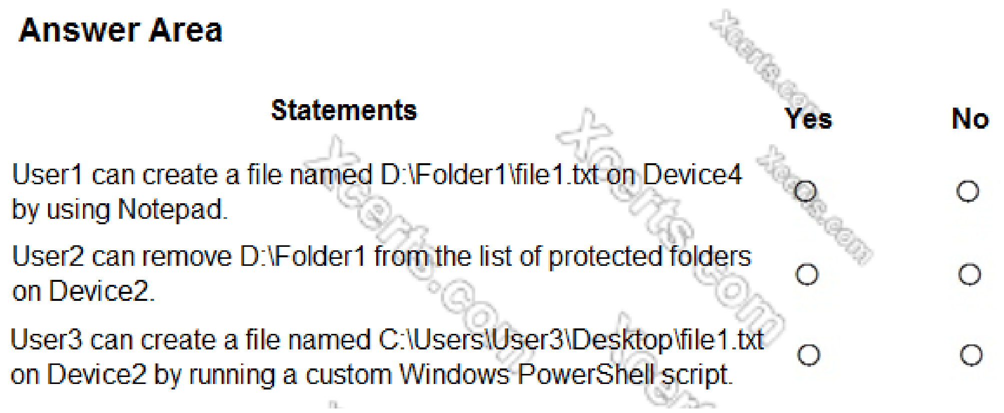
Endpoint Administrator (beta)

1. For each of the following statements, select Yes if the statement is true. Otherwise, select No.
NOTE: Each correct selection is worth one point.



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.	○	○

A. See Explanation section for answer.

Answer(s): A

---

2. Which devices are registered by using the Windows Autopilot deployment service?

A. Device1 only

B. Device3 only

C. Device1 and Device3 only

D. Device1, Device2, and Device3

Answer(s): A

---

3. You implement Boundary1 based on the planned changes.
Which devices have a network boundary of 192.168.1.0/24 applied?

A. Device2 only

B. Device3 only

C. Device1, Device2, and Device5 only

D. Device1, Device2, Device3, and Device4 only

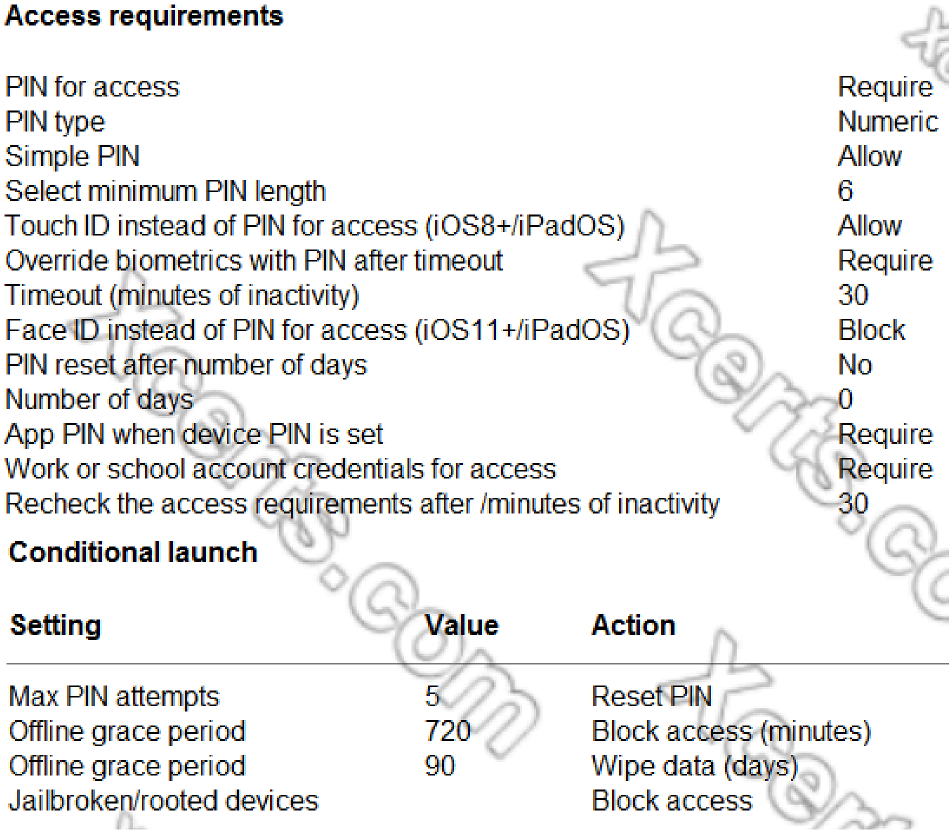
Answer(s): D

4. HOTSPOT (Drag and Drop is not supported)

You have a Microsoft 365 subscription.

You use Microsoft Intune Suite to manage devices.

You have the iOS app protection policy shown in the following exhibit.



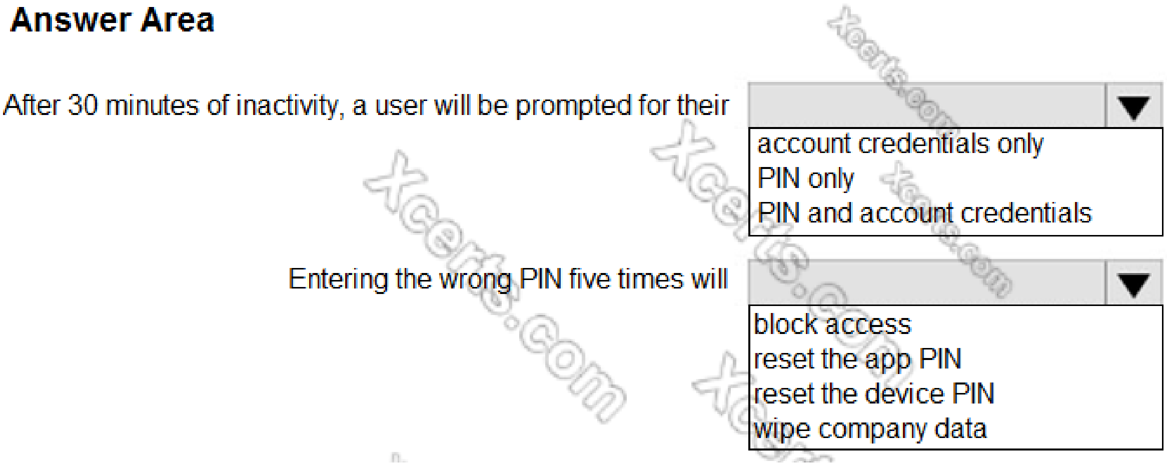
Access requirements

PIN for access	Require
PIN type	Numeric
Simple PIN	Allow
Select minimum PIN length	6
Touch ID instead of PIN for access (iOS8+/iPadOS)	Allow
Override biometrics with PIN after timeout	Require
Timeout (minutes of inactivity)	30
Face ID instead of PIN for access (iOS11+/iPadOS)	Block
PIN reset after number of days	No
Number of days	0
App PIN when device PIN is set	Require
Work or school account credentials for access	Require
Recheck the access requirements after /minutes of inactivity	30

Conditional launch

Setting	Value	Action
Max PIN attempts	5	Reset PIN
Offline grace period	720	Block access (minutes)
Offline grace period	90	Wipe data (days)
Jailbroken/rooted devices		Block access

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

After 30 minutes of inactivity, a user will be prompted for their

Entering the wrong PIN five times will

A. See Explanation section for answer.

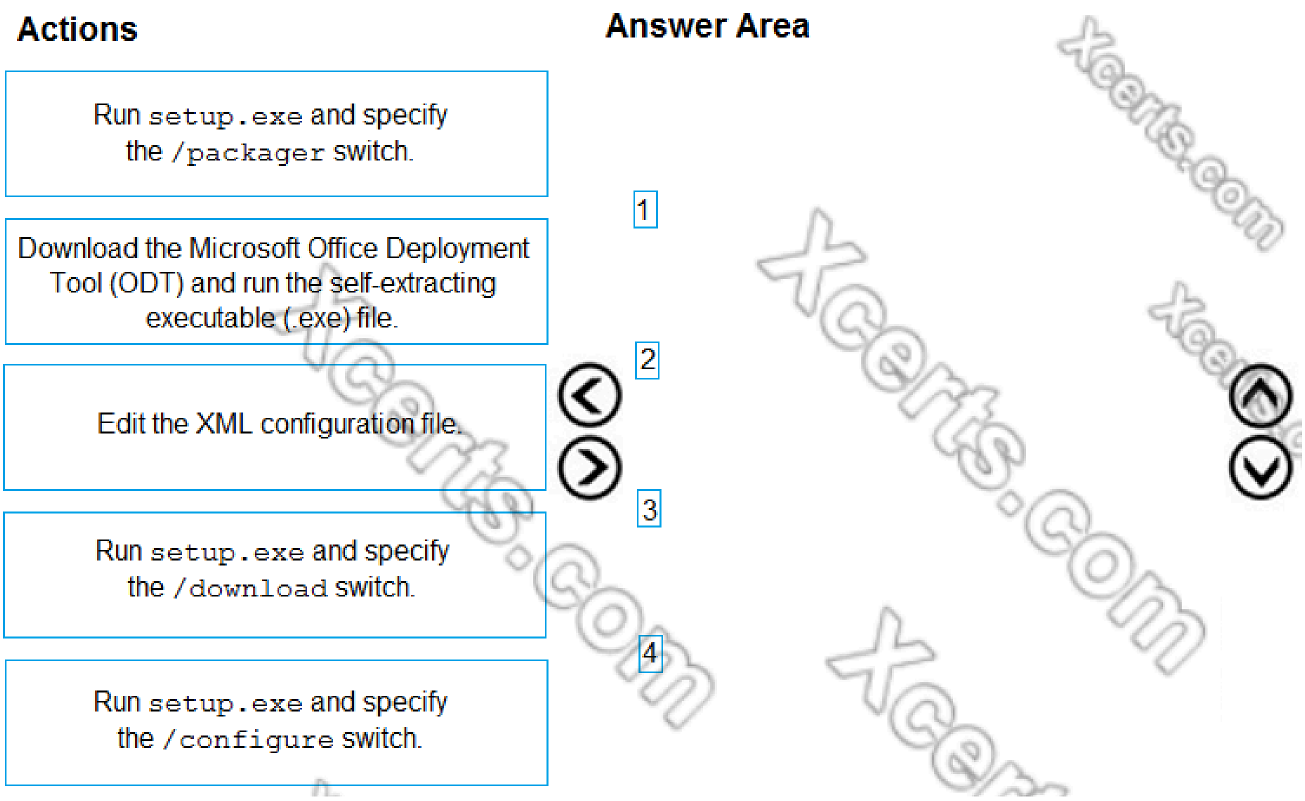
Answer(s): A

5. DRAG DROP (Drag and Drop is not supported)

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

1

2

3

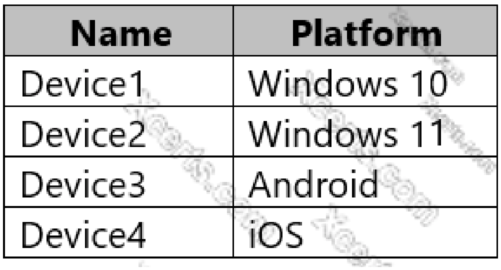
4

A. See Explanation section for answer.

Answer(s): A

---

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



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

On which devices can you apply app configuration policies?

A. Device2 only

B. Device1 and Device2 only

C. Device3 and Device4 only

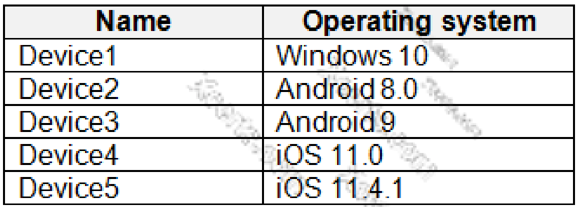
D. Device2, Device3, and Device4 only

E. Device1, Device2, Device B, and Device4

Answer(s): D

7. HOTSPOT (Drag and Drop is not supported)

You have an Azure AD tenant named contoso.com that contains the devices shown in the following table.

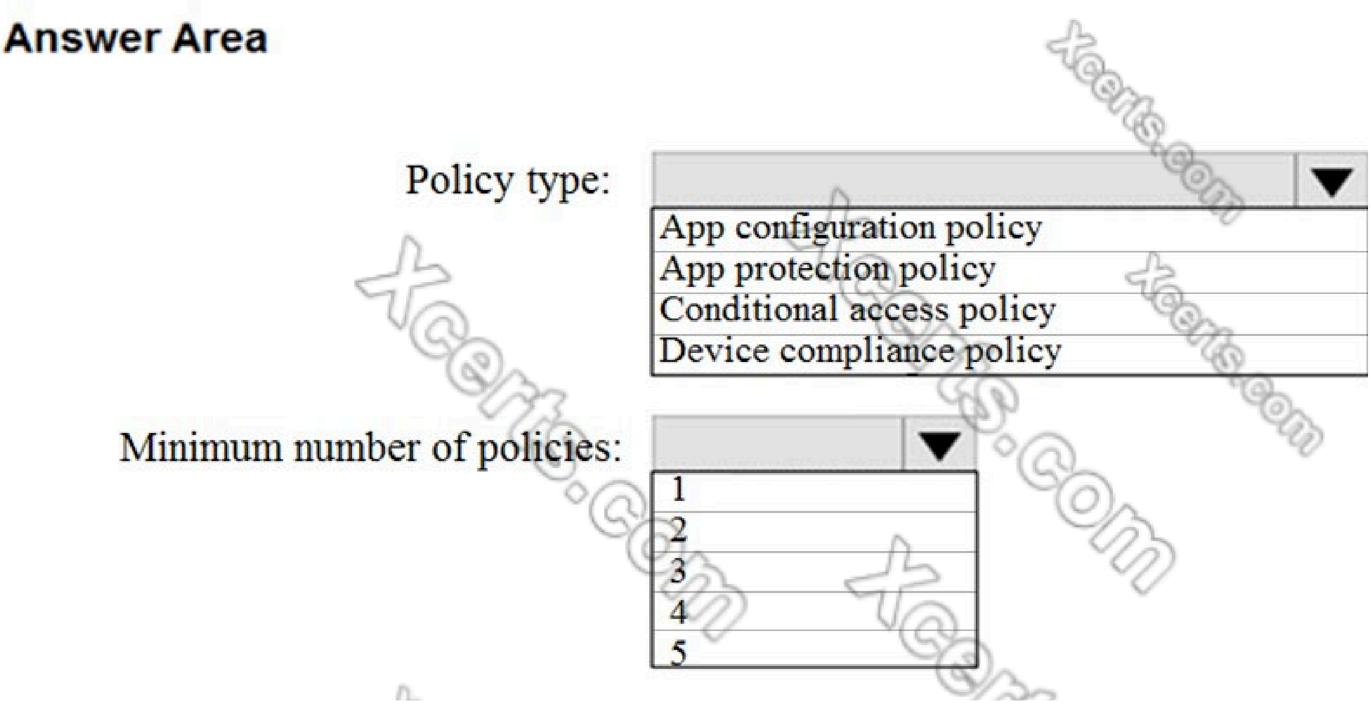


Name	Operating system
Device1	Windows 10
Device2	Android 8.0
Device3	Android 9
Device4	iOS 11.0
Device5	iOS 11.4.1

AH devices contain an app named App1 and are enrolled in Microsoft Intune.

You need to prevent users from copying data from App1 and pasting the data into other apps. Which type of policy and how many policies should you create in Intune? To answer, select the appropriate options in the answer area.

NOTE: Each correct selection is worth one point.



Answer Area

Policy type: ▼

- App configuration policy
- App protection policy
- Conditional access policy
- Device compliance policy

Minimum number of policies: ▼

- 1
- 2
- 3
- 4
- 5

A. See Explanation section for answer.

Answer(s): A

8. You have a Microsoft 365 subscription that uses Microsoft Intune Suite. You use Microsoft Intune to manage devices.

You plan to deploy two apps named App1 and App2 to all Windows devices. Appl must be installed before App2.

From the Intune admin center, you create and deploy two Windows app (Win32) apps. You need to ensure that App1 is installed before App2 on every device.

What should you configure?

A. the App1 deployment configurations

B. a dynamic device group

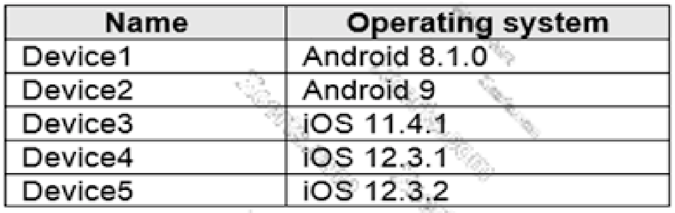
C. a detection rule

D. the App2 deployment configurations

Answer(s): D

---

9. You have a Microsoft Intune subscription.
You have devices enrolled in intune as shown in the following table.



Name	Operating system
Device1	Android 8.1.0
Device2	Android 9
Device3	iOS 11.4.1
Device4	iOS 12.3.1
Device5	iOS 12.3.2

An app named App1 is installed on each device.
What is the minimum number of app configuration policies required to manage Appl?

A. 1

B. 2

C. 3

D. 4

E. 5

Answer(s): B

---

10. You have a Microsoft 365 E5 subscription that contains 100 iOS devices enrolled in Microsoft Intune. You need to deploy a custom line-of-business (LOB) app to the devices by using Intune.
Which extension should you select for the app package file?

A. .intunemac

B. .ipa

C. .apk

D. .appx

Answer(s): B

---

11. You have a Microsoft 365 E5 subscription that contains a user named User! and a web app named Appl.
App1 must only accept modern authentication requests.
You plan to create a Conditional Access policy named CAPolicy1 that will have the following settings:
-Assignments
-Users or workload identities: User1
-Cloud apps or actions: App1
-Access controls
-Grant: Block access
You need to block only legacy authentication requests to Appl. Which condition should you add to CAPolicy1?

A. Filter for devices

B. Device platforms

C. User risk

D. Sign-in risk

E. Client apps

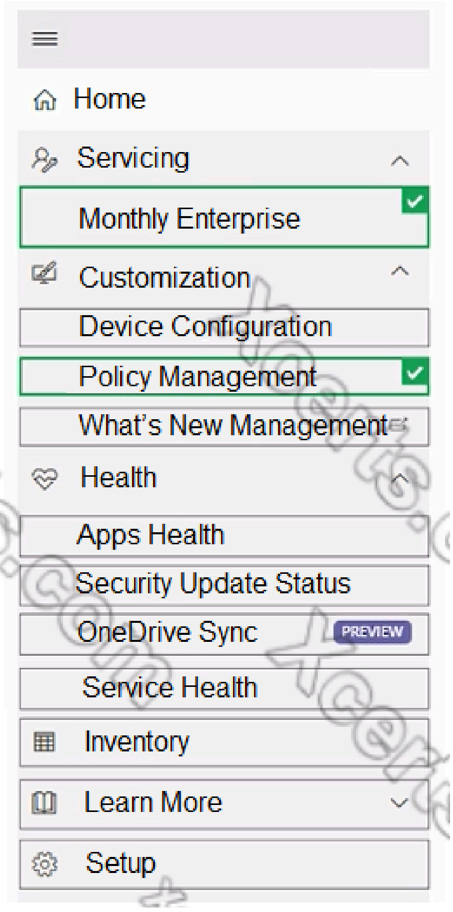
Answer(s): E

---

12. HOTSPOT (Drag and Drop is not supported)
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



A. See Explanation section for answer.

Answer(s): A

---

13. You have a Microsoft 365 subscription.
You have 10 computers that run Windows 10 and are enrolled in mobile device management (MDM).
You need to deploy the Microsoft 36S Apps for enterprise suite to all the computers. What should you do?

A. From the Microsoft Intune admin center, create a Windows 10 device profile.

B. From Azure AD, add an app registration.

C. From Azure AD. add an enterprise application.

D. From the Microsoft Intune admin center, add an app.

Answer(s): D

---

14. You have a Microsoft 365 subscription that uses Microsoft Intune Suite. You use Microsoft Intune to manage devices.
You have a Windows 11 device named Device1 that is enrolled in Intune. Device1 has been offline for 30

days.
You need to remove Device1 from Intune immediately. The solution must ensure that if the device checks in again, any apps and data provisioned by Intune are removed. User-installed apps, personal data, and OEM-installed apps must be retained.
What should you use?

A. a Delete action

B. a Retire action

C. a Fresh Start action

D. an Autopilot Reset action

Answer(s): A

---

15. You have a Microsoft 365 subscription that uses Microsoft Intune Suite. You use Microsoft Intune to manage devices.
You need to review the startup times and restart frequencies of the devices. What should you use?

A. Azure Monitor

B. intune Data Warehouse

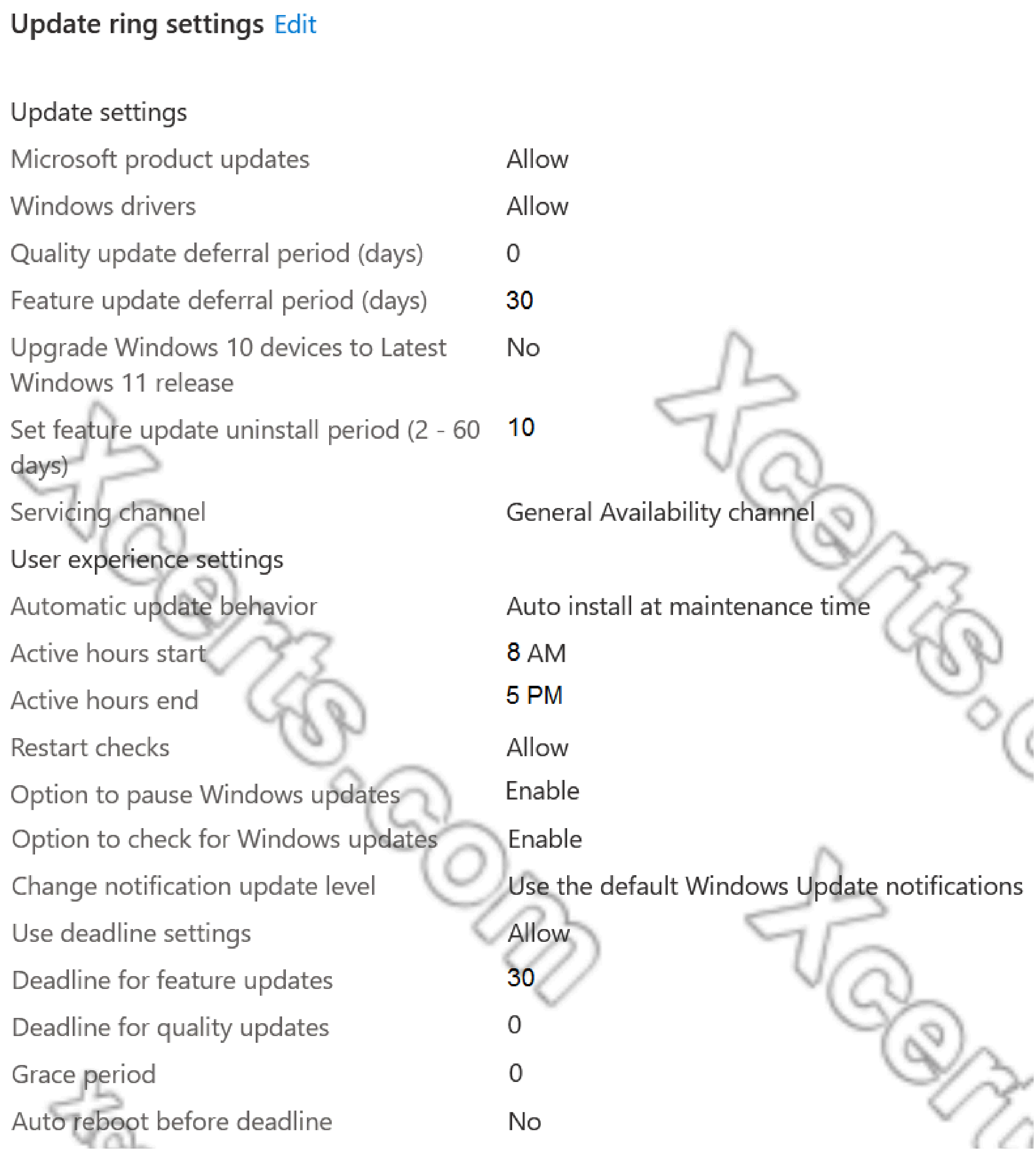
C. Microsoft Defender for Endpoint

D. Endpoint analytics

Answer(s): D

---

16. HOTSPOT (Drag and Drop is not supported)
You have a Microsoft 365 E5 subscription.
You create a new update rings policy named Policy1 as shown in the following exhibit.



Update ring settings Edit

Update settings

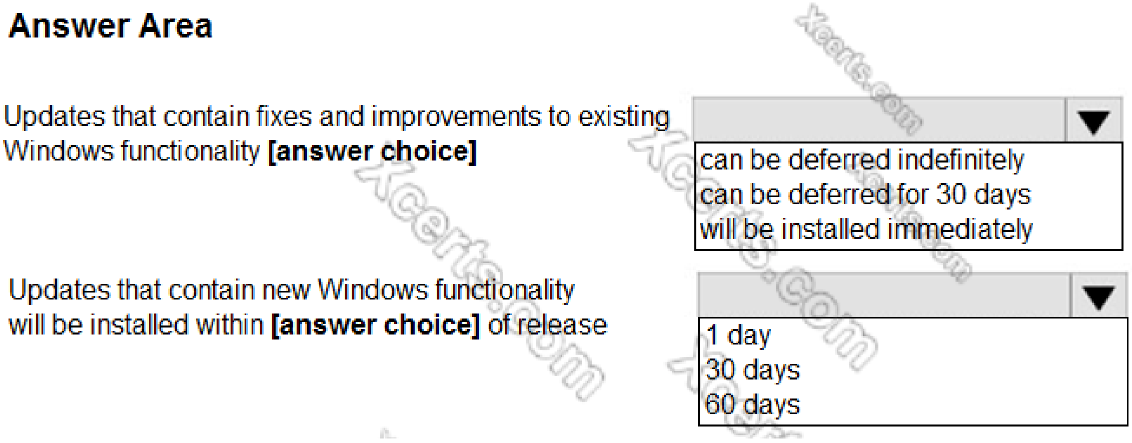
Microsoft product updates	Allow
Windows drivers	Allow
Quality update deferral period (days)	0
Feature update deferral period (days)	30
Upgrade Windows 10 devices to Latest Windows 11 release	No
Set feature update uninstall period (2 - 60 days)	10
Servicing channel	General Availability channel

User experience settings

Automatic update behavior	Auto install at maintenance time
Active hours start	8 AM
Active hours end	5 PM
Restart checks	Allow
Option to pause Windows updates	Enable
Option to check for Windows updates	Enable
Change notification update level	Use the default Windows Update notifications
Use deadline settings	Allow
Deadline for feature updates	30
Deadline for quality updates	0
Grace period	0
Auto reboot before deadline	No

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

Updates that contain fixes and improvements to existing Windows functionality **[answer choice]**

- can be deferred indefinitely
- can be deferred for 30 days
- will be installed immediately

Updates that contain new Windows functionality will be installed within **[answer choice]** of release

- 1 day
- 30 days
- 60 days

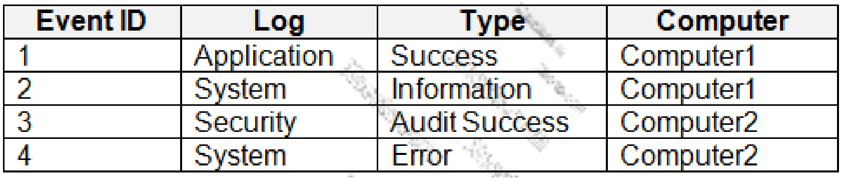
A. See Explanation section for answer.

Answer(s): A

---

17. You have computer that run Windows 10 and connect to an Azure Log Analytics workspace. The workspace is configured to collect all available events from Windows event logs.

The computers have the logged events shown in the following table.



Event ID	Log	Type	Computer
1	Application	Success	Computer1
2	System	Information	Computer1
3	Security	Audit Success	Computer2
4	System	Error	Computer2

Which events are collected in the Log Analytics workspace?

A. 1 only

B. 2 and 3 only

C. 1 and 3 only

D. 1, 2, and 4 on

E. 1, 2, 3, and 4

Answer(s): D

---

18. 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

Answer(s): D

---

19. 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(s): D

---

20. 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(s): D E