DUMPSARENA

Endpoint Administrator

Microsoft MD-102

Version Demo

Total Demo Questions: 10

Total Premium Questions: 179

Buy Premium PDF

https://dumpsarena.co

sales@dumpsarena.co

sales@dumpsarena.co
dumpsarena.co

Topic Break Down

Topic	No. of Questions
Topic 1, Case Study Contoso, Ltd. Overview	9
Topic 2, Litware inc	9
Topic 3, Mix Question	161
Total	179

QUESTION NO: 1 - (HOTSPOT)

HOTSPOT

You have a Microsoft 365 subscription.

All users have Microsoft 365 apps deployed.

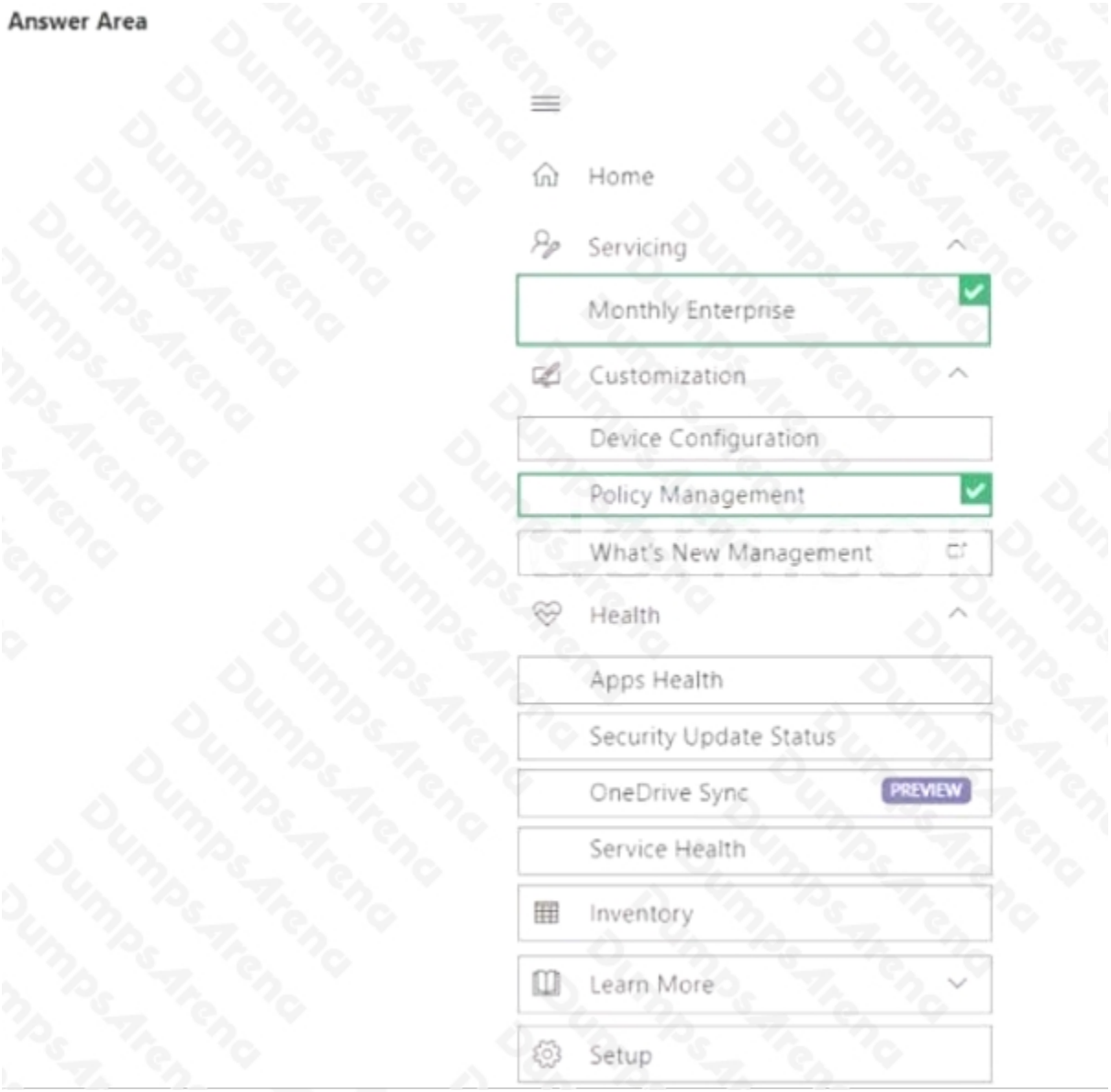
You need to configure Microsoft 365 apps to meet the following requirements: Enable the automatic installation of WebView2 Runtime.

