Question #1*Topic 1*

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 are deploying Microsoft Endpoint Manager.
You successfully enroll Windows 10 devices in Endpoint Manager.
When you try to enroll an iOS device in Endpoint Manager, you get an error.
You need to ensure that you can enroll the iOS device in Endpoint Manager.
Solution: You add your user account as a device enrollment manager.
Does this meet the goal?

- A. Yes
- B. No

Question #2*Topic 1*

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 are deploying Microsoft Endpoint Manager.
You successfully enroll Windows 10 devices in Endpoint Manager.
When you try to enroll an iOS device in Endpoint Manager, you get an error.
You need to ensure that you can enroll the iOS device in Endpoint Manager.
Solution: You configure the Apple MDM Push certificate.
Does this meet the goal?

- A. Yes
- B. No

Question #3*Topic 1*

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 are deploying Microsoft Endpoint Manager.
You successfully enroll Windows 10 devices in Endpoint Manager.
When you try to enroll an iOS device in Endpoint Manager, you get an error.
You need to ensure that you can enroll the iOS device in Endpoint Manager.
Solution: You create an Apple Configurator enrollment profile.
Does this meet the goal?

- A. Yes
- B. No

Question #4*Topic 1*

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 network contains an Active Directory domain named contoso.com that is synced to Microsoft Azure Active Directory (Azure AD).
You manage Windows 10 devices by using Microsoft System Center Configuration Manager (Current Branch).
You configure pilot co-management.
You add a new device named Device1 to the domain. You install the Configuration Manager client on Device1.
You need to ensure that you can manage Device1 by using Microsoft Intune and Configuration Manager.
Solution: You create a device configuration profile from the Device Management admin center.
Does this meet the goal?

- A. Yes
- B. No

Question #5*Topic 1*

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 network contains an Active Directory domain named contoso.com that is synced to Microsoft Azure Active Directory (Azure AD).
You manage Windows 10 devices by using Microsoft System Center Configuration Manager (Current Branch).
You configure pilot co-management.
You add a new device named Device1 to the domain. You install the Configuration Manager client on Device1.
You need to ensure that you can manage Device1 by using Microsoft Intune and Configuration Manager.
Solution: You add Device1 to an Active Directory group.
Does this meet the goal?

- A. Yes
- B. No

Question #6*Topic 1*

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 network contains an Active Directory domain named contoso.com that is synced to Microsoft Azure Active Directory (Azure AD).
You manage Windows 10 devices by using Microsoft System Center Configuration Manager (Current Branch).
You configure pilot co-management.
You add a new device named Device1 to the domain. You install the Configuration Manager client on Device1.
You need to ensure that you can manage Device1 by using Microsoft Intune and Configuration Manager.
Solution: You unjoin Device1 from the Active Directory domain.
Does this meet the goal?

- A. Yes
- B. No

Question #7*Topic 1*

HOTSPOT -

Your network contains an Active Directory forest named contoso.com that is synced to Microsoft Azure Active Directory (Azure AD).

You use Microsoft Endpoint Configuration Manager for device management.

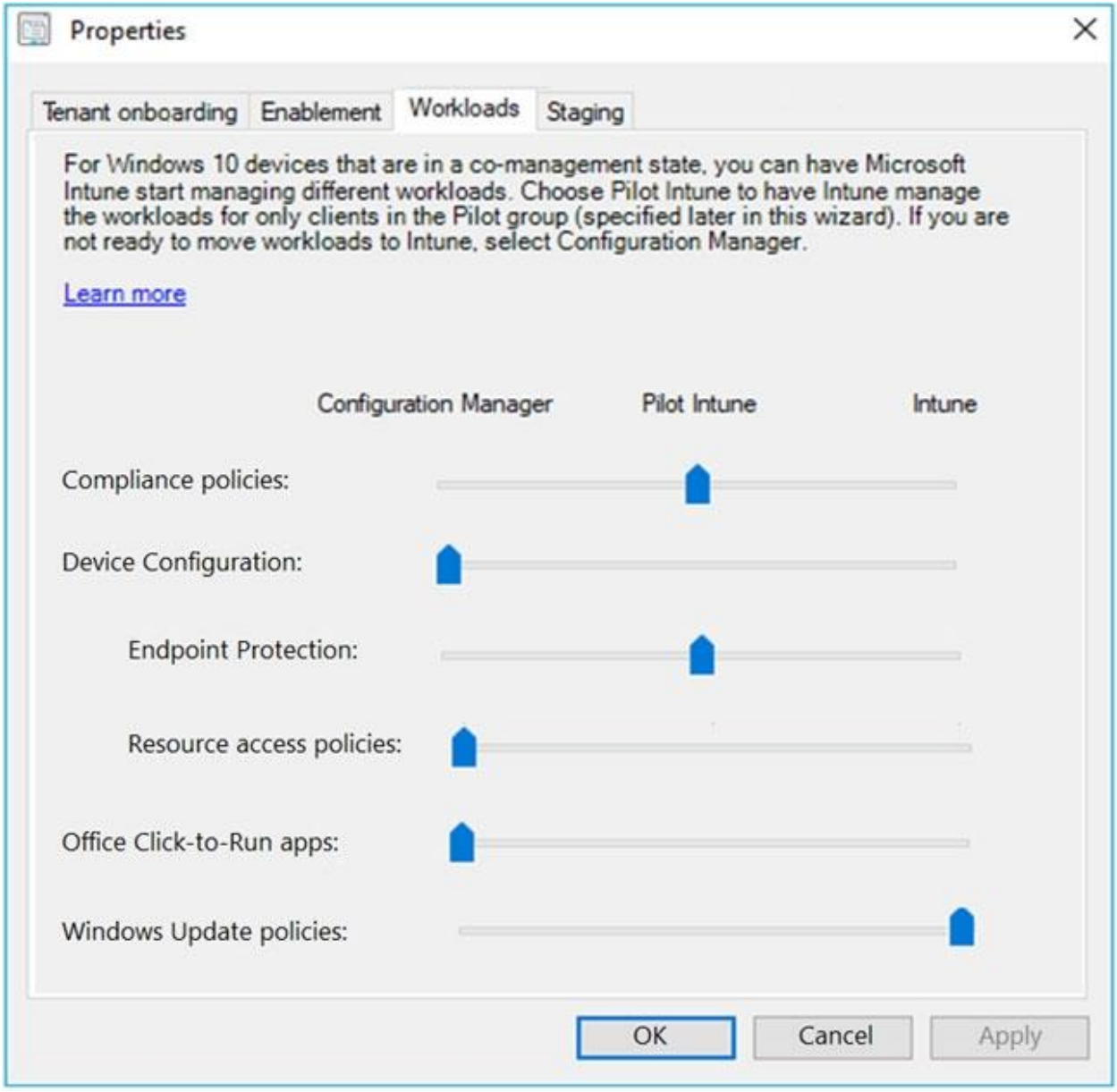
You have the Windows 10 devices shown in the following table.

Name	Collection
Device1	Collection1
Device2	Collection2

You configure Endpoint Configuration Manager co-management as follows:

- Automatic enrollment in Intune: Pilot
- Pilot collection for all workloads: Collection2

You configure co-management workloads as shown in the following exhibit.



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
Microsoft Intune manages the compliance policies for Device1.	○	◯
Configuration Manager manages the Windows Update policies for Device1.	○	◯
Microsoft Intune manages Endpoint Protection for Device2.	◯	○

Question #8 *Topic 1*

HOTSPOT -

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

Name	Platform	Member of
Device1	Windows 10	Group1
Device2	Android	Group2, Group3
Device3	Windows 10	Group2, Group3

The device compliance policies in Intune are configured as shown in the following table.

Name	Platform	Assigned
Policy1	Windows 10 and later	Yes
Policy2	Android	No
Policy3	Windows 10 and later	Yes

The device compliance policies have the assignments shown in the following table.

Name	Include	Exclude
Policy1	Group3	*None*
Policy2	Group2	Group3

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
Policy1 applies to Device3.	○	○
Policy2 applies to Device2.	○	○

Question #9 *Topic 1*

You have Windows 10 Pro devices that are joined to an Active Directory domain.

You plan to create a Microsoft 365 tenant and to upgrade the devices to Windows 10 Enterprise.

You are evaluating whether to deploy Windows Hello for Business.

What are two prerequisites of the deployment? Each correct answer presents a complete solution.

NOTE: Each correct selection is worth one point.

- A. Microsoft Endpoint Manager enrollment
- B. Microsoft Azure Active Directory (Azure AD)
- C. smartcards
- D. TPM-enabled devices

Question #10 *Topic 1*

You have a Microsoft 365 tenant.
All users are assigned the Enterprise Mobility + Security license.
You need to ensure that when users join their device to Microsoft Azure Active Directory (Azure AD), the device is enrolled in Microsoft Endpoint Manager automatically.
What should you configure?

- A. Enrollment restrictions from the Endpoint Manager admin center
- B. device enrollment managers from the Endpoint Manager admin center
- C. MAM User scope from the Azure Active Directory admin center
- D. MDM User scope from the Azure Active Directory admin center

Question #11 *Topic 1*

HOTSPOT -
You have several devices enrolled in Microsoft Endpoint Manager.
You have a Microsoft Azure Active Directory (Azure AD) tenant that includes the users shown in the following table.

Name	Member of
User1	Group1
User2	Group1, Group2
User3	**None**

The device type restrictions in Endpoint Manager are configured as shown in the following table.

Priority	Name	Allowed platform	Assigned to
1	Policy1	Android, iOS, Windows (MDM)	**None**
2	Policy2	Windows (MDM)	Group2
3	Policy3	Android, iOS	Group1
Default	All users	Android, Windows (MDM)	All users

You add User3 as a device enrollment manager in Endpoint Manager.
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 enroll Windows devices in Endpoint Manager.	○	○
User2 can enroll Android devices in Endpoint Manager.	○	○
User3 can enroll iOS devices in Endpoint Manager.	○	○

Question #12 *Topic 1*

- HOTSPOT -
  You create two device compliance policies for Android devices as shown in the following table.

Policy	Configuration	Action	Assigned to
Policy1	Require encryption of the data storage on the device.	Mark as noncompliant immediately.	Group1
Policy2	Require Google Play services.	Mark as noncompliant immediately.	Group2

  You have the Android devices shown in the following table.

Name	User	Configuration
Android1	User1	Not encrypted
Android2	User2	Google Play services not configured
Android3	User3	Not encrypted Google Play services configured

  The users belong to the groups shown in the following table.

User	Group
User1	Group1
User2	Group1, Group2
User3	Group2

  The users enroll their device in Microsoft Endpoint Manager.
  For each of the following statements, select Yes if the statement is true. Otherwise, select No.
  NOTE: Each correct selection is worth one point.

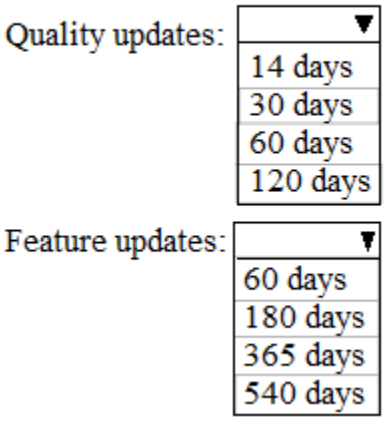
Answer Area

Statements	Yes	No
The device of User1 is compliant.	○	○
The device of User2 is compliant.	○	○
The device of User3 is compliant.	○	○

Question #13*Topic 1*

HOTSPOT -
Your network contains an Active Directory domain named contoso.com. All client devices run Windows 10 and are joined to the domain.
You update the Windows 10 devices by using Windows Update for Business.
What is the maximum amount of time you can defer Windows 10 updates? To answer, select the appropriate options in the answer area.
NOTE: Each correct selection is worth one point.
Hot Area:

Answer Area



Feature Updates: 365 Quality Updates: 30

Question #14*Topic 1*

Your company uses Microsoft Endpoint Configuration Manager and Microsoft Endpoint Manager to co-manage devices.
Which two actions can be performed only from Endpoint Manager? Each correct answer presents a complete solution.
NOTE: Each correct selection is worth one point.

- A. Deploy applications to Windows 10 devices.
- B. Deploy VPN profiles to iOS devices.
- C. Deploy VPN profiles to Windows 10 devices.
- D. Publish applications to Android devices.

Question #15 *Topic 1*

HOTSPOT -
Your network contains an Active Directory domain named contoso.com that uses Microsoft System Center Configuration Manager (Current Branch).
You have Windows 10 and Windows 8.1 devices.
You need to ensure that you can analyze the upgrade readiness of all the Windows 8.1 devices and analyze the update compliance of all the Windows 10 devices.
What should you do? To answer, select the appropriate options in the answer area.
NOTE: Each correct selection is worth one point.

Answer Area

First action to perform:

- Enroll the devices in Microsoft Intune.
- Configure device compliance in Microsoft Intune.
- Create a Microsoft Azure Log Analytics workspace.
- Add an alias (CNAME) record to the DNS zone of contoso.com.

Second action to perform:

- Configure all the devices to have a commercial ID.
- Configure software inventory in Configuration Manager.
- Configure all the devices to join the Windows Insider Program.
- Configure and restart the Windows Update service on all the devices.

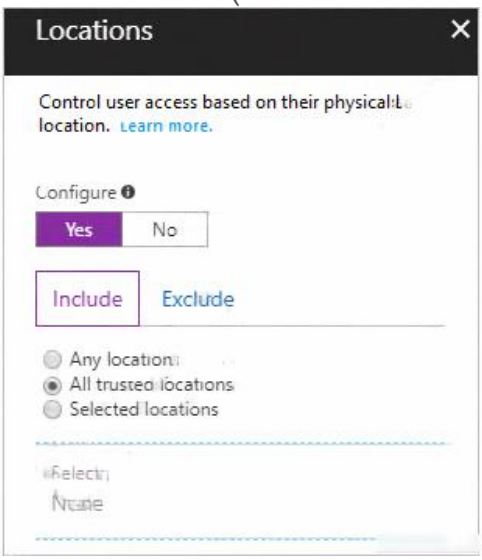
Question #16 *Topic 1*

You have a Microsoft Azure Active Directory (Azure AD) tenant named contoso.onmicrosoft.com.
You have a Microsoft 365 subscription.
You need to ensure that administrators can manage the configuration settings for all the Windows 10 devices in your organization.
What should you configure?

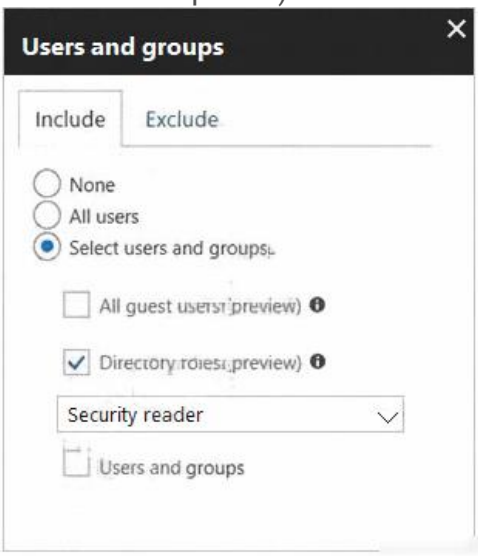
- A. the Enrollment restrictions
- B. the mobile device management (MDM) authority Most Voted
- C. the Exchange on-premises access settings
- D. the Windows enrollment settings

Question #17*Topic 1*

You configure a conditional access policy. The locations settings are configured as shown in the Locations exhibit. (Click the Locations tab.)



The users and groups settings are configured as shown in the Users and Groups exhibit. (Click Users and Groups tab.)



Members of the Security reader group report that they cannot sign in to Microsoft Active Directory (Azure AD) on their device while they are in the office.

You need to ensure that the members of the Security reader group can sign in in to Azure AD on their device while they are in the office. The solution must use the principle of least privilege.

What should you do?

- A. From the conditional access policy, configure the device state.
- B. From the Azure Active Directory admin center, create a custom control.
- C. From the Endpoint Manager admin center, create a device compliance policy.
- D. From the Azure Active Directory admin center, create a named location.

Question #18*Topic 1*

You have computers that run Windows 10 Enterprise and are joined to the domain.
You plan to delay the installation of new Windows builds so that the IT department can test application compatibility.
You need to prevent Windows from being updated for the next 30 days.
Which two Group Policy settings should you configure? Each correct answer presents part of the solution.
NOTE: Each correct selection is worth one point.

- A. Select when Quality Updates are received
- B. Select when Preview Builds and Feature Updates are received
- C. Turn off auto-restart for updates during active hours
- D. Manage preview builds
- E. Automatic updates detection frequency

Question #19*Topic 1*

HOTSPOT -
You have three devices enrolled in Microsoft Endpoint Manager as shown in the following table.

Name	Platform	BitLocker Drive Encryption (BitLocker)	Member of
Device1	Windows 10	Disabled	Group1, Group2
Device2	Windows 10	Disabled	Group2, Group3
Device3	Windows 10	Disabled	Group3

The device compliance policies in Endpoint Manager are configured as shown in the following table.

Name	Require BitLocker	Mark noncompliant after (days)	Assigned
Policy1	Require	5	No
Policy2	Require	10	Yes
Policy3	Non configured	15	Yes

The device compliance policies have the assignments shown in the following table.

Name	Assigned to
Policy2	Group2
Policy3	Group3

Answer Area

Statements	Yes	No
Device1 is marked as noncompliant after 10 days.	○	○
Device2 is marked as noncompliant after 10 days.	○	○
Device3 is marked as noncompliant after 15 days.	○	○

Question #20*Topic 1*

You have a Microsoft Azure Active Directory (Azure AD) tenant named contoso.com.
You need to provide a user with the ability to sign up for Microsoft Store for Business for contoso.com. The solution must use the principle of least privilege.
Which role should you assign to the user?

- A. Cloud application administrator
- B. Application administrator
- C. Global administrator **Most Voted**
- D. Service administrator

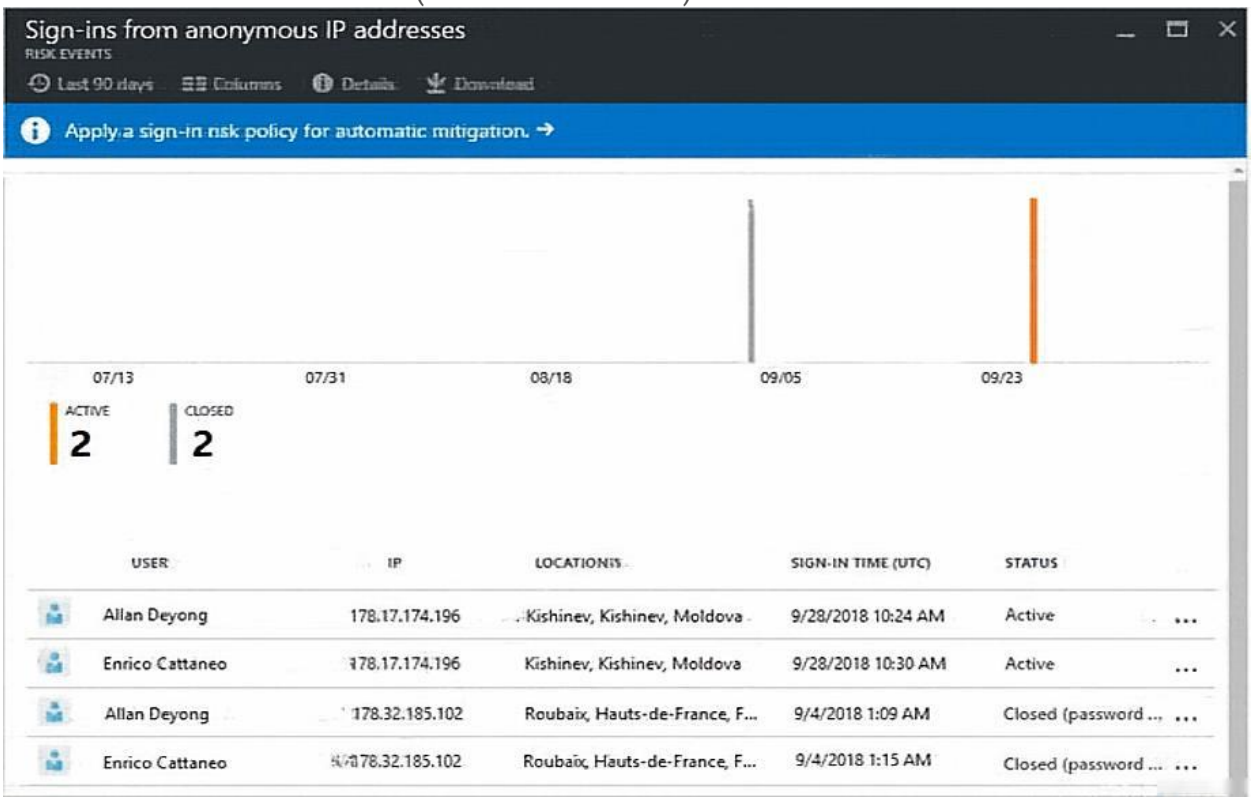
Question #22*Topic 1*

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 network contains an Active Directory domain named contoso.com that is synced to Microsoft Azure Active Directory (Azure AD).
You manage Windows 10 devices by using Microsoft System Center Configuration Manager (Current Branch).
You configure pilot co-management.
You add a new device named Device1 to the domain. You install the Configuration Manager client on Device1.
You need to ensure that you can manage Device1 by using Microsoft Intune and Configuration Manager.
Solution: You add Device1 to a Configuration Manager device collection.
Does this meet the goal?

- A. Yes
- B. No **Most Voted**

Question #23*Topic 1*

From the Microsoft Azure Active Directory (Azure AD) Identity Protection dashboard, you view the risk events shown in the exhibit. (Click the Exhibit tab.)



You need to reduce the likelihood that the sign-ins are identified as risky.
What should you do?

- A. From the Security & Compliance admin center, create a classification label.
- B. From the Security & Compliance admin center, add the users to the Security Readers role group.
- C. From the Azure Active Directory admin center, configure the trusted IPs for multi-factor authentication.
- D. From the Conditional access blade in the Azure Active Directory admin center, create named locations

Question #24 *Topic 1*

Your company has a Microsoft 365 E5 subscription.
Users in the research department work with sensitive data.
You need to prevent the research department users from accessing potentially unsafe websites by using hyperlinks embedded in email messages and documents.
Users in other departments must not be restricted.
What should you do?

- A. Create a data loss prevention (DLP) policy that has a Content is shared condition.
- B. Modify the default safe links policy.
- C. Create a data loss prevention (DLP) policy that has a Content contains condition.
- D. Create a new safe links policy.

Question #25 *Topic 1*

You have a Microsoft 365 tenant.
You have a line-of-business application named App1 that users access by using the My Apps portal.
After some recent security breaches, you implement a conditional access policy for App1 that uses Conditional Access App Control.
You need to be alerted by email if impossible travel is detected for a user of App1. The solution must ensure that alerts are generated for App1 only.
What should you do?

- A. From Microsoft Cloud App Security, create a Cloud Discovery anomaly detection policy. Most Voted
- B. From Microsoft Cloud App Security, modify the impossible travel alert policy.
- C. From Microsoft Cloud App Security, create an app discovery policy.
- D. From the Azure Active Directory admin center, modify the conditional access policy.

Question #26 *Topic 1*

A user receives the following message when attempting to sign in to https://myapps.microsoft.com:
ג€Your sign-in was blocked. We've detected something unusual about this sign-in. For example, you might be signing in from a new location, device, or app. Before you can continue, we need to verify your identity. Please contact your admin.ג€
Which configuration prevents the users from signing in?

- A. Microsoft Azure Active Directory (Azure AD) Identity Protection policies Most Voted
- B. Microsoft Azure Active Directory (Azure AD) conditional access policies
- C. Endpoint Manager compliance policies
- D. Security & Compliance data loss prevention (DLP) policies

Question #27 *Topic 1*

- HOTSPOT -
  You have the Microsoft Azure Active Directory (Azure AD) users shown in the following table.

