DUMPSQUEEN

Endpoint Administrator

Microsoft MD-102

Version Demo

Total Demo Questions: 10

Total Premium Questions: 179

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

What should you upgrade before you can configure the environment to support co-management?

A. the domain functional level

B. Configuration Manager

C. the domain controllers

D. Windows Server Update Services (WSUS)

ANSWER: B

Explanation:

Reference:

https://docs.microsoft.com/en-us/sccm/comanage/tutorial-co-manage-clients

QUESTION NO: 3

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.

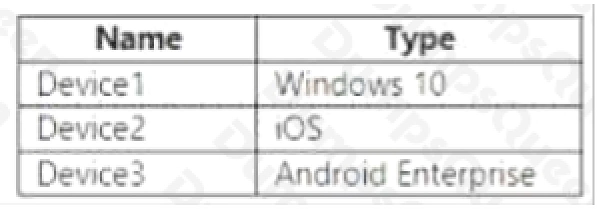
ANSWER: C E

Explanation:

QUESTION NO: 4 - (DRAG DROP)

DRAG DROP

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

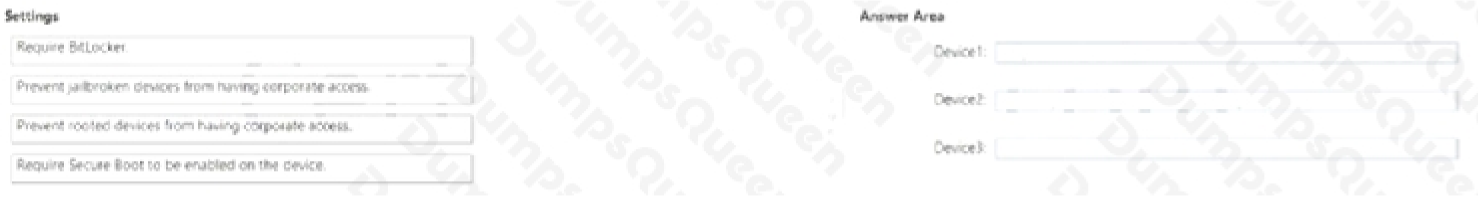


Name	Type
Device1	Windows 10
Device2	iOS
Device3	Android Enterprise

You need to ensure that only devices running trusted firmware or operating system build can access network resources.

Which compliance policy setting should you configure for each device? To answer, drag the appropriate settings to the correct devices. Each setting 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.



Settings

Require BitLocker

Prevent jailbroken devices from having corporate access.

Prevent rooted devices from having corporate access.

Require Secure Boot to be enabled on the device.

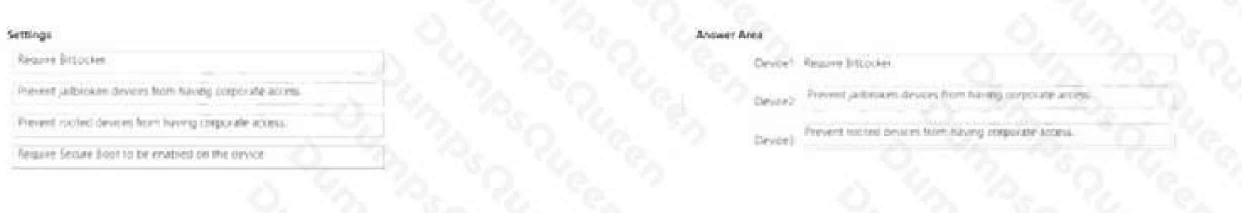
Answer Area

Device1:

Device2:

Device3:

ANSWER:



Settings

Require BitLocker

Prevent jailbroken devices from having corporate access.

Prevent rooted devices from having corporate access.

Require Secure Boot to be enabled on the device.

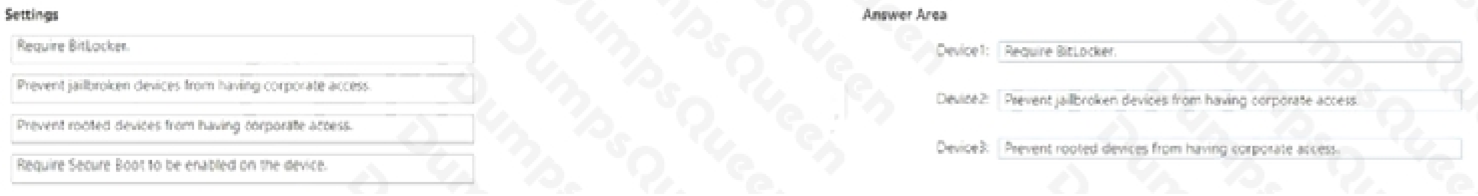
Answer Area

Device1: Require BitLocker

Device2: Prevent jailbroken devices from having corporate access.

Device3: Prevent rooted devices from having corporate access.

Explanation:



Settings

Require BitLocker.

Prevent jailbroken devices from having corporate access.

Prevent rooted devices from having corporate access.

Require Secure Boot to be enabled on the device.

Answer Area

Device1: Require BitLocker.

Device2: Prevent jailbroken devices from having corporate access.

Device3: Prevent rooted devices from having corporate access.

QUESTION NO: 5

You have a Microsoft 365 E5 subscription that contains a group named Group1.

You create a Conditional Access policy named CAPolicy1 and assign CAPolicy1 to Group1.

You need to configure CAPolicy1 to require the members of Group1 to reauthenticate every eight hours when they connect to Microsoft Exchange Online.

What should you configure?

A. Session access controls

B. an assignment that uses a User risk condition

C. an assignment that uses a Sign-in risk condition

D. Grant access controls

ANSWER: A

Explanation:

User sign-in frequency

Sign-in frequency defines the time period before a user is asked to sign in again when attempting to access a resource.

The Azure Active Directory (Azure AD) default configuration for user sign-in frequency is a rolling window of 90 days.

Sign-in frequency control

Sign in to the Azure portal as a global administrator, security administrator, or Conditional Access administrator.

Browse to Azure Active Directory > Security > Conditional Access. Select New policy.

Give your policy a name. We recommend that organizations create a meaningful standard for the names of their policies.

Choose all required conditions for customers environment, including the target cloud apps.

Under Access controls > Session.

Select Sign-in frequency.

Choose Periodic reauthentication and enter a value of hours or days or select Every time. Save your policy.

Reference: https://docs.microsoft.com/en-us/azure/active-directory/conditional-access/howtoconditional- access-session-lifetime

QUESTION NO: 6

You have 200 computers that run Windows 10 and are joined to an Active Directory domain.

You need to enable Windows Remote Management (WinRM) on all the computers by using Group Policy.

Which three actions should you perform? Each correct answer presents part of the solution. NOTE: Each correct selection is worth one point.

A. Set the Startup Type of the Windows Remote Management (WS-Management) service to Automatic.

B. Enable the Windows Firewall: Allow inbound remote administration exception setting.

C. Enable the Allow remote server management through WinRM setting.

D. Enable the Windows Firewall: Allow inbound Remote Desktop exceptions setting.

E. Enable the Allow Remote Shell access setting.

F. Set the Startup Type of the Remote Registry service to Automatic.

ANSWER: A B C

Explanation:

Reference:

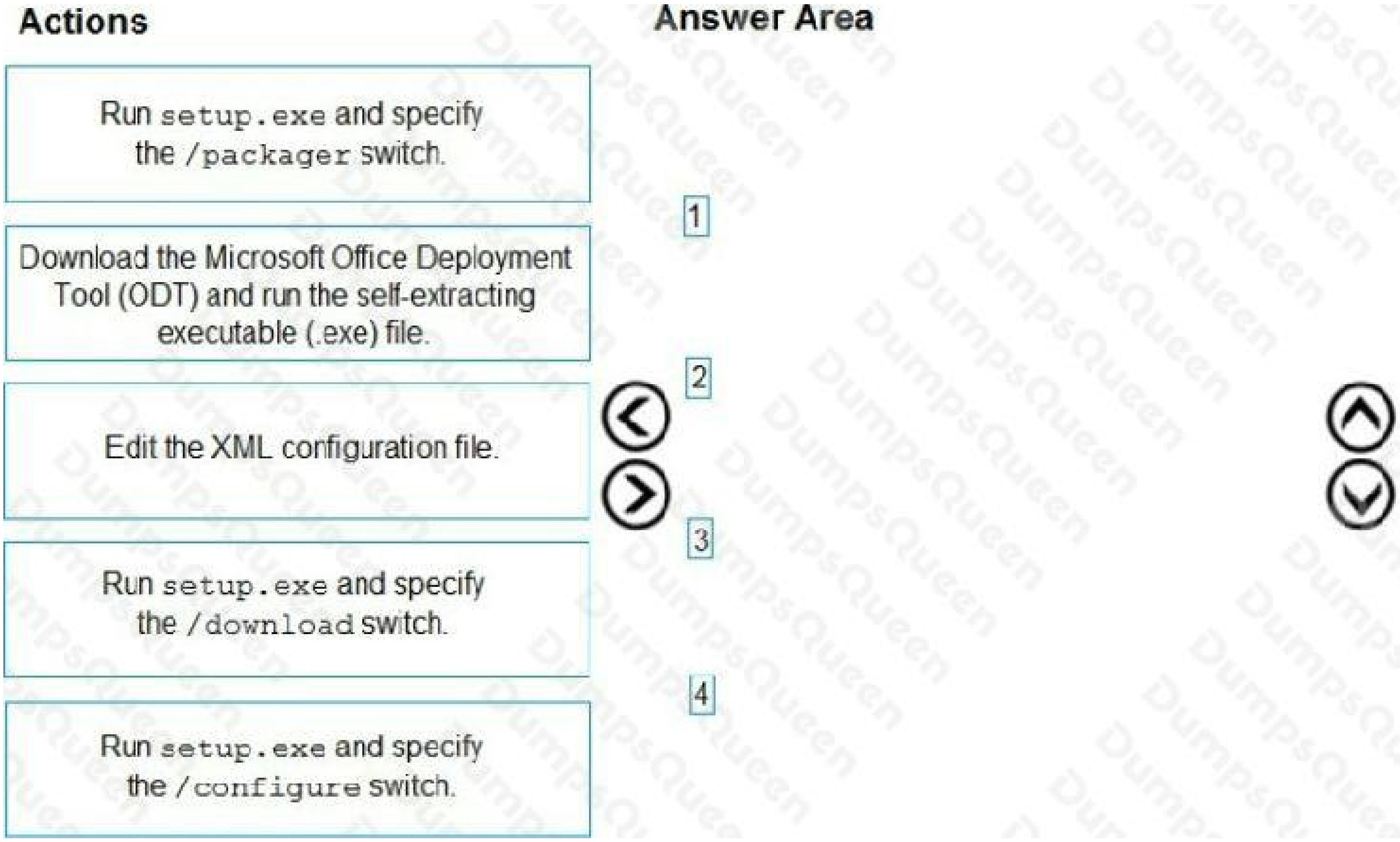
https://support.auvik.com/hc/en-us/articles424994-How-to-enable-WinRM-with-domaincontroller- Group-Policy-for-WMI-monitoring

QUESTION NO: 7 - (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.



Actions

Run `setup.exe` and specify the `/packager` switch.

Download the Microsoft Office Deployment Tool (ODT) and run the self-extracting executable (.exe) file.

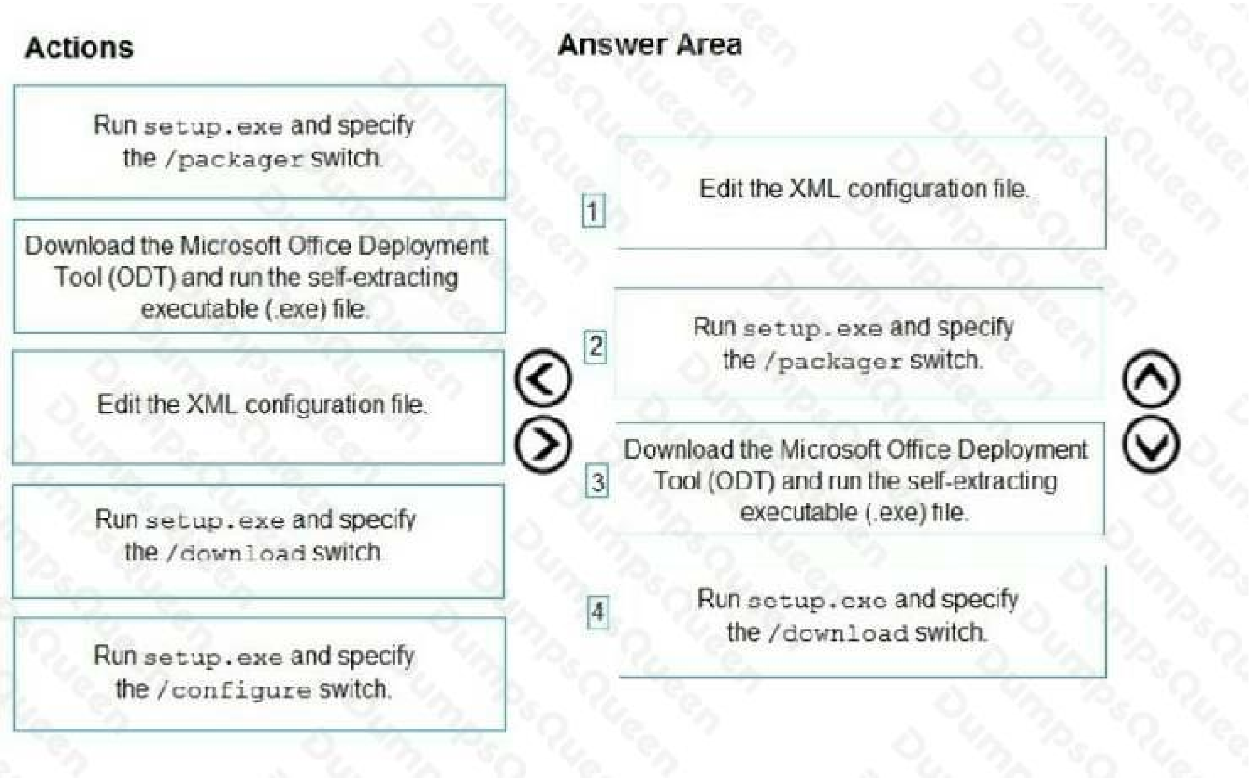
Edit the XML configuration file.

Run `setup.exe` and specify the `/download` switch.

Run `setup.exe` and specify the `/configure` switch.

Answer Area

ANSWER:



Actions

- Run `setup.exe` and specify the `/packager` switch.
- Download the Microsoft Office Deployment Tool (ODT) and run the self-extracting executable (.exe) file.
- Edit the XML configuration file.
- Run `setup.exe` and specify the `/download` switch.
- Run `setup.exe` and specify the `/configure` switch.

Answer Area

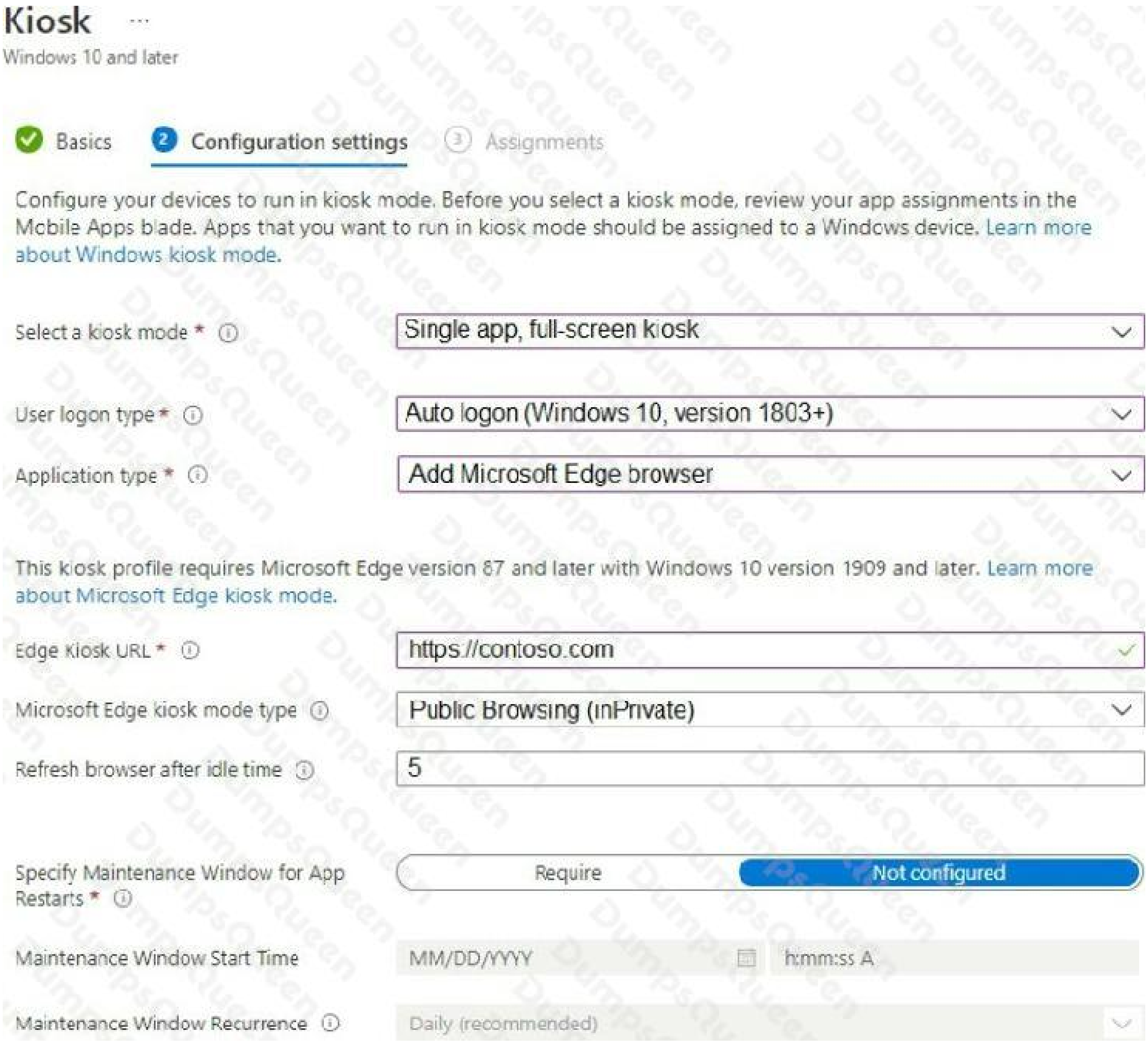
1. Edit the XML configuration file.
2. Run `setup.exe` and specify the `/packager` switch.
3. Download the Microsoft Office Deployment Tool (ODT) and run the self-extracting executable (.exe) file.
4. Run `setup.exe` and specify the `/download` switch.

Explanation:

QUESTION NO: 8 - (HOTSPOT)

HOTSPOT -

You have the device configuration profile shown in the following exhibit.



Kiosk ···

Windows 10 and later

Configure your devices to run in kiosk mode. Before you select a kiosk mode, review your app assignments in the Mobile Apps blade. Apps that you want to run in kiosk mode should be assigned to a Windows device. Learn more about Windows kiosk mode.

Select a kiosk mode * ⓘ: Single app, full-screen kiosk

User logon type * ⓘ: Auto logon (Windows 10, version 1803+)

Application type * ⓘ: Add Microsoft Edge browser

This kiosk profile requires Microsoft Edge version 87 and later with Windows 10 version 1909 and later. Learn more about Microsoft Edge kiosk mode.

Edge Kiosk URL * ⓘ: https://contoso.com ✓

Microsoft Edge kiosk mode type ⓘ: Public Browsing (inPrivate)

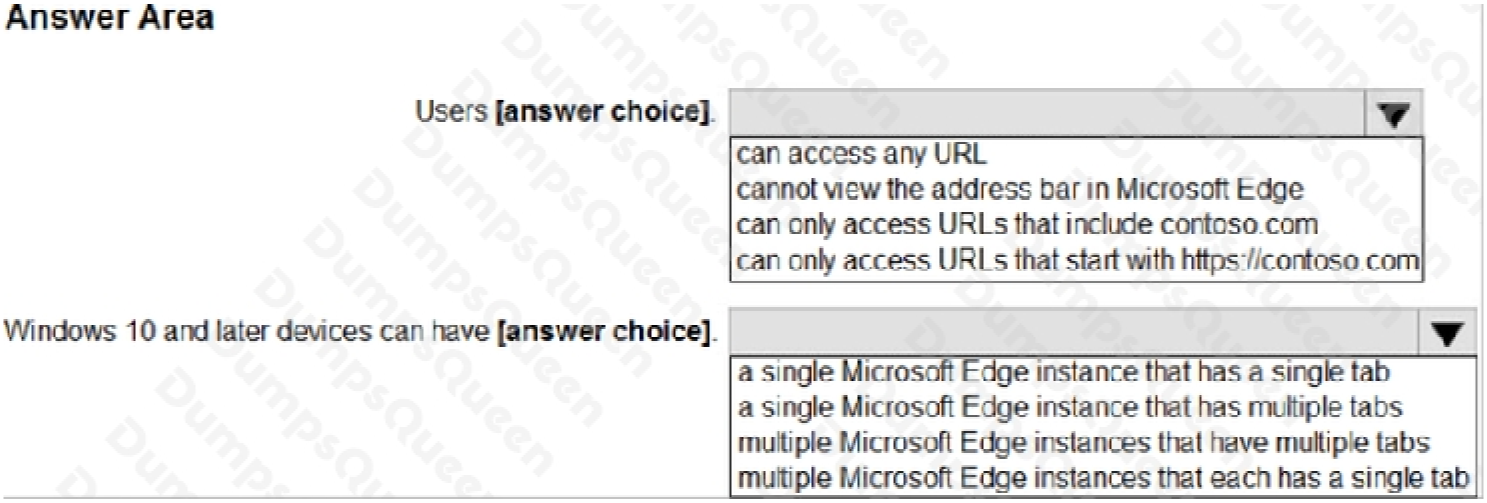
Refresh browser after idle time ⓘ: 5

Specify Maintenance Window for App Restarts * ⓘ: Require [✓ Not configured]

Maintenance Window Start Time: MM/DD/YYYY h:mm:ss A

Maintenance Window Recurrence ⓘ: Daily (recommended)

Use the drop-down menus to select the answer choice that completes each statement based on the information presented in the graphic. NOTE: Each correct selection is worth one point.



Answer Area

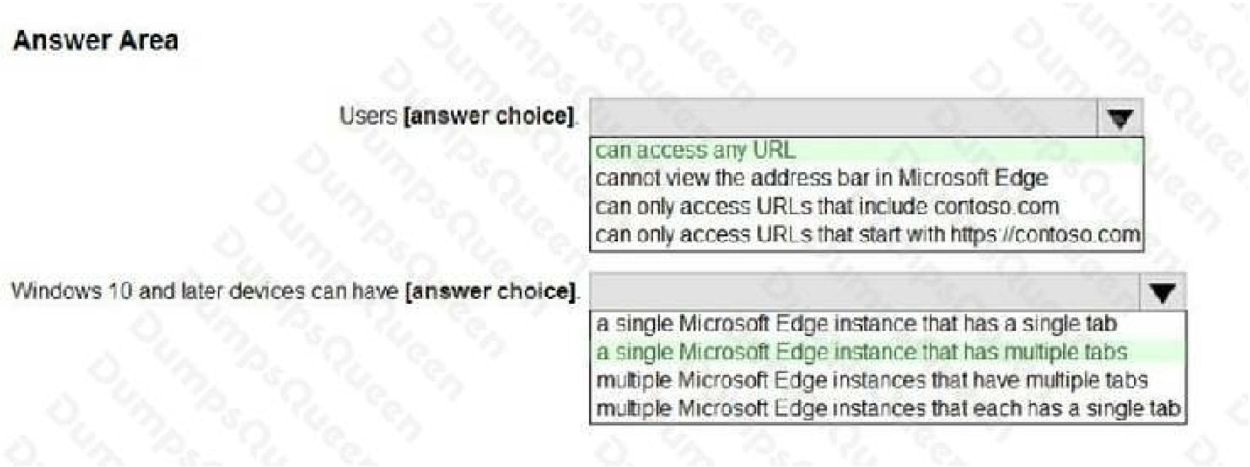
Users **[answer choice]**.

- can access any URL
- cannot view the address bar in Microsoft Edge
- can only access URLs that include contoso.com
- can only access URLs that start with https://contoso.com

Windows 10 and later devices can have **[answer choice]**.

- a single Microsoft Edge instance that has a single tab
- a single Microsoft Edge instance that has multiple tabs
- multiple Microsoft Edge instances that have multiple tabs
- multiple Microsoft Edge instances that each has a single tab

ANSWER:



Answer Area

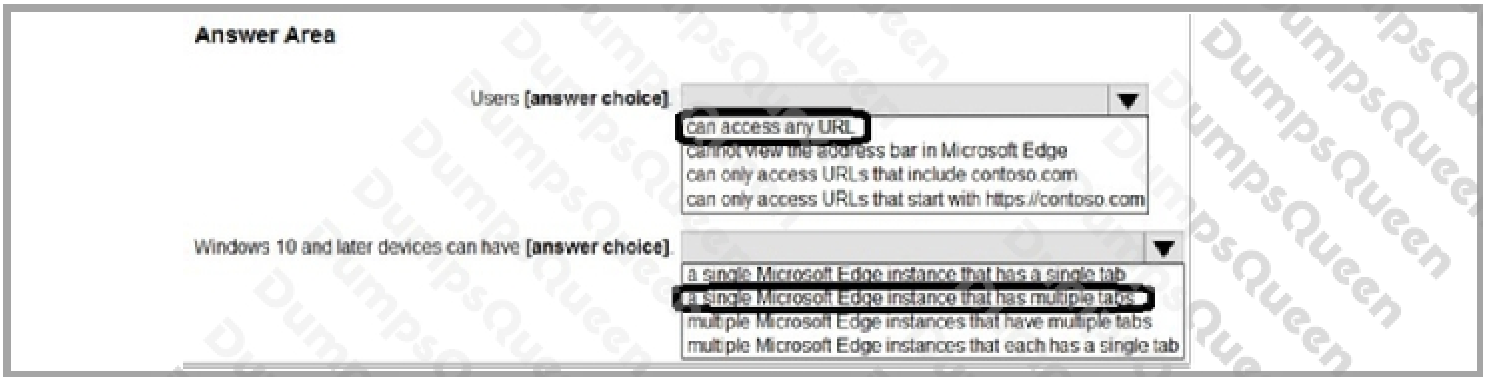
Users **[answer choice]**.

- [✓ can access any URL]
- cannot view the address bar in Microsoft Edge
- can only access URLs that include contoso.com
- can only access URLs that start with https://contoso.com

Windows 10 and later devices can have **[answer choice]**.

- a single Microsoft Edge instance that has a single tab
- [✓ a single Microsoft Edge instance that has multiple tabs]
- multiple Microsoft Edge instances that have multiple tabs
- multiple Microsoft Edge instances that each has a single tab

Explanation:



Answer Area

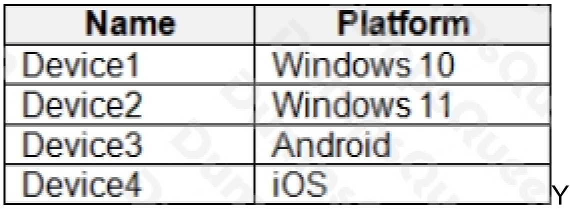
Users **[answer choice]**.

- [✓ can access any URL]
- cannot view the address bar in Microsoft Edge
- can only access URLs that include contoso.com
- can only access URLs that start with https://contoso.com

Windows 10 and later devices can have **[answer choice]**.

- a single Microsoft Edge instance that has a single tab
- [✓ a single Microsoft Edge instance that has multiple tabs]
- multiple Microsoft Edge instances that have multiple tabs
- multiple Microsoft Edge instances that each has a single tab

QUESTION NO: 9



Name	Platform
Device1	Windows 10
Device2	Windows 11
Device3	Android
Device4	iOS

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

On which devices can you apply app configuration policies?

A. Device2 only

B. Device1 and Device2 only

C. Device3 and Device4 only

D. Device2, Device3, and Device4 only

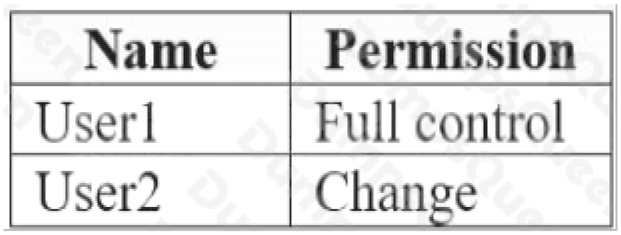
E. Device1, Device2, Device3, and Device4

ANSWER: C

Explanation:

QUESTION NO: 10

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:

Reference:

https://www.varonis.com/blog/ntfs-permissions-vs-share/