Prevent users from submitting feedback.

Which two settings should you configure in the Microsoft 365 Apps admin center? To answer, select the appropriate settings in the answer area.

NOTE: Each correct selection is worth one point.

Answer Area



ANSWER:

Answer Area

Explanation:

Answer Area

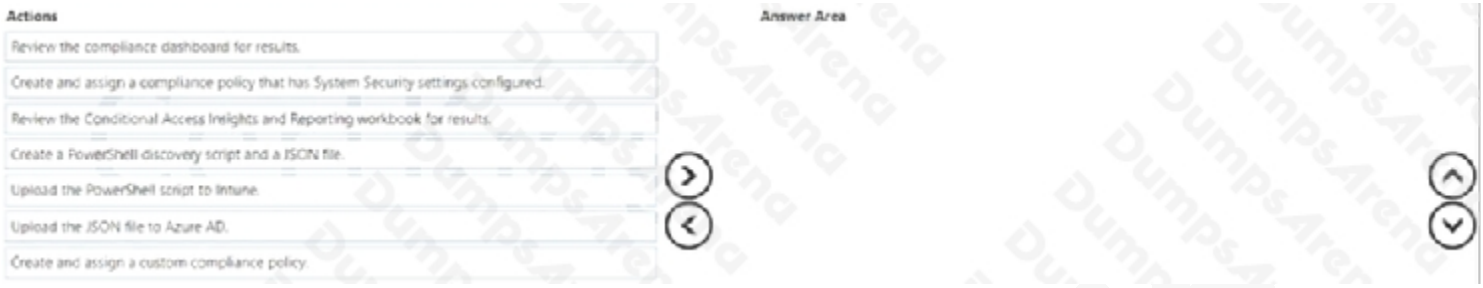
QUESTION NO: 2 - (DRAG DROP)

DRAG DROP

You have a Microsoft 365 subscription that contains 1,000 Windows 11 devices enrolled in Microsoft Intune.

You plan to create and monitor the results of a compliance policy used to validate the BIOS version of the devices.

Which four 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.



ANSWER:

Explanation:

QUESTION NO: 3

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 presents a complete solution. NOTE: Each correct selection is worth one point.

A. failure events from the Security log

B. the list of processes and their execution times

C. the average processor utilization

D. error events from the System log

E. third-party application logs stored as text files

ANSWER: C D E

Explanation:

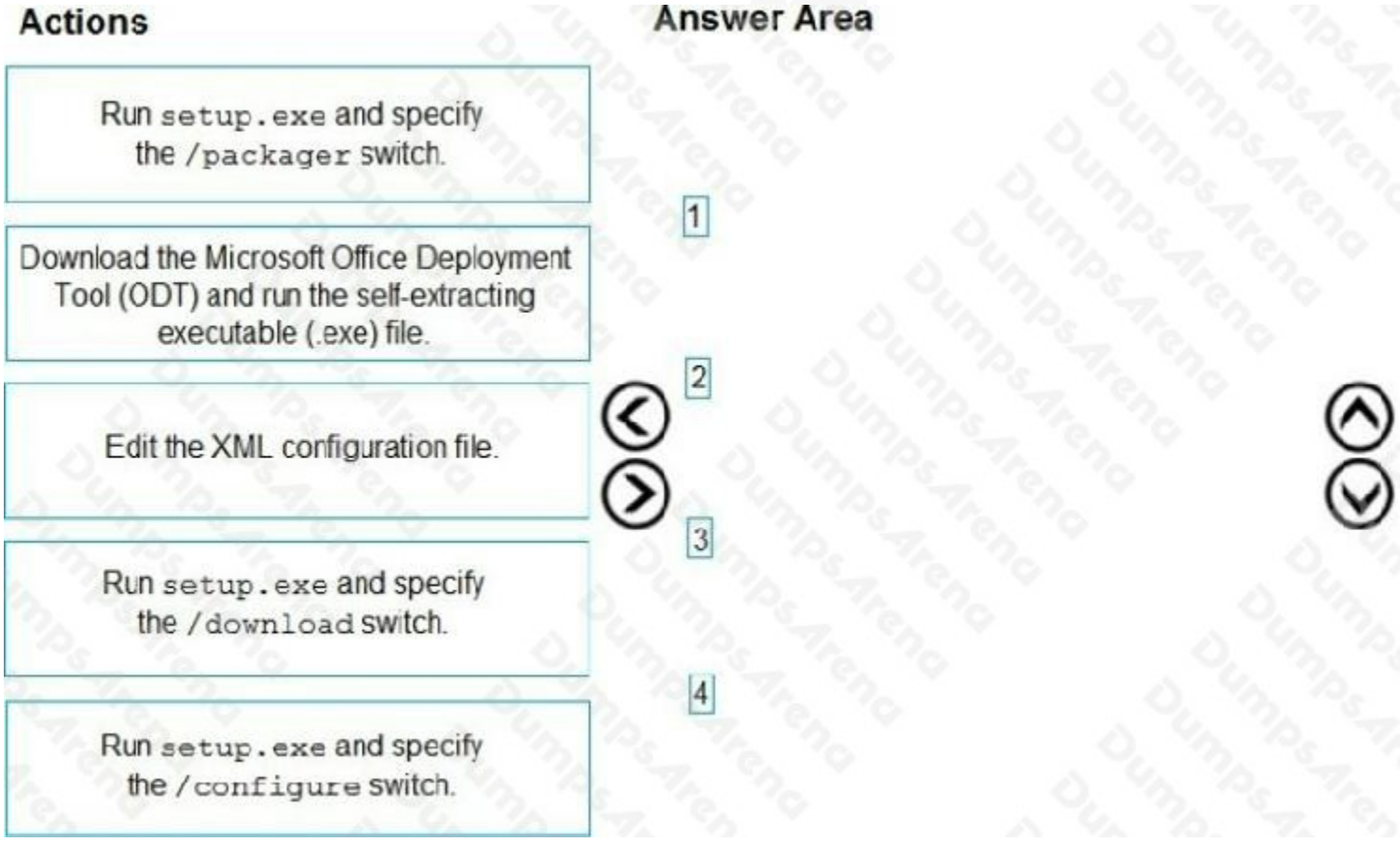
You can collect performance metrics such as average processor utilization, event logs like error events from the System log, and custom logs such as third-party application logs stored as text files using Azure Log Analytics agents on Windows 10 computers. However, failure events from the Security log and detailed process execution times are not typically collected by default through Log Analytics without additional configuration or solutions.
For more information, see Azure Monitor Data Collection from Windows agents.

QUESTION NO: 4 - (DRAG DROP)

