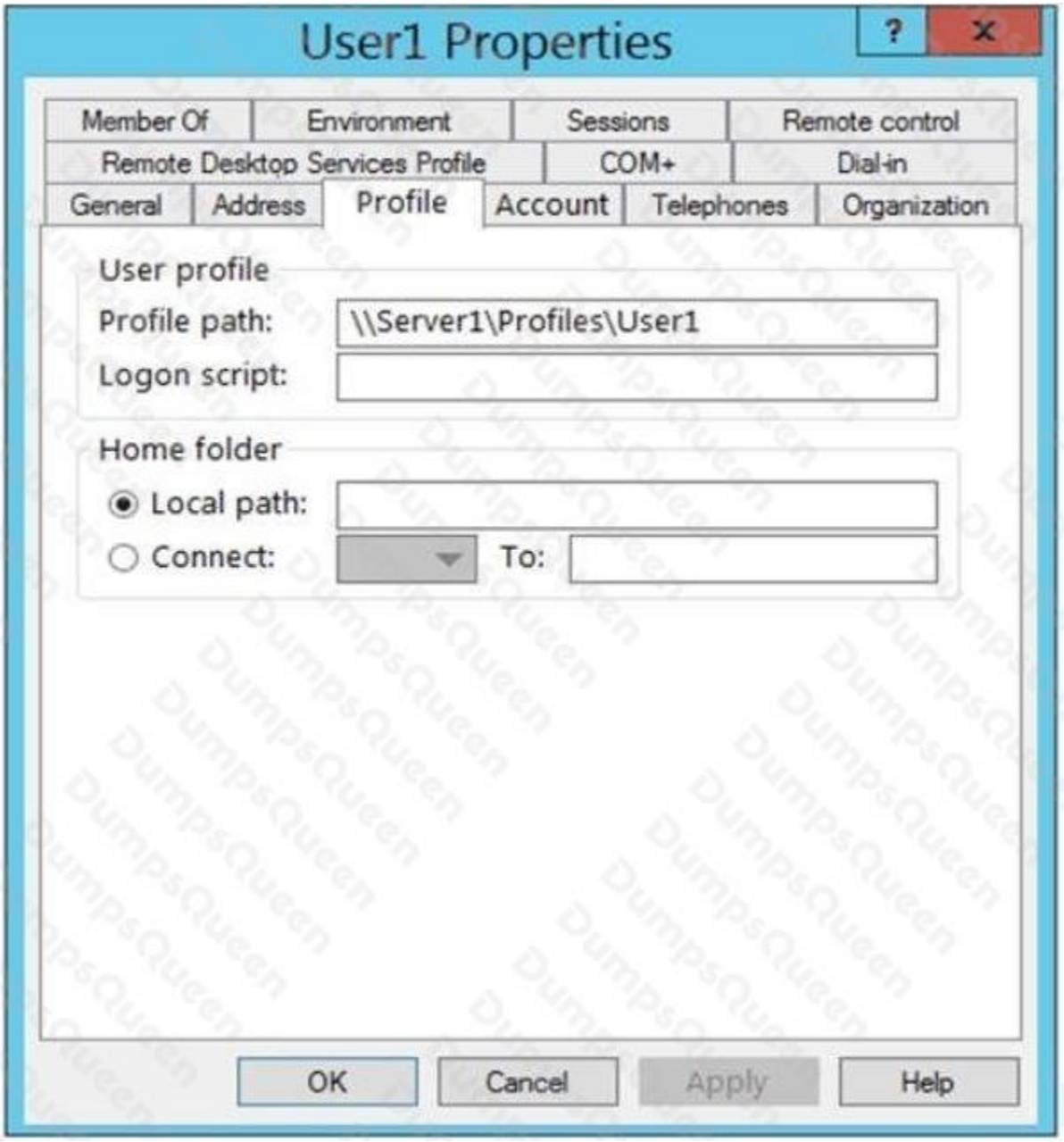
Reference: https://docs.microsoft.com/en-us/intune/apps-add https://docs.microsoft.com/en-us/sccm/apps/get-started/create-and-deploy-an-application

QUESTION NO: 13 - (HOTSPOT)

HOTSPOT

Your network contains an on-premises Active Directory forest named contoso.com. The forest contains a user named User1 and two computers named Computer1 and Computer2 that run Windows 10.

User1 is configured as shown in the following exhibit.



You rename file \\Server1\Profiles\User1.V6\NTUSER.DAT as NTUSER.MAN.

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
On Computer1, if User1 adds a shortcut to the desktop, the shortcut will appear when the user signs in to Computer2.	○	○
On Computer1, if User1 modifies the background, and then signs out, the user will see the modified background when signing back in to Computer1.	○	○
On Computer1, if User1 modifies the background, and then signs out, the user will see the modified background when signing in to Computer2.	○	○

ANSWER:

Answer Area

Statements	Yes	No
On Computer1, if User1 adds a shortcut to the desktop, the shortcut will appear when the user signs in to Computer2.	○	○
On Computer1, if User1 modifies the background, and then signs out, the user will see the modified background when signing back in to Computer1.	○	○
On Computer1, if User1 modifies the background, and then signs out, the user will see the modified background when signing in to Computer2.	○	○

Explanation:

A mandatory user profile is a roaming user profile that has been pre-configured by an administrator to specify settings for users. Settings commonly defined in a mandatory profile include (but are not limited to): icons that appear on the desktop, desktop backgrounds, user preferences in Control Panel, printer selections, and more. Configuration changes made during a user's session that are normally saved to a roaming user profile are not saved when a mandatory user profile is assigned.

The .man extension causes the user profile to be a read-only profile.

Reference:

https://docs.microsoft.com/en-us/windows/client-management/mandatory-user-profile

Manage and Protect Devices

QUESTION NO: 14

You have a Microsoft 365 tenant.

You plan to enable Enterprise State Roaming.

Which three types of data will sync across devices? Each con-eel answer presents a complete solution.

NOTE: Each correct selection is worth one point.

A. desktop theme settings

B. internet passwords

C. Microsoft Edge Chromium settings

D. Microsoft Teams settings

E. mouse settings

ANSWER: A B C

QUESTION NO: 15

You have a Microsoft 365 subscription that contains 1,000 Android devices enrolled in Microsoft intune. You create an app configuration policy that contains the following settings:

• Device enrollment type: Managed devices

• Profile Type: All Profile Types

• Platform: Android Enterprise

Which two types of apps can be associated with the policy? Each correct answer presents a complete solution. NOTE: Each correct selection is worth one point.

A. Android Enterprise system app

B. Android store app

C. Web link

D. Managed Google Play store app

E. Built-in Android app

ANSWER: A D

QUESTION NO: 16

Your company uses Microsoft Intune to manage devices. You need to ensure that only Android devices that use Android work profiles can enroll in Intune.

Which two configurations should you perform in the device enrollment restrictions? Each correct answer presents part of the solution.

NOTE: Each correct selection is worth one point.

A. From Platform Settings, set Android Enterprise (work profile) to Allow.

B. From Platform Settings, set Android device administrator Personally Owned to Block.

C. From Platform Settings, set Android device administrator Personally Owned to Allow.

D. From Platform Settings, set Android device administrator to Block.

ANSWER: A D

Explanation:

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

QUESTION NO: 17

Your network contains an on-premises Active Directory domain named contoso.com that syncs to Azure Active Directory (Azure AD).

You have the Windows 10 devices shown in the following table.

Name	Active Directory	Endpoint Configuration Manager agent	Microsoft Intune	Azure AD
Device1	Joined	Not installed	Enrolled	Registered
Device2	Not joined	Installed	Enrolled	Registered
Device3	Not joined	Not installed	Enrolled	Joined
Device4	Joined	Installed	Not enrolled	Registered
Device5	Not joined	Installed	Not enrolled	Joined
Device6	Joined	Installed	Enrolled	Joined

You need to ensure that you can use co-management to manage all the Windows 10 devices.

Which two actions should you perform? Each correct answer presents part of the solution.

NOTE: Each correct selection is worth one point.

A. Join Device 1, Device2, and Device4 to Azure AD.

B. Unjoin Device3, Device5, and Device6 from Azure AD, and then register the devices in Azure AD.

C. Enroll Device4 and Device5 in Intune.

D. Join Device2, Device3, and Device5 to the domain.

E. Install the Endpoint Configuration Manager agent on Device1 and Device3.

ANSWER: C E

Explanation:

Co-management enables you to concurrently manage Windows 10 devices by using both Configuration Manager and Microsoft Intune.

Co-management requires Configuration Manager version 1710 or later and enrollment in Microsoft Intune. Windows 10 devices must be hybrid Azure AD joined.

Reference: https://docs.microsoft.com/en-us/mem/configmgr/comanage/overview

QUESTION NO: 18

You have 100 computers that run Windows 10 and connect to an Azure Log Analytics workspace.

Which three types of data can you collect from the computers by using Log Analytics? Each correct answer a complete solution.

NOTE: Each correct selection is worth one point.

A. error events from the System log

B. failure events from the Security log

C. third-party application logs stored as text files

D. the list of processes and their execution times

E. the average processor utilization

ANSWER: A D E

Explanation:

Log Analytics is a tool in the Azure portal to edit and run log queries from data collected by Azure Monitor logs, such as the system log, and interactively analyze their results.

Reference: https://docs.microsoft.com/en-us/azure/azure-monitor/logs/log-analytics-tutorialhttps://docs.microsoft.com/en-us/azure/azure-monitor/logs/log-analytics-tutorial

QUESTION NO: 19

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 an Azure Active Directory (Azure AD) tenant named contoso.com and a Microsoft Intune subscription.

Contoso.com contains a user named user1@contoso.com.

You have a computer named Computer1 that runs Windows 8.1.

You need to perform an in-place upgrade of Computer1 to Windows 10.

Solution: You start Computer1 from the Windows 10 installation media and use the Install option.

Does this meet the goal?

A. Yes

B. No

ANSWER: B

QUESTION NO: 20

You have a hybrid deployment of Azure Active Directory (Azure AD) that contains 50 Windows 10 devices. All the devices are enrolled in Microsoft Endpoint Manager.

You discover that Group Policy settings override the settings configured in Microsoft Endpoint Manager policies.

You need to ensure that the settings configured in Microsoft Endpoint Manager override the Group Policy settings.

What should you do?

A. From the Microsoft Endpoint Manager admin center, create an Administrative Templates device profile

B. From Group Policy Management Editor, configure the Computer Configuration settings in the Default Domain Policy

C. From the Microsoft Endpoint Manager admin center, create a custom device profile

D. From Group Policy Management Editor, configure the User Configuration settings in the Default Domain Policy

ANSWER: C

Explanation:

Reference: https://uem4all.com/2018/04/02/windows-10-group-policy-vs-intune-mdm-policy-who-wins/