Name	Member of
User1	Group1
User2	Group2

Your company uses Microsoft Intune.
Several devices are enrolled in Intune as shown in the following table.

Name	Platform	BitLocker Drive Encryption (BitLocker)	Member of
Device1	Windows 10	Disabled	Group3
Device2	Windows 10	Disabled	Group4

The device compliance policies in Intune are configured as shown in the following table.

Name	Require BitLocker	Assigned to
Policy1	Not configured	Group3
Policy2	Require	Group4

You create a conditional access policy that has the following settings:
☞ The Assignments settings are configured as follows:
1. Users and groups: Group1
2. Cloud apps: Microsoft Office 365 Exchange Online
3. Conditions: Include All device state, exclude Device marked as compliant
☞ Access controls is set to Block access.
For each of the following statements, select Yes if the statement is true. Otherwise, select No.

Answer Area

Statements	Yes	No
User1 can access Microsoft Exchange Online from Device1.	○	○
User1 can access Microsoft Exchange Online from Device2.	○	○
User2 can access Microsoft Exchange Online from Device2.	○	○

Question #28*Topic 1*

HOTSPOT -

You have several devices enrolled in Microsoft Endpoint Manager.

You have a Microsoft Azure Active Directory (Azure AD) tenant that includes the users shown in the following table.

Name	Role	Member of
User1	Cloud device administrator	GroupA
User2	Intune administrator	GroupB
User3	**None**	**None**

The device limit restrictions in Endpoint Manager are configured as shown in the following table.

Priority	Name	Device limit	Assigned to
1	Policy1	15	GroupB
2	Policy2	10	GroupA
Default	All users	5	All Users

You add User3 as a device enrollment manager in Endpoint Manager.

For each of the following statements, select Yes if the statement is true. Otherwise, select No.

Answer Area

Statements	Yes	No
User1 can enroll a maximum of 10 devices in Endpoint Manager.	○	○
User2 can enroll a maximum of 10 devices in Endpoint Manager.	○	○
User3 can enroll an unlimited number of devices in Endpoint Manager.	○	○

HOTSPOT -
Your company has a Microsoft 365 tenant.
You plan to allow users that are members of a group named Engineering to enroll their mobile device in mobile device management (MDM).
The device type restrictions are configured as shown in the following table.

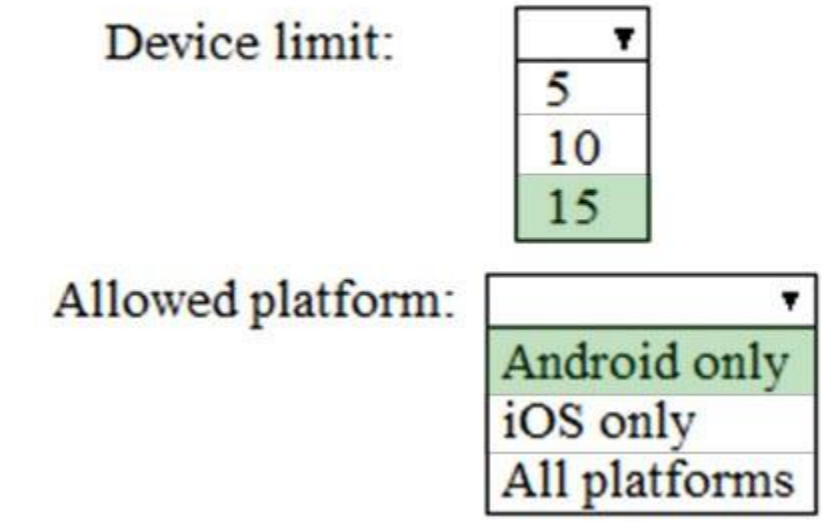
Priority	Name	Allowed platform	Assigned to
1	iOS	iOS	Marketing
2	Android	Android	Engineering
Default	All users	All platforms	All users

The device limit restrictions are configured as shown in the following table.

Priority	Name	Device limit	Assigned to
1	Engineering	15	Engineering
2	West Region	5	Engineering
Default	All users	10	All users

What is the effective configuration for the members of the Engineering group? To answer, select the appropriate options in the answer area.

Answer Area



Question #30*Topic 1*

Your network contains an Active Directory domain named contoso.com. The domain contains 100 Windows 8.1 devices.
You plan to deploy a custom Windows 10 Enterprise image to the Windows 8.1 devices.
You need to recommend a Windows 10 deployment method.
What should you recommend?

- A. a provisioning package
- B. an in-place upgrade
- C. wipe and load refresh **Most Voted**
- D. Windows Autopilot

Question #31*Topic 1*

You use Microsoft System Center Configuration Manager (Current Branch) to manage devices.
Your company uses the following types of devices:

- Windows 10
- Windows 8.1
- Android
- iOS

Which devices can be managed by using co-management?

- A. Windows 10 and Windows 8.1 only
- B. Windows 10, Android, and iOS only
- C. Windows 10 only
- D. Windows 10, Windows 8.1, Android, and iOS

HOTSPOT -
You have three devices enrolled in Microsoft Endpoint Manager as shown in the following table.

Name	Platform	BitLocker Drive Encryption (BitLocker)	Member of
Device1	Windows 10	Disabled	Group3
Device2	Windows 10	Disabled	Group2, Group3
Device3	Windows 10	Disabled	Group2

The device compliance policies in Endpoint Manager are configured as shown in the following table.

Name	Platform	Require BitLocker	Assigned
Policy1	Windows 10 and later	Require	Yes
Policy2	Windows 10 and later	Not configured	Yes
Policy3	Windows 10 and later	Require	No

The device compliance policies have the assignments shown in the following table.

Name	Assigned to
Policy1	Group3
Policy2	Group2

Answer Area

Statements	Yes	No
Device1 is compliant.	○	◯
Device2 is compliant.	○	◯
Device3 is compliant.	◯	○

Question #33 *Topic 1*

Your company has a Microsoft 365 E3 subscription.
All devices run Windows 10 Pro and are joined to Microsoft Azure Active Directory (Azure AD).
You need to change the edition of Windows 10 to Enterprise the next time users sign in to their computer. The solution must minimize downtime for the users.
What should you use?

- A. Windows Autopilot
- B. Windows Update
- C. Subscription Activation
- D. an in-place upgrade

Question #34*Topic 1*

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 network contains an Active Directory domain named contoso.com that is synced to Microsoft Azure Active Directory (Azure AD).
You manage Windows 10 devices by using Microsoft System Center Configuration Manager (Current Branch).
You configure pilot co-management.
You add a new device named Device1 to the domain. You install the Configuration Manager client on Device1.
You need to ensure that you can manage Device1 by using Microsoft Intune and Configuration Manager.
Solution: Define a Configuration Manager device collection as the pilot collection. Add Device1 to the collection.
Does this meet the goal?

- A. Yes
- B. No

Question #36*Topic 1*

Your company has 10 offices.
The network contains an Active Directory domain named contoso.com. The domain contains 500 client computers. Each office is configured as a separate subnet.
You discover that one of the offices has the following:
☞ Computers that have several preinstalled applications
☞ Computers that use nonstandard computer names
☞ Computers that have Windows 10 preinstalled
☞ Computers that are in a workgroup
You must configure all computers in the office to meet the following corporate requirements:
All computers in the office must be joined to the domain.
▪
☞ All computers in the office must have computer names that use a prefix of CONTOSO.
☞ All computers in the office must only have approved corporate applications installed.
You need to recommend a solution to redeploy the computers. The solution must minimize the deployment time.
Which deployment method should you recommend?

- A. a provisioning package Most Voted
- B. wipe and load refresh

- C. Windows Autopilot
- D. an in-place upgrade

Question #37 *Topic 1*

Your company has a Microsoft 365 subscription. The subscription contains 500 devices that run Windows 10 and 100 devices that run iOS.
You need to create Microsoft Endpoint Manager device configuration profiles to meet the following requirements:
☞ Configure Wi-Fi connectivity to a secured network named ContosoNet.
☞ Require passwords of at least six characters to lock the devices.
What is the minimum number of device configuration profiles that you should create?

- A. 4 50% Voted
- B. 2 50% Voted
- C. 1

Question #38 *Topic 1*

Your company has a Microsoft Azure Active Directory (Azure AD) tenant named contoso.com and a Microsoft 365 subscription.
The company recently hired four new users who have the devices shown in the following table.

Name	Operating system
User1	Windows 8
User2	Windows 10
User3	Android 8.0
User4	iOS 11

You configure the Microsoft 365 subscription to ensure that the new devices enroll in Microsoft Endpoint Manager automatically.
Which users have a device that can enroll in Microsoft Endpoint Manager automatically?

- A. User1, User2, User3, and User4
- B. User2 only
- C. User1 and User2 only
- D. User1, User2, and User3 only

Question #39*Topic 1*

Your company has a Microsoft 365 subscription that contains the domains shown in the following table.

Name	Can enroll devices to Microsoft Endpoint Manager by using auto-discovery
Contoso.com	Yes
Contoso.onmicrosoft.com	Yes

The company plans to add a custom domain named fabrikam.com to the subscription, and then to enable enrollment of devices to Endpoint Manager by using auto-discovery for fabrikam.com.
You need to add a DNS record to the fabrikam.com domain to enable device enrollment by using auto-discovery.
Which record type should you use for the new record?

- A. PTR
- B. SRV
- C. CNAME
- D. TXT

Question #40*Topic 1*

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 network contains an on-premises Active Directory domain. The domain contains 2,000 computers that run Windows 8.1 and have applications installed as shown in the following table.

Name	Application count	Used by
App1	20	Finance department, sales department
App2	100	Marketing department

You enroll all the computers in Upgrade Readiness.
You need to ensure that App1 and App2 have an UpgradeDecision status of Ready to upgrade.
Solution: You set the ReadyForWindows status of App2 to Highly adopted.
Does this meet the goal?

- A. Yes
- B. No

Question #41 *Topic 1*

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 network contains an on-premises Active Directory domain. The domain contains 2,000 computers that run Windows 8.1 and have applications installed as shown in the following table.

Name	Application count	Used by
App1	20	Finance department, sales department
App2	100	Marketing department

You enroll all the computers in Upgrade Readiness.
You need to ensure that App1 and App2 have an UpgradeDecision status of Ready to upgrade.
Solution: You set the Importance status of App1 to Business critical.
Does this meet the goal?

- A. Yes
- B. No

Question #42 *Topic 1*

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 network contains an on-premises Active Directory domain. The domain contains 2,000 computers that run Windows 8.1 and have applications installed as shown in the following table.

Name	Application count	Used by
App1	20	Finance department, sales department
App2	100	Marketing department

You enroll all the computers in Upgrade Readiness.
You need to ensure that App1 and App2 have an UpgradeDecision status of Ready to upgrade.
Solution: You set the ReadyForWindows status of App1 to Highly adopted.
Does this meet the goal?

- A. Yes
- B. No Most Voted

Question #43*Topic 1*

HOTSPOT -
You have 100 computers that run Windows 8.1 and are enrolled in Upgrade Readiness.
Two of the computers are configured as shown in the following table.

Name	Architecture	Memory	Applications installed
Computer1	64-bit	1 GB	App1
Computer2	32-bit	2 GB	App2

From Upgrade Readiness, you view the applications shown in the following table.

Name	UpgradeDecision
App1	Ready to upgrade
App2	Review in progress

You enroll a computer named Computer3 in Upgrade Readiness. Computer3 has the following configurations:

- 8 GB of memory
- 64-bit architecture
- An application named App3 installed

App3 is installed on Computer3 only.

Answer Area

Statements	Yes	No
Computer1 has an UpgradeDecision status of Ready to upgrade.	○	○
Computer2 has an UpgradeDecision status of Ready to upgrade.	○	○
Computer3 has an UpgradeDecision status of Ready to upgrade.	○	○

Question #44 *Topic 1*

Your network contains an on-premises Active Directory domain that syncs to Azure Active Directory (Azure AD).
The domain contains two servers named Server1 and Server2 that run Windows Server 2016.
Server1 has the File Server Resource Manager role service installed.
You need to configure Server1 to use the Azure Rights Management (Azure RMS) connector.
You install the Microsoft Management connector on Server1.
What should you do next on Server1?

- A. Run the GenConnectorConfig.ps1 script.
- B. Configure the URL of the AIPMigrated group.
- C. Enable BitLocker Drive Encryption (BitLocker).
- D. Install a certification authority (CA).

Question #45 *Topic 1*

Your company has a Microsoft Azure Active Directory (Azure AD) tenant named contoso.com.
You sign up for Microsoft Store for Business.
The tenant contains the users shown in the following table.

Name	Microsoft Store for Business role	Azure AD role
User1	Purchaser	*None*
User2	Basic Purchaser	*None*
User3	*None*	Application administrator
User4	*None*	Cloud application administrator

Microsoft Store for Business has the following Shopping behavior settings:
☞ Make everyone a Basic Purchaser is set to Off.
☞ Allow app requests is set to On.
You need to identify which users can add apps to the Microsoft Store for Business private store.
Which users should you identify?

- A. User1 and User2 only
- B. User3 only
- C. User1 only Most Voted
- D. User3 and User4 only

Question #46 *Topic 1*

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 network contains an on-premises Active Directory domain. The domain contains 2,000 computers that run Windows 8.1 and have applications installed as shown in the following table.

Name	Application count	Used by
App1	20	Finance department, sales department
App2	100	Marketing department

You enroll all the computers in Upgrade Readiness.
You need to ensure that App1 and App2 have an UpgradeDecision status of Ready to upgrade.
Solution: You set the importance status of App2 to Low install count.
Does this meet the goal?

- A. Yes Most Voted
- B. No

Question #48 *Topic 1*

You have a Microsoft 365 E5 subscription that uses an Azure Active Directory (Azure AD) tenant named contoso.com.
You need to ensure that users can enroll devices in Microsoft Endpoint Manager without manually entering the address of Microsoft Endpoint Manager.
Which two DNS records should you create? Each correct answer presents part of the solution.
NOTE: Each correct selection is worth one point.

- A. a CNAME record for AutoDiscover.contoso.com
- B. a CNAME record for EnterpriseEnrollment.contoso.com
- C. a TXT record for EnterpriseRegistration.contoso.com
- D. an SRV record for _SIP._TLS.contoso.com
- E. an SRV record for _SIPfederationTLS.contoso.com
- F. a CNAME record for EnterpriseRegistration.contoso.com
- G. a TXT record for EnterpriseEnrollment.contoso.com

Question #47*Topic 1*

You have two conditional access policies named Policy1 and Policy2.
Policy1 has the following settings:
☞ Assignments:
- Users and groups: User1
- Cloud apps or actions: Office 365 Exchange Online
- Conditions: 0 conditions selected
☞ Access controls:
- Grant: Grant access
- Session: 0 controls selected
☞ Enable policy: On
Policy2 has the following settings:
☞ Assignments:
- Users and groups: User1
- Cloud apps or actions: Office 365 Exchange Online
- Conditions: 0 conditions selected
☞ Access controls:
- Grant: Block access
- Session: 0 controls selected
☞ Enable policy: On
You need to ensure that User1 can access Microsoft Exchange Online only from devices that are marked as compliant.
What should you do?

- A. Modify the Grant settings of Policy2.
- B. Disable Policy2.
- C. Modify the Conditions settings of Policy2.
- D. Modify the Grant settings of Policy1.

Question #49 *Topic 1*

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 network contains an on-premises Active Directory domain. The domain contains domain controllers that run Windows Server 2019. The functional level of the forest and the domain is Windows Server 2012 R2.
The domain contains 100 computers that run Windows 10 and a member server named Server1 that runs Windows Server 2012 R2.
You plan to use Server1 to manage the domain and to configure Windows 10 Group Policy settings.
You install the Group Policy Management Console (GPMC) on Server1.
You need to configure the Windows Update for Business Group Policy settings on Server1.
Solution: You raise the forest functional level to Windows Server 2016. You copy the Group Policy Administrative Templates from a Windows 10 computer to the
Netlogon share on all the domain controllers.
Does this meet the goal?

- A. Yes
- B. No

Question #50 *Topic 1*

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 network contains an on-premises Active Directory domain. The domain contains domain controllers that run Windows Server 2019. The functional level of the forest and the domain is Windows Server 2012 R2.
The domain contains 100 computers that run Windows 10 and a member server named Server1 that runs Windows Server 2012 R2.
You plan to use Server1 to manage the domain and to configure Windows 10 Group Policy settings.
You install the Group Policy Management Console (GPMC) on Server1.
You need to configure the Windows Update for Business Group Policy settings on Server1.
Solution: You copy the Group Policy Administrative Templates from a Windows 10 computer to Server1.
Does this meet the goal?

- A. Yes
- B. No Most Voted

Question #51 *Topic 1*

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 network contains an on-premises Active Directory domain. The domain contains domain controllers that run Windows Server 2019. The functional level of the forest and the domain is Windows Server 2012 R2.
The domain contains 100 computers that run Windows 10 and a member server named Server1 that runs Windows Server 2012 R2.
You plan to use Server1 to manage the domain and to configure Windows 10 Group Policy settings.
You install the Group Policy Management Console (GPMC) on Server1.
You need to configure the Windows Update for Business Group Policy settings on Server1.
Solution: You upgrade Server1 to Windows Server 2019.
Does this meet the goal?

- A. Yes
- B. No

Question #52 *Topic 1*

You have a hybrid Azure Active Directory (Azure AD) tenant and a Microsoft Endpoint Configuration Manager deployment.
You have the devices shown in the following table.

Name	Platform	Configuration
Device1	Windows 10	Hybrid joined to on-premises Active Directory and Azure AD only
Device2	Windows 10	Joined to Azure AD and enrolled in Configuration Manager only
Device3	Windows 10	Enrolled in Microsoft Endpoint Manager and has the Configuration Manager agent installed only

You plan to enable co-management.
You need to identify which devices support co-management without requiring the installation of additional software.
Which devices should you identify?

- A. Device1 only
- B. Device2 only
- C. Device3 only Most Voted
- D. Device2 and Device3 only
- E. Device1, Device2, and Device3

Question #53 *Topic 1*

- HOTSPOT -
  You have a Microsoft 365 subscription that contains the users shown in the following table.

Name	Member of	Azure Active Directory (Azure AD) role
User1	Group1	Global administrator
User2	Group2	Cloud device administrator

You configure an Enrollment Status Page profile as shown in the following exhibit.

You assign the policy to Group1.
You purchase the devices shown in the following table.

Name	Platform
Device1	Windows 10
Device2	Android

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
If User1 performs the initial device enrollment for Device1, the Enrollment Status Page will show.	○	○
If User1 performs the initial device enrollment for Device2, the Enrollment Status Page will show.	○	○
If User2 performs the initial device enrollment for Device2, the Enrollment Status Page will show.	○	○

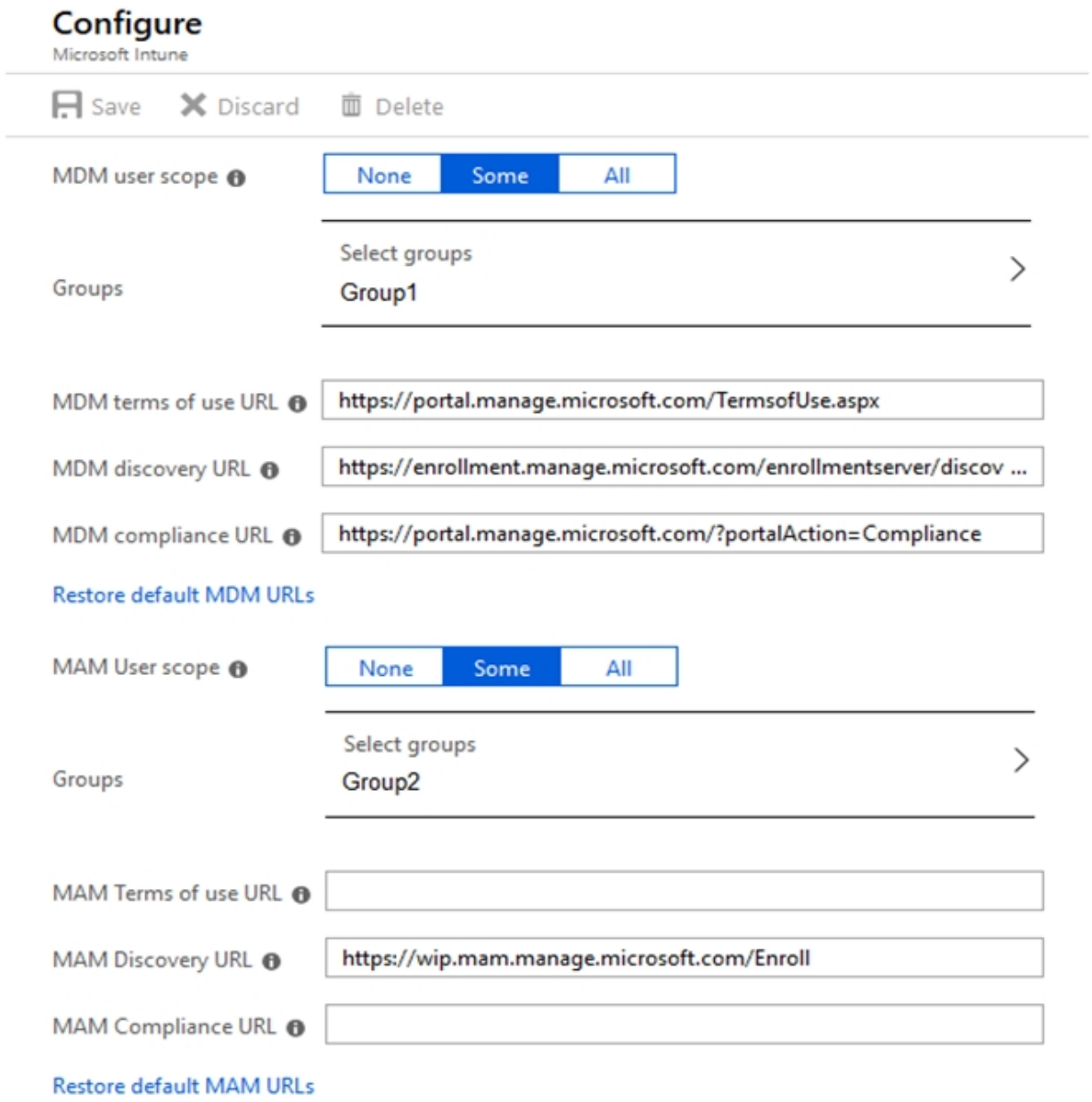
Question #54 *Topic 1*

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
User3	Group1, Group2

You integrate Microsoft Intune and contoso.com as shown in the following exhibit.



You purchase a Windows 10 device named Device1.

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
If User1 joins Device1 to contoso.com, Device1 is enrolled in Intune automatically.	○	○
If User2 joins Device1 to contoso.com, Device1 is enrolled in Intune automatically.	○	○
If User3 registers Device1 in contoso.com, Device1 is enrolled in Intune automatically.	○	○

Question #55*Topic 1*

HOTSPOT -
You have an Azure subscription and an on-premises Active Directory domain. The domain contains 50 computers that run Windows 10.
You need to centrally monitor System log events from the computers.
What should you do? To answer, select the appropriate options in the answer area.
NOTE: Each correct selection is worth one point.
Hot Area:

Answer Area

In Azure:
- Add and configure the Diagnostics settings for the Azure Activity Log.
- Add and configure an Azure Log Analytics workspace.
- Add an Azure Storage account and Azure Cognitive Search
- Add an Azure Storage account and a file share.

On the computers:
- Create an event subscription.
- Modify the membership of the Event Log Readers group.
- Enroll in Microsoft Endpoint Manager.
- Install the Microsoft Monitoring Agent.