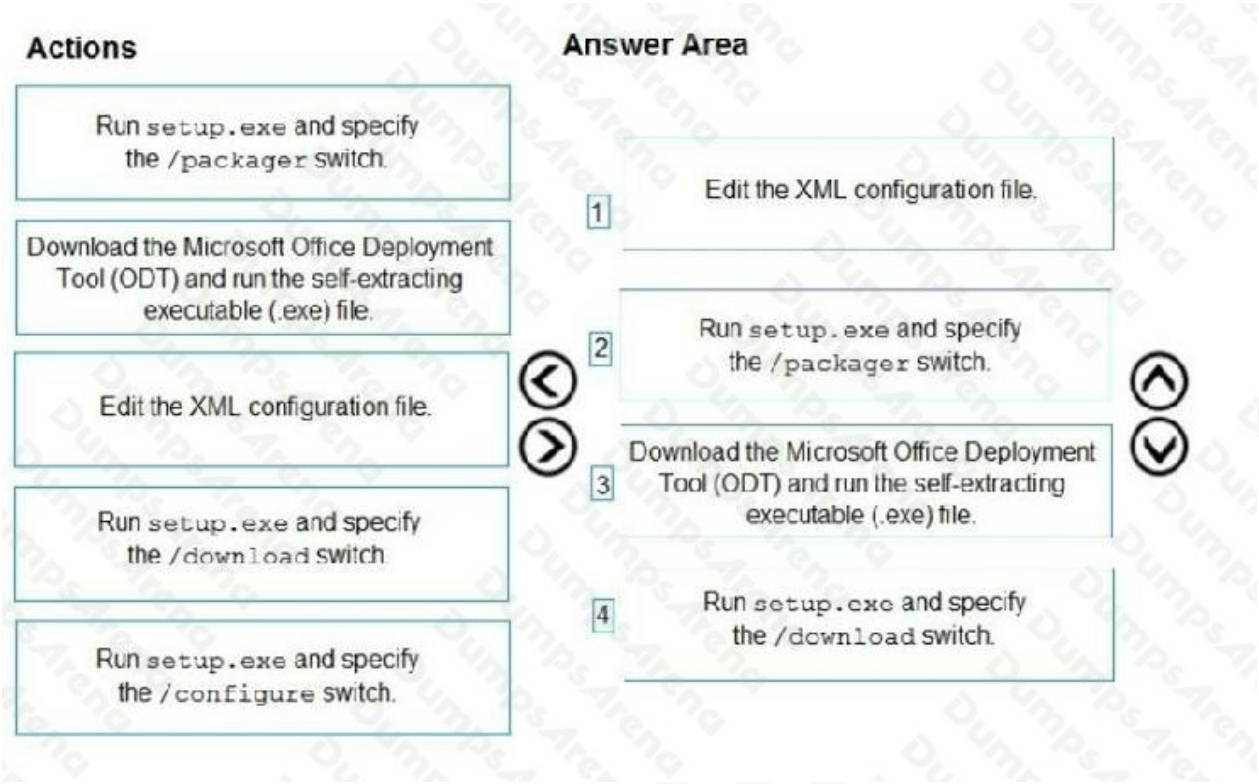
DRAG DROP -

You have a Microsoft 365 E5 subscription and a computer that runs Windows 11. You need to create a customized installation of Microsoft 365 Apps for enterprise.

Which four actions should you perform in sequence? To answer, move the appropriate cmdlets from the list of cmdlets to the answer area and arrange them in the correct order.



ANSWER:



Explanation:

QUESTION NO: 5

You have an 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 Group Policy Object (GPO) and configure the Windows Defender Antivirus settings.

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

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

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

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

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

ANSWER: C E

Explanation:

To configure Microsoft Defender Firewall and Microsoft Defender Antivirus on Azure AD joined devices managed by Microsoft Intune, the best practice is to create a device configuration profile within Intune and configure the Endpoint protection settings. This method centralizes management and minimizes administrative effort compared to using Group Policy Objects (GPOs), which are designed for on-premises Active Directory environments. This approach applies configurations through Intune, suitable for Azure AD joined devices.

Reference: https://learn.microsoft.com/en-us/mem/intune/protect/endpoint-protection-windows-10

QUESTION NO: 6

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

Name	Description
Group1	Azure AD group that contains a user named User1
Group2	Azure AD group that contains iOS devices

You create a Conditional Access policy named CAPolicy1 that will block access to Microsoft Exchange Online from iOS devices. You assign CAPolicy1 to Group1.

You discover that User1 can still connect to Exchange Online from an iOS device. You need to ensure that CAPolicy1 is enforced.

What should you do?

A. Configure a new terms of use (TOU).

B. Assign CAPolicy1 to Group2.

C. Enable CAPolicy1

D. Add a condition in CAPolicy1 to filter for devices.

ANSWER: B

Explanation:

Conditional Access policies are applied based on the assignment of users or devices to the policy. In this scenario, CAPolicy1 is assigned to Group1, which includes the user User1. However, the policy blocks access from iOS devices, and the devices themselves are in Group2 (which contain iOS devices).

Since CAPolicy1 is assigned to the user group (Group1) but not to the iOS device group (Group2), the policy does not effectively target iOS devices used by User1. To ensure that the policy blocks access from iOS devices for User1, you need to assign the policy to the group containing the iOS devices (Group2).

Therefore, assigning CAPolicy1 to Group2 will enforce the policy on those devices, preventing User1 from connecting to Exchange Online from an iOS device.

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

QUESTION NO: 7

Your network contains an Active Directory domain named contoso.com. The domain contains named Computer1 that runs Windows 10.

Name	Permission
User1	Full control
User2	Change

When accessing Share1, which two actions can be performed by User1 but not by User2? Each correct answer presents part of the solution.

NOTE: Each correct selection is worth one point.

A. Delete a file created by another user.

B. Set the permissions for a file.

C. Rename a file created by another user.

D. Take ownership of file.

E. Copy a file created by another user to a subfolder.

ANSWER: B D

Explanation:

In this scenario, User1 has Full Control share permissions, and User2 has Change share permissions, while NTFS permissions on the folder grant Everyone Full Control. Since the most restrictive permission applies, the effective permissions are the combination of share and NTFS permissions, where the lower permission limits actions. Full Control share permission allows User1 to perform all actions including setting permissions and taking ownership of files. Change share permission (User2) allows modifying files (create, delete, and change data) but does not allow changing permissions or taking ownership. Therefore, User1 can perform "Set the permissions for a file" and "Take ownership of file," whereas

User2 cannot. Reference: https://learn.microsoft.com/en-us/windows/security/identity-protection/access-control/share-and-ntfs-permissions

QUESTION NO: 8

You have a Microsoft 365 E5 subscription that contains 500 macOS devices enrolled in Microsoft Intune.

You need to ensure that you can apply Microsoft Defender for Endpoint antivirus policies to the macOS devices. The solution must minimize administrative effort.

What should you do?

A. Onboard the macOS devices to the Microsoft Purview compliance portal.

B. From the Microsoft Intune admin center, create a security baseline.

C. Install Defender for Endpoint on the macOS devices.

D. From the Microsoft Intune admin center, create a configuration profile.

ANSWER: C

Explanation:

To apply Microsoft Defender for Endpoint antivirus policies to macOS devices enrolled in Intune, you must first install the Defender for Endpoint agent on those devices. This installation allows Intune to manage and apply the antivirus policies effectively. Simply creating configuration profiles or security baselines without the Defender for Endpoint installed will not enable antivirus management on macOS devices. Onboarding devices to the Microsoft Purview compliance portal does not relate directly to antivirus policy deployment for macOS. For detailed guidance, refer to the official Microsoft documentation: https://learn.microsoft.com/en-us/mem/intune/protect/antivirus-macos

QUESTION NO: 9 - (HOTSPOT)

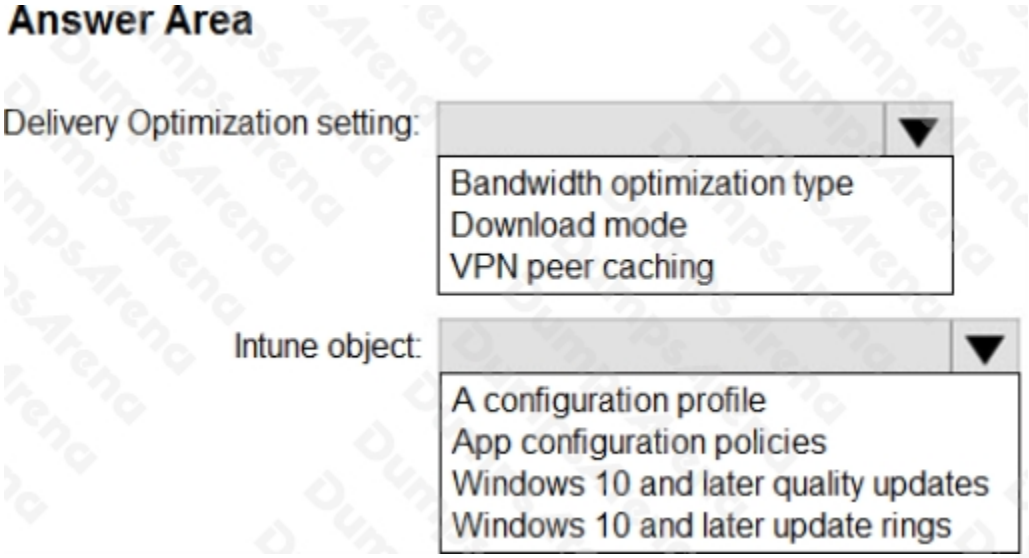
HOTSPOT -

You have 100 Windows 10 devices enrolled in Microsoft Intune.