Question #56*Topic 1*

HOTSPOT -

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

Name	Member of
User1	Group1
User2	Group1, Group2
User3	Group3

In Microsoft Endpoint Manager, you create two device type restrictions that have the settings shown in the following table.

Priority	Name	Allowed platform	Assigned to
1	TypeRest1	Android, Windows (MDM)	Group1
2	TypeRest2	iOS	Group2

In Microsoft Endpoint Manager, you create three device limit restrictions that have the settings shown in the following table.

Priority	Name	Device limit	Assigned to
1	LimitRest1	7	Group2
2	LimitRest2	10	Group1
3	LimitRest3	5	Group3

Answer Area

Statements	Yes	No
User1 can enroll up to 10 Windows 10 devices in Microsoft Endpoint Manager.	○	○
User2 can enroll up to 10 iOS devices in Microsoft Endpoint Manager.	○	○
User3 can enroll up to five Android devices in Microsoft Endpoint Manager.	○	○

Question #57*Topic 1*

DRAG DROP -

You have a Microsoft 365 E5 subscription.

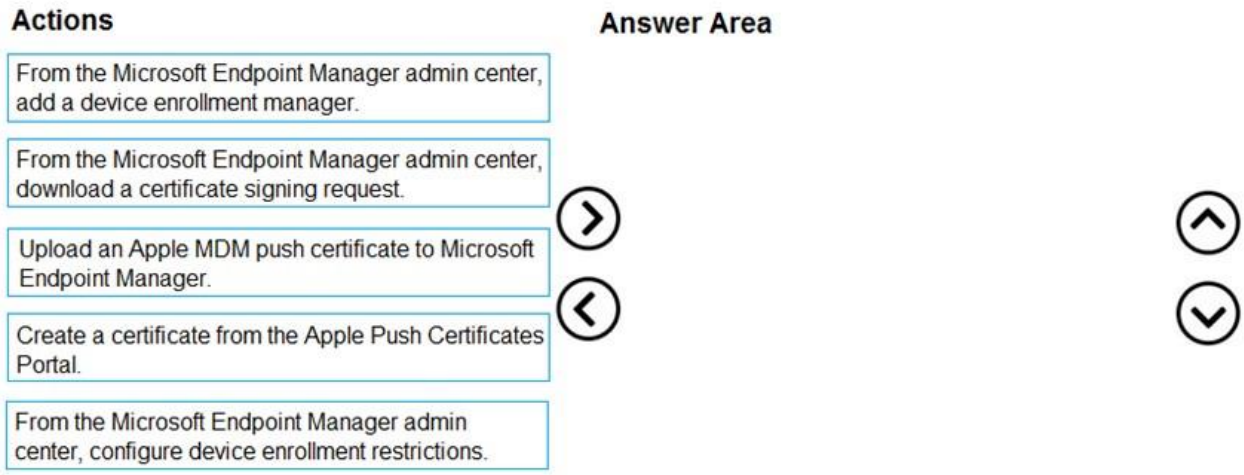
Several users have iOS devices.

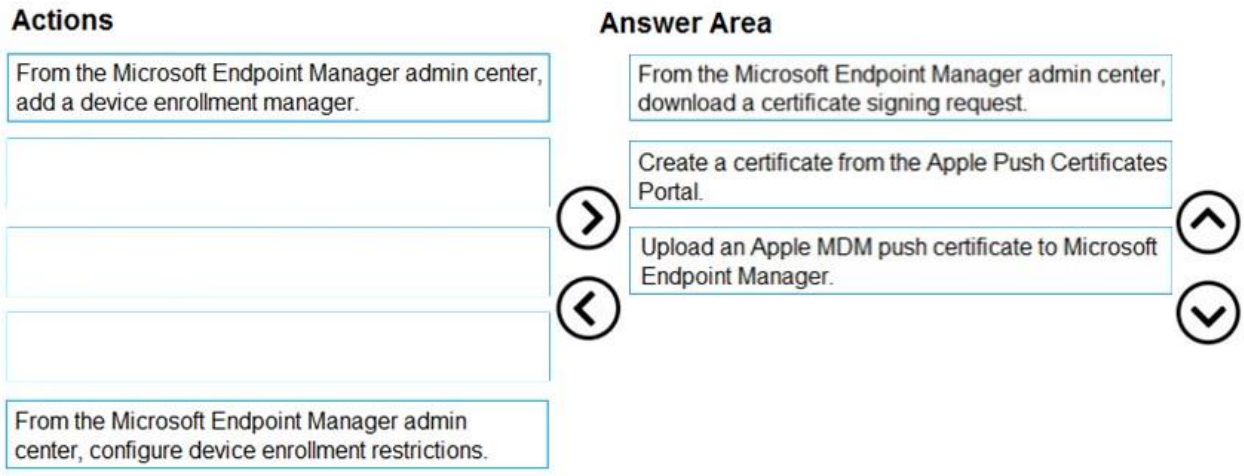
You plan to enroll the iOS devices in Microsoft Endpoint Manager.

You need to ensure that you can create an iOS/iPadOS enrollment profile in Microsoft Endpoint Manager.

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:





Question #58*Topic 1*

HOTSPOT -

You have a Microsoft 365 E5 tenant that contains the users shown in the following table.

Name	Member of
User1	UserGroup1
User2	UserGroup2
User3	UserGroup3

The tenant contains the devices shown in the following table.

Name	Owner	Installed apps	Platform	Microsoft Intune
Device1	User1	*None*	Windows 10	Enrolled
Device2	User2	App2	Android	Not enrolled
Device3	User3	*None*	iOS	Not enrolled

You have the apps shown in the following table.

Name	Type
App1	iOS store app
App2	Android store app
App3	Microsoft store app

You plan to use Microsoft Endpoint Manager to manage the apps for the users.

Answer Area

Statements	Yes	No
App1 can be assigned as a required install for User3.	○	○
App2 can be uninstalled from Device2 by using Microsoft Endpoint Manager.	○	○
App3 can be installed automatically for UserGroup1.	○	○

Question #59 *Topic 1*

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 network contains an on-premises Active Directory domain. The domain contains domain controllers that run Windows Server 2019. The functional level of the forest and the domain is Windows Server 2012 R2.
The domain contains 100 computers that run Windows 10 and a member server named Server1 that runs Windows Server 2012 R2.
You plan to use Server1 to manage the domain and to configure Windows 10 Group Policy settings.
You install the Group Policy Management Console (GPMC) on Server1.
You need to configure the Windows Update for Business Group Policy settings on Server1.
Solution: You raise the domain functional level to Windows Server 2019. You copy the Group Policy Administrative Templates from a Windows 10 computer to the
Netlogon share on all the domain controllers.
Does this meet the goal?

- A. Yes
- B. No

Question #60 *Topic 1*

You have a Microsoft 365 E5 subscription.
You plan to deploy 100 new Windows 10 devices.
You need to identify the appropriate version of Windows 10 for the new devices. The version must meet the following requirements:
☞ Be serviced for a minimum of 24 months.
Support Microsoft Application Virtualization (App-V).
▪
Which version should you identify?

- A. Windows 10 Pro, version 1909
- B. Windows 10 Pro, version 2004
- C. Windows 10 Enterprise, version 1909 **Most Voted**
- D. Windows 10 Enterprise, version 2004

Question #61*Topic 1*

HOTSPOT -

You have a Microsoft 365 E5 tenant that contains two users named User1 and User2 and the groups shown in the following table.

Name	Members
Group1	User1
Group2	User2, Group1

You have a Microsoft Intune enrollment policy that has the following settings:

☞ MDM user scope: Some

- Groups: Group1

☞ MAM user scope: Some

- Groups: Group2

You purchase the devices shown in the following table.

Name	Platform
Device1	Windows 10
Device2	Android

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 enroll Device1 in Intune by using automatic enrollment	○	○
User1 can enroll Device2 in Intune by using automatic enrollment	○	○
User2 can enroll Device2 in Intune by using automatic enrollment	○	○

Question #62*Topic 1*

HOTSPOT -

You have a Microsoft 365 tenant that contains devices enrolled in Microsoft Intune. The devices are configured as shown in the following table.

Name	Platform
Device1	Windows 10
Device2	Android
Device3	iOS

You plan to perform the following device management tasks in Microsoft Endpoint Manager:

Deploy a VPN connection by using a VPN device configuration profile.

- ☞ Configure security settings by using an Endpoint Protection device configuration profile.

You need to identify which devices will support the management tasks.

What should you identify? To answer, select the appropriate options in the answer area.

NOTE: Each correct selection is worth one point.

Answer Area

VPN device configuration profile:

- Device1 only
- Device1 and Device2 only
- Device1 and Device3 only
- Device1, Device2 and Device3

Endpoint Protection device configuration profile:

- Device1 only
- Device1 and Device2 only
- Device1 and Device3 only
- Device1, Device2 and Device3

Question #63*Topic 1*

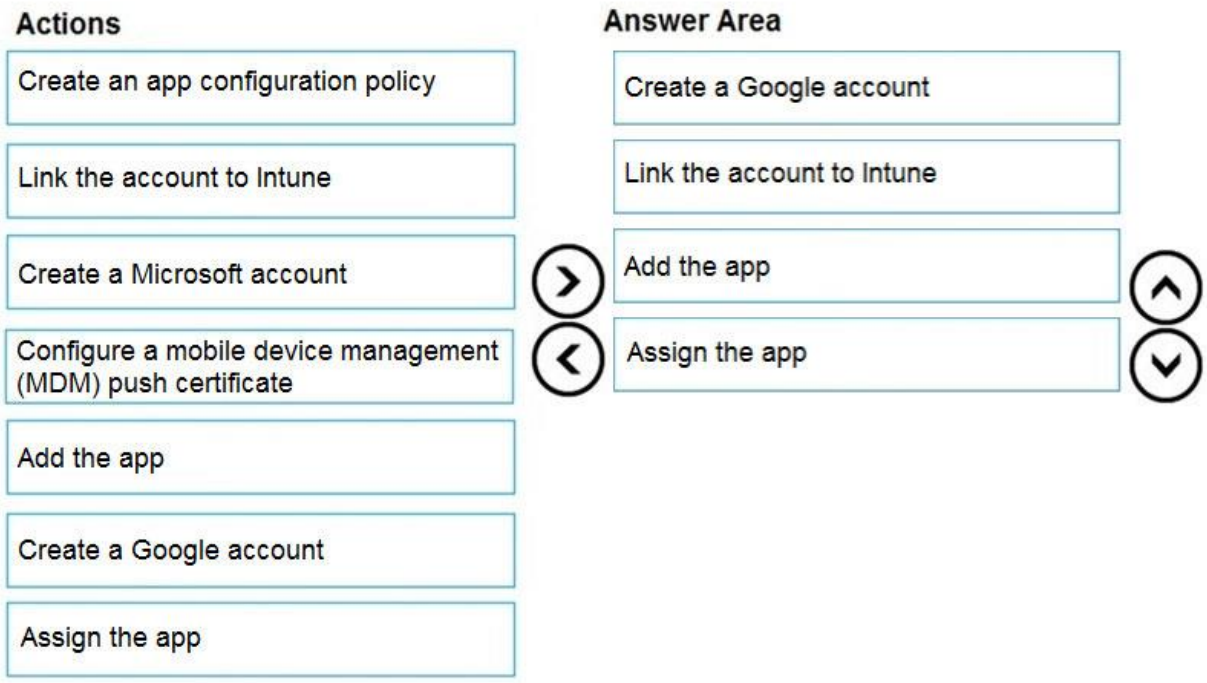
DRAG DROP -

You have a Microsoft 365 E5 tenant that contains 500 Android devices enrolled in Microsoft Intune.

You need to use Microsoft Endpoint Manager to deploy a managed Google Play app to 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.

Select and Place:



Question #64*Topic 1*

You have a Microsoft 365 E5 tenant that contains four devices enrolled in Microsoft Intune as shown in the following table.

Name	Platform
Device1	Windows 10
Device2	Android
Device3	macOS
Device4	iOS

You plan to deploy Microsoft 365 Apps for enterprise by using Microsoft Endpoint Manager.
To which devices can you deploy Microsoft 365 Apps for enterprise?

- A. Device1 only
- B. Device1 and Device3 only
- C. Device2 and Device4 only
- D. Device1, Device2, and Device3 only
- E. Device1, Device2, Device3, and Device4

Question #65*Topic 1*

You have a Microsoft 365 E5 tenant that contains the devices shown in the following table.

Name	Platform	Azure Active Directory (Azure AD)
Device1	Windows 10	Joined
Device2	Windows 10	Registered
Device3	Windows 10	Not joined or registered
Device4	Android	Registered

You plan to review device startup performance issues by using Endpoint analytics.
Which devices can you monitor by using Endpoint analytics?

- A. Device1 only
- B. Device1 and Device2 only
- C. Device1, Device2, and Device3 only
- D. Device1, Device2, and Device4 only
- E. Device1, Device2, Device3, and Device4

Question #66*Topic 1*

You have a Microsoft 365 E5 tenant that contains 100 Windows 10 devices.
You plan to deploy a Windows 10 Security Baseline profile that will protect secrets stored in memory.
What should you configure in the profile?

- A. Microsoft Defender Credential Guard
- B. BitLocker Drive Encryption (BitLocker)
- C. Microsoft Defender
- D. Microsoft Defender Exploit Guard

Question #67*Topic 1*

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 have a computer that runs Windows 10.
You need to verify which version of Windows 10 is installed.
Solution: From Device Manager, you view the computer properties.
Does this meet the goal?

- A. Yes
- B. No

Question #69*Topic 1*

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 have a computer that runs Windows 10.
You need to verify which version of Windows 10 is installed.
Solution: From the Settings app, you select Update & Security to view the update history.
Does this meet the goal?

- A. Yes
- B. No

Question #70 *Topic 1*

You have a Microsoft 365 tenant that uses Microsoft Endpoint Manager for device management.
You need to add the phone number of the help desk to the Company Portal app.
What should you do?

- A. From the Microsoft 365 admin center, modify Organization information.
- B. From the Microsoft Endpoint Manager admin center, create an app configuration policy.
- C. From Customization in the Microsoft Endpoint Manager admin center, modify the support information for the tenant.
- D. From the Microsoft 365 admin center, modify Help desk information.

Question #71 *Topic 1*

You have a Microsoft 365 E5 tenant.
You plan to deploy 1,000 new iOS devices to users. The devices will be shipped directly from the supplier to the users.
You need to recommend a Microsoft Intune enrollment option that meets the following requirements:

☞ Minimizes user interaction
☞ Minimizes administrative effort
☞ Automatically installs corporate apps

What should you recommend?

- A. Apple Configurator enrollment
- B. Automated Device Enrollment (ADE)
- C. bring your own device (BYOD) user and device enrollment.

Question #72*Topic 1*

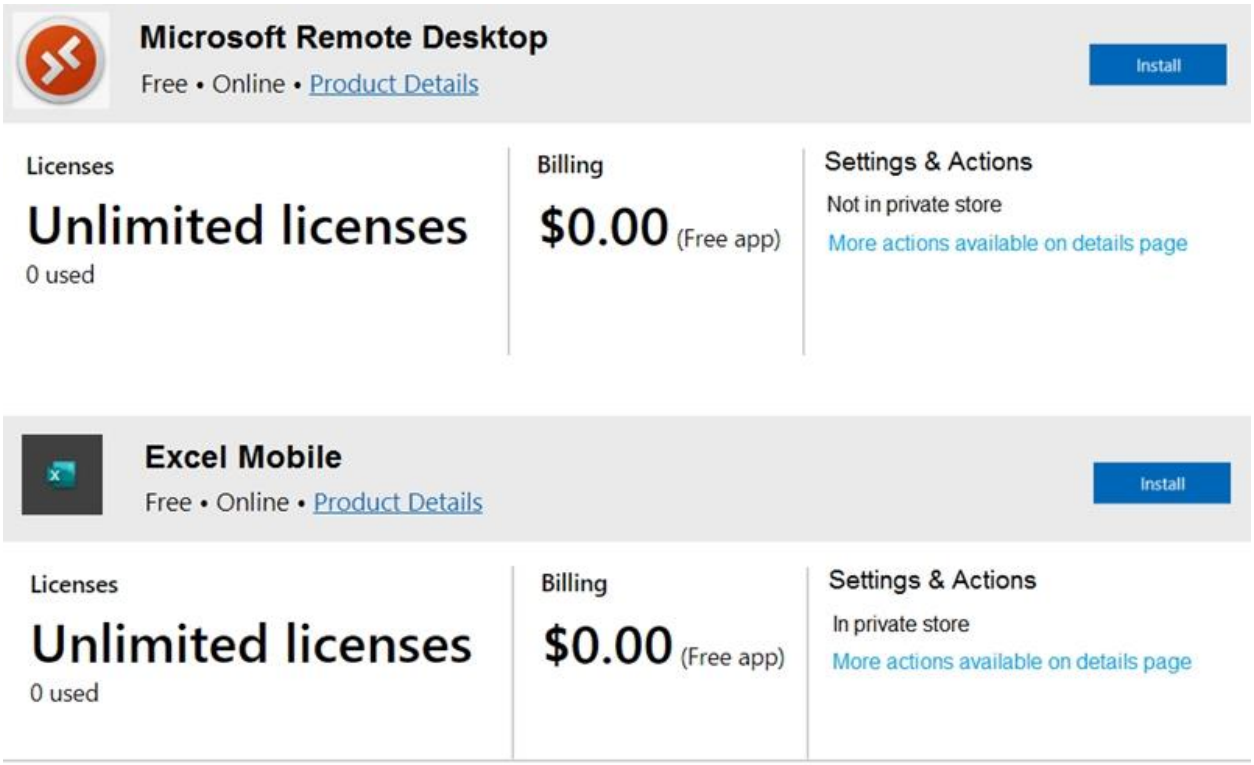
HOTSPOT -

You have a Microsoft 365 tenant that is signed up for Microsoft Store for Business and contains the users shown in the following table.

Name	Microsoft Store for Business role	Azure Active Directory (Azure AD) role
User1	Purchaser	Billing administrator
User2	Admin	Global administrator
User3	Basic Purchaser	None
User4	Basic Purchaser, Device Guard signer	Global reader

All users have Windows 10 Enterprise devices.

The Products & services settings in Microsoft Store for Business are shown in the following exhibit.



Answer Area

Statements	Yes	No
User2 can install the Microsoft Remote Desktop app from the private store.	○	○
User1 can install the Microsoft Remote Desktop app from Microsoft Store for Business.	○	○
User4 can manage the Microsoft Remote Desktop app from the private store.	○	○

Question #73*Topic 1*

Your company has offices in five cities.
The company has a Microsoft 365 tenant.
Each office is managed by a local administrator.
You plan to deploy Microsoft Intune.
You need to recommend a solution to manage resources in Intune that meets the following requirements:

☞ Local administrators must be able to manage only the resources in their respective office.
☞ Local administrators must be prevented from managing resources in other offices.
☞ Administrative effort must be minimized.

What should you include in the recommendation?

- A. scope tags
- B. device categories
- C. configuration profiles
- D. conditional access policies

Question #74*Topic 1*

HOTSPOT -

You have a Microsoft 365 E5 tenant that contains the users shown in the following table.

Name	Microsoft 365 role
User1	Cloud application administrator
User2	Application administrator
User3	Application developer
User4	**None**

Users are assigned Microsoft Store for Business roles as shown in the following table.

User	Role
User1	**None**
User2	Basic Purchaser
User3	Purchaser
User4	Device Guard signer

Which users can add apps to the private store in Microsoft Store for Business, and which users can install apps from the private store? To answer, select the appropriate options in the answer area.

Answer Area

Add apps to the private store:

- User3 only
- **User2 and User3 only**
- User1 and User3 only
- User1, User2 and User3 only
- User1, User2, User3, and User4

Install apps from the private store:

- User3 only
- User2 and User3 only
- User1 and User3 only
- User2, User3 and User4 only
- **User1, User2, User3, and User4**

Question #75*Topic 1*

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 have a computer that runs Windows 10.
You need to verify which version of Windows 10 is installed.
Solution: From the Settings app, you select System, and then you select About to view information about the system.
Does this meet the goal?

- A. Yes
- B. No

Question #76*Topic 1*

You have a Microsoft 365 tenant that contains 1,000 iOS devices enrolled in Microsoft Intune.
You plan to purchase volume-purchased apps and deploy the apps to the devices.
You need to track used licenses and manage the apps by using Intune.
What should you use to purchase the apps?

- A. Microsoft Store for Business
- B. Apple Configurator
- C. Apple Business Manager
- D. Apple iTunes Store

Question #77*Topic 1*

You have a Microsoft 365 E5 tenant that contains the devices shown in the following table.

Name	Windows 10 edition	Azure Active Directory (Azure AD)	Mobile device management (MDM) enrollment
Device1	Windows 10 Pro	Registered	Microsoft Intune
Device2	Windows 10 Enterprise	Joined	Microsoft Intune
Device3	Windows 10 Pro	Joined	Not enrolled
Device4	Windows 10 Enterprise	Registered	Microsoft Intune
Device5	Windows 10 Enterprise	Joined	Not enrolled

You add custom apps to the private store in Microsoft Store Business.
You plan to create a policy to show only the private store in Microsoft Store for Business.
To which devices can the policy be applied?

- A. Device2 only
- B. Device1 and Device3 only
- C. Device2 and Device4 only
- D. Device2, Device3, and Device5 only
- E. Device1, Device2, Device3, Device4, and Device5

HOTSPOT -
You have a Microsoft 365 E5 subscription that uses Microsoft Intune.
You have devices enrolled in Intune as shown in the following table.

Name	Platform	Member of	Scope (Tags)
Device1	Windows 10	Group1 Group3	Tag1
Device2	Android	Group2	Tag2

You create the device configuration profiles shown in the following table.

Name	Platform	Assignments: Included groups	Assignments: Excluded groups	Scope tags
Profile1	Windows 10 and later	Group1	Group3	Tag1, Tag2
Profile2	Android Enterprise	All devices	Group2	Tag1, Tag2
Profile3	Android Enterprise	Group2, Group3	Group3	Tag1
Profile4	Windows 10 and later	Group3	**None**	Default

Answer Area

Device1:

- No profiles
- Profile1 only
- Profile4 only
- Profile1 and Profile4 only
- Profile1, Profile1, and Profile4 only

Device2:

- No profiles
- Profile1 only
- Profile2 only
- Profile3 only
- Profile1 and Profile2 only
- Profile2 and Profile3 only

Question #79*Topic 1*

You have a Microsoft 365 E5 tenant that uses Microsoft Intune.
You need to ensure that users can select a department when they enroll their device in Intune.
What should you create?

- A. scope tags
- B. device configuration profiles
- C. device categories
- D. device compliance policies

HOTSPOT -
You have a Microsoft 365 E5 tenant that contains the users shown in the following table.

Name	Azure Active Directory (Azure AD) role	Microsoft Store for Business role	Member of
User1	Application administrator	Basic Purchaser	Group1
User2	**None**	Purchaser	Group2
User3	**None**	Basic Purchaser	Group3

You perform the following actions:
- Provision the private store in Microsoft Store for Business.
- Add an app named App1 to the private store.
- Set Private store availability for App1 to Specific groups, and then select Group3.

Answer Area

Statements	Yes	No
User1 can install App1 from the private store.	○	○
User2 can install App1 from the private store.	○	○
User3 can install App1 from the private store.	○	○

Question #81 *Topic 1*

You have a Microsoft 365 tenant that is signed up for Microsoft Store for Business and contains a user named User1.
You need to ensure that User1 can perform the following tasks in Microsoft Store for Business:

- ☞ Assign licenses to users.
- ☞ Procure apps from Microsoft Store.
- ☞ Manage private store availability for all items.

The solution must use the principle of least privilege.
Which Microsoft Store for Business role should you assign to User1?

- A. Admin
- B. Device Guard signer
- C. Basic Purchaser
- D. Purchaser

Question #82 *Topic 1*

Your company has multiple offices.
You have a Microsoft 365 E5 tenant that uses Microsoft Intune for device management. Each office has a local administrator.
You need to ensure that the local administrators can manage only the devices in their respective office.
What should you use?

- A. scope tags
- B. configuration profiles
- C. device categories
- D. conditional access policies

Question #83*Topic 1*

HOTSPOT -

You have a Microsoft 365 E5 tenant that contains the users shown in the following table.

Name	Member of
User1	Group1
User2	Group2

You purchase the devices shown in the following table.

Name	Platform
Device1	Windows 10
Device2	Android

In Microsoft Endpoint Manager, you create an enrollment status page profile that has the following settings:

- Show app and profile configuration progress: Yes
- Allow users to collect logs about installation errors: Yes
- Only show page to devices provisioned by out-of-box experience (OOBE): No
- Assignments: Group2

Answer Area

Statements	Yes	No
If User1 enrolls Device1 in Microsoft Endpoint Manager, the enrollment status page will appear.	○	○
If User2 enrolls Device1 in Microsoft Endpoint Manager, the enrollment status page will appear.	○	○
If User2 enrolls Device2 in Microsoft Endpoint Manager, the enrollment status page will appear.	○	○

Question #84*Topic 1*

DRAG DROP -
You have a Microsoft 365 E5 tenant.
You need to implement compliance solutions that meet the following requirements:
☞ Use a file plan to manage retention labels.
☞ Identify, monitor, and automatically protect sensitive information.
Capture employee communications for examination by designated reviewers.

▪
Which solution should you use for each requirement? To answer, drag the appropriate solutions to the correct requirements. Each solution 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.

Solutions

- Data loss prevention
- Information governance
- Insider risk management
- Records management

Answer Area

Identify, monitor, and automatically protect sensitive information:	Data loss prevention
Capture employee communications for examination by designated reviewers:	Insider risk management
Use a file plan to manage retention labels:	Information governance

Question #2*Topic 2*

You have a Microsoft 365 subscription.
You need to be notified if users receive email containing a file that has a virus.
What should you do?

- A. From the Exchange admin center, create an in-place eDiscovery & hold.
- B. From the Security & Compliance admin center, create a safe attachments policy.
- C. From the Security & Compliance admin center, create a data loss prevention (DLP) policy.
- D. From the Security & Compliance admin center, create an alert policy.

Question #3*Topic 2*

You have a Microsoft Azure Active Directory (Azure AD) tenant.
The organization needs to sign up for Microsoft Store for Business. The solution must use the principle of least privilege.
Which role should you assign to the user?

- A. Global administrator
- B. Cloud application administrator
- C. Application administrator
- D. Service administrator

Question #5*Topic 2*

You have a Microsoft 365 subscription and an on-premises Active Directory domain named contoso.com. All client computers run Windows 10 Enterprise and are joined to the domain.
You need to enable Windows Defender Credential Guard on all the computers.
What should you do?

- A. From the Microsoft 365 Defender, configure the DKIM signatures for the domain.
- B. From a domain controller, create a Group Policy object (GPO) that enables the Restrict delegation of credentials to remote servers setting.
- C. From the Security & Compliance admin center, create a device security policy.
- D. From a domain controller, create a Group Policy object (GPO) that enabled the Turn On Virtualization Based Security setting.

Question #6*Topic 2*

Your company has a Microsoft 365 subscription that uses an Azure Active Directory (Azure AD) tenant named contoso.com.
The company purchases a cloud app named App1 that supports Microsoft Cloud App Security monitoring.
You configure App1 to be available from the My Apps portal.
You need to ensure that you can monitor App1 from Cloud App Security.
What should you do?

- A. From the Azure Active Directory admin center, create a conditional access policy.
- B. From the Azure Active Directory admin center, create an app registration.
- C. From the Endpoint Management admin center, create an app protection policy.
- D. From the Endpoint Management admin center, create an app configuration policy.

Question #7*Topic 2*

HOTSPOT -

You use Microsoft Defender for Endpoint.

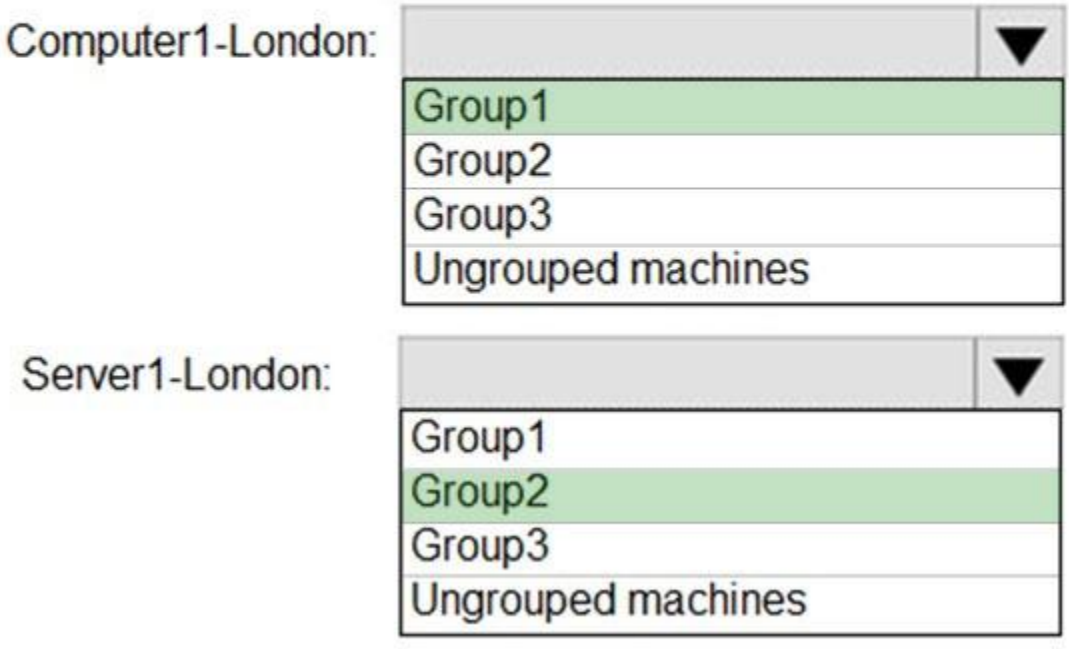
You have the Microsoft Defender for Endpoint machine groups shown in the following table.

Name	Rank	Members
Group1	1	Operating system in Windows 10
Group2	2	Name ends with London
Group3	3	Operating system in Windows Server 2016
Ungrouped machines (default)	Last	*Not applicable*

You plan to onboard computers to Microsoft Defender for Endpoint as shown in the following table.

Name	Operating system
Computer1-London	Windows 10
Server1-London	Windows Server 2016

Answer Area



Question #8*Topic 2*

Your company has 5,000 Windows 10 devices. All the devices are protected by using Microsoft Defender Advanced Threat Protection (ATP).
You need to create a filtered view that displays which Microsoft Defender ATP alert events have a high severity and occurred during the last seven days.
What should you use in Microsoft Defender ATP?

- A. the threat intelligence API
- B. Automated investigations
- C. Threat analytics
- D. Advanced hunting

Question #10*Topic 2*

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 have an Azure Active Directory (Azure AD) tenant that contains a user named User1.
Your company purchases a Microsoft 365 subscription.
You need to ensure that User1 is assigned the required role to create file policies and manage alerts in the Cloud App Security admin center.
Solution: From the Security & Compliance admin center, you assign the Security Administrator role to User1.
Does this meet the goal?

- A. Yes
- B. No

Question #11*Topic 2*

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 have an Azure Active Directory (Azure AD) tenant that contains a user named User1.
Your company purchases a Microsoft 365 subscription.
You need to ensure that User1 is assigned the required role to create file policies and manage alerts in the Cloud App Security admin center.
Solution: From the Azure Active Directory admin center, you assign the Security administrator role to User1.
Does this meet the goal?

- A. Yes
- B. No

Question #12*Topic 2*

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 have an Azure Active Directory (Azure AD) tenant that contains a user named User1.
Your company purchases a Microsoft 365 subscription.
You need to ensure that User1 is assigned the required role to create file policies and manage alerts in the Cloud App Security admin center.
Solution: From the Azure Active Directory admin center, you assign the Compliance administrator role to User1.
Does this meet the goal?

- A. Yes
- B. No

Question #13*Topic 2*

HOTSPOT -

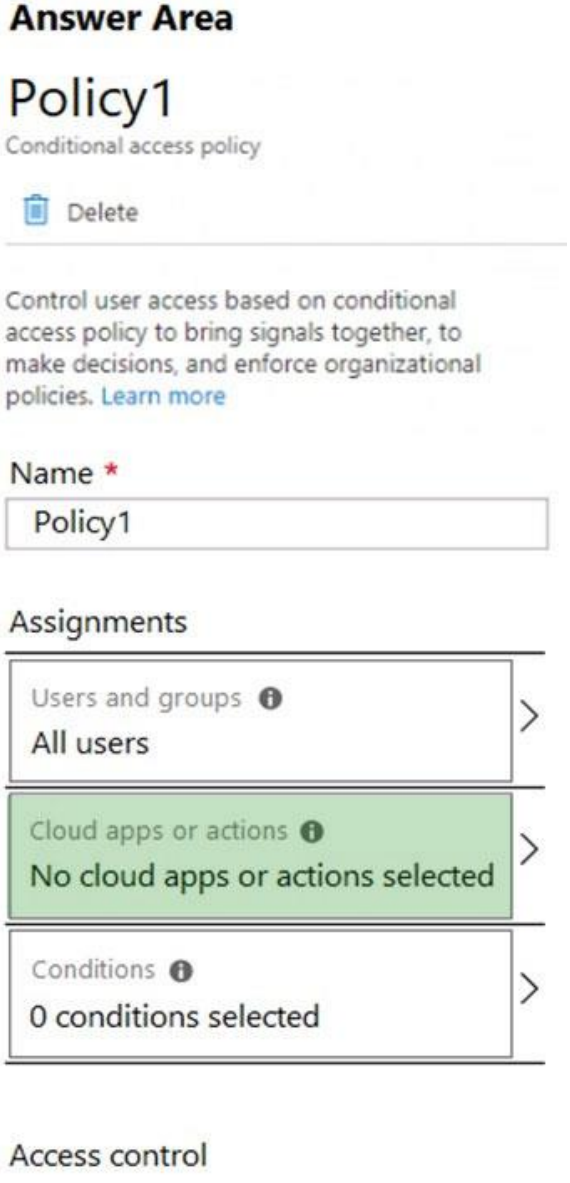
Your company purchases a cloud app named App1.

You plan to publish App1 by using a conditional access policy named Policy1.

You need to ensure that you can control access to App1 by using a Microsoft Cloud App Security session policy.

Which two settings should you modify in Policy1? To answer, select the appropriate settings in the answer area.

Answer Area



Question #14 *Topic 2*

HOTSPOT -

Your company uses Microsoft Defender Advanced Threat Protection (ATP). Microsoft Defender ATP includes the machine groups shown in the following table.

Rank	Machine group	Members
1	Group1	`Tag Equals demo And OS In Windows 10`
2	Group2	`Tag Equals demo`
3	Group3	`Domain Equals adatum.com`
4	Group4	`Domain Equals adatum.com And OS In Windows 10`
Last	Ungrouped machines (default)	*Not applicable*

Answer Area

Computer1 will be a member of **[answer choice]**.

- Group3 only
- Group4 only
- **Group3 and Group4 only**
- Ungrouped machines

If you add the tag demo to Computer1, the computer will be a member of **[answer choice]**.

- Group1 only
- Group1 and Group2 only
- **Group1, Group2, Group3, and Group4**
- Ungrouped machines

Question #15 *Topic 2*

HOTSPOT -

You have a Microsoft 365 subscription.

You are planning a threat management solution for your organization.

You need to minimize the likelihood that users will be affected by the following threats:

- Opening files in Microsoft SharePoint that contain malicious content
- Impersonation and spoofing attacks in email messages

Which policies should you create in the Microsoft 365 Defender? To answer, select the appropriate options in the answer area.

Answer Area

Opening files in SharePoint that contain malicious content:

- Anti-spam
- anti-phishing
- **safe attachments**
- Safe Links

Impersonation and spoofing attacks in email messages:

- Anti-spam
- **anti-phishing**
- safe attachments
- Safe Links

Question #16 *Topic 2*

You have a Microsoft 365 subscription.
All users have their email stored in Microsoft Exchange Online.
In the mailbox of a user named User1, you need to preserve a copy of all the email messages that contain the word ProjectX.
What should you do first?

- A. From Microsoft Cloud App Security, create an access policy.
- B. From the Security & Compliance admin center, create an eDiscovery case. Most Voted
- C. From Microsoft Cloud App Security, create an activity policy.
- D. From the Security & Compliance admin center, create a data loss prevention (DLP) policy.

Question #17 *Topic 2*

You have a Microsoft 365 subscription.
From the subscription, you perform an audit log search, and you download all the results.
You plan to review the audit log data by using Microsoft Excel.
You need to ensure that each audited property appears in a separate Excel column.
What should you do first?

- A. From Power Query Editor, transform the JSON data.
- B. Format the Operations column by using conditional formatting.
- C. Format the AuditData column by using conditional formatting.
- D. From Power Query Editor, transform the XML data.

Question #18 *Topic 2*

You have a Microsoft 365 subscription.
You need to be notified if users receive email containing a file that has a virus.
What should you do?

- A. From the Exchange admin center, create a spam filter policy.
- B. From the Security & Compliance admin center, create a data governance event.
- C. From the Security & Compliance admin center, create an alert policy.
- D. From the Exchange admin center, create a mail flow rule.

Question #19 *Topic 2*

DRAG DROP -

You have the Microsoft Azure Advanced Threat Protection (ATP) workspace shown in the Workspace exhibit. (Click the Workspace tab.)

Workspace

Manage Azure ATP user roles

Create Workspace

NAME	TYPE	INTEGRATION	GEOLOCATION
testwrkspace	Primary	Windows Defender ATP	Europe

The sensors settings for the workspace are configured as shown in the Sensors exhibit. (Click the Sensors tab.)

Sensors

Configure Directory Services to install the first Sensor or Standalone Sensor.

NAME	TYPE	DOMAIN CO...	VERSION	SERVICE STATUS	HEALTH
No Sensors registered					

You need to ensure that Azure ATP stores data in Asia.

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.

Actions
Modify the integration setting for the workspace.
Delete the workspace.
Regenerate the access keys.
Create a new workspace.
Modify the Azure ATP user roles.

Answer Area
Delete the workspace.
Create a new workspace.
Regenerate the access keys.

Question #20 *Topic 2*

Your company has five security information and event management (SIEM) appliances. The traffic logs from each appliance are saved to a file share named Logs.
You need to analyze the traffic logs.
What should you do from Microsoft Cloud App Security?

- A. Click Investigate, and then click Activity log.
- B. Click Control, and then click Policies. Create a file policy.
- C. Click Discover, and then click Create snapshot report.
- D. Click Investigate, and then click Files.

Question #21 *Topic 2*

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 have an Azure Active Directory (Azure AD) tenant that contains a user named User1.
Your company purchases a Microsoft 365 subscription.
You need to ensure that User1 is assigned the required role to create file policies and manage alerts in the Cloud App Security admin center.
Solution: From the Cloud App Security admin center, you assign the App/instance admin role for all Microsoft Online Services to User1.
Does this meet the goal?

- A. Yes
- B. No

Your company has a Microsoft 365 subscription that uses an Azure Active Directory (Azure AD) tenant named contoso.com.
The tenant is configured to use Azure AD Identity Protection.
You plan to use an application named App1 that creates reports of Azure AD Identity Protection usage.
You register App1 in the tenant.
You need to ensure that App1 can read the risk event information of contoso.com.
To which API should you delegate permissions?

- A. Windows Azure Service Management API
- B. Windows Azure Active Directory
- C. Microsoft Graph Most Voted
- D. Office 365 Management

Question #23*Topic 2*

Your company has a Microsoft 365 subscription that uses an Azure Active Directory (Azure AD) tenant named contoso.com. The tenant contains computers that run Windows 10 Enterprise and are managed by using Microsoft Endpoint Manager. The computers are configured as shown in the following table.

Name	CPU	Cores	RAM	TPM
Computer1	64-bit	2	12 GB	Enabled
Computer2	64-bit	4	12 GB	Enabled
Computer3	64-bit	8	16 GB	Disabled
Computer4	32-bit	4	4 GB	Disabled

You plan to implement Windows Defender Application Guard for contoso.com.
You need to identify on which two Windows 10 computers Windows Defender Application Guard can be installed.
Which two computers should you identify? Each correct answer presents part of the solution.
NOTE: Each correct selection is worth one point.

- A. Computer1
- B. Computer3
- C. Computer2
- D. Computer4

Minimum CPU = 4 Cores

Minimum RAM = 8 GB

Question #24 *Topic 2*

HOTSPOT -

Your company uses Microsoft Defender for Endpoint.

The devices onboarded to Microsoft Defender for Endpoint are shown in the following table.

Name	Machine group
Device1	ATP1
Device2	ATP1
Device3	ATP2

The alerts visible in the Microsoft Defender for Endpoint alerts queue are shown in the following table.

Name	Machine
Alert1	Device1
Alert2	Device2
Alert3	Device3

You create a suppression rule that has the following settings:

- Triggering IOC: Any IOC
- Action: Hide alert
- Suppression scope: Alerts on ATP1 machine group

For each of the following statements, select Yes if the statement is true. Otherwise, select No.

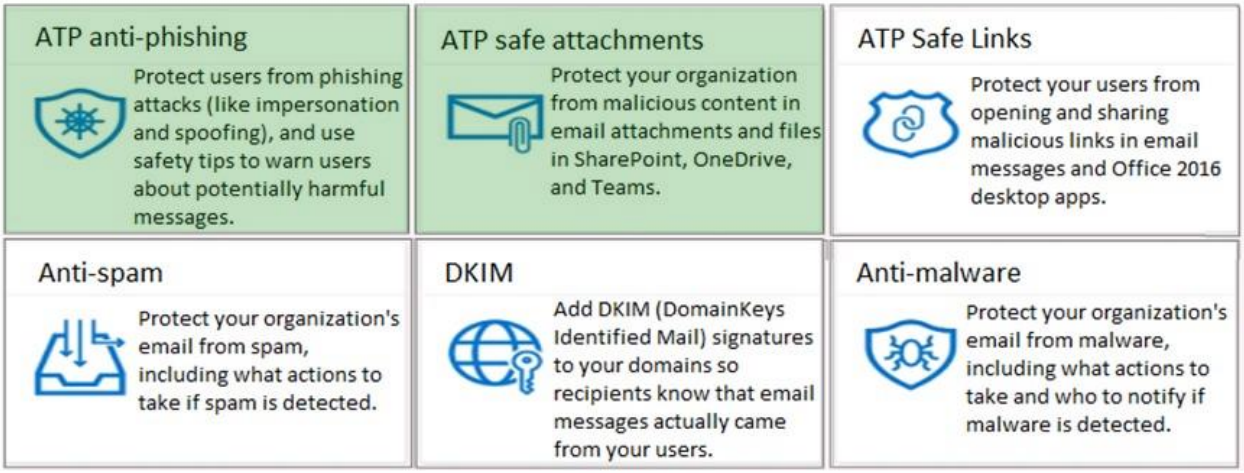
Answer Area

Statements	Yes	No
After you create the suppression rule, Alert1 is visible in the alerts queue.	○	○
After you create the suppression rule, Alert3 is visible in the alerts queue.	○	○
After you create the suppression rule, a new alert triggered on Device2 is visible in the alerts queue.	○	○

Question #25 *Topic 2*

HOTSPOT -
Your company has a Microsoft 365 subscription.
You need to configure Microsoft 365 to meet the following requirements:
☞ Malware found in email attachments must be quarantined for 20 days.
☞ The email address of senders to your company must be verified.
Which two options should you configure in the Security & Compliance admin center? To answer, select the appropriate options in the answer area.

Answer Area



Question #26 *Topic 2*

You have a Microsoft 365 subscription that uses Microsoft Defender Advanced Threat Protection (Microsoft Defender ATP).
All the devices in your organization are onboarded to Microsoft Defender ATP.
You need to ensure that an alert is generated if malicious activity was detected on a device during the last 24 hours.
What should you do?

- A. From Alerts queue, create a suppression rule and assign an alert
- B. From the Security & Compliance admin center, create an audit log search
- C. From Advanced hunting, create a query and a detection rule
- D. From the Security & Compliance admin center, create a data loss prevention (DLP) policy

Question #27 *Topic 2*

You have an Azure Active Directory (Azure AD) tenant and a Microsoft 365 E5 subscription. The tenant contains the users shown in the following table.

Name	Role
User1	Security administrator
User2	Security operator
User3	Security reader
User4	Compliance administrator

You plan to implement Microsoft Defender for Endpoint.
You verify that role-based access control (RBAC) is turned on in Microsoft Defender for Endpoint.
You need to identify which user can view security incidents from the Microsoft Defender Security Center.
Which user should you identify?

- A. User1
- B. User2
- C. User3
- D. User4

Question #28 *Topic 2*

Your network contains an on-premises Active Directory domain named contoso.com. The domain contains 1,000 Windows 10 devices.
You perform a proof of concept (PoC) deployment of Microsoft Defender for Endpoint for 10 test devices. During the onboarding process, you configure Microsoft
Defender for Endpoint-related data to be stored in the United States.
You plan to onboard all the devices to Microsoft Defender for Endpoint.
You need to store the Microsoft Defender for Endpoint data in Europe.
What should you do first?

- A. Create a workspace.
- B. Onboard a new device.
- C. Delete the workspace.
- D. Offboard the test devices.

Question #29*Topic 2*

You have a Microsoft 365 subscription.
You need to be notified if users receive email containing a file that has a virus.
What should you do?

- A. From the Exchange admin center, create an in-place eDiscovery & hold.
- B. From the Security & Compliance admin center, create a data loss prevention (DLP) policy.
- C. From the Exchange admin center, create an anti-malware policy.
- D. From the Exchange admin center, create a mail flow rule.

Question #30*Topic 2* *[Hostspot]*

You have a Microsoft 365 subscription that contains 500 users.
You have several hundred computers that run the 64-bit version of Windows 10 Enterprise and have the following configurations:

- ☞ Two volumes that contain data
- ☞ A CPU that has two cores
- ☞ TPM disabled
- ☞ 4 GB of RAM

All the computers are managed by using Microsoft Endpoint Manager.
You need to ensure that you can turn on Windows Defender Application Guard on the computers.
What should you do first?

- A. Modify the edition of Windows 10.
- B. Create an additional volume.
- C. Replace the CPU and enable TPM.
- D. Replace the CPU and increase the RAM.

Question #31*Topic 2*

You have a Microsoft 365 E5 subscription that uses Microsoft Defender for Endpoint.
From Microsoft Defender for Endpoint, you turn on the Allow or block file advanced feature.
You need to block users from downloading a file named File1.exe.
What should you use?

- A. a suppression rule
- B. an indicator
- C. a device configuration profile

Question #32*Topic 2*

You have a Microsoft 365 E5 subscription that uses Microsoft Defender for Endpoint.
When users attempt to access the portal of a partner company, they receive the message shown in the following exhibit.

You need to enable user access to the partner company's portal.
Which Microsoft Defender for Endpoint setting should you modify?

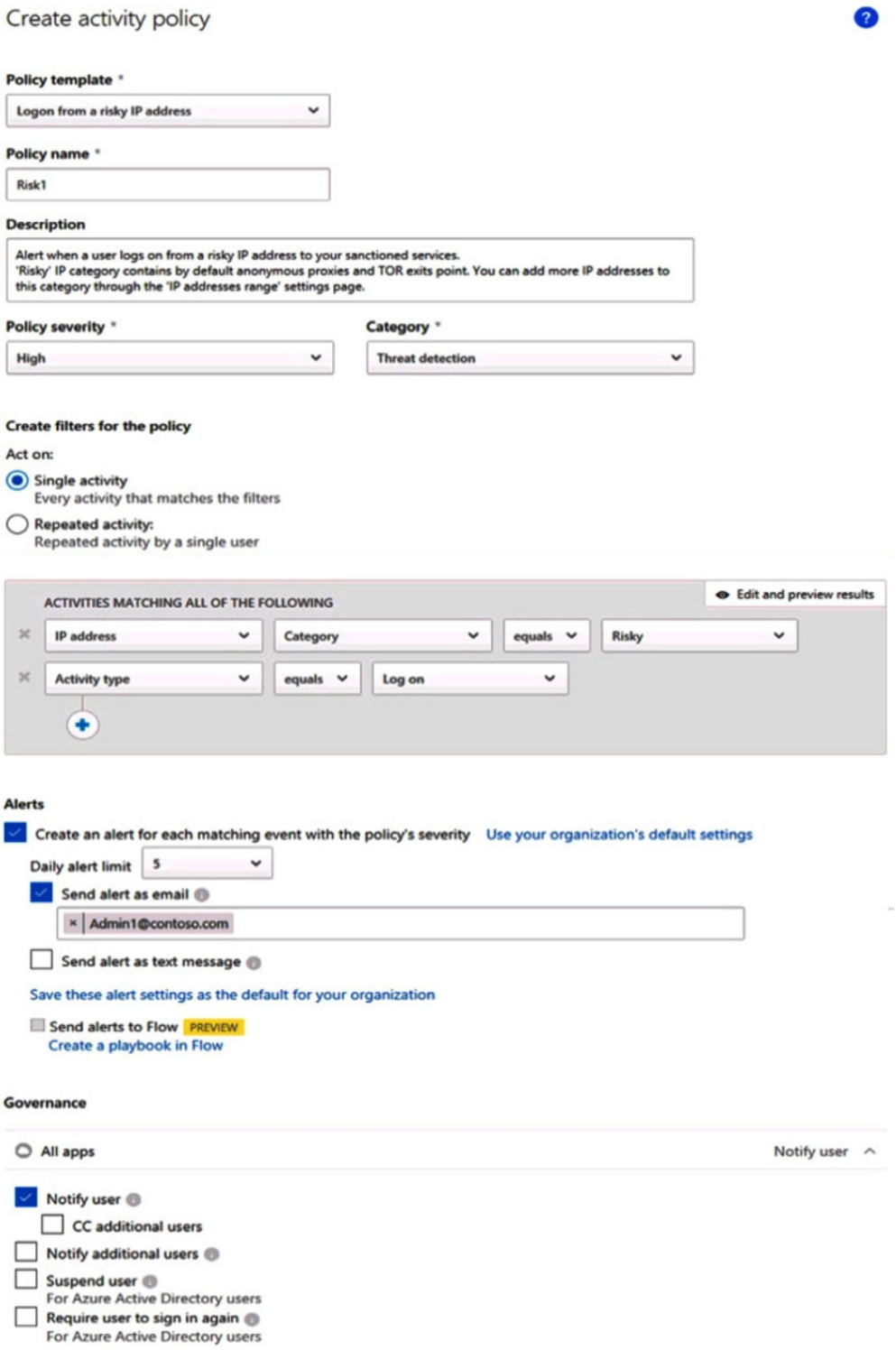
- A. Custom detections
- B. Advanced hunting
- C. Alert notifications
- D. Indicators
- E. Alert suppression

Question #33 *Topic 2* *[Hotspot]*

HOTSPOT -

You have a Microsoft 365 subscription.

You create a Microsoft Cloud App Security policy named Risk1 based on the Logon from a risky IP address template as shown in the following exhibit.



You have two users named User1 and User2. Each user signs in to Microsoft SharePoint Online from a risky IP address 10 times within 24 hours.
Use the drop-down menus to select the answer choice that completes each statement based on the information presented in the graphic.

Answer Area

Admin1 will receive **[answer choice].**

- one notification
- five notifications
- ten notifications
- no notifications

User1 will receive **[answer choice].**

- one notification
- five notifications
- ten notifications
- no notifications

Question #34*Topic 2*

HOTSPOT -

You have a Microsoft Azure Activity Directory (Azure AD) tenant contains the users shown in the following table.

Name	Member of
User1	Group1
User2	Group2
User3	Group3

Group3 is a member of Group1.

Your company uses Microsoft Defender Advanced Threat Protection (ATP). Microsoft Defender ATP contains the roles shown in the following table.

Name	Permission	Assigned user group
Microsoft Defender ATP administrator (default)	View data, Alerts investigation, Active remediation actions, Manage security settings	*None*
Role1	View data, Alerts investigation	Group1
Role2	View data	Group2

Microsoft Defender ATP contains the device groups shown in the following table.

Rank	Machine group	Machine	User access
1	ATP1	Device1	Group1
Last	Ungrouped machines (default)	Device2	*None*

For each of the following statements, select Yes if the statement is true. Otherwise, select No.

Answer Area

Statements	Yes	No
User1 can view Device1 in Microsoft Defender Security Center.	○	○
User2 can sign in to Microsoft Defender Security Center.	○	○
User3 can view Device1 in Microsoft Defender Security Center.	○	○

Question #35*Topic 2*

HOTSPOT -

Your company uses Microsoft Cloud App Security.

You plan to integrate Cloud App Security and security information and event management (SIEM).

You need to deploy a SIEM agent on a server that runs Windows Server 2016.

What should you do? To answer, select the appropriate settings in the answer area.

NOTE: Each correct selection is worth one point.

Answer Area

First action to perform:

- Install Java 8.
- Install Microsoft .NET Framework 3.5.
- Add the Windows Internal Database feature.
- Add the Setup and Boot Event Collection feature.

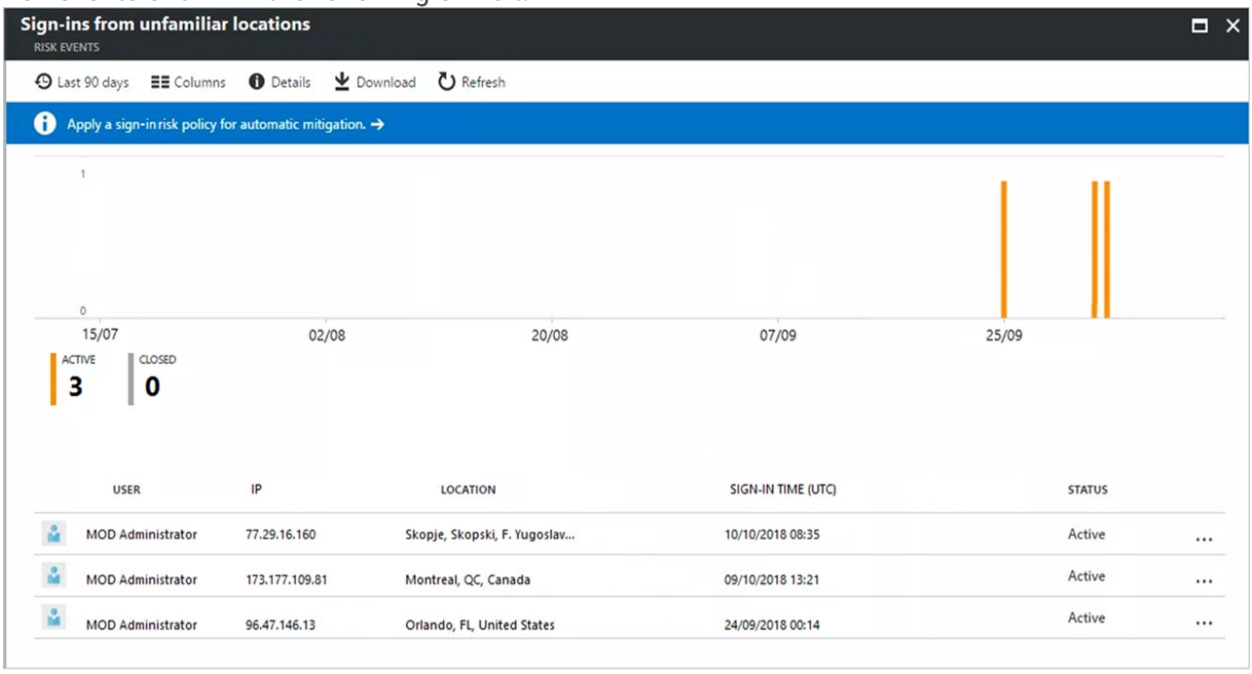
Second action to perform:

- Run the Set-MMagent cmdlet.
- Add the Setup and Boot Event Collection feature.
- Run the java command and specify the -jar parameter.
- Run the Install-WindowsFeature cmdlet and specify the -source parameter.

Question #36 *Topic 2*

HOTSPOT -

From the Microsoft Azure Active Directory (Azure AD) Identity Protection dashboard, you view the risk events shown in the following exhibit.



Use the drop-down menus to select the answer choice that completes each statement based on the information presented in the graphic.

Answer Area

To require multi-factor authentication when signing in to unfamiliar locations, you must create a [**answer choice**].

named location in Azure AD
sign-in risk policy
user risk policy

To avoid generating alerts when signing in to the Montreal location, create [**answer choice**].

a named location in Azure AD
a sign-in risk policy
a user risk policy

Question #37*Topic 2*

Your company uses Microsoft Defender for Identity and Microsoft 365 Defender.
You need to integrate Microsoft Defender for Identity and Microsoft 365 Defender.
What should you do?

- A. From Microsoft Defender for Identity, configure the notifications and reports.
- B. From Microsoft Defender for Identity, configure the data sources.
- C. From Microsoft Defender Security Center, configure the Machine management settings.
- D. From Microsoft Defender Security Center, configure the General settings.

Question #38*Topic 2*

HOTSPOT -
You have a Microsoft Azure Activity Directory (Azure AD) tenant that contains the users shown in the following table.

Name	Member of
User1	Group1
User2	Group2
User3	Group3

Your company uses Microsoft Defender for Endpoint. Microsoft Defender for Endpoint contains the roles shown in the following table.

Name	Permission	Assigned user group
Microsoft Defender for Endpoint administrator (default)	View data, Alerts investigation, Active remediation actions, Manage security settings	Group3
Role1	View data, Alerts investigation	Group1
Role2	View data	Group2

Microsoft Defender for Endpoint contains the device groups shown in the following table.

Rank	Machine group	Machine	User access
1	ATP1	Device1	Group1
Last	Ungrouped machines (default)	Device2	Group2

Answer Area

Statements	Yes	No
User1 can run an antivirus scan on Device2.	○	◯
User2 can collect an investigation package from Device2.	○	◯
User3 can isolate Device1.	◯	○

Question #39 *Topic 2*

HOTSPOT -

You have a Microsoft 365 subscription. All client devices are managed by Microsoft Endpoint Manager.

You need to implement Microsoft Defender Advanced Threat Protection (ATP) for all the supported devices enrolled in mobile device management (MDM).

What should you include in the device configuration profile? To answer, select the appropriate options in the answer area.

Answer Area

Platform: ▼
- Android
- iOS
- Windows 10 and later
- Windows 8.1 and later

Settings: ▼
- Offboard package
- Onboard package
- Windows Defender Applicaion Guard
- Windows Defender Firewall

Question #40 *Topic 2*

You have a Microsoft 365 subscription.
Your company purchases a new financial application named App1.
From Cloud Discovery in Microsoft Cloud App Security, you view the Discovered apps page and discover that many applications have a low score because they are missing information about domain registration and consumer popularity.
You need to prevent the missing information from affecting the App1 score.
What should you configure from the Cloud Discover settings?

- A. Organization details
- B. Default behavior
- C. Score metrics
- D. App tags

Question #41 *Topic 2*

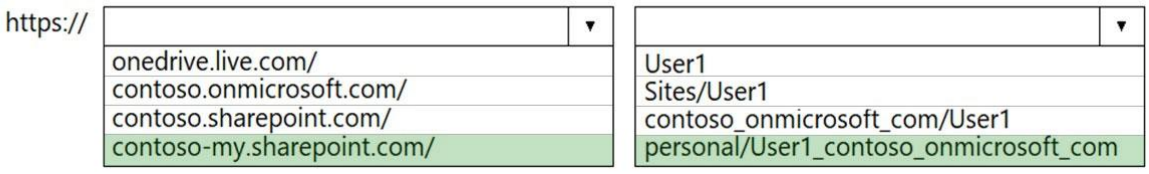
You have a Microsoft 365 E5 subscription.
You need to be notified if users receive email containing a file that has a virus.
What should you do?

- A. From the Exchange admin center, create an in-place eDiscovery & hold.
- B. From the Exchange admin center, create a spam filter policy.
- C. From the Exchange admin center, create an anti-malware policy.
- D. From the Exchange admin center, create a mail flow rule.

Question #42 *Topic 2*

HOTSPOT -
You have a Microsoft 365 subscription that links to an Azure Active Directory (Azure AD) tenant named contoso.onmicrosoft.com.
A user named User1 stores documents in Microsoft OneDrive.
You need to place the contents of User1's OneDrive account on an eDiscovery hold.
Which URL should you use for the eDiscovery hold? To answer, select the appropriate options in the answer area.

Answer Area



Question #43*Topic 2*

HOTSPOT -

You have a Microsoft 365 E5 subscription linked to an Azure Active Directory (Azure AD) tenant.

The tenant contains a group named Group1 and the users shown in the following table:

Name	Role
Admin1	Conditional Access administrator
Admin2	Security administrator
Admin3	User administrator

The tenant has a conditional access policy that has the following configurations:

☞ Name: Policy1

☞ Assignments:

- Users and groups: Group1
- Cloud aps or actions: All cloud apps

☞ Access controls:

☞ Grant, require multi-factor authentication

☞ Enable policy: Report-only

You set Enabled Security defaults to Yes for the tenant.

For each of the following settings select Yes, if the statement is true. Otherwise, select No.

Answer Area

Statements	Yes	No
Admin1 can set Enable policy for Policy1 to **On**.	○	○
Admin2 can set Enable policy for Policy1 to **Off**.	○	○
Admin3 can set Users and groups for Policy1 to **All users**.	○	○

Question #44*Topic 2*

Your network contains an on-premises Active Directory domain.
Your company has a security policy that prevents additional software from being installed on domain controllers.
You need to monitor a domain controller by using Microsoft Defender for Identity.
What should you do? More than one answer choice may achieve the goal. Choose the BEST answer.

- A. Deploy a Microsoft Defender for identity sensor, and then configure port mirroring.
- B. Deploy a Microsoft Defender for identity sensor, and then configure detections.
- C. Deploy a Microsoft Defender for Identity standalone sensor, and then configure detections.
- D. Deploy a Microsoft Defender for Identity standalone sensor, and then configure port mirroring.

Question #45*Topic 2*

Your company has digitally signed applications.
You need to ensure that Microsoft Defender for Endpoint considers the digitally signed applications safe and never analyzes them.
What should you create in the Microsoft Defender Security Center?

- A. a custom detection rule
- B. an allowed/blocked list rule
- C. an alert suppression rule
- D. an indicator

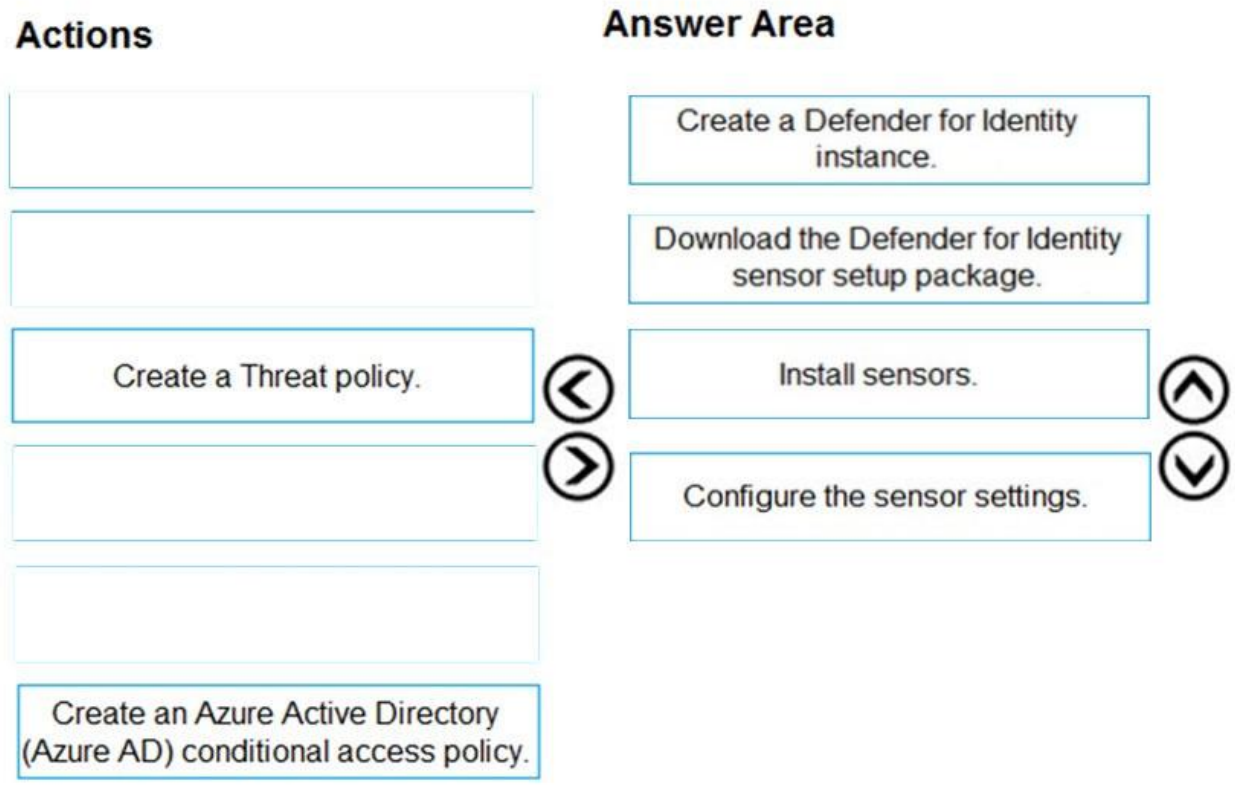
Question #46 *Topic 2*

DRAG DROP -

You create a Microsoft 365 subscription.

You need to create a deployment plan for Microsoft Defender for Identity.

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.



Question #47 *Topic 2*

You have a Microsoft 365 E5 subscription that uses Azure Advanced Threat Protection (ATP).

You need to create a detection exclusion in Azure ATP.

Which tool should you use?

- A. the Security & Compliance admin center
- B. Microsoft Defender Security Center
- C. the Microsoft 365 admin center
- D. the Azure Advanced Threat Protection portal
- E. the Cloud App Security portal

Question #49*Topic 2*

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 have a Microsoft 365 E5 subscription.
You create an account for a new security administrator named SecAdmin1.
You need to ensure that SecAdmin1 can manage Microsoft Defender for Office 365 settings and policies for Microsoft Teams, SharePoint, and OneDrive.
Solution: From the Azure Active Directory admin center, you assign SecAdmin1 the Security administrator role.
Does this meet the goal?

- A. Yes
- B. No

Question #52*Topic 2*

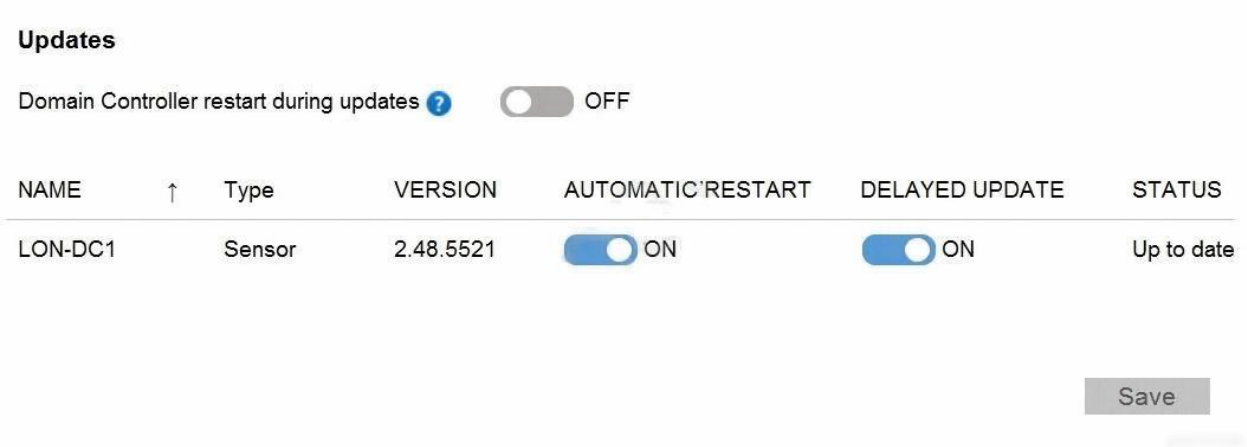
You have a Microsoft 365 subscription.
You need to be notified if users receive email containing a file that has a virus.
What should you do?

- A. From the Exchange admin center, create an in-place eDiscovery & hold.
- B. From the Security & Compliance admin center, create a data governance event.
- C. From the Exchange admin center, create an anti-malware policy.
- D. From the Exchange admin center, create a mail flow rule.

Question #53*Topic 2*

You implement Microsoft Defender for Identity.

You have a Defender for Identity sensor configured as shown in the following exhibit.



How long after the Azure ATP cloud service is updated will the sensor update?

- A. 72 hours
- B. 12 hours
- C. 48 hours
- D. 7 days
- E. 20 hours

Question #54*Topic 2*

HOTSPOT -

Your company uses Microsoft Defender Advanced Threat Protection (ATP). Microsoft Defender ATP contains the device groups shown in the following table.

Rank	Machine group	Member
1	Group1	Name starts with COMP
2	Group2	Name starts with Comp And OS In Windows 10
3	Group3	OS In Windows Server 2016
Last	Ungrouped machines (default)	*Not applicable*

You onboard computers to Microsoft Defender ATP as shown in the following table.

Name	Operating system
Computer1	Windows 10
Computer2	Windows Server 2016

Of which groups are Computer1 and Computer2 members? To answer, select the appropriate options in the answer area.

Answer Area

Computer1:
- Group1 only
- Group2 only
- Group1 and Group2
- Ungrouped machines

Computer2:
- Group1 only
- Group3 only
- Group1 and Group3

When a device is matched to more than one group, it is added only to the highest ranked group.

Question #55*Topic 2*

You have Windows 10 devices that are managed by using Microsoft Endpoint Manager.
You need to configure the security settings in Microsoft Edge.
What should you create in Microsoft Endpoint Manager?

- A. an app configuration policy
- B. an app
- C. a device configuration profile
- D. a device compliance policy

Question #56*Topic 2*

HOTSPOT -

You have a Microsoft 365 E5 tenant that contains the users shown in the following table.

Name	Role
User1	Global admin
User2	*None*
User3	*None*

You provision the private store in Microsoft Store for Business.

You assign Microsoft Store for Business roles to the users as shown in the following table.

Name	Role
User1	*None*
User2	Purchaser
User3	Basic Purchaser

You need to identify which users can add apps to the private store, and which users can assign apps from Microsoft Store for Business.

Answer Area

Can add apps to the private store:

- User2 only
- User1 and User2 only
- User2 and User3 only
- User1, User2, and User3

Can assign apps from Microsoft Store for Business:

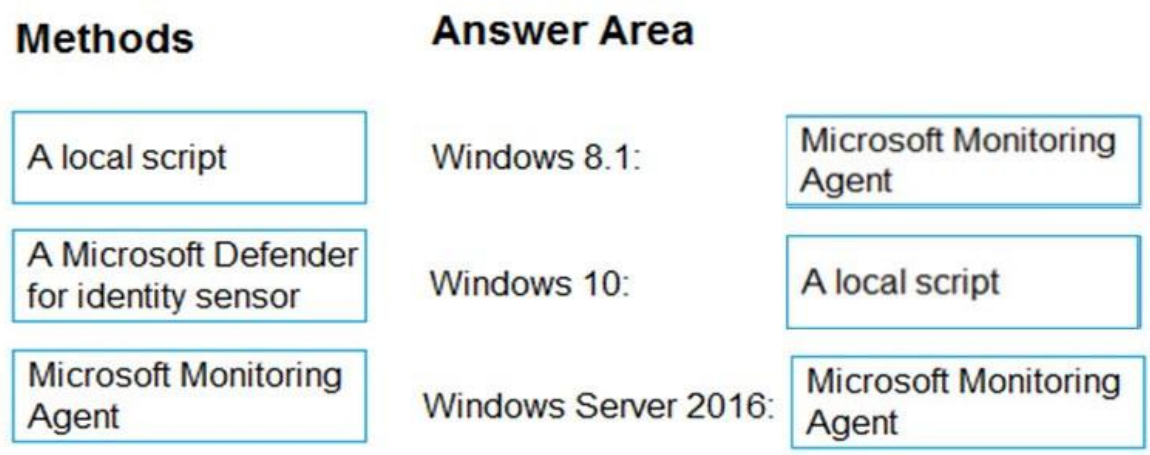
- User2 only
- User1 and User2 only
- User2 and User3 only
- User1, User2, and User3

Question #57 *Topic 2*

DRAG DROP -
You have a Microsoft 365 subscription.
You have the devices shown in the following table.

Operating system	Quantity
Windows 8.1	5
Windows 10	5
Windows Server 2016	5

You need to onboard the devices to Microsoft Defender for Endpoint. The solution must avoid installing software on the devices whenever possible.
Which onboarding method should you use for each operating system? To answer, drag the appropriate methods to the correct operating systems. Each method 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.



Question #58 *Topic 2*

The users at your company use Dropbox Business to store documents. The users access Dropbox Business by using the MyApps portal.
You need to ensure that user access to Dropbox Business is authenticated by using a Microsoft 365 identity. The documents must be protected if the data is downloaded to a device that is not trusted.
What should you do?

- A. From the Azure Active Directory admin center, configure conditional access settings.
- B. From the Azure Active Directory admin center, configure the device settings.
- C. From the Azure Active Directory admin center, configure organizational relationships settings.
- D. From the Endpoint Manager admin center, configure device enrollment settings.

Question #60 *Topic 2*

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 have a Microsoft 365 subscription.
You need to prevent users from accessing your Microsoft SharePoint Online sites unless the users are connected to your on-premises network.
Solution: From the Device Management admin center, you create a trusted location and a compliance policy
Does this meet the goal?

- A. Yes
- B. No

Question #61 *Topic 2*

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 have a Microsoft 365 subscription.
You need to prevent users from accessing your Microsoft SharePoint Online sites unless the users are connected to your on-premises network.
Solution: From the Microsoft 365 admin center, you configure the Organization profile settings.
Does this meet the goal?

- A. Yes
- B. No

Question #62*Topic 2*

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 have a Microsoft 365 subscription.
You need to prevent users from accessing your Microsoft SharePoint Online sites unless the users are connected to your on-premises network.
Solution: From the Azure Active Directory admin center, you create a trusted location and a conditional access policy.
Does this meet the goal?

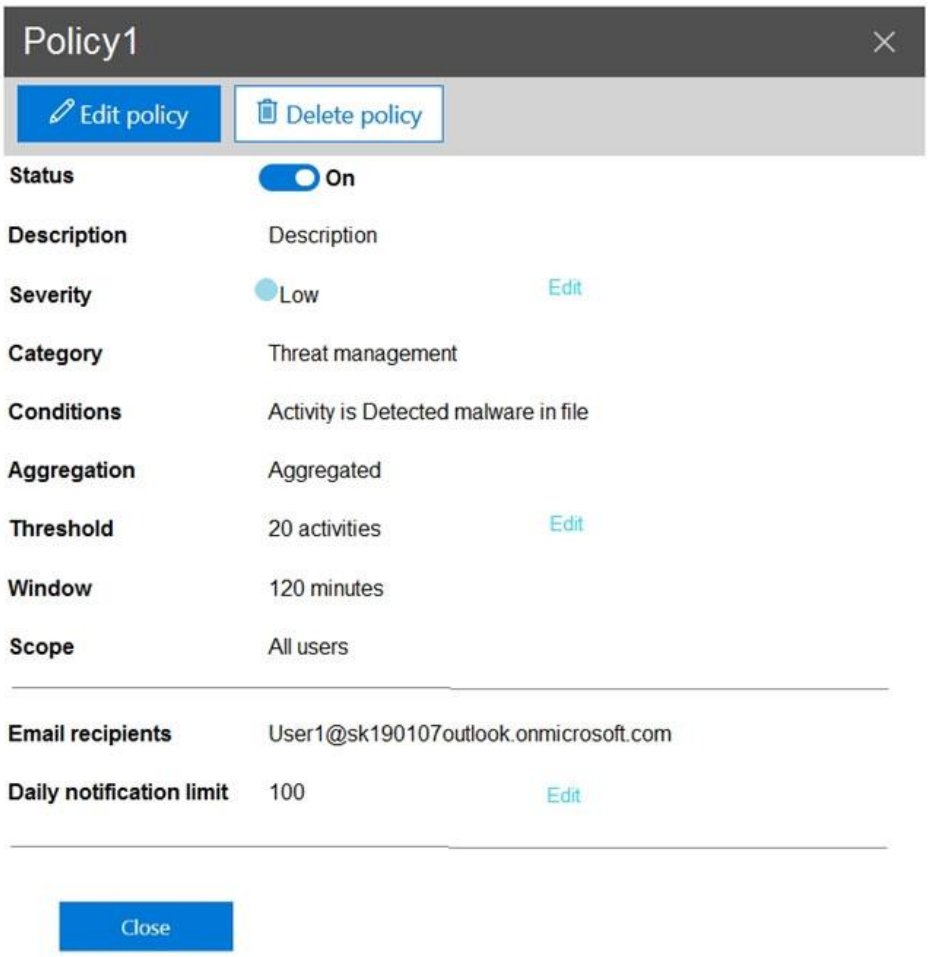
- A. Yes
- B. No

Question #63*Topic 2*

HOTSPOT -

You have Microsoft 365 subscription.

You create an alert policy as shown in the following exhibit.



Answer Area

Policy1 will trigger an alert if malware is detected in

- Exchange Online only
- SharePoint Online only
- SharePoint Online or OneDrive only
- Exchange Online, SharePoint Online, or OneDrive

The maximum number of email messages that Policy1 will generate per day is

- 5
- 12
- 20
- 100

Question #64*Topic 2*

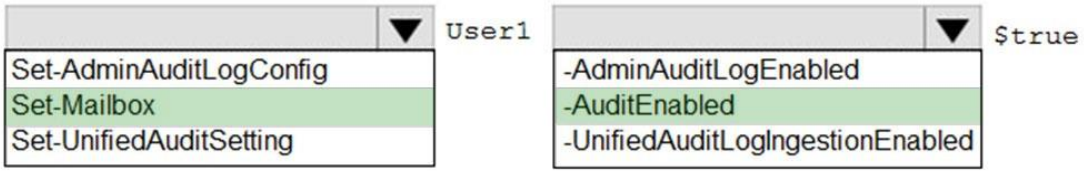
You have a Microsoft 365 subscription.
All users have their email stored in Microsoft Exchange Online.
In the mailbox of a user named User1, you need to preserve a copy of all the email messages that contain the word ProjectX.
What should you do?

- A. From the Security & Compliance admin center, create a label and a label policy.
- B. From the Exchange admin center, create a mail flow rule.
- C. From the Security & Compliance admin center, start a message trace.
- D. From Exchange admin center, start a mail flow message trace.

Question #65*Topic 2*

HOTSPOT -
You have a new Microsoft 365 subscription.
A user named User1 has a mailbox in Microsoft Exchange Online.
You need to log any changes to the mailbox folder permissions of User1.
Which command should you run? To answer, select the appropriate options in the answer area.

Answer Area



Question #66*Topic 2*

You have a Microsoft 365 subscription.
You recently configured a Microsoft SharePoint Online tenant in the subscription.
You plan to create an alert policy.
You need to ensure that an alert is generated only when malware is detected in more than five documents stored in SharePoint Online during a period of 10 minutes.
What should you do first?

- A. Enable Microsoft Office 365 Cloud App Security.
- B. Deploy Microsoft Defender Advanced Threat Protection (Microsoft Defender ATP)
- C. Enable Microsoft Office 365 Analytics.

Question #67*Topic 2*

DRAG DROP -

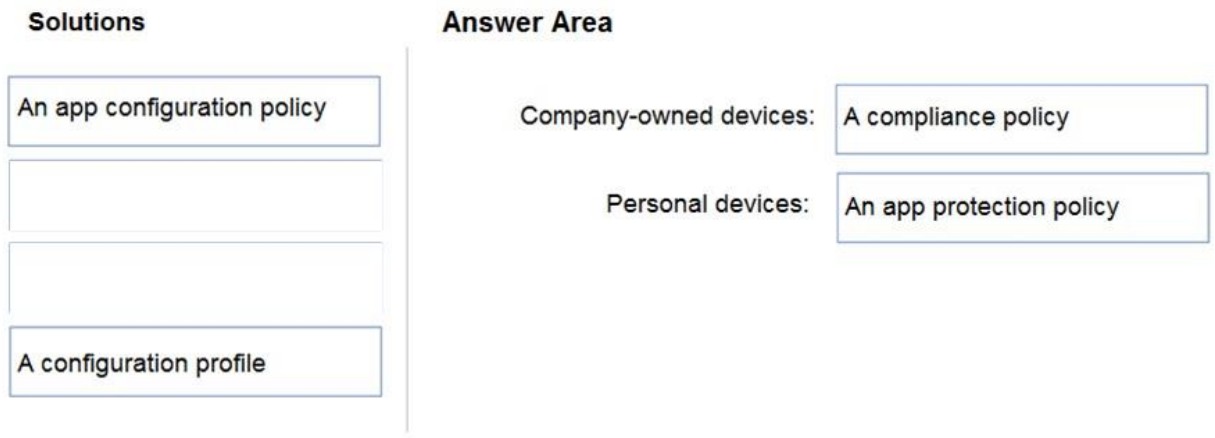
Your company has a Microsoft 365 E5 tenant.

Users access resources in the tenant by using both personal and company-owned Android devices.

Company policies requires that the devices have a threat level of medium or lower to access Microsoft Exchange Online mailboxes.

You need to recommend a solution to identify the threat level of the devices and to control access of the devices to the resources.

What should you include in the solution for each device type? To answer, drag the appropriate components to the correct devices. Each component 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.



Question #68*Topic 2*

HOTSPOT -

You have a Microsoft 365 E5 tenant that contains five devices enrolled in Microsoft Intune as shown in the following table.

Name	Platform
Device1	Windows 10
Device2	Android 8.1.0
Device3	Android 10
Device4	iOS 12
Device5	iOS 14

All the devices have an app named App1 installed.

You need to prevent users from copying data from App1 and pasting the data into other apps.

Which policy should you create in Microsoft Endpoint Manager, and what is the minimum number of required policies? To answer, select the appropriate options in the answer area.

Answer Area

Policy to create in Microsoft Endpoint Manager:

- An app configuration policy
- **An app protection policy**
- A conditional access policy
- A device compliance policy

Minimum number of required policies:

- **1**
- 2
- 3
- 5

Question #69 *Topic 2*

You have a Microsoft 365 tenant.
You plan to manage incidents in the tenant by using the Microsoft 365 Defender.
Which Microsoft service source will appear on the Incidents page of the Microsoft 365 Defender?

- A. Microsoft Cloud App Security
- B. Azure Sentinel
- C. Azure Web Application Firewall
- D. Azure Information Protection

Question #70 *Topic 2*

You have a Microsoft 365 tenant.
You plan to manage incidents in the tenant by using the Microsoft 365 Defender.
Which Microsoft service source will appear on the Incidents page of the Microsoft 365 Defender?

- A. Azure Sentinel
- B. Azure Information Protection
- C. Azure Security Center
- D. Microsoft Defender for Identity

Question #71 *Topic 2*

You have a Microsoft 365 E5 subscription.
All users have Mac computers. All the computers are enrolled in Microsoft Endpoint Manager and onboarded to Microsoft Defender Advanced Threat Protection
(Microsoft Defender ATP).
You need to configure Microsoft Defender ATP on the computers.
What should you create from the Endpoint Management admin center?

- A. a Microsoft Defender ATP baseline profile
- B. a device configuration profile
- C. an update policy for iOS
- D. a mobile device management (MDM) security baseline profile

Question #72*Topic 2*

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

Name	Severity	Status	Comment	Category
Alert1	Medium	Active	Comment1	Threat management
Alert2	Low	Resolved	Comment2	Other

Which properties of the alerts can you modify?

- A. Status only
- B. Status and Comment only
- C. Status and Severity only
- D. Status, Severity, and Comment only
- E. Status, Severity, Comment and Category

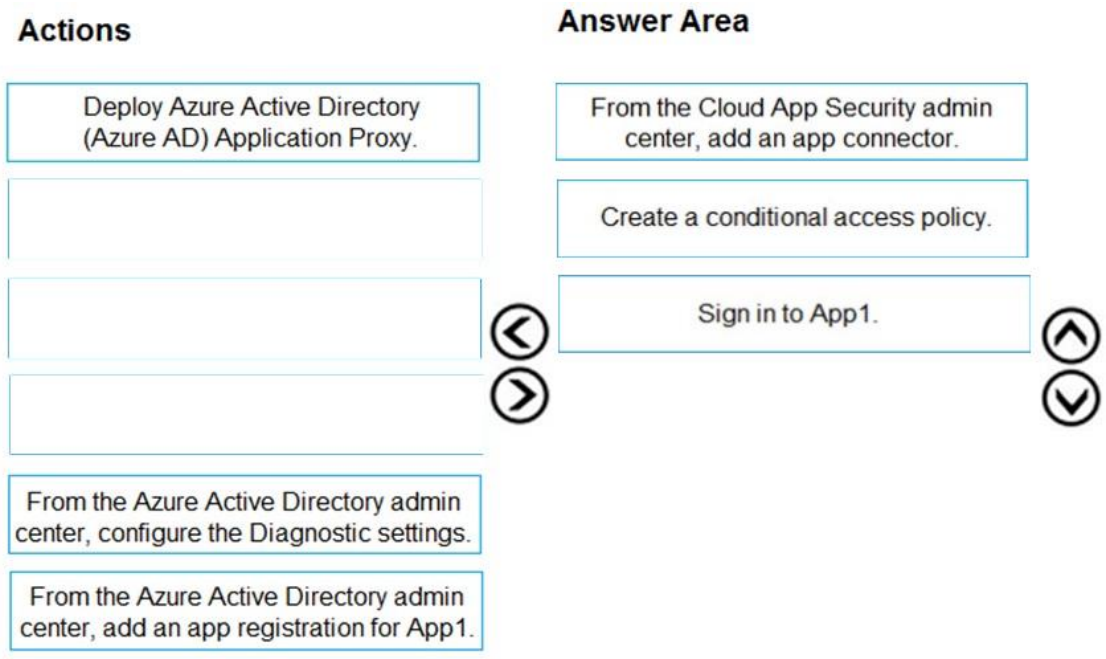
Question #73*Topic 2*

DRAG DROP -

Your company purchases a cloud app named App1.

You need to ensure that you can use Microsoft Cloud App Security to block downloads in App1. App1 supports session controls.

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.



Question #74*Topic 2*

You have a Microsoft 365 E5 subscription that has Microsoft Defender for Endpoint integrated with Microsoft Endpoint Manager.
Devices are onboarded by using Microsoft Defender for Endpoint.
You plan to block devices based on the results of the machine risk score calculated by Microsoft Defender for Endpoint.
What should you create first?

- A. a device configuration policy
- B. a device compliance policy Most Voted
- C. a conditional access policy
- D. an endpoint detection and response policy

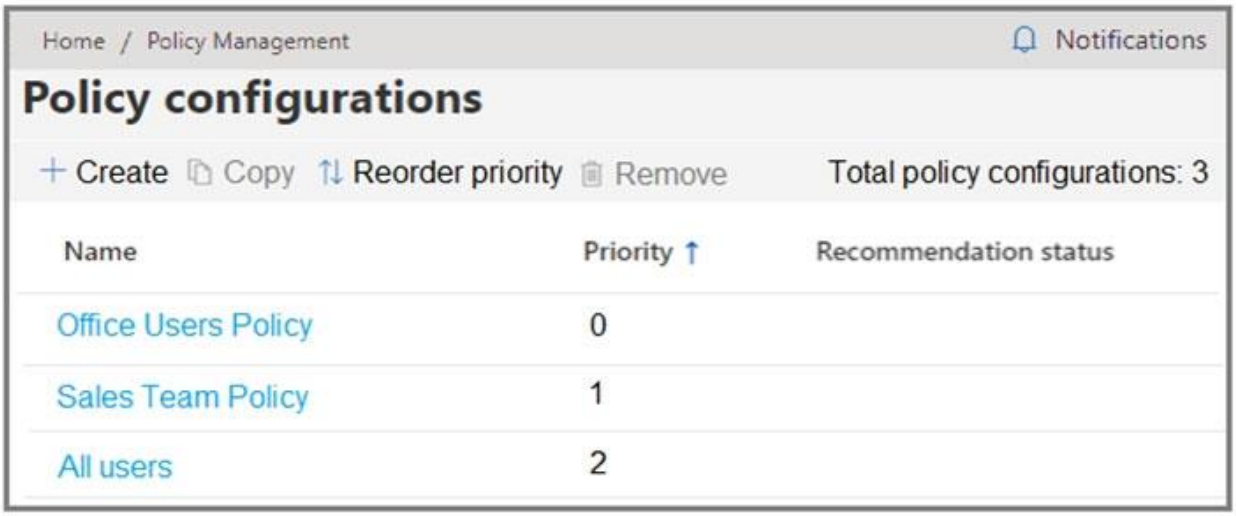
Question #75*Topic 2*

HOTSPOT -

You have a Microsoft 365 subscription that contains three groups named All users, Sales team, and Office users, and two users shown in the following table.

Name	Member of
User1	All users, Sales team
User2	All users, Office users

In Microsoft Endpoint Manager, you have the Policies for Office apps settings shown in the following exhibit.

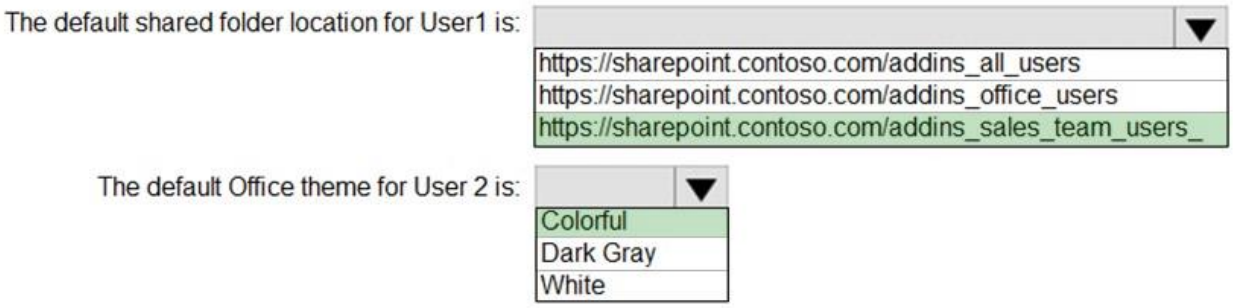


The policies use the settings shown in the following table.

Policy	Default Shared Folder Location	Default Office Theme
All users	https://sharepoint.contoso.com/addins_all_users	Colorful
Office Users Policy	https://sharepoint.contoso.com/addins_office_users	White
Sales Team Policy	https://sharepoint.contoso.com/addins_sales_team_users_	Dark Gray

What is the default share folder location for User1 and the default Office theme for User2? To answer, select the appropriate options in the answer area.

Answer Area



Question #76 *Topic 2*

You have a Microsoft 365 tenant that contains a Windows 10 device. The device is onboarded to Microsoft Defender for Endpoint.
From Microsoft Defender Security Center, you perform a security investigation.
You need to run a PowerShell script on the device to collect forensic information.
Which action should you select on the device page?

- A. Initiate Live Response Session
- B. Initiate Automated Investigation
- C. Collect investigation package
- D. Go hunt

Question #77 *Topic 2*

You have a Microsoft 365 E5 subscription.
You plan to implement Microsoft 365 compliance policies to meet the following requirements:
☞ Identify documents that are stored in Microsoft Teams and SharePoint Online that contain Personally Identifiable Information (PII).
☞ Report on shared documents that contain PII.
What should you create?

- A. an alert policy
- B. a data loss prevention (DLP) policy
- C. a retention policy
- D. a Microsoft Cloud App Security policy

Question #78*Topic 2*

HOTSPOT -

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

Name	Member of
User1	Group1, Group2
User2	Group2, Group3
User3	Group1, Group3

In Microsoft Endpoint Manager, you have the Policies for Office apps settings shown in the following table.

Name	Priority	Applies to
Policy1	0	Group1
Policy2	1	Group2
Policy3	2	Group3

The policies use the settings shown in the following table.

Name	Cursor movement	Clear cache on close
Policy1	Logical	Disabled
Policy2	Not configured	Enabled
Policy3	Visual	Enabled

For each of the following statements, select Yes if the statement is true. Otherwise, select No.

Answer Area

Statements	Yes	No
User1 has their cache cleared on close.	○	○
User2 has Cursor movement set to Visual.	○	○
User3 has Cursor movement set to Visual.	○	○

Question #79 *Topic 2*

You have a Microsoft 365 E5 tenant that contains the devices shown in the following table.

Name	Platform
Device1	MacOS
Device2	Windows 10 Pro
Device3	Windows 10 Enterprise
Device4	Ubuntu 18.04 LTS

You plan to implement attack surface reduction (ASR) rules.
Which devices will support the ASR rules?

- A. Device1, Device2, Device3, and Device4
- B. Device1, Device2, and Device3 only
- C. Device2 and Device3 only Most Voted
- D. Device3 only

Question #80 *Topic 2*

You have a Microsoft 365 tenant.
You plan to enable BitLocker Disk Encryption (BitLocker) automatically for all Windows 10 devices that enroll in Microsoft Intune.
What should you use?

- A. an attack surface reduction (ASR) policy
- B. an app configuration policy
- C. a device compliance policy
- D. a device configuration profile

Question #81 *Topic 2*

You have a Microsoft 365 tenant.
You plan to implement Endpoint Protection device configuration profiles.
Which platform can you manage by using the profiles?

- A. Android Enterprise
- B. Windows 10
- C. Windows 8.1
- D. Android

Question #82*Topic 2*

You have a Microsoft 365 tenant that contains 500 Windows 10 devices and a Microsoft Endpoint Manager device compliance policy.
You need to ensure that only devices marked as compliant can access Microsoft Office 365 apps.
Which policy type should you configure?

- A. conditional access
- B. account protection
- C. attack surface reduction (ASR)
- D. Endpoint detection and response

Question #83*Topic 2*

You have a Microsoft 365 tenant that contains a Windows 10 device named Device1 and the Microsoft Endpoint Manager policies shown in the following table.

Name	Type	Block execution of potentially obfuscated scripts (js/vbs/ps)
Policy1	Attack surface reduction (ASR)	Audit mode
Policy2	Microsoft Defender ATP Baseline	Disable
Policy3	Device configuration profile	Not configured

The policies are assigned to Device1.
Which policy settings will be applied to Device1?

- A. only the settings of Policy1
- B. only the settings of Policy2
- C. only the settings of Policy3
- D. no settings

Hide Solution | Discussion 17

Correct Answer: *C*

Community vote distribution

A (100%)

Question #84*Topic 2*

HOTSPOT -

You have a Microsoft 365 E5 tenant that contains 100 Windows 10 devices.

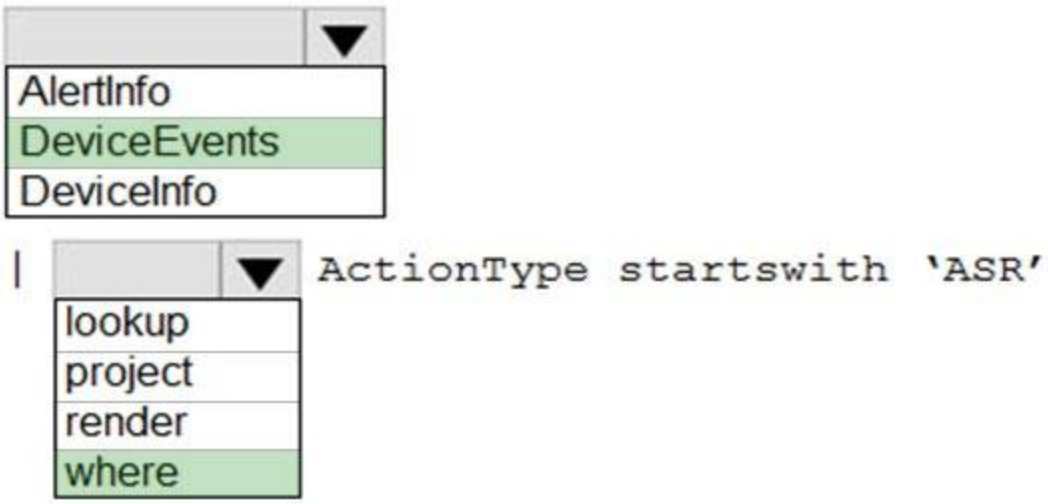
You plan to attack surface reduction (ASR) rules for the Windows 10 devices.

You configure the ASR rules in audit mode and collect audit data in a Log Analytics workspace.

You need to find the ASR rules that match the activities on the devices.

How should you complete the Kusto query? To answer, select the appropriate options in the answer area.

Answer Area



Question #85*Topic 2*

HOTSPOT -

You have a Microsoft 365 E5 tenant that connects to Microsoft Defender for Endpoint.

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

Name	Platform
Device1	Windows 10
Device2	Windows 8.1
Device3	iOS
Device4	Android

You plan to use risk levels in Microsoft Defender for Endpoint to identify whether a device is compliant. Noncompliant devices must be blocked from accessing corporate resources.

You need to identify which devices can be onboarded to Microsoft Defender for Endpoint, and which Endpoint security policies must be configured.

Answer Area

Devices that can onboarded to Microsoft Defender for Endpoint:

- Device 1 only
- Device 1 and Device 2 only
- Device 1 and Device 3 only
- Device 1 and Device 4 only
- Device 1, Device 2, and Device 4 only
- Device 1, Device 2, Device 3, and Device 4

Endpoint security policies that must be configured:

- A conditional access policy only
- A device compliance policy only
- A device configuration profile only
- A device configuration profile and a conditional access policy only
- Device configuration profile, device compliance policy, and conditional access policy

Question #86*Topic 2*

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

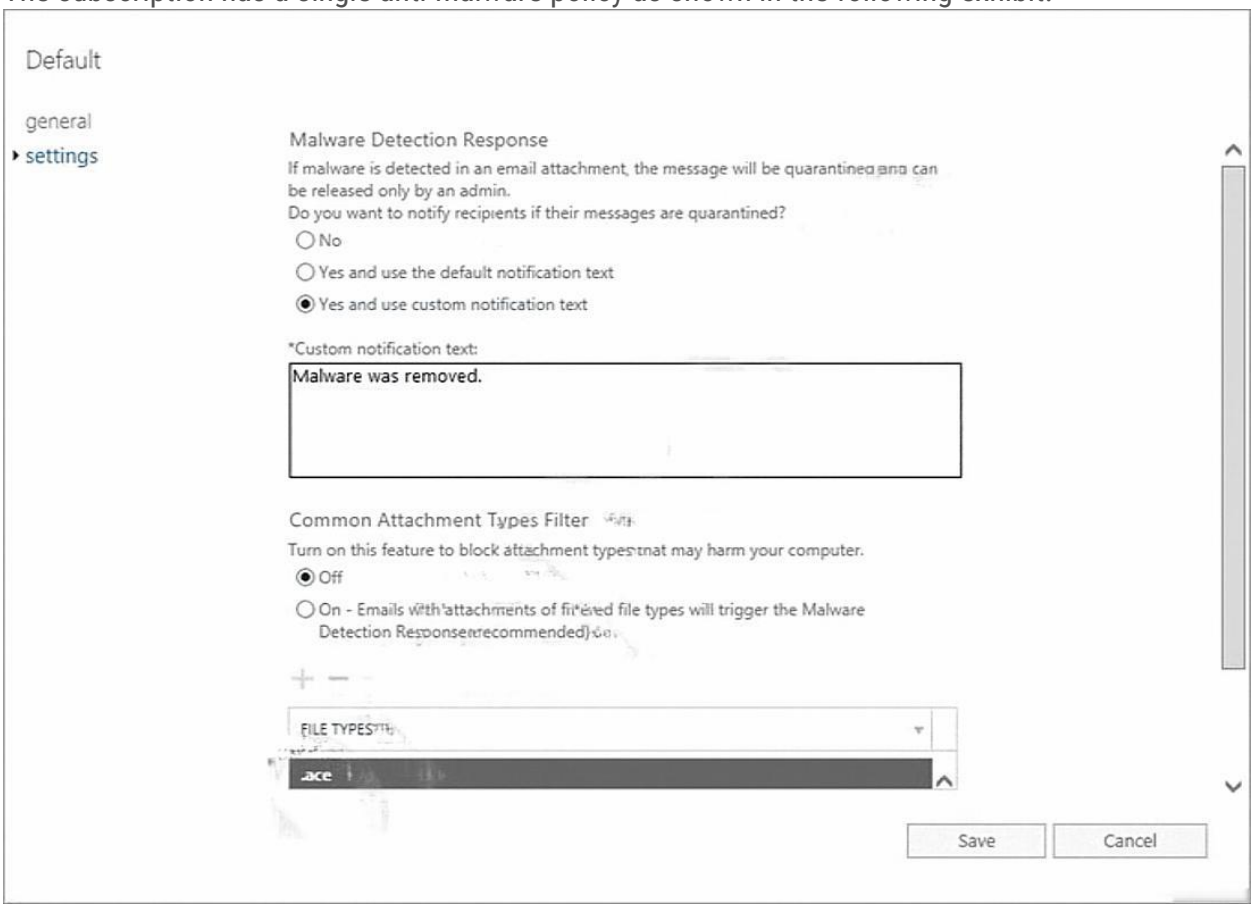
Name	Type
Group1	Distribution
Group2	Mail-enabled security
Group3	Security

You plan to create a new Windows 10 Security Baseline profile.
To which groups can you assign to the profile?

- A. Group3 only
- B. Group1 and Group3 only
- C. Group2 and Group3 only Most Voted
- D. Group1, Group2, and Group3

Question #87 *Topic 2*

You have a Microsoft 365 E5 subscription that contains a user named User1.
The subscription has a single anti-malware policy as shown in the following exhibit.



An email message that contains text and two attachments is sent to User1. One attachment is infected with malware.
How will the email message and the attachments be processed?

- A. Both attachments will be removed. The email message will be quarantined, and User1 will receive an email message without any attachments and an email message that includes the following text: ג€Malware was removed.ג€
- B. The email message will be quarantined, and the message will remain undelivered.
- C. Both attachments will be removed. The email message will be quarantined, and User1 will receive a copy of the message containing the original text and a new attachment that includes the following text: ג€Malware was removed.ג€ **Most Voted**
- D. The malware-infected attachment will be removed. The email message will be quarantined, and User1 will receive a copy of the message containing only the uninfected attachment.

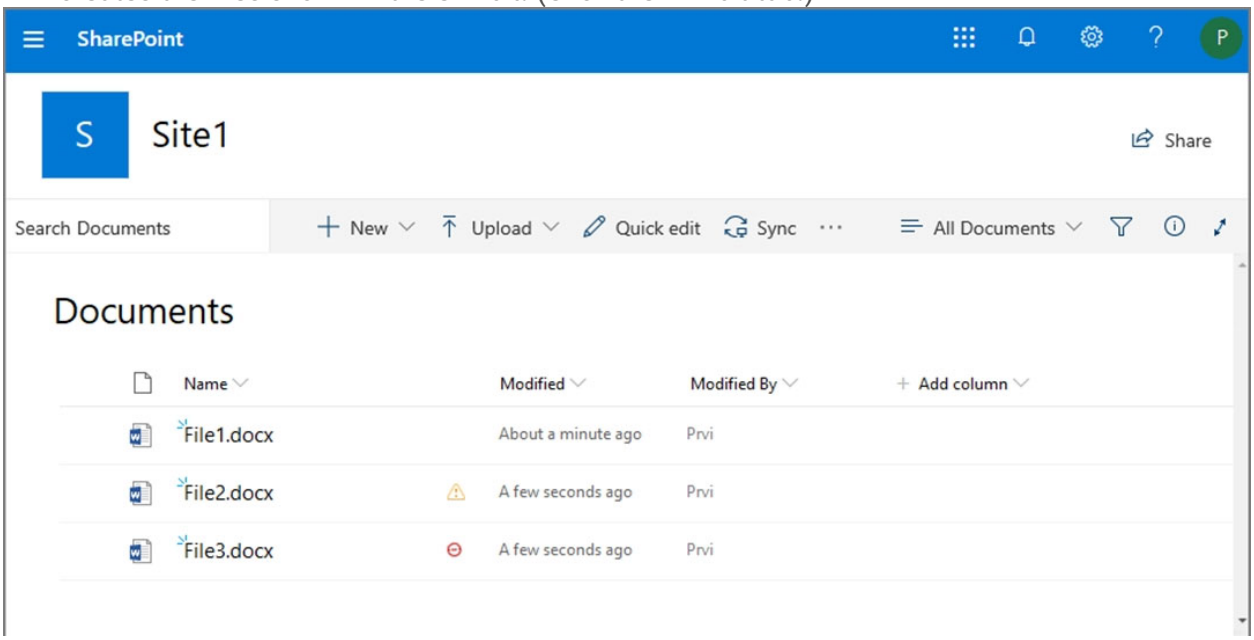
Question #88 *Topic 2*

HOTSPOT -

From the Microsoft 365 compliance center, you configure a data loss prevention (DLP) policy for a Microsoft SharePoint Online site named Site1. Site1 contains the roles shown in the following table.

Role	Member
Site owner	Prvi
Site member	User1
Site visitor	User2

Prvi creates the files shown in the exhibit. (Click the Exhibit tab.)



Which files can User1 and User2 open? To answer, select the appropriate options in the answer area.

Answer Area

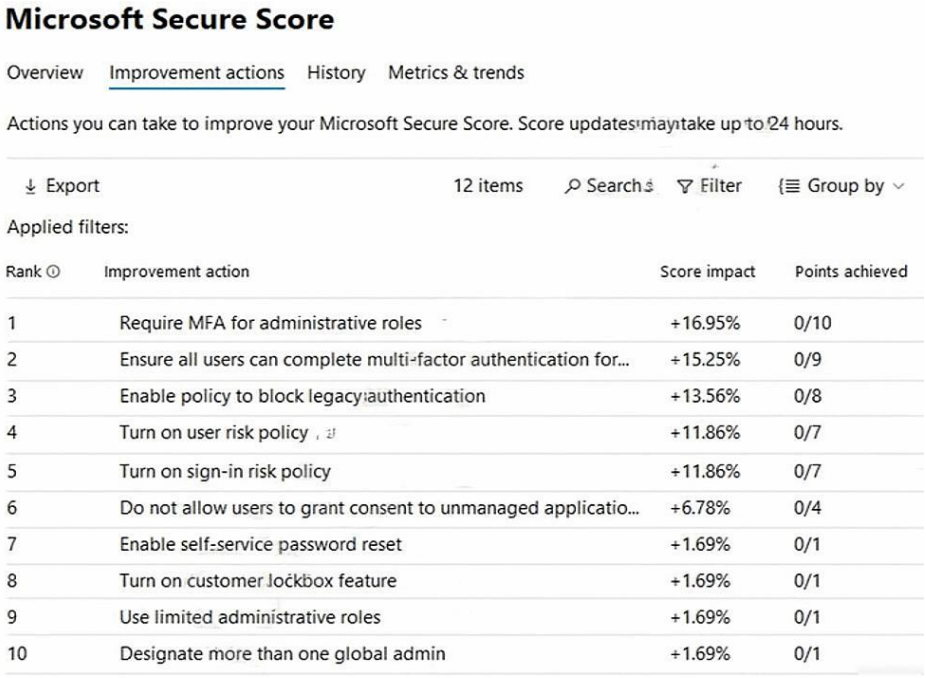
User1:
- File1.docx only
- File1.docx and File2.docx only
- File1.docx, File2.docx, and File3.docx

User2:
- File1.docx only
- File1.docx and File2.docx only
- File1.docx, File2.docx, and File3.docx

Question #89 *Topic 2*

You have a Microsoft 365 E5 tenant.

The Microsoft Secure Score for the tenant is shown in the following exhibit.



Microsoft Secure Score

Overview | Improvement actions | History | Metrics & trends

Actions you can take to improve your Microsoft Secure Score. Score updates may take up to 24 hours.

Export | 12 items | Search | Filter | Group by

Applied filters:

Rank	Improvement action	Score impact	Points achieved
1	Require MFA for administrative roles	+16.95%	0/10
2	Ensure all users can complete multi-factor authentication for...	+15.25%	0/9
3	Enable policy to block legacy authentication	+13.56%	0/8
4	Turn on user risk policy	+11.86%	0/7
5	Turn on sign-in risk policy	+11.86%	0/7
6	Do not allow users to grant consent to unmanaged applicatio...	+6.78%	0/4
7	Enable self-service password reset	+1.69%	0/1
8	Turn on customer lockbox feature	+1.69%	0/1
9	Use limited administrative roles	+1.69%	0/1
10	Designate more than one global admin	+1.69%	0/1

You plan to enable Security defaults for Azure Active Directory (Azure AD).

- A. Require MFA for administrative roles. Most Voted
- B. Ensure all users can complete multi-factor authentication for secure access Most Voted
- C. Enable policy to block legacy authentication Most Voted
- D. Enable self-service password reset
- E. Use limited administrative roles

Question #90*Topic 2*

You have a Microsoft 365 E5 subscription.
You need to identify which users accessed Microsoft Office 365 from anonymous IP addresses during the last seven days.
What should you do?

- A. From the Cloud App Security admin center, select Users and accounts.
- B. From the Microsoft 365 Defender, view the Threat tracker.
- C. From the Microsoft 365 admin center, view the Security & compliance report.
- D. From the Azure Active Directory admin center, view the Risky sign-ins report. Most Voted

- Question #91*Topic 2*
- HOTSPOT -
  You have a Microsoft 365 tenant that contains 100 Windows 10 devices. The devices are managed by using Microsoft Endpoint Manager.
  You plan to create two attack surface reduction (ASR) policies named ASR1 and ASR2.
  ASR1 will be used to configure Microsoft Defender Application Guard.
  ASR2 will be used to configure Microsoft Defender SmartScreen.
  Which ASR profile type should you use for each policy? To answer, select the appropriate options in the answer area.
  NOTE: Each correct selection is worth one point.

Answer Area

ASR1:

Device control
Exploit protection
Application control
App and browser isolation
Attack surface reduction rules

ASR2:

Device control
Exploit protection
Application control
App and browser isolation
Attack surface reduction rules

Question #92*Topic 2*

You have a Microsoft 365 tenant.
You plan to implement Endpoint Protection device configuration profiles.
Which platform can you manage by using the profiles?

- A. Ubuntu Linux
- B. macOS
- C. iOS
- D. Android

uestion #93*Topic 2*

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 have a Microsoft 365 E5 subscription that contains a user named User1.
You need to enable User1 to create Compliance Manager assessments.
Solution: From the Microsoft 365 admin center, you assign User1 the Compliance data admin role.
Does this meet the goal?

- A. Yes
- B. No

Question #94*Topic 2*

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 have a Microsoft 365 E5 subscription that contains a user named User1.
You need to enable User1 to create Compliance Manager assessments.
Solution: From the Microsoft 365 admin center, you assign User1 the Compliance admin role.
Does this meet the goal?

- A. Yes
- B. No

Question #95*Topic 2*

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 have a Microsoft 365 E5 subscription that contains a user named User1.
You need to enable User1 to create Compliance Manager assessments.
Solution: From the Microsoft 365 compliance center, you add User1 to the Compliance Manager Assessors role group.
Does this meet the goal?

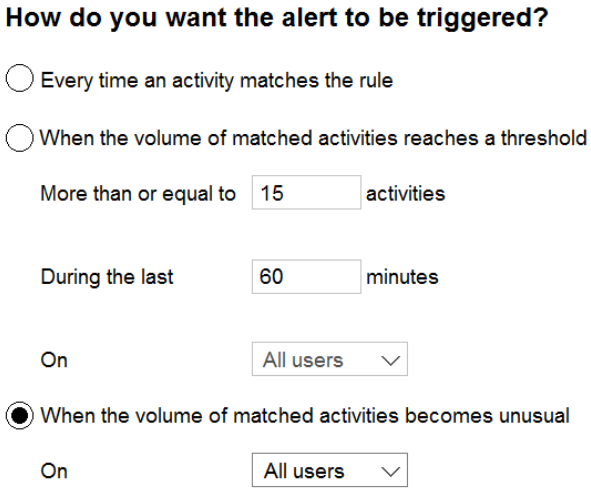
- A. Yes
- B. No

Question #96 *Topic 2*

HOTSPOT -

You have a Microsoft 365 E5 subscription.

You configure a new alert policy as shown in the following exhibit.



You need to identify the following:

- How many days it will take to establish a baseline for unusual activity.
- Whether alerts will be triggered during the establishment of the baseline.

What should you identify? To answer, select the appropriate options in the answer area.

Answer Area

How many days it will take to establish the baseline:

- 1
- 5
- 7
- 10

Whether the alerts will be triggered during the establishment of the baseline:

- Alerts will be triggered.
- Alerts will not be triggered.
- Alerts will be triggered only after the process to establish the baseline has been running for one day.

Question #97 *Topic 2*

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

Platform	Count
Windows 10	50
Android	50
Linux	50

You need to configure an incident email notification rule that will be triggered when an alert occurs only on a Windows 10 device. The solution must minimize administrative effort.
What should you do first?

- A. From the Microsoft 365 admin center, create a mail-enabled security group.
- B. From the Microsoft 365 Defender portal, create a device group.
- C. From the Microsoft Endpoint Manager admin center, create a device category.
- D. From the Azure Active Directory admin center, create a dynamic device group.

Question #1 *Topic 3*

You have a Microsoft 365 subscription.
All users have their email stored in Microsoft Exchange Online.
In the mailbox of a user named User1, you need to preserve a copy of all the email messages that contain the word ProjectX.
What should you do?

- A. From the Security & Compliance admin center, create a data loss prevention (DLP) policy.
- B. From the Security & Compliance admin center, create a label and a label policy.
- C. From the Security & Compliance admin center, start a message trace.
- D. From Microsoft Cloud App Security, create an activity policy.

Question #2*Topic 3*

You have a Microsoft 365 tenant.
You discover that administrative tasks are unavailable in the Microsoft 365 audit logs of the tenant.
You run the Get-AdminAuditLogConfig cmdlet and receive the following output:

You need to ensure that administrative tasks are logged in the Microsoft 365 audit logs.
Which attribute should you modify?

- A. TestCmdletLoggingEnabled
- B. UnifiedAuditLogIngestionEnabled
- C. AdminAuditLogEnabled

Question #3*Topic 3*

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 have a new Microsoft 365 subscription.
You need to prevent users from sending email messages that contain Personally Identifiable Information (PII).
Solution: From the Microsoft 365 compliance center, you create a data loss prevention (DLP) policy.
Does this meet the goal?

- A. Yes Most Voted
- B. No

Question #5*Topic 3*

HOTSPOT -

You configure an anti-phishing policy as shown in the following exhibit.

Policy setting	**Policy name**	Managers	
	Description		
	Applied to	If the email is sent to: IrvinS@M365x289755.OnMicrosoft.com MiriamG@M365x289755.OnMicrosoft.com Except if the email is sent to member of: test1ww@M365x289755.OnMicrosoft.com	Edit
Impersonation	**Users to protect**	On - 3 User(s) specified	
	Protect all domains I own	On	
	Protect specific domains	On - 2 Domain(s) specified	
	Action > User impersonation	Move message to the recipients' Junk Email folders	
	Action > Domain impersonation	Delete the message before it's delivered	Edit
	Safety tips > User impersonation	Off	
	Safety tips > Domain impersonation	Off	
	Safety tips > Unusual characters	Off	
	Mailbox intelligence	Off	
Spoof	**Enable antispoofing protection**	On	
	Action	Quarantine the message	Edit
Advanced settings	**Advanced phishing thresholds**	3 - More Aggressive	Edit

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

If a message is identified as a domain impersonation, **[answer choice]**.

- the message is delivered to the Inbox folder
- the message is moved to the Deleted Items folder
- the message is moved to the Junk Email folder
- **the message is NOT delivered**

To reduce the likelihood of the impersonation policy generating false positives, configure **[answer choice]**.

- Domain impersonation
- Enable antispoofing protection
- **Mailbox intelligence**

Question #6*Topic 3*

You need to notify the manager of the human resources department when a user in the department shares a file or folder from the department's Microsoft
SharePoint Online site.
What should you do?

- A. From the Security & Compliance admin center, create an alert policy.
- B. From the SharePoint Online site, create an alert.
- C. From the SharePoint Online admin center, modify the sharing settings.
- D. From the Security & Compliance admin center, create a data loss prevention (DLP) policy.

- Question #7*Topic 3*
- HOTSPOT -
  You have a Microsoft 365 subscription.
  You are configuring permissions for Security & Compliance.
  You need to ensure that the users can perform the tasks shown in the following table.

Name	Task
User1	Download all Security & Compliance reports
User2	Create and manage Security & Compliance alerts.

The solution must use the principle of least privilege.
To which role should you assign each user? To answer, select the appropriate options in the answer area.

Answer Area

User1:
- Records Management
- Security Administrator
- Security Reader
- Supervisory Review

User2:
- Compliance Administrator
- Organization Management
- Security Administrator
- Security Reader
- Supervisory Review

Question #8*Topic 3*

HOTSPOT -

You have a Microsoft Azure Active Directory (Azure AD) tenant.

Your company implements Windows Information Protection (WIP).

You need to modify which users and applications are affected by WIP.

What should you do? To answer, select the appropriate options in the answer area.

NOTE: Each correct selection is worth one point.

Hot Area:

Answer Area

To modify which users are affected by WIP, configure:

- The Azure AD app registration
- The Azure AD device settings
- **The MAM User scope**
- The mobile device management (MDM) authority

To modify which applications are affected by WIP, configure:

- App configuration policies
- **App protection policies**
- Compliance policies
- Device configuration profiles

Question #9*Topic 3*

HOTSPOT -

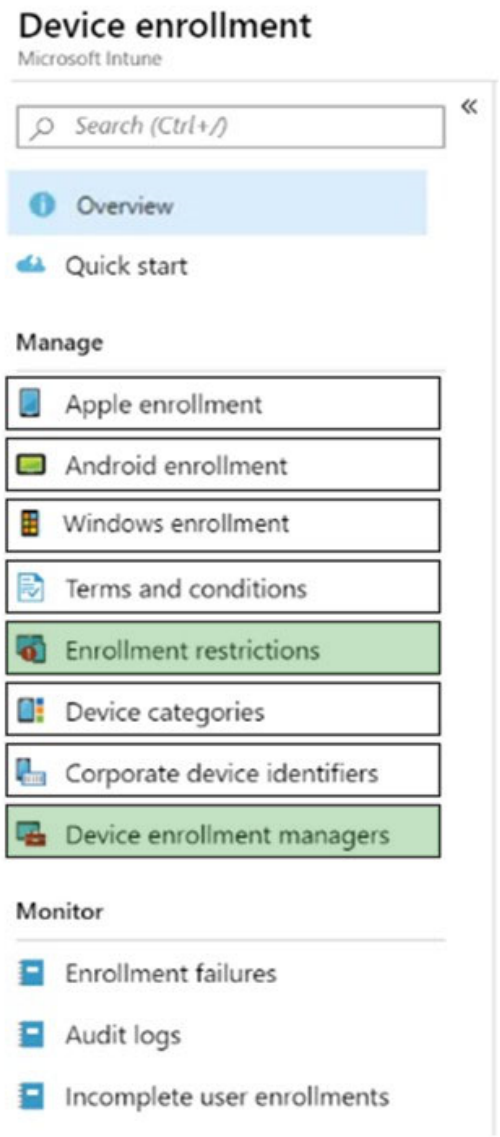
You have a Microsoft 365 subscription.

All users are assigned Microsoft Azure Active Directory Premium licenses.

From the Device Management admin center, you set Microsoft Intune as the MDM authority.

You need to ensure that when the members of a group named Marketing join a device to Azure Active Directory (Azure AD), the device is enrolled automatically in
Intune. The Marketing group members must be limited to five devices enrolled in Intune.

Which two options should you use to perform the configurations? To answer, select the appropriate blades in the answer area.



Question #10*Topic 3*

You have a Microsoft 365 subscription.
You plan to enable Microsoft Azure Information Protection.
You need to ensure that only the members of a group named PilotUsers can protect content.
What should you do?

- A. Run the Set-AadrmOnboardingControlPolicy cmdlet. Most Voted
- B. Run the Add-AadrmRoleBasedAdministrator cmdlet.
- C. Create an Azure Information Protection policy.
- D. Configure the protection activation status for Azure Information Protection.

uestion #11*Topic 3*

Your company has a Microsoft 365 subscription.
You need to identify which users performed the following privileged administration tasks:
☞ Deleted a folder from the second-stage Recycle Bin of Microsoft SharePoint
☞ Opened a mailbox of which the user was not the owner
☞ Reset a user password
What should you use?

- A. Microsoft Azure Active Directory (Azure AD) audit logs
- B. Microsoft 365 compliance content search
- C. Microsoft Azure Active Directory (Azure AD) sign-ins
- D. Microsoft 365 compliance audit log search Most Voted

Question #12*Topic 3*

You have a Microsoft 365 subscription. You have a user named User1.
You need to ensure that User1 can place a litigation hold on all mailbox content.
What permission should you assign to User1?

- A. the eDiscovery Manager role from the Microsoft 365 compliance center
- B. the Compliance Management role from the Exchange admin center
- C. the User management administrator role from Microsoft 365 admin center
- D. the Information Protection administrator role from the Azure Active Directory admin center

Question #13*Topic 3*

You have a Microsoft 365 subscription.
All users are assigned a Microsoft 365 E3 license.
You enable auditing for your organization.
What is the maximum amount of time data will be retained in the Microsoft 365 audit log?

- A. 2 years
- B. 1 year
- C. 30 days
- D. 90 days

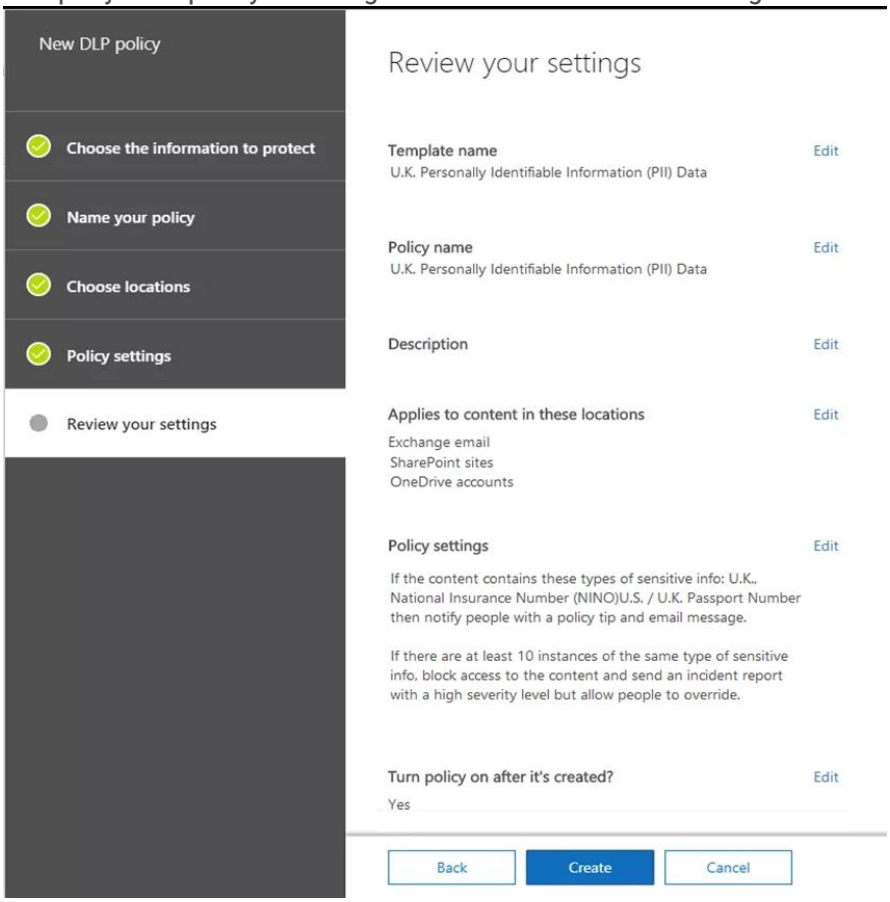
Question #14*Topic 3*

HOTSPOT -

Your company is based in the United Kingdom (UK).

Users frequently handle data that contains Personally Identifiable Information (PII).

You create a data loss prevention (DLP) policy that applies to users inside and outside the company. The policy is configured as shown in the following exhibit.



Answer Area

If a user attempts to upload a document to a Microsoft SharePoint site, and the document contains one UK passport number, the document will be [**answer choice**].

- allowed
- blocked without warning
- **blocked, but the user can override the policy**

If a user attempts to email 100 UK passport numbers to a user in the same company, the email message will be [**answer choice**].

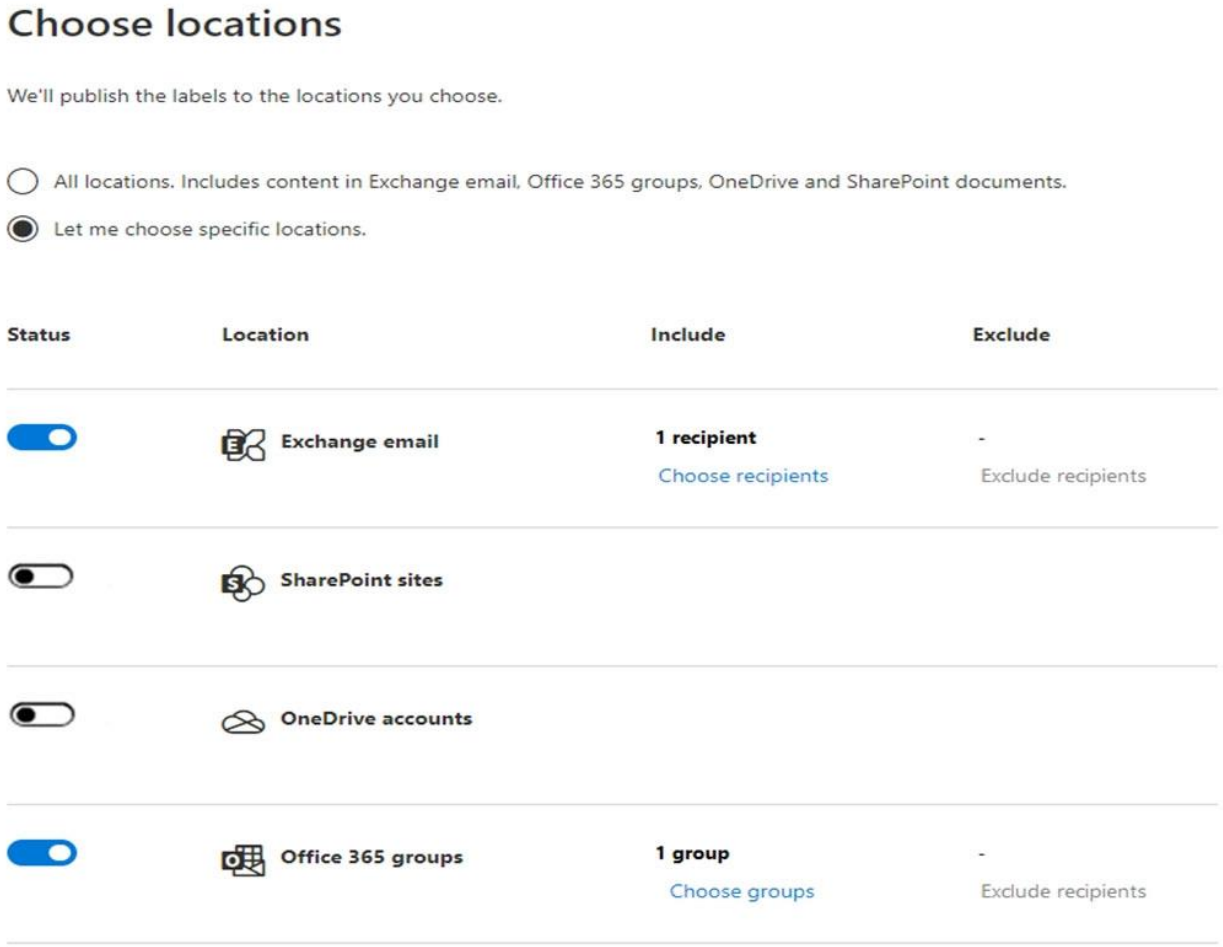
- allowed
- **blocked without warning**
- blocked, but the user can override the policy

Question #15*Topic 3*

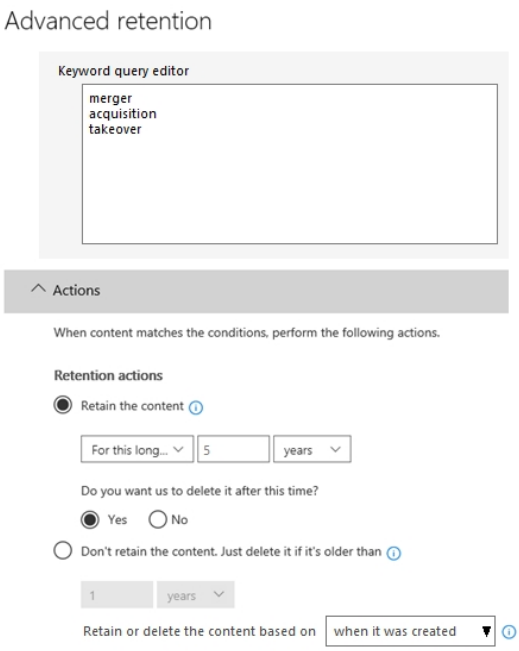
HOTSPOT -

You have a Microsoft 365 subscription that contains all the user data.

You plan to create the retention policy shown in the Choose Locations exhibit. (Click the Choose Locations tab.)



You configure the Advanced retention settings as shown in the Retention exhibit. (Click the Retention tab.)



The locations specified in the policy include the groups shown in the following table.

Location	Include
Exchange email	A distribution group named LegalDL
Office 365 groups	A security group named LegalSG

Answer Area

Statements	Yes	No
Any file stored in the Microsoft SharePoint Online group library by a user in the LegalSG group will be stored for five years, and then deleted.	○	○
An email message that contains the word takeover and is sent by a user in the LegalDL group will be deleted automatically after five years.	○	○
A user sends an email message that contains the word takeover. The following week, the user is added to the LegalDL group. The message will be deleted automatically after five years.	○	○

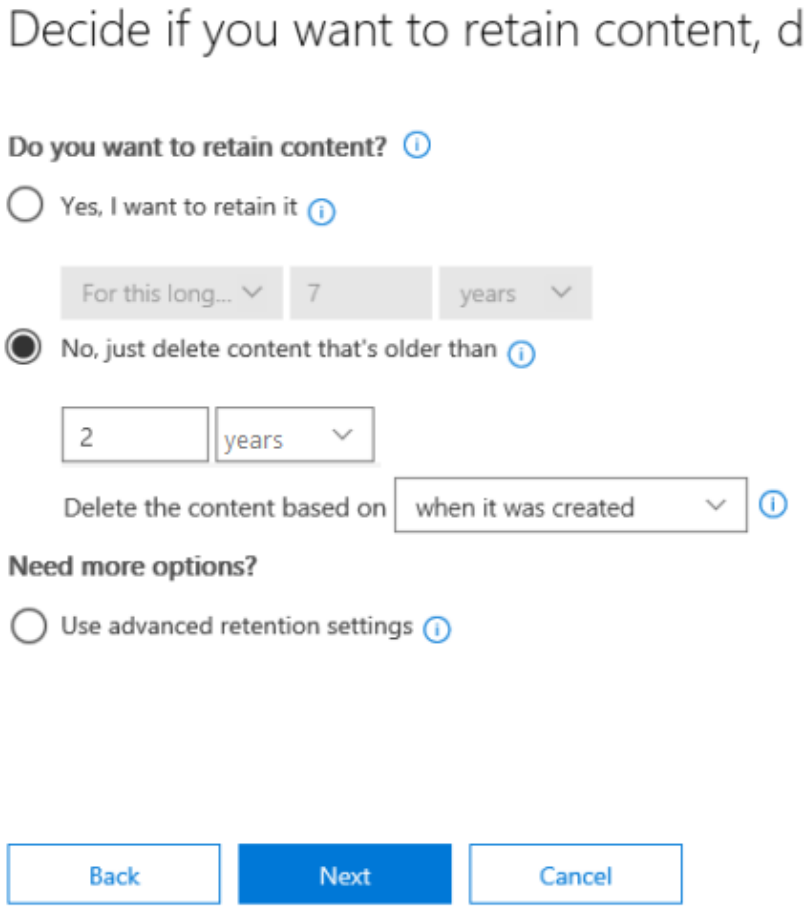
Question #16*Topic 3*

HOTSPOT -

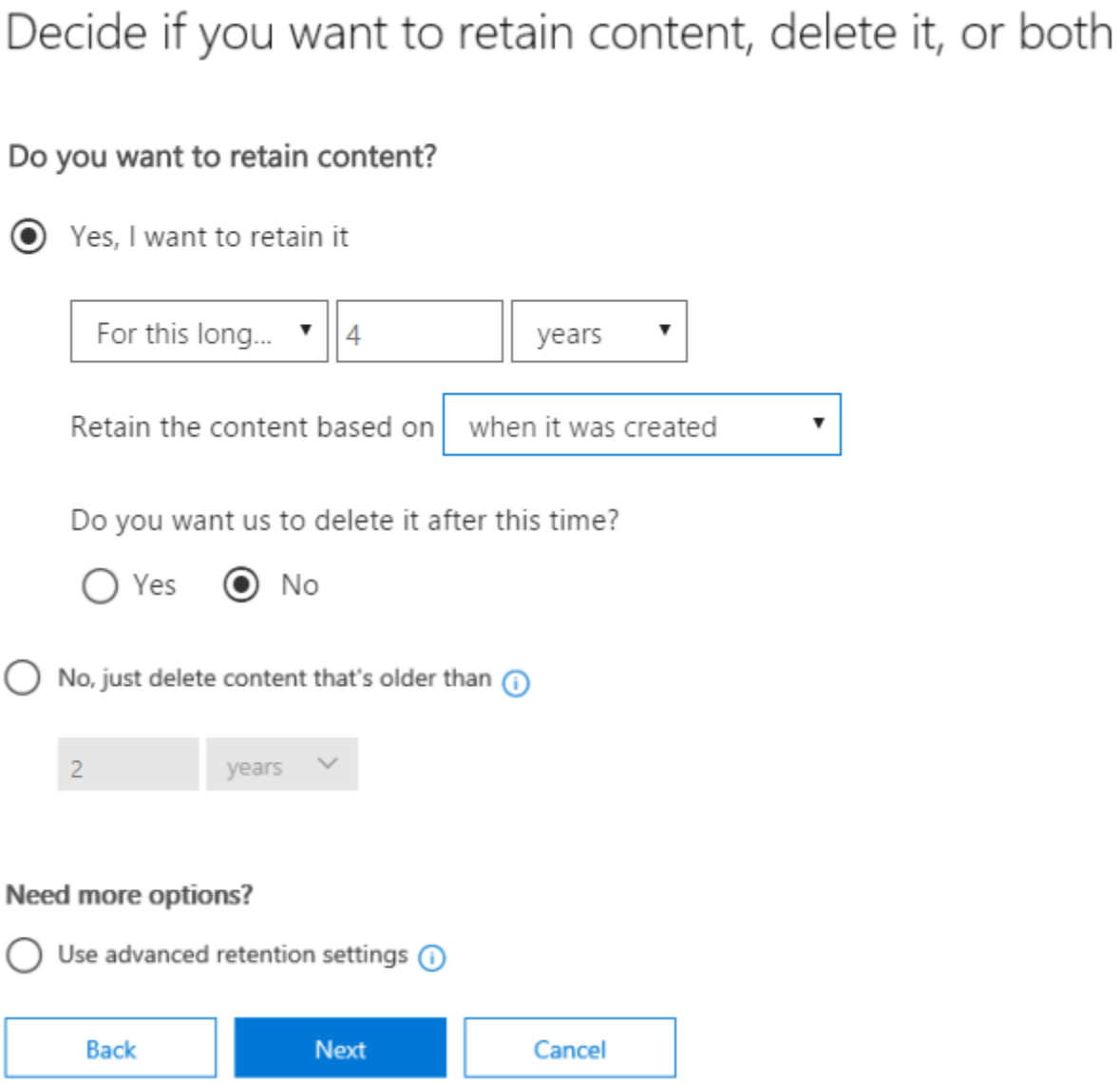
You have retention policies in Microsoft 365 as shown in the following table.

Name	Location
Policy1	OneDrive accounts
Policy2	Exchange email, Exchange public folders, Office 365 groups, OneDrive accounts, SharePoint sites

Policy1 is configured as shown in the Policy1 exhibit. (Click the Policy1 tab.)



Policy2 is configured as shown in the Policy2 exhibit. (Click the Policy2 tab.)



For each of the following statements, select Yes if the statement is true. Otherwise, select No.

Answer Area

Statements	Yes	No
If a user creates a file in Microsoft OneDrive on January 1, 2018, users will be able to access the file on January 15, 2020.	○	○
If a user deletes a Microsoft OneDrive file that was created on January 1, 2018, an administrator will be able to recover the file on April 15, 2020.	○	○
If a user deletes a Microsoft OneDrive file that was created on January 1, 2018, an administrator will be able to recover the file on April 15, 2023.	○	○

Question #17*Topic 3*

You have a Microsoft 365 subscription.
You configure a data loss prevention (DLP) policy.
You discover that users are incorrectly marking content as false positive and bypassing the DLP policy.
You need to prevent the users from bypassing the DLP policy.
What should you configure?

- A. incident reports
- B. actions
- C. exceptions
- D. user overrides

Question #18*Topic 3*

You have a Microsoft 365 subscription.
All users have their email stored in Microsoft Exchange Online.
In the mailbox of a user named User1, you need to preserve a copy of all the email messages that contain the word ProjectX.
What should you do?

- A. From the Security & Compliance admin center, create an eDiscovery case.
- B. From the Exchange admin center, create a mail flow rule.
- C. From the Security & Compliance admin center, start a message trace.
- D. From Microsoft Cloud App Security, create an access policy.

Question #19*Topic 3*

You have a Microsoft 365 E5 subscription.
You run an eDiscovery search that returns the following Azure Rights Management (Azure RMS) ג€" encrypted content:

- Microsoft Exchange emails
- Microsoft OneDrive documents
- Microsoft SharePoint documents

Which content can be decrypted when you export the eDiscovery search results?

- A. Exchange emails only
- B. SharePoint documents, OneDrive documents, and Exchange emails
- C. OneDrive documents only
- D. SharePoint documents and OneDrive documents only
- E. SharePoint documents only

Question #20*Topic 3*

You have a Microsoft 365 subscription.

You plan to connect to Microsoft Exchange Online PowerShell and run the following cmdlets:

- Search-MailboxAuditLog
- Test-ClientAccessRule
- Set-GroupMailbox

Get-Mailbox -

▪

Which cmdlet will generate an entry in the Microsoft Office 365 audit log?

- A. Search-MailboxAuditLog
- B. Test-ClientAccessRule
- C. Set-GroupMailbox
- D. Get-Mailbox

- Question #21*Topic 3*
- HOTSPOT -

  Your company has a Microsoft 365 subscription that uses an Azure Active Directory (Azure AD) tenant named contoso.com. The tenant contains the users shown in the following table.

Name	Role	Office 365 role group
User1	*None*	Compliance data administrator
User2	Global administrator	*None*

  You create a retention label named Label1 that has the following configurations:

  - Retains content for five years
  - Automatically deletes all content that is older than five years

  You turn on Auto labeling for Label1 by using a policy named Policy1. Policy1 has the following configurations:

  - Applies to content that contains the word Merger
  - Specifies the OneDrive accounts and SharePoint sites locations

  You run the following command.

  Set-RetentionCompliancePolicy Policy1 ג€"RestrictiveRetention $true -Force

  For each of the following statements, select Yes if the statement is true. Otherwise, select No.

  1. YES
  2. NO
  3. YES

Question #22*Topic 3*

HOTSPOT -

You have an Azure Active Directory (Azure AD) tenant that contains two users named User1 and User2.

On September 5, 2019, you create and enforce a terms of use (ToU) in the tenant. The ToU has the following settings:

- Name: Terms1
- Display name: Terms1 name
- Require users to expand the terms of use: Off
- Require users to consent on every device: Off
- Expire consents: On
- Expire starting on: October 10, 2019
- Frequency: Monthly

User1 accepts Terms1 on September 5, 2019. User2 accepts Terms1 on October 5, 2019.

When will Terms1 expire for the first time for each user? To answer, select the appropriate options in the answer area.

Answer Area

Question #23*Topic 3*

Your company uses on-premises Windows Server File Classification Infrastructure (FCI). Some documents on the on-premises file servers are classified as
Confidential.
You migrate the files from the on-premises file servers to Microsoft SharePoint Online.
You need to ensure that you can implement data loss prevention (DLP) policies for the uploaded files based on the Confidential classification.
What should you do first?

- A. From the SharePoint admin center, configure hybrid search.
- B. From the SharePoint admin center, create a managed property. **Most Voted**
- C. From the Security & Compliance Center PowerShell, run the New-DataClassification cmdlet.
- D. From the Security & Compliance Center PowerShell, run the New-DlpComplianceRule cmdlet.

Question #24*Topic 3*

You have a Microsoft 365 subscription.
From the Microsoft 365 compliance center, you create a content search of all the mailboxes that contain the word ProjectX.
You need to export the results of the content search.
What do you need to download the report?

- A. a certification authority (CA) certificate
- B. an export key
- C. a password
- D. a user certificate

Question #28*Topic 3*

You have a Microsoft 365 subscription.
You need to investigate user activity in Microsoft 365, including from where users signed in, which applications were used, and increases in activity during the past month. The solution must minimize administrative effort.
Which admin center should you use?

- A. Azure ATP
- B. Security & Compliance
- C. Cloud App Security
- D. Flow