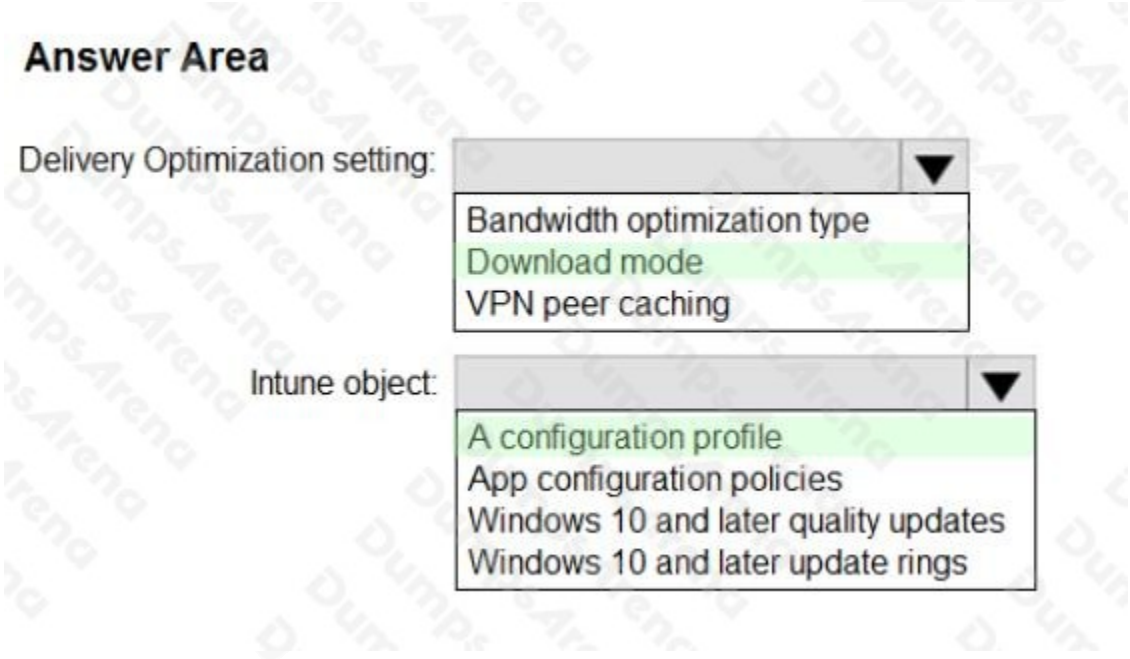
You need to configure the devices to retrieve Windows updates from the internet and from other computers on a local network.

Which Delivery Optimization setting should you configure, and which type of Intune object should you create? To answer, select the appropriate options in the answer area.

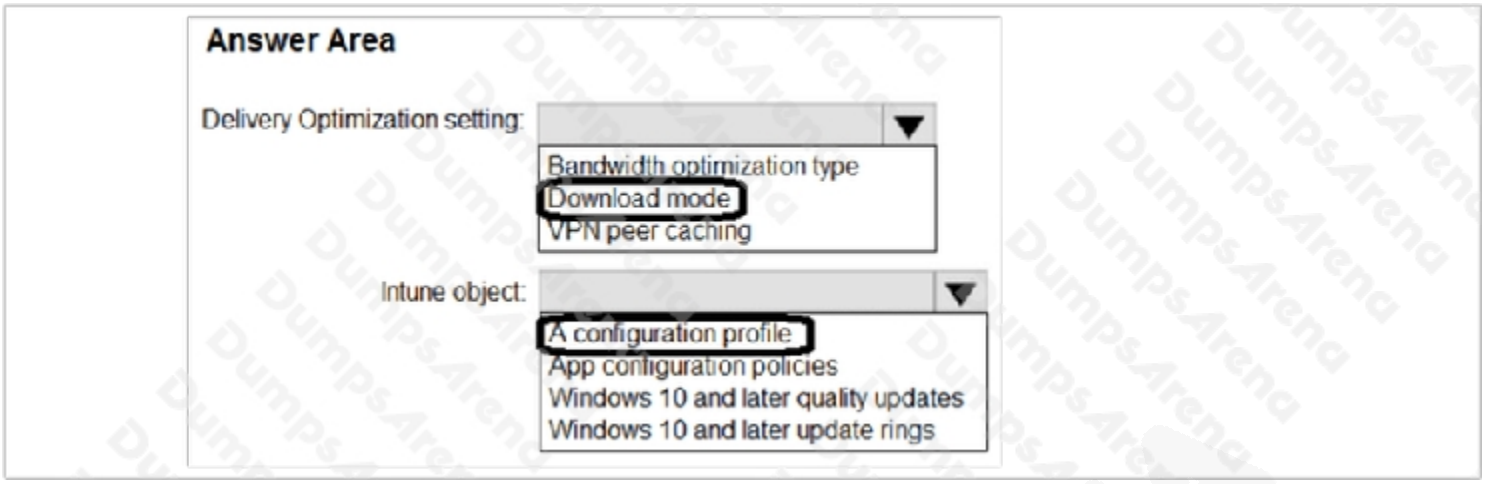
NOTE: Each correct selection is worth one point.



ANSWER:



Explanation:



QUESTION NO: 10

On Computer1, you need to configure the custom Visual Effects performance settings. Which user accounts can you use?

A. Admm1,User11, and User13 only

B. Admin1 only

C. Admin1, User11, and User12 only

D. Admin1, User11, User12, and User13

ANSWER: D

Explanation: