# MS-101.prepaway.premium.exam.126q

Number: MS-101
Passing Score: 800
Time Limit: 120 min
File Version: 3.0

**MS-101**

**Microsoft 365 Mobility and Security**

**Version 3.0**

NoOne

**Question Set 1**

**QUESTION 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 Intune.

You successfully enroll Windows 10 devices in Intune.

When you try to enroll an iOS device in Intune, you get an error.

You need to ensure that you can enroll the iOS device in Intune.

Solution: You add your user account as a device enrollment manager.

Does this meet the goal?

A. Yes
B. No

**Correct Answer:** B
**Section: [none]**
**Explanation**

**Explanation/Reference:**

**QUESTION 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 are deploying Microsoft Intune.

You successfully enroll Windows 10 devices in Intune.

When you try to enroll an iOS device in Intune, you get an error.

You need to ensure that you can enroll the iOS device in Intune.

Solution: You configure the Apple MDM Push certificate.

Does this meet the goal?

A. Yes
B. No

**Correct Answer:** A
**Section: [none]**
**Explanation**

**Explanation/Reference:**
References:
https://docs.microsoft.com/en-us/intune/apple-mdm-push-certificate-get

**QUESTION 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 are deploying Microsoft Intune.

You successfully enroll Windows 10 devices in Intune.

When you try to enroll an iOS device in Intune, you get an error.

You need to ensure that you can enroll the iOS device in Intune.

Solution: You create an Apple Configurator enrollment profile.

Does this meet the goal?

A. Yes
B. No

**Correct Answer:** B
**Section: [none]**
**Explanation**

**Explanation/Reference:**

**QUESTION 4**
**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 Intune admin center.

Does this meet the goal?

A. Yes

B. No

**Correct Answer:** B
**Section: [none]**
**Explanation**

**Explanation/Reference:**

**QUESTION 5**
**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

**Correct Answer:** A
**Section: [none]**
**Explanation**

**Explanation/Reference:**
References:
https://www.scconfigmgr.com/2017/11/30/how-to-setup-co-management-part-6/

**QUESTION 6**
**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

**Correct Answer:** B
**Section: [none]**
**Explanation**

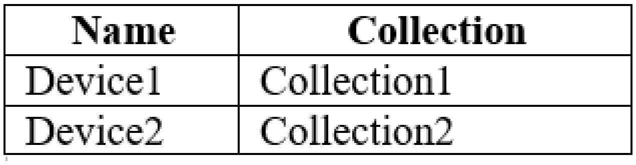
**Explanation/Reference:**

**QUESTION 7**
HOTSPOT

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

You use Microsoft System Center Configuration Manager (Current Branch) for device management.

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

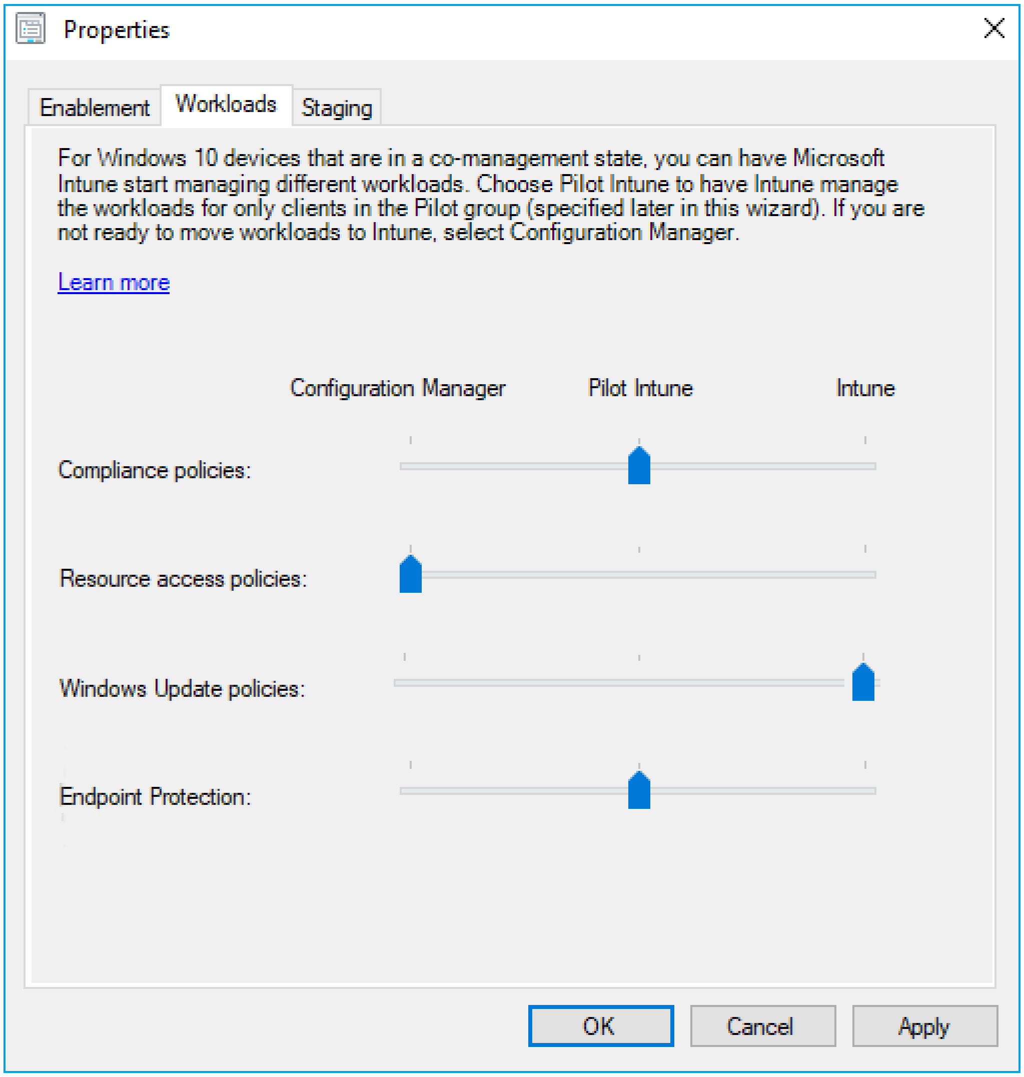


| Name | Collection |
|---|---|
| Device1 | Collection1 |
| Device2 | Collection2 |

You configure Configuration Manager co-management as follows:

- Automatic enrollment in Intune: Pilot
- Pilot collection: Collection2

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



Properties

For Windows 10 devices that are in a co-management state, you can have Microsoft Intune start managing different workloads. Choose Pilot Intune to have Intune manage the workloads for only clients in the Pilot group (specified later in this wizard). If you are not ready to move workloads to Intune, select Configuration Manager.

Learn more

| | Configuration Manager | Pilot Intune | Intune |
|---|---|---|---|
| Compliance policies: | | ● | |
| Resource access policies: | ● | | |
| Windows Update policies: | | | ● |
| Endpoint Protection: | | ● | |

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:**

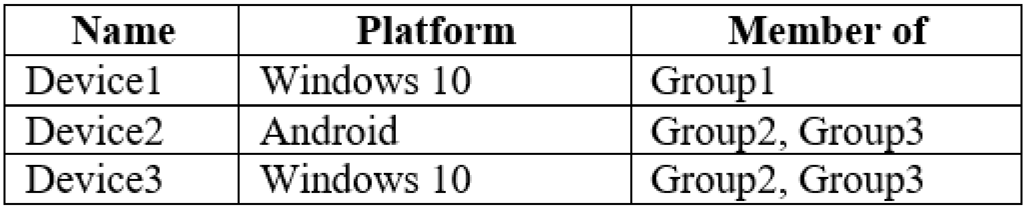
**Correct Answer:**

**Section: [none]**
**Explanation**

**Explanation/Reference:**

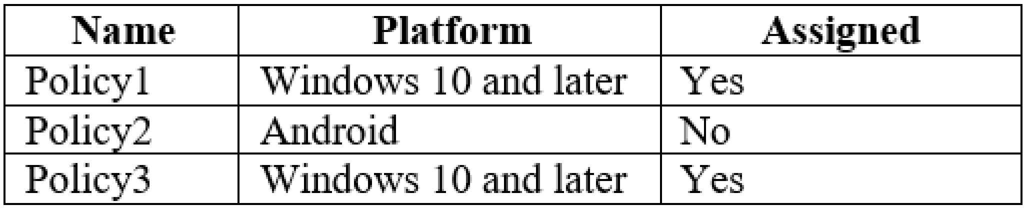
**QUESTION 8**
HOTSPOT

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



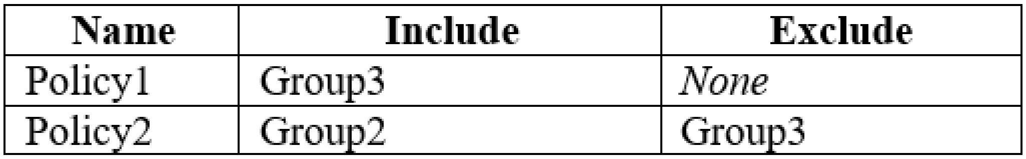
| Name | Platform | Member of |
|---|---|---|
| Device1 | Windows 10 | Group1 |
| Device2 | Android | Group2, Group3 |
| Device3 | Windows 10 | Group2, Group3 |

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:**

**Correct Answer:**

**Section: [none]**
**Explanation**

**Explanation/Reference:**

**QUESTION 9**
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 for SSO to Microsoft 365 services.

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

**NOTE**: Each correct selection is worth one point.

A. computers that have biometric hardware features
B. Microsoft Intune enrollment
C. Microsoft Azure Active Directory (Azure AD)
D. smartcards
E. TPM-enabled devices

**Correct Answer:** BC
**Section: [none]**
**Explanation**

**Explanation/Reference:**
References:
https://docs.microsoft.com/en-us/windows/security/identity-protection/hello-for-business/hello-hybrid-aadj-sso-base

**QUESTION 10**
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 Intune automatically.

What should you configure?

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

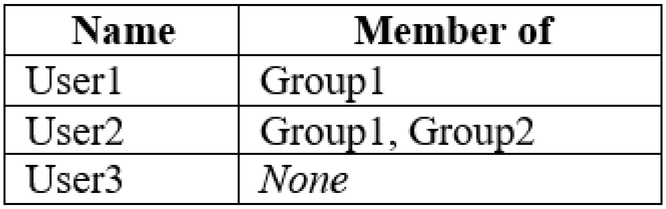
**Correct Answer:** D
**Section: [none]**
**Explanation**

**Explanation/Reference:**
References:
https://docs.microsoft.com/en-us/intune/windows-enroll

**QUESTION 11**
HOTSPOT

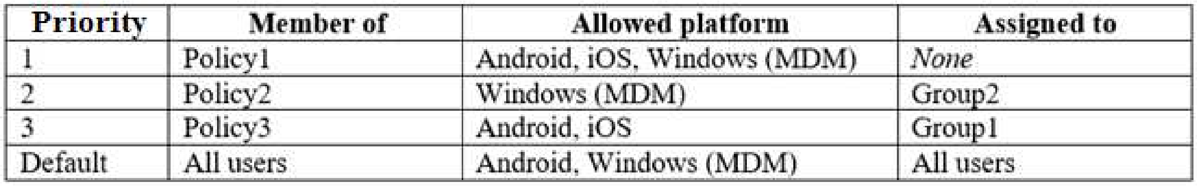
You have several devices enrolled in Microsoft Intune.

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 Intune are configured as shown in the following table.



| Priority | Member of | 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 Intune.

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:**

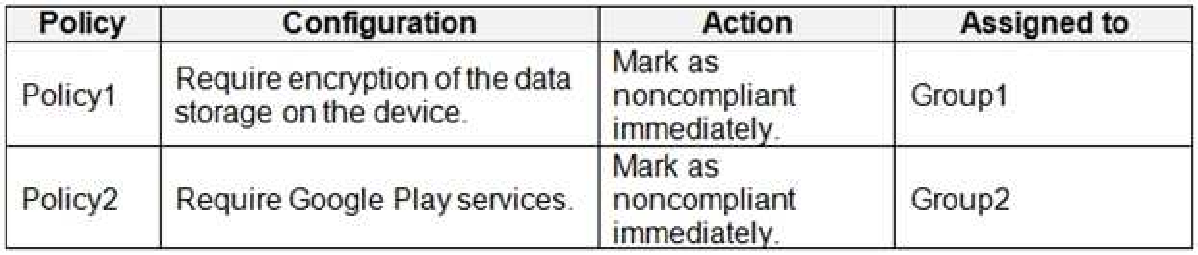
**Correct Answer:**

**Section: [none]**
**Explanation**

**Explanation/Reference:**

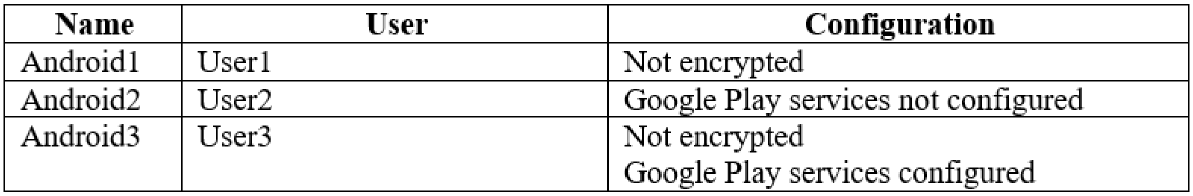
**QUESTION 12**
HOTSPOT

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



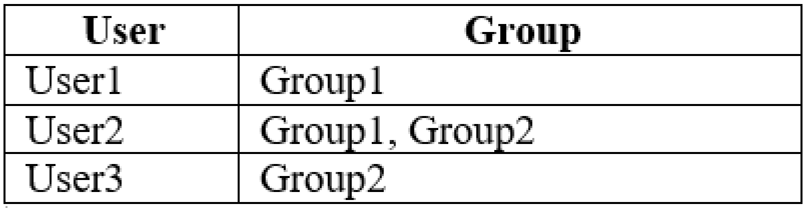
| Policy | Configuration | Action | Assigned to |
|---|---|---|---|
| Policy1 | Require encryption of the data storage on the device. | Mark as noncompliant immediately. | Group1 |
| Policy2 | Require Google Play services. | Mark as noncompliant immediately. | Group2 |

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<br>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 Intune.

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:**

**Correct Answer:**

**Section: [none]**
**Explanation**

**Explanation/Reference:**
References:
https://docs.microsoft.com/en-us/intune-user-help/enroll-your-device-in-intune-android

**QUESTION 13**
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:**

**Correct Answer:**

**Section: [none]**
**Explanation**

**Explanation/Reference:**
References:
https://docs.microsoft.com/en-us/windows/deployment/update/waas-manage-updates-wufb

**QUESTION 14**
Your company uses Microsoft System Center Configuration Manager (Current Branch) and Microsoft Intune to co-manage devices.

Which two actions can be performed only from Intune? 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.

**Correct Answer:** BD
**Section: [none]**
**Explanation**

**Explanation/Reference:**
References:
https://docs.microsoft.com/en-us/sccm/comanage/overview

https://docs.microsoft.com/en-us/sccm/mdm/deploy-use/create-vpn-profiles

**QUESTION 15**
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.

**Hot Area:**

**Correct Answer:**

**Section: [none]**
**Explanation**

**Explanation/Reference:**
References:
https://docs.microsoft.com/en-us/windows/deployment/upgrade/upgrade-readiness-get-started

https://docs.microsoft.com/en-us/windows/deployment/update/update-compliance-get-started

**QUESTION 16**
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 users can manage the configuration settings for all the Windows 10 devices in your organization.

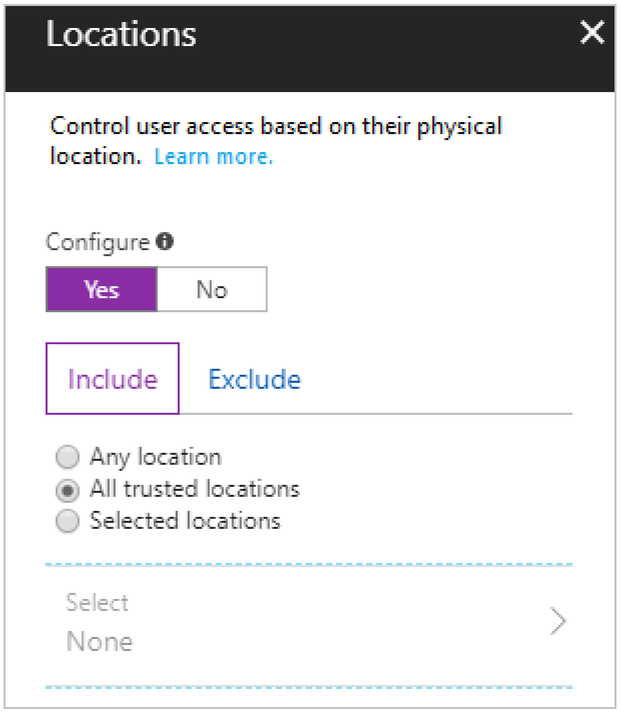
What should you configure?

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

**Correct Answer:** B
**Section: [none]**
**Explanation**

**Explanation/Reference:**
References:
https://docs.microsoft.com/en-us/intune/mdm-authority-set

**QUESTION 17**
You configure a conditional access policy. The locations settings are configured as shown in the Locations exhibit. (Click the **Locations** tab.)



Locations

Control user access based on their physical location. Learn more.

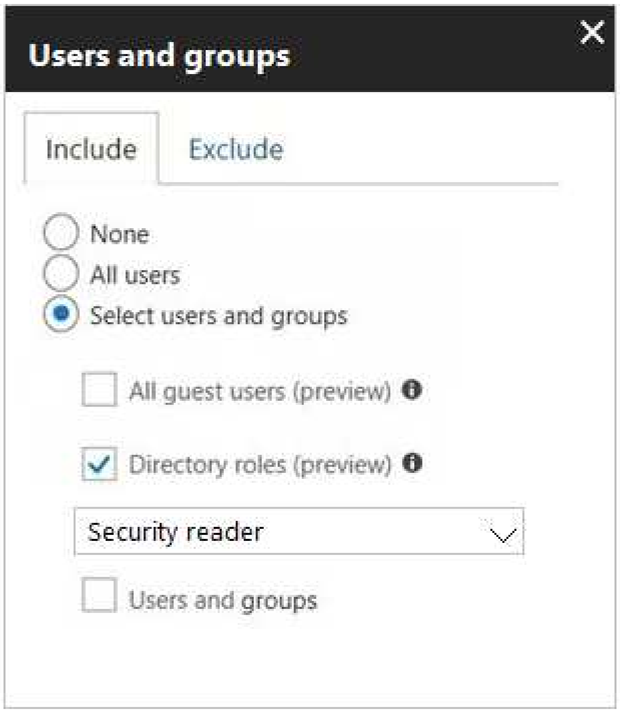
Configure

Include | Exclude

○ Any location
● All trusted locations
○ Selected locations

Select
None

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



Users and groups

Include | Exclude

○ None
○ All users
● Select users and groups

□ All guest users (preview)

☑ Directory roles (preview)

Security reader

□ Users and groups

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 Intune admin center, create a device compliance policy.
D. From the Azure Active Directory admin center, create a named location.

**Correct Answer:** D
**Section: [none]**
**Explanation**

**Explanation/Reference:**
References:
https://docs.microsoft.com/en-us/azure/active-directory/conditional-access/location-condition

**QUESTION 18**
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.

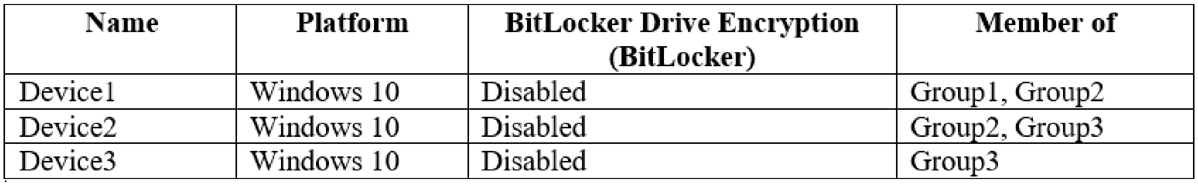
A. Select when Quality Updates are received
B. Select when Preview Builds and Feature Updates are received
C. Turn off auto-restart for updates during active hours
D. Manage preview builds
E. Automatic updates detection frequency

**Correct Answer:** BD
**Section: [none]**
**Explanation**

**Explanation/Reference:**
References:
https://insider.windows.com/en-us/for-business-organization-admin/

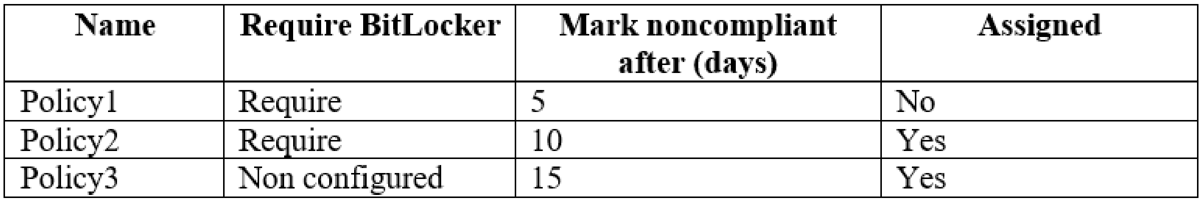
**QUESTION 19**
HOTSPOT

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



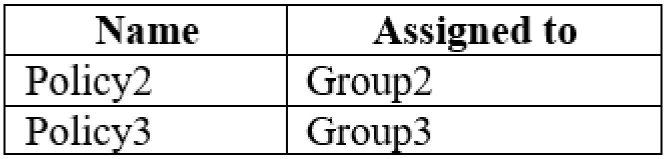
| Name | Platform | BitLocker Drive Encryption (BitLocker) | Member of |
|---|---|---|---|
| Device1 | Windows 10 | Disabled | Group1, Group2 |
| Device2 | Windows 10 | Disabled | Group2, Group3 |
| Device3 | Windows 10 | Disabled | Group3 |

The device compliance policies in Intune 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 |

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:**

**Correct Answer:**

**Section: [none]**
**Explanation**

**Explanation/Reference:**

**QUESTION 20**
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
D. Service administrator

**Correct Answer:** C
**Section: [none]**
**Explanation**

**Explanation/Reference:**
References:
https://docs.microsoft.com/en-us/microsoft-store/roles-and-permissions-microsoft-store-for-business

**QUESTION 21**
**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 Intune.

You successfully enroll Windows 10 devices in Intune.

When you try to enroll an iOS device in Intune, you get an error.

You need to ensure that you can enroll the iOS device in Intune.

Solution: You create the Mobility (MDM and MAM) settings.

Does this meet the goal?

A. Yes
B. No

**Correct Answer:** B
**Section: [none]**
**Explanation**

**Explanation/Reference:**

**QUESTION 22**
**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?

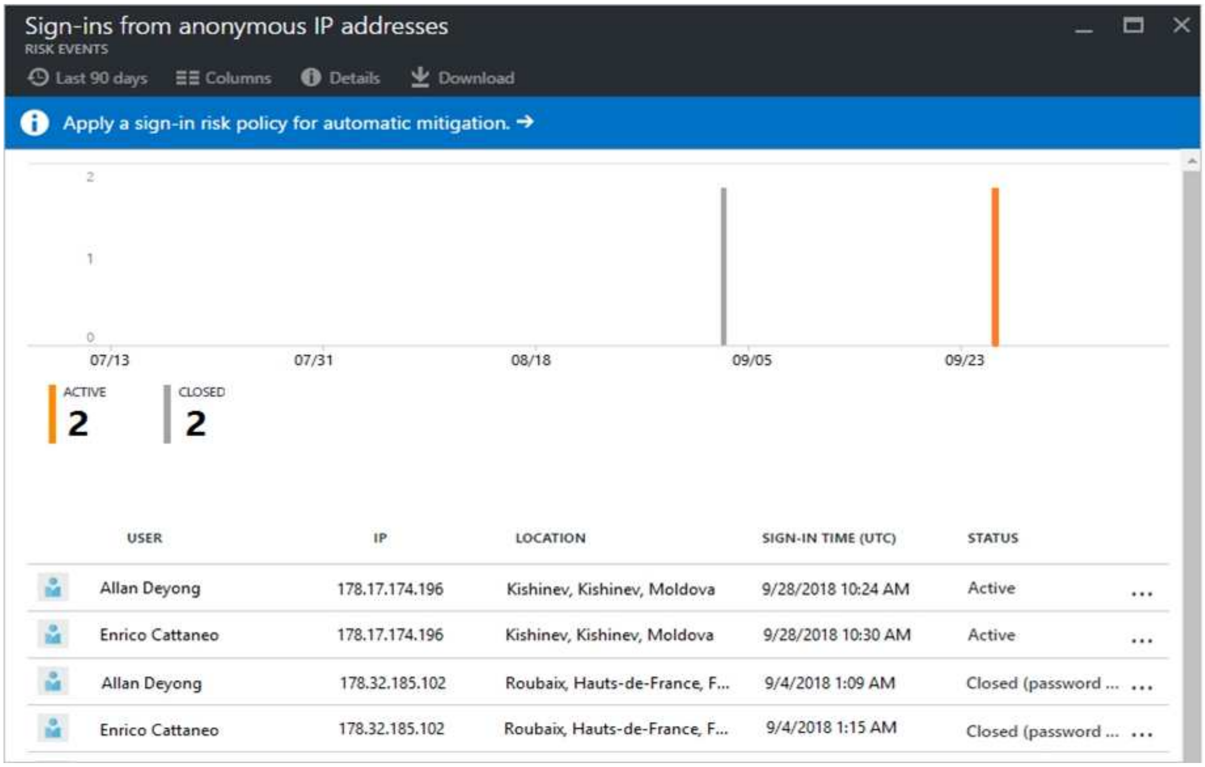
A. Yes
B. No

**Correct Answer:** B
**Section: [none]**
**Explanation**

**Explanation/Reference:**

**QUESTION 23**
From the Microsoft Azure Active Directory (Azure AD) Identity Protection dashboard, you view the risk events

shown in the exhibit. (Click the **Exhibit** tab.)



Sign-ins from anonymous IP addresses
RISK EVENTS

Apply a sign-in risk policy for automatic mitigation. →

ACTIVE 2

CLOSED 2

| USER | IP | LOCATION | SIGN-IN TIME (UTC) | STATUS |
|---|---|---|---|---|
| Allan Deyong | 178.17.174.196 | Kishinev, Kishinev, Moldova | 9/28/2018 10:24 AM | Active |
| Enrico Cattaneo | 178.17.174.196 | Kishinev, Kishinev, Moldova | 9/28/2018 10:30 AM | Active |
| Allan Deyong | 178.32.185.102 | Roubaix, Hauts-de-France, F... | 9/4/2018 1:09 AM | Closed (password ... |
| Enrico Cattaneo | 178.32.185.102 | Roubaix, Hauts-de-France, F... | 9/4/2018 1:15 AM | Closed (password ... |

You need to reduce the likelihood that the sign-ins are identified at 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.

**Correct Answer:** D
**Section: [none]**
**Explanation**

**Explanation/Reference:**
References:
https://docs.microsoft.com/en-us/azure/active-directory/conditional-access/location-condition

**QUESTION 24**
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 from the Security & Compliance admin center?

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.

**Correct Answer:** D
**Section: [none]**
**Explanation**

**Explanation/Reference:**
References:
https://docs.microsoft.com/en-us/office365/securitycompliance/set-up-atp-safe-links-policies#policies-that-apply-to-specific-email-recipients

**QUESTION 25**
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.
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.

**Correct Answer:** A
**Section: [none]**
**Explanation**

**Explanation/Reference:**
References:
https://docs.microsoft.com/en-us/cloud-app-security/cloud-discovery-anomaly-detection-policy

**QUESTION 26**
A user receives the following message when attempting to sign in to https://myapps.microsoft.com:

“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.”

Which configuration prevents the users from signing in?

A. Microsoft Azure Active Directory (Azure AD) Identity Protection policies
B. Microsoft Azure Active Directory (Azure AD) conditional access policies
C. Security & Compliance supervision policies
D. Security & Compliance data loss prevention (DLP) policies

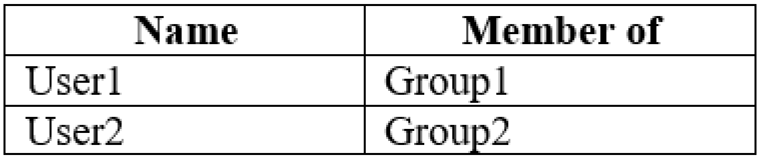
**Correct Answer:** B
**Section: [none]**
**Explanation**

**Explanation/Reference:**

References:
https://docs.microsoft.com/en-us/azure/active-directory/conditional-access/overview

**QUESTION 27**
HOTSPOT

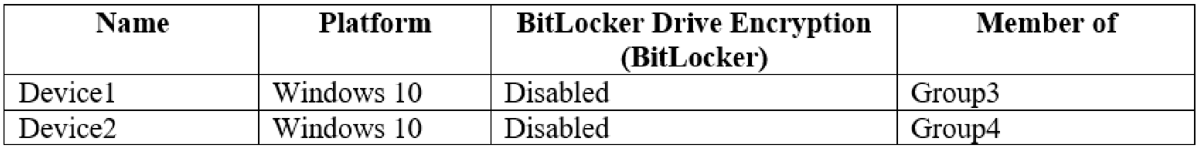
You have the Microsoft Azure Active Directory (Azure AD) users shown in the following table.



| Name | Member of |
|---|---|
| User1 | Group1 |
| User2 | Group2 |

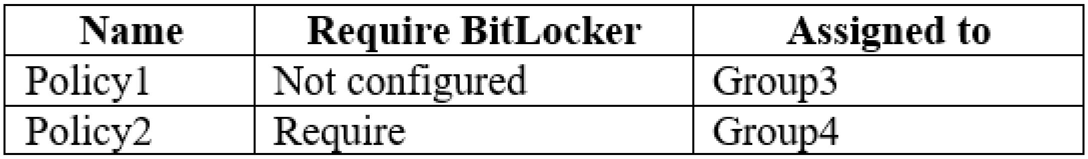
Your company uses Microsoft Intune.

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.

**NOTE**: Each correct selection is worth one point.

**Hot Area:**

**Correct Answer:**

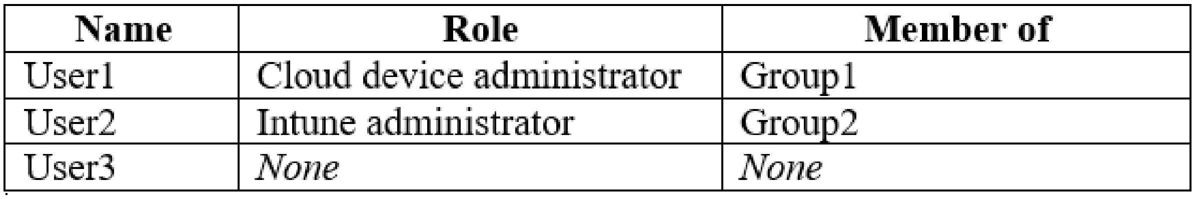
**Section: [none]**
**Explanation**

**Explanation/Reference:**

**QUESTION 28**
HOTSPOT

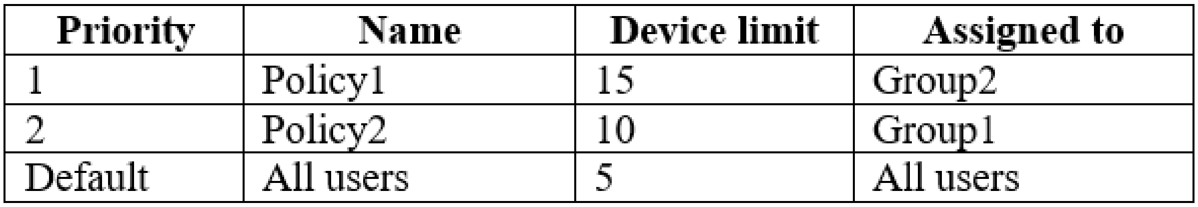
You have several devices enrolled in Microsoft Intune.

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 | Group1 |
| User2 | Intune administrator | Group2 |
| User3 | *None* | *None* |

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



| Priority | Name | Device limit | Assigned to |
|---|---|---|---|
| 1 | Policy1 | 15 | Group2 |
| 2 | Policy2 | 10 | Group1 |
| Default | All users | 5 | All users |

You add User3 as a device enrollment manager in Intune.

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:**

**Correct Answer:**

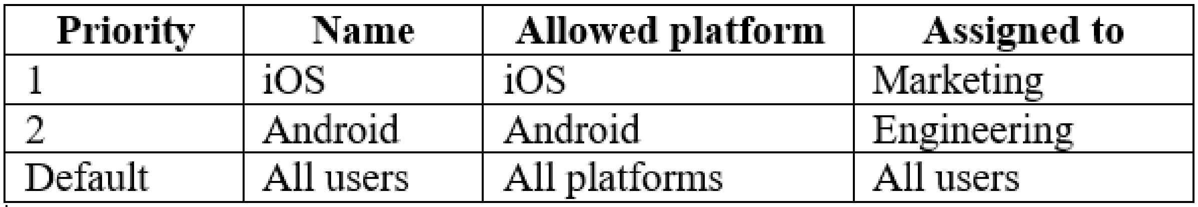
**Section: [none]**
**Explanation**

**Explanation/Reference:**
References:
https://docs.microsoft.com/en-us/sccm/mdm/deploy-use/enroll-devices-with-device-enrollment-manager

**QUESTION 29**
HOTSPOT

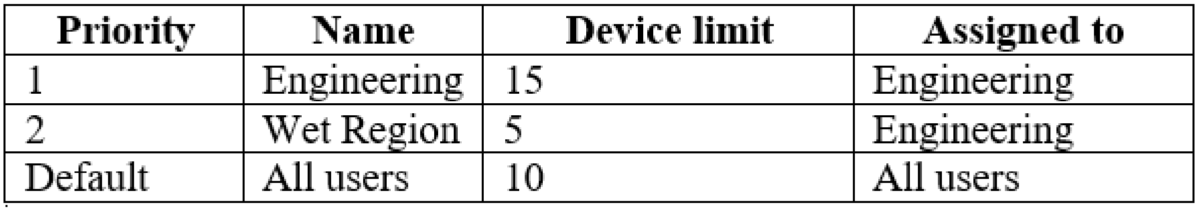
You plan to allow users from the engineering department to enroll their mobile device in mobile device management (MDM).

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.

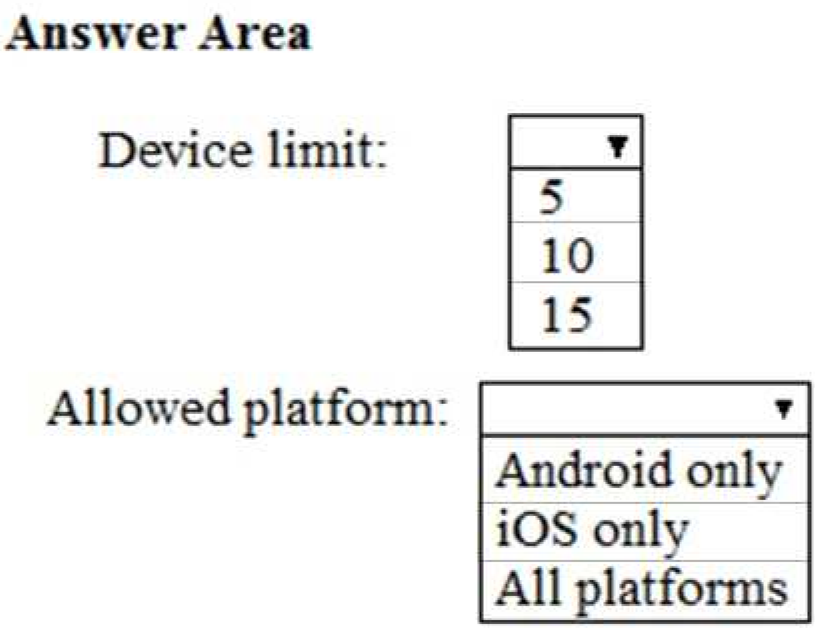


| Priority | Name | Device limit | Assigned to |
|---|---|---|---|
| 1 | Engineering | 15 | Engineering |
| 2 | Wet Region | 5 | Engineering |
| Default | All users | 10 | All users |

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

**NOTE**: Each correct selection is worth one point.

**Hot Area:**

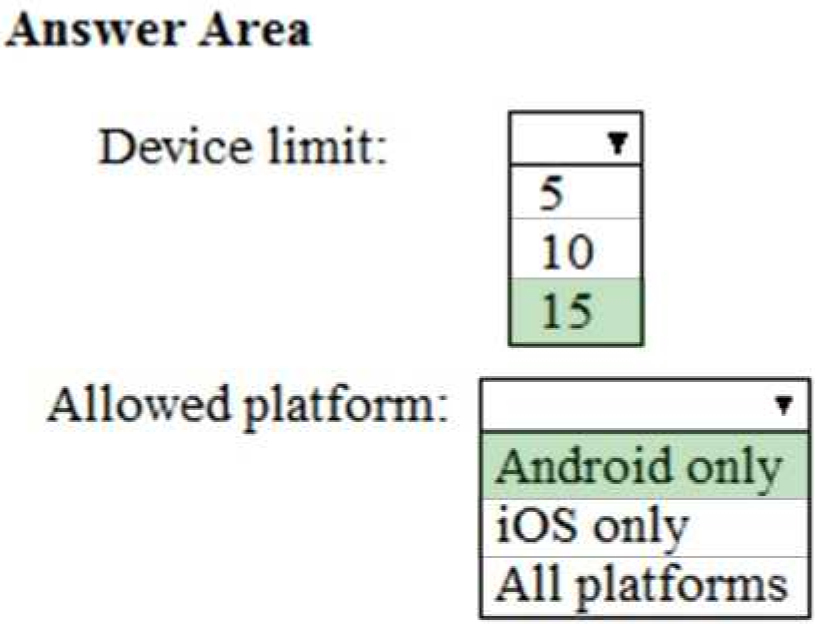


Answer Area

Device limit: ▼
- 5
- 10
- 15

Allowed platform: ▼
- Android only
- iOS only
- All platforms

**Correct Answer:**



Answer Area

Device limit:

- 5
- 10
- [✓ 15]

Allowed platform:

- [✓ Android only]
- iOS only
- All platforms

**Section: [none]**
**Explanation**

**Explanation/Reference:**

**QUESTION 30**
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
D. Windows Autopilot

**Correct Answer:** B
**Section: [none]**
**Explanation**

**Explanation/Reference:**
References:
https://docs.microsoft.com/en-us/microsoft-365/enterprise/windows10-infrastructure

**QUESTION 31**
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?

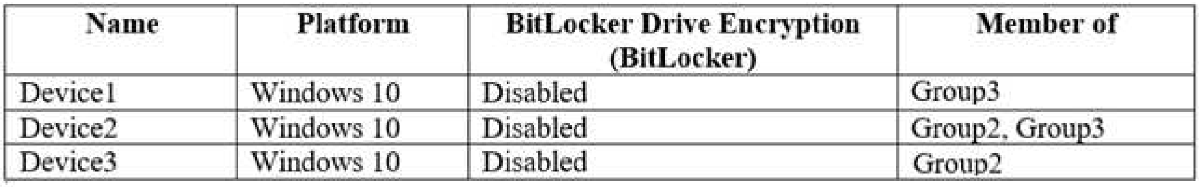
A. Windows 10 and Windows 8.1 only
B. Windows 10, Android, and iOS only
C. Windows 10 only
D. Windows 10, Windows 8.1, Android, and iOS

**Correct Answer:** D
**Section: [none]**
**Explanation**

**Explanation/Reference:**
References:
https://docs.microsoft.com/en-us/sccm/core/plan-design/choose-a-device-management-solution#bkmk_intune

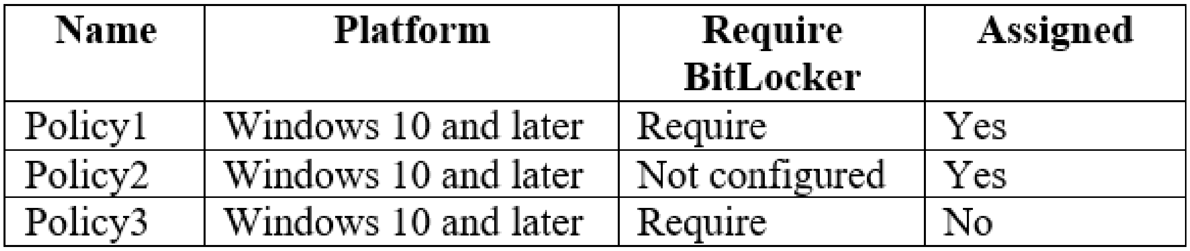
**QUESTION 32**
HOTSPOT

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



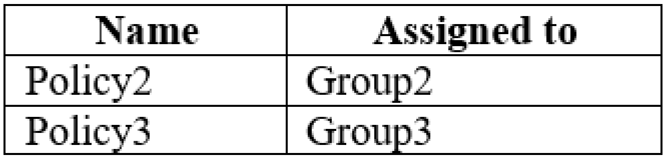
| Name | Platform | BitLocker Drive Encryption (BitLocker) | Member of |
|---|---|---|---|
| Device1 | Windows 10 | Disabled | Group3 |
| Device2 | Windows 10 | Disabled | Group2, Group3 |
| Device3 | Windows 10 | Disabled | Group2 |

The device compliance policies in Intune 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 |
|---|---|
| Policy2 | Group2 |
| Policy3 | 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:**

**Correct Answer:**

**Section: [none]**
**Explanation**

**Explanation/Reference:**

**QUESTION 33**
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

**Correct Answer:** A
**Section: [none]**
**Explanation**

**Explanation/Reference:**
References:
https://docs.microsoft.com/en-us/windows/deployment/windows-autopilot/windows-autopilot

**QUESTION 34**
**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

**Correct Answer:** B
**Section: [none]**
**Explanation**

**Explanation/Reference:**

**QUESTION 35**
**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 Intune.

You successfully enroll Windows 10 devices in Intune.

When you try to enroll an iOS device in Intune, you get an error.

You need to ensure that you can enroll the iOS device in Intune.

Solution: You configure the Mobility (MDM and MAM) settings.

Does this meet the goal?

A. Yes
B. No

**Correct Answer:** B
**Section: [none]**
**Explanation**

**Explanation/Reference:**

**QUESTION 36**
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 the computers to meet the following corporate requirements:

- All the computers must be joined to the domain.
- All the computers must have computer names that use a prefix of CONTOSO.
- All the computers must only have approved corporate applications installed.

You need to recommend a solution to redeploy the computers. The solution must minimize the deployment time.

What should you recommend?

A. a provisioning package

B. wipe and load refresh

C. Windows Autopilot

D. an in-place upgrade

**Correct Answer:** A
**Section: [none]**
**Explanation**

**Explanation/Reference:**
Explanation:
By using a Provisioning, IT administrators can create a self-contained package that contains all of the configuration, settings, and apps that need to be applied to a device.

Incorrect Answers:
C: With Windows Autopilot the user can set up pre-configure devices without the need consult their IT administrator.
D: Use the In-Place Upgrade option when you want to keep all (or at least most) existing applications.

References:
https://docs.microsoft.com/en-us/windows/deployment/windows-10-deployment-scenarios

https://docs.microsoft.com/en-us/windows/deployment/windows-autopilot/windows-autopilot

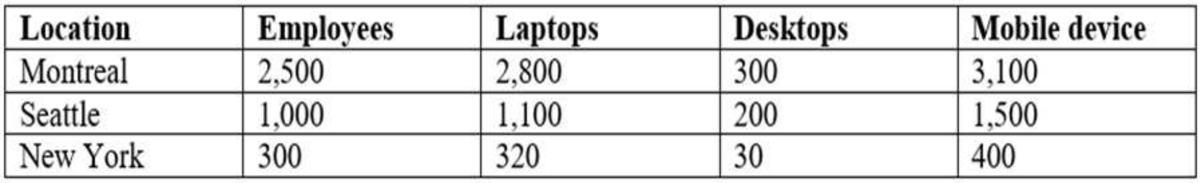
**Testlet 2**

**Case Study**

**Overview**

Contoso, Ltd. is a consulting company that has a main office in Montreal and two branch offices in Seattle and New York.

The company has the employees and devices shown in the following table.

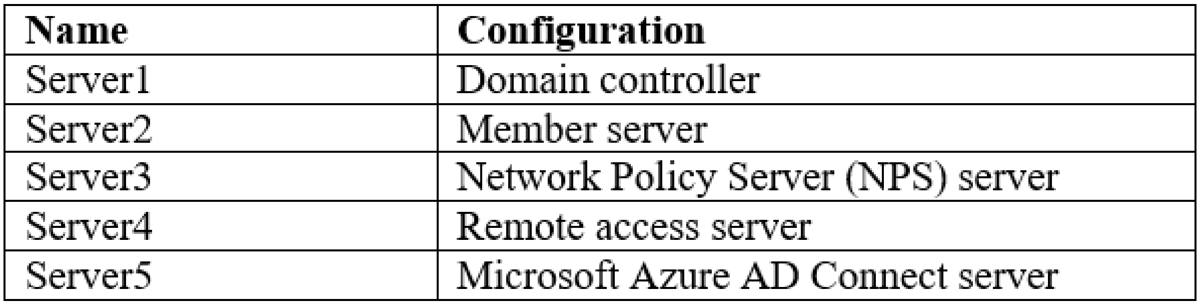


| Location | Employees | Laptops | Desktops | Mobile device |
|---|---|---|---|---|
| Montreal | 2,500 | 2,800 | 300 | 3,100 |
| Seattle | 1,000 | 1,100 | 200 | 1,500 |
| New York | 300 | 320 | 30 | 400 |

Contoso recently purchased a Microsoft 365 E5 subscription.

**Existing Environment**

The network contains an on-premises Active Directory forest named contoso.com. The forest contains the servers shown in the following table.

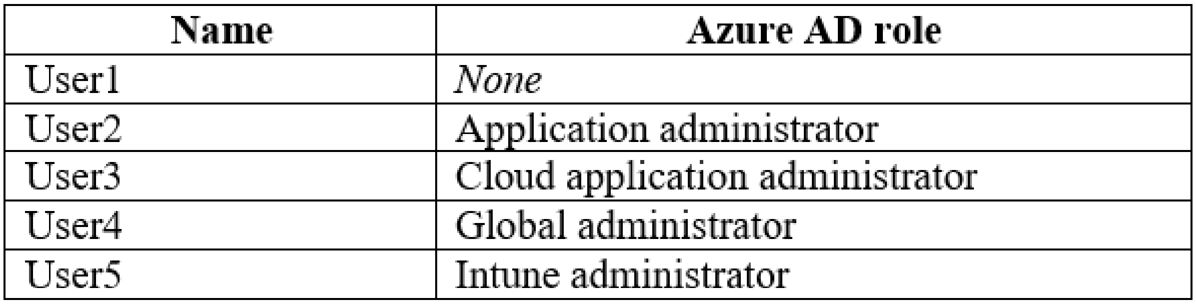


| Name | Configuration |
|---|---|
| Server1 | Domain controller |
| Server2 | Member server |
| Server3 | Network Policy Server (NPS) server |
| Server4 | Remote access server |
| Server5 | Microsoft Azure AD Connect server |

All servers run Windows Server 2016. All desktops and laptops run Windows 10 Enterprise and are joined to the domain.

The mobile devices of the users in the Montreal and Seattle offices run Android. The mobile devices of the users in the New York office run iOS.

The domain is synced to Azure Active Directory (Azure AD) and includes the users shown in the following table.



| Name | Azure AD role |
|---|---|
| User1 | *None* |
| User2 | Application administrator |
| User3 | Cloud application administrator |
| User4 | Global administrator |
| User5 | Intune administrator |

The domain also includes a group named Group1.

## Requirements

### Planned Changes

Contoso plans to implement the following changes:

- Implement Microsoft 365.
- Manage devices by using Microsoft Intune.
- Implement Azure Advanced Threat Protection (ATP).
- Every September, apply the latest feature updates to all Windows computers. Every March, apply the latest feature updates to the computers in the New York office only.

### Technical Requirements

Contoso identifies the following technical requirements:

- When a Windows 10 device is joined to Azure AD, the device must enroll in Intune automatically.
- Dedicated support technicians must enroll all the Montreal office mobile devices in Intune.
- User1 must be able to enroll all the New York office mobile devices in Intune.
- Azure ATP sensors must be installed and must **NOT** use port mirroring.
- Whenever possible, the principle of least privilege must be used.
- A Microsoft Store for Business must be created.

### Compliance Requirements

Contoso identifies the following compliance requirements:

- Ensure that the users in Group1 can only access Microsoft Exchange Online from devices that are enrolled in Intune and configured in accordance with the corporate policy.
- Configure Windows Information Protection (WIP) for the Windows 10 devices.

**QUESTION 1**
You need to ensure that the support technicians can meet the technical requirement for the Montreal office mobile devices.

What is the minimum of dedicated support technicians required?

A. 1

B. 4

C. 7

D. 31

**Correct Answer:** B
**Section: [none]**
**Explanation**

**Explanation/Reference:**
References:
https://docs.microsoft.com/en-us/sccm/mdm/deploy-use/enroll-devices-with-device-enrollment-manager

**QUESTION 2**
You need to create the Microsoft Store for Business.

Which user can create the store?

A. User2

B. User3
C. User4
D. User5

**Correct Answer:** C
**Section: [none]**
**Explanation**

**Explanation/Reference:**
References:
https://docs.microsoft.com/en-us/microsoft-store/roles-and-permissions-microsoft-store-for-business

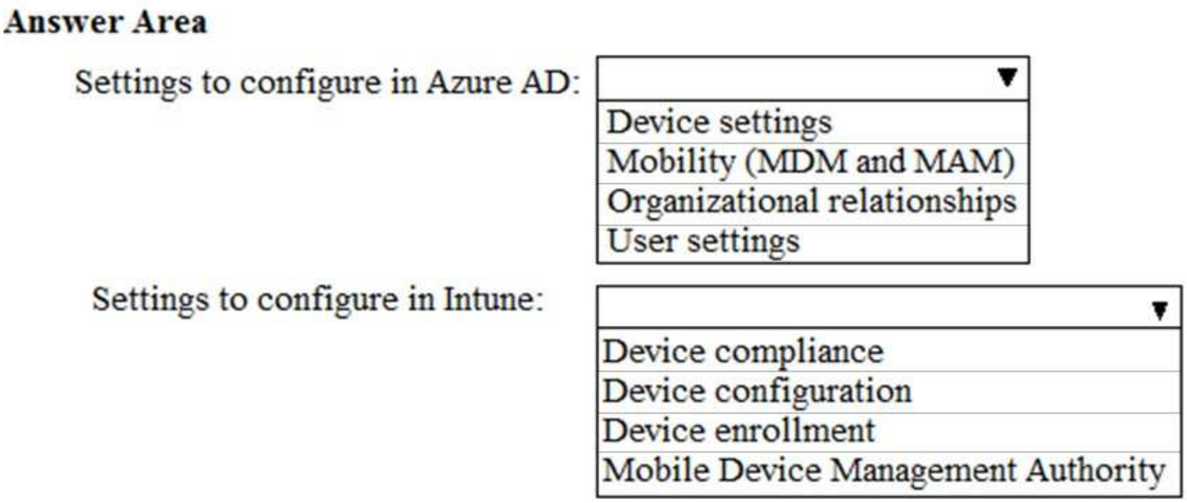
**QUESTION 3**
HOTSPOT

You need to meet the Intune requirements for 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.

**Hot Area:**

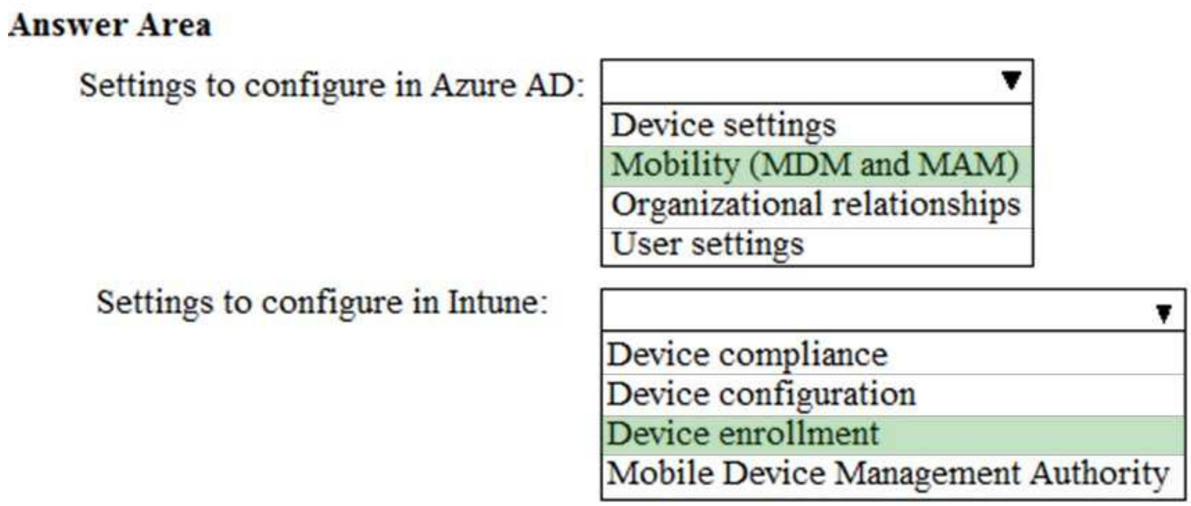


**Answer Area**

Settings to configure in Azure AD: ▼
- Device settings
- Mobility (MDM and MAM)
- Organizational relationships
- User settings

Settings to configure in Intune: ▼
- Device compliance
- Device configuration
- Device enrollment
- Mobile Device Management Authority

**Correct Answer:**



**Answer Area**

Settings to configure in Azure AD: ▼

- Device settings
- [✓ Mobility (MDM and MAM)]
- Organizational relationships
- User settings

Settings to configure in Intune: ▼

- Device compliance
- Device configuration
- [✓ Device enrollment]
- Mobile Device Management Authority

**Section: [none]**
**Explanation**

**Explanation/Reference:**
References:
https://docs.microsoft.com/en-us/intune/windows-enroll

**QUESTION 4**
HOTSPOT

You need to configure a conditional access policy to meet the compliance requirements.

You add Exchange Online as a cloud app.

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

**NOTE**: Each correct selection is worth one point.

**Hot Area:**

**Correct Answer:**

**Section: [none]**
**Explanation**

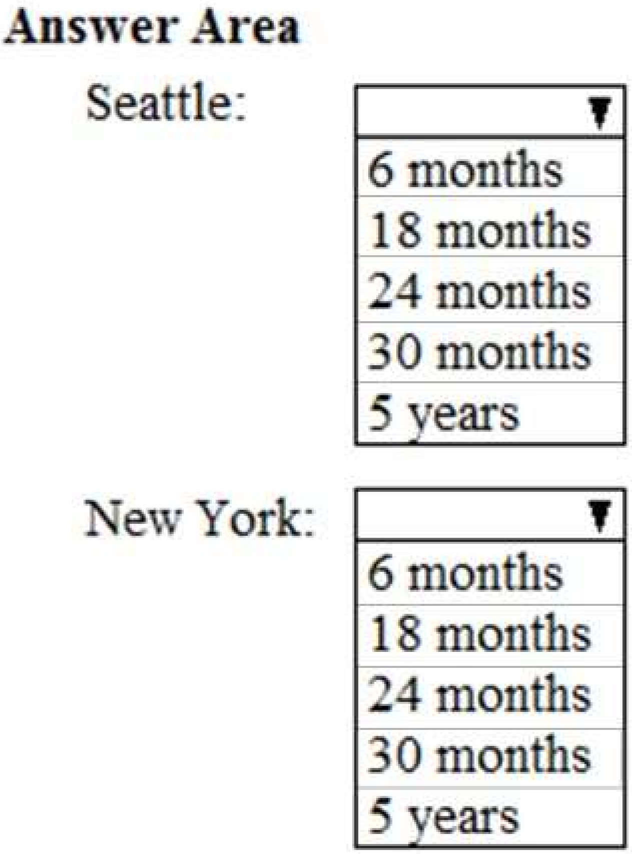
**Explanation/Reference:**
References:
https://docs.microsoft.com/en-us/intune/create-conditional-access-intune

**QUESTION 5**
HOTSPOT

As of March, how long will the computers in each office remain supported by Microsoft? To answer, select the appropriate options in the answer area.

**NOTE**: Each correct selection is worth one point.

**Hot Area:**



**Answer Area**

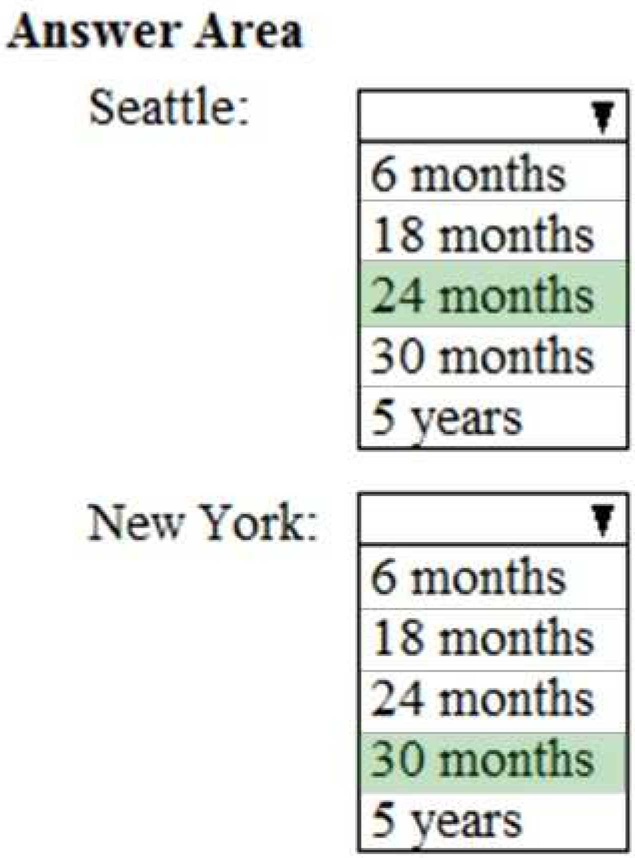
Seattle: ▼

- 6 months
- 18 months
- 24 months
- 30 months
- 5 years

New York: ▼

- 6 months
- 18 months
- 24 months
- 30 months
- 5 years

**Correct Answer:**



Answer Area

Seattle:

- 6 months
- 18 months
- [✓ 24 months]
- 30 months
- 5 years

New York:

- 6 months
- 18 months
- 24 months
- [✓ 30 months]
- 5 years

**Section: [none]**
**Explanation**

**Explanation/Reference:**
References:
https://www.windowscentral.com/whats-difference-between-quality-updates-and-feature-updates-windows-10

**QUESTION 6**
You need to ensure that User1 can enroll the devices to meet the technical requirements.

What should you do?

A. From the Azure Active Directory admin center, assign User1 the Cloud device administrator role.
B. From the Azure Active Directory admin center, configure the Maximum number of devices per user setting.
C. From the Intune admin center, add User1 as a device enrollment manager.
D. From the Intune admin center, configure the Enrollment restrictions.

**Correct Answer:** C
**Section: [none]**
**Explanation**

**Explanation/Reference:**
References:
https://docs.microsoft.com/en-us/sccm/mdm/deploy-use/enroll-devices-with-device-enrollment-manager

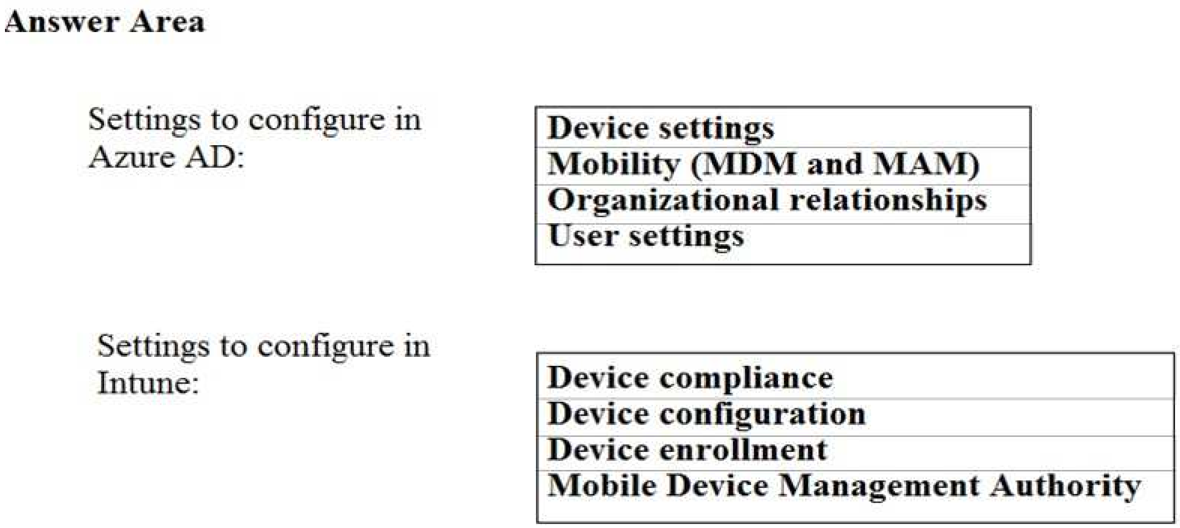
**QUESTION 7**
HOTSPOT

You need to meet the technical requirements and planned changes for Intune.

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

**NOTE:** Each correct selection is worth one point.

**Hot Area:**



**Answer Area**

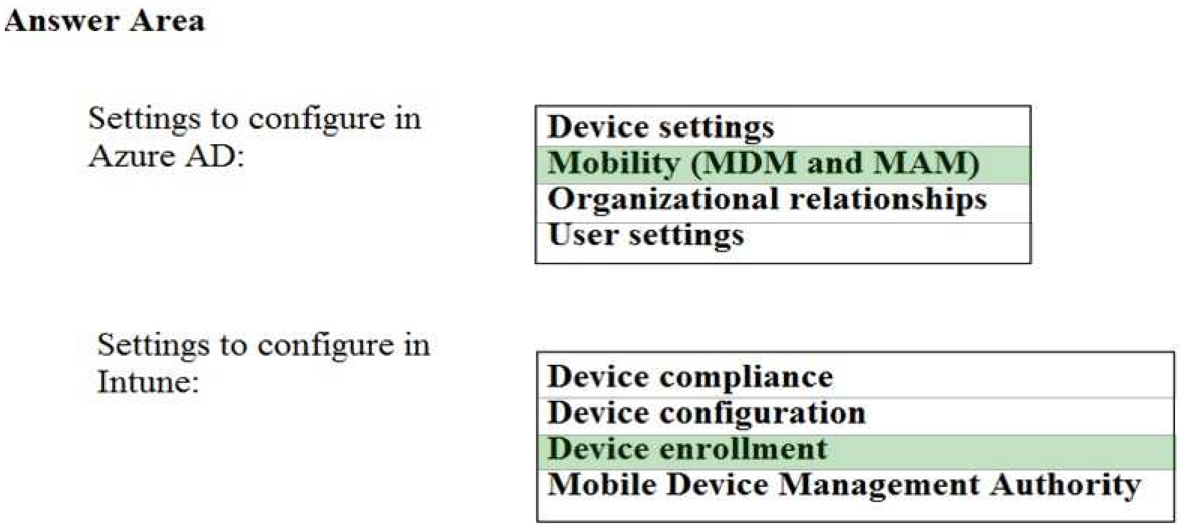
Settings to configure in Azure AD:

- Device settings
- Mobility (MDM and MAM)
- Organizational relationships
- User settings

Settings to configure in Intune:

- Device compliance
- Device configuration
- Device enrollment
- Mobile Device Management Authority

**Correct Answer:**



**Answer Area**

Settings to configure in Azure AD:

- Device settings
- [✓ Mobility (MDM and MAM)]
- Organizational relationships
- User settings

Settings to configure in Intune:

- Device compliance
- Device configuration
- [✓ Device enrollment]
- Mobile Device Management Authority

**Section: [none]**
**Explanation**

**Explanation/Reference:**
Reference:
https://docs.microsoft.com/en-us/intune/windows-enroll

## Testlet 3

## Case Study

### Overview

ADatum Corporation is an international financial services company that has 5,000 employees.

ADatum has six offices: a main office in New York and five branch offices in Germany, the United Kingdom, France, Spain, and Italy.

All the offices are connected to each other by using a WAN link. Each office connects directly to the Internet.

### Existing Environment

### Current Infrastructure

ADatum recently purchased a Microsoft 365 subscription.

All user files are migrated to Microsoft 365.

All mailboxes are hosted in Microsoft 365. The users in each office have email suffixes that include the country of the user, for example, user1@us.adatum.com or user2@uk.adatum.com.

Each office has a security information and event management (SIEM) appliance. The appliance comes from three different vendors.

ADatum uses and processes Personally Identifiable Information (PII).

### Problem Statements

ADatum entered into litigation. The legal department must place a hold on all the documents of a user named User1 that are in Microsoft 365.

### Requirements

### Business Goals

ADatum wants to be fully compliant with all the relevant data privacy laws in the regions where is operates.

ADatum wants to minimize the cost of hardware and software whenever possible.

### Technical Requirements

ADatum identifies the following technical requirements:

- Centrally perform log analysis for all offices.
- Aggregate all data from the SIEM appliances to a central cloud repository for later analysis.
- Ensure that a SharePoint administrator can identify who accessed a specific file stored in a document library.
- Provide the users in the finance department with access to Service assurance information in Microsoft Office 365.
- Ensure that documents and email messages containing the PII data of European Union (EU) citizens are preserved for 10 years.
- If a user attempts to download 1,000 or more files from Microsoft SharePoint Online within 30 minutes, notify a security administrator and suspend the user's user account.
- A security administrator requires a report that shown which Microsoft 365 users signed in. Based on the

report, the security administrator will create a policy to require multi-factor authentication when a sign-in is high risk.

- Ensure that the users in the New York office can only send email messages that contain sensitive U.S. PII data to other New York office uses. Email messages must be monitored to ensure compliance. Auditors in the New York office must have access to reports that show the sent and received email messages containing sensitive U.S. PII data.

**QUESTION 1**

You need to recommend a solution for the security administrator. The solution must meet the technical requirements.

What should you include in the recommendation?

A. Microsoft Azure Active Directory (Azure AD) Privileged Identity Management

B. Microsoft Azure Active Directory (Azure AD) Identity Protection

C. Microsoft Azure Active Directory (Azure AD) conditional access policies

D. Microsoft Azure Active Directory (Azure AD) authentication methods

**Correct Answer:** C

**Section: [none]**

**Explanation**

**Explanation/Reference:**

References:

https://docs.microsoft.com/en-us/azure/active-directory/conditional-access/untrusted-networks

**Question Set 1**

**QUESTION 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 Microsoft 365 subscription.

You discover that some external users accessed content on a Microsoft SharePoint site. You modify the SharePoint sharing policy to prevent sharing outside your organization.

You need to be notified if the SharePoint sharing policy is modified in the future.

Solution: From the Security & Compliance admin center, you create a threat management policy.

Does this meet the goal?

A. Yes

B. No

**Correct Answer:** A

**Section: [none]**

**Explanation**

**Explanation/Reference:**

**QUESTION 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 discover that some external users accessed content on a Microsoft SharePoint site. You modify the SharePoint sharing policy to prevent sharing outside your organization.

You need to be notified if the SharePoint sharing policy is modified in the future.

Solution: From the SharePoint site, you create an alert.

Does this meet the goal?

A. Yes

B. No

**Correct Answer:** B

**Section: [none]**

**Explanation**

**Explanation/Reference:**

**QUESTION 3**
Your company has 5,000 Windows 10 devices. All the devices are protected by using Windows Defender Advanced Threat Protection (ATP).

You need to create a filtered view that displays which Windows Defender ATP alert events have a high severity and occurred during the last seven days.

What should you use in Windows Defender ATP?

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

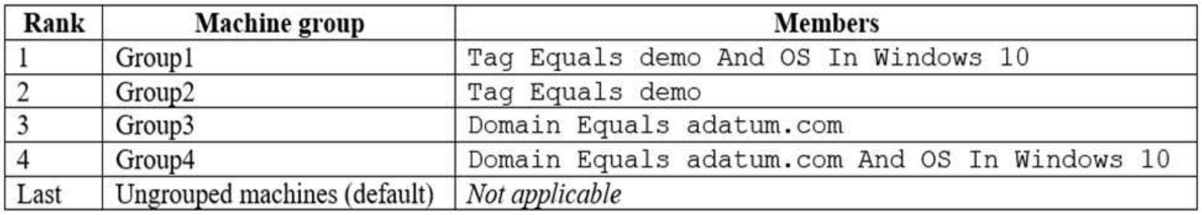
**Correct Answer:** B
**Section: [none]**
**Explanation**

**Explanation/Reference:**
References:
https://docs.microsoft.com/en-us/windows/security/threat-protection/windows-defender-atp/investigate-alerts-windows-defender-advanced-threat-protection

https://docs.microsoft.com/en-us/windows/security/threat-protection/windows-defender-atp/automated-investigations-windows-defender-advanced-threat-protection

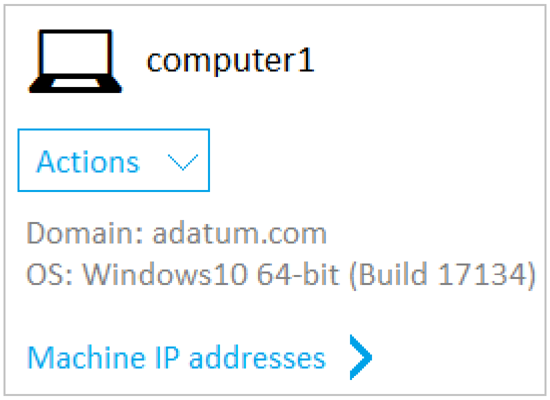
**QUESTION 4**
HOTSPOT

Your company uses Windows Defender Advanced Threat Protection (ATP). Windows 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* |

You onboard a computer named computer1 to Windows Defender ATP as shown in the following exhibit.



computer1

Domain: adatum.com
OS: Windows10 64-bit (Build 17134)

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.

**Hot Area:**

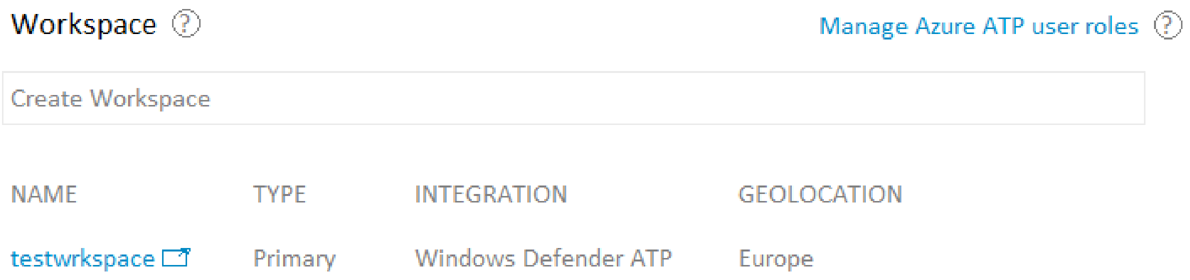
**Correct Answer:**

**Section: [none]**
**Explanation**

**Explanation/Reference:**

**QUESTION 5**
DRAG DROP

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



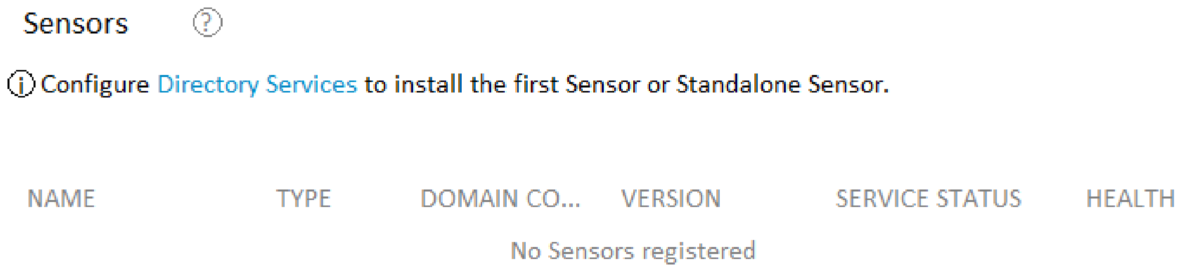
Workspace ⓘ

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.

**Select and Place:**

**Correct Answer:**

**Section: [none]**
**Explanation**

**Explanation/Reference:**

**QUESTION 6**
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**.

**Correct Answer:** A
**Section: [none]**
**Explanation**

**Explanation/Reference:**
References:
https://docs.microsoft.com/en-us/office365/securitycompliance/investigate-an-activity-in-office-365-cas

**QUESTION 7**
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 Windows Defender Advanced Threat Protection (ATP) for 10 test devices. During the onboarding process, you configure Windows Defender ATP-related data to be stored in the United States.

You plan to onboard all the devices to Windows Defender ATP.

You need to store the Windows Defender ATP data in Europe.

What should you first?

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

**Correct Answer:** D
**Section: [none]**
**Explanation**

**Explanation/Reference:**

**QUESTION 8**
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.

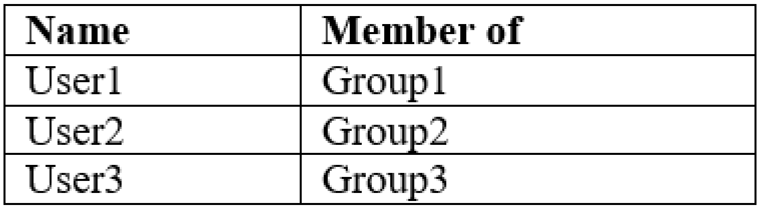
C. From the Exchange admin center, create an anti-malware policy.
D. From the Security & Compliance admin center, create a safe attachments policy.
E. From the Security & Compliance admin center, create a data loss prevention (DLP) policy.
F. From the Exchange admin center, create a mail flow rule.

**Correct Answer:** C
**Section: [none]**
**Explanation**

**Explanation/Reference:**
References:
https://docs.microsoft.com/en-us/office365/servicedescriptions/exchange-online-service-description/anti-spam-and-anti-malware-protection

**QUESTION 9**
HOTSPOT

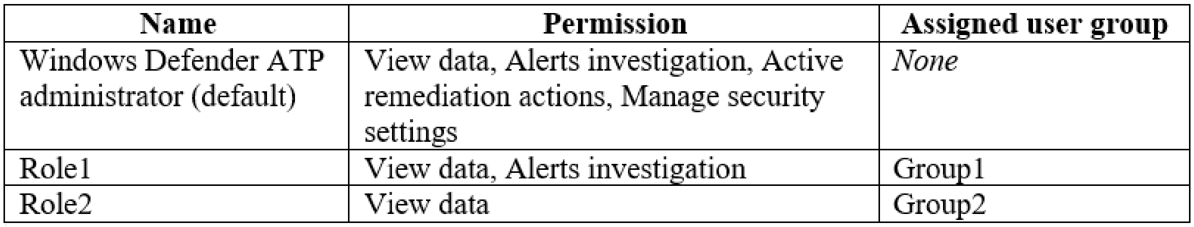
You have a Microsoft Azure Activity Directory (Azure AD) tenant contains the users shown in the following table.



| Name | Member of |
|---|---|
| User1 | Group1 |
| User2 | Group2 |
| User3 | Group3 |

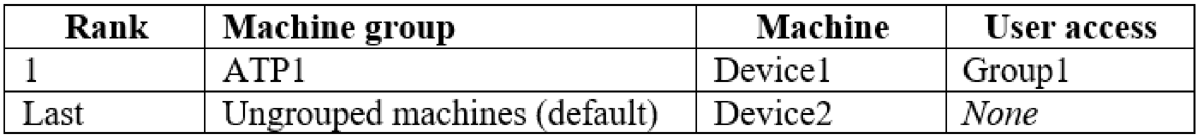
Group3 is a member of Group1.

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



| Name | Permission | Assigned user group |
|---|---|---|
| Windows 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 |

Windows 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.

**NOTE**: Each correct selection is worth one point.

**Hot Area:**

**Correct Answer:**

**Section: [none]**
**Explanation**

**Explanation/Reference:**

**QUESTION 10**
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.

**Hot Area:**

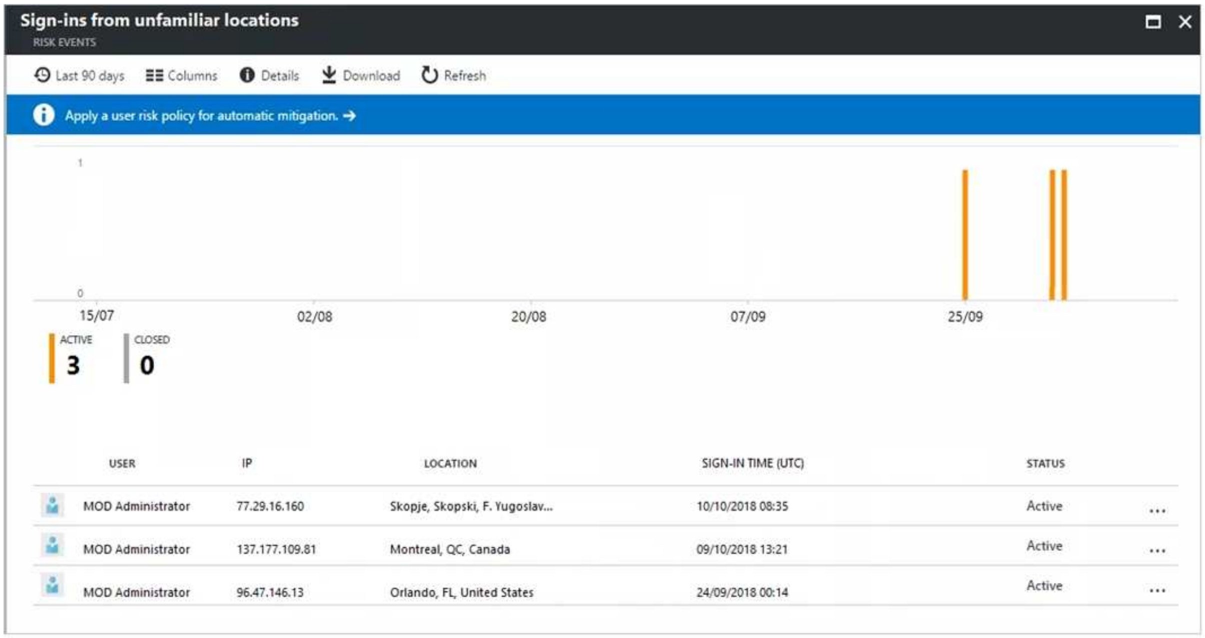
**Correct Answer:**

**Section: [none]**
**Explanation**

**Explanation/Reference:**
References:
https://docs.microsoft.com/en-us/office365/securitycompliance/integrate-your-siem-server-with-office-365-cas

**QUESTION 11**
HOTSPOT

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



| USER | IP | LOCATION | SIGN-IN TIME (UTC) | STATUS | |
|---|---|---|---|---|---|
| MOD Administrator | 77.29.16.160 | Skopje, Skopski, F. Yugoslav... | 10/10/2018 08:35 | Active | ... |
| MOD Administrator | 137.177.109.81 | Montreal, QC, Canada | 09/10/2018 13:21 | Active | ... |
| MOD Administrator | 96.47.146.13 | Orlando, FL, United States | 24/09/2018 00:14 | Active | ... |

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.

**Hot Area:**

**Correct Answer:**

**Section: [none]**
**Explanation**

**Explanation/Reference:**
References:
https://docs.microsoft.com/en-us/azure/active-directory/authentication/howto-mfa-getstarted

https://docs.microsoft.com/en-us/azure/active-directory/identity-protection/howto-sign-in-risk-policy

https://docs.microsoft.com/en-us/azure/active-directory/reports-monitoring/quickstart-configure-named-locations

**QUESTION 12**
Your company uses Microsoft Azure Advanced Threat Protection (ATP) and Windows Defender ATP.

You need to integrate Windows Defender ATP and Azure ATP.

What should you do?

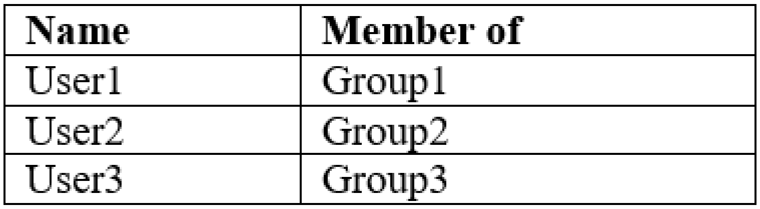
A. From Azure ATP, configure the notifications and reports.
B. From Azure ATP, configure the data sources.
C. From Windows Defender Security Center, configure the Machine management settings.
D. From Windows Defender Security Center, configure the General settings.

**Correct Answer:** B
**Section: [none]**
**Explanation**

**Explanation/Reference:**
References:
https://docs.microsoft.com/en-us/azure-advanced-threat-protection/integrate-wd-atp

**QUESTION 13**
HOTSPOT

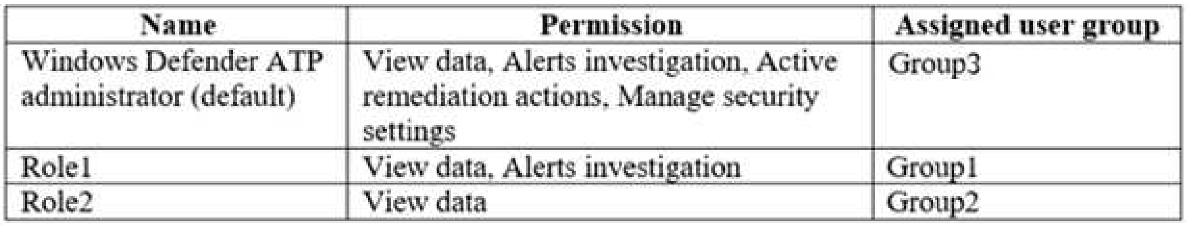
You have a Microsoft Azure Activity Directory (Azure AD) tenant contains the users shown in the following table.



| Name | Member of |
|---|---|
| User1 | Group1 |
| User2 | Group2 |
| User3 | Group3 |

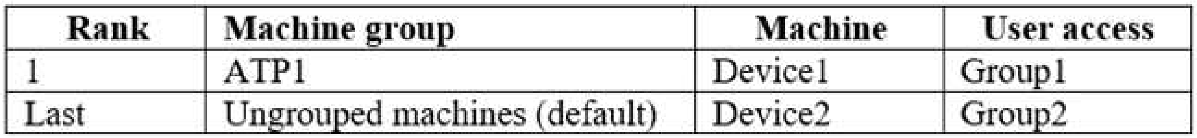
Group3 is a member of Group1.

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



| Name | Permission | Assigned user group |
|---|---|---|
| Windows Defender ATP administrator (default) | View data, Alerts investigation, Active remediation actions, Manage security settings | Group3 |
| Role1 | View data, Alerts investigation | Group1 |
| Role2 | View data | Group2 |

Windows 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 | Group2 |

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:**

**Correct Answer:**

**Section: [none]**
**Explanation**

**Explanation/Reference:**
References:
https://docs.microsoft.com/en-us/windows/security/threat-protection/windows-defender-atp/user-roles-windows-defender-advanced-threat-protection

**QUESTION 14**
HOTSPOT

You have a Microsoft 365 subscription.

You need to implement Windows 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.

**NOTE**: Each correct selection is worth one point.

**Hot Area:**

**Correct Answer:**

**Section: [none]**
**Explanation**

**Explanation/Reference:**
References:
https://docs.microsoft.com/en-us/intune/advanced-threat-protection

**QUESTION 15**
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 score.

What should you configure from the Cloud Discover settings?

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

**Correct Answer:** D
**Section: [none]**
**Explanation**

**Explanation/Reference:**
References:
https://docs.microsoft.com/en-us/cloud-app-security/discovered-app-queries

**QUESTION 16**
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 Azure Advanced Threat Protection (ATP).

What should you do? More than one answer choice may achieve the goal. Select the **BEST** answer.

A. Deploy an Azure ATP sensor, and then configure port mirroring.
B. Deploy an Azure ATP sensor, and then configure detections.
C. Deploy an Azure ATP standalone sensor, and then configure detections.
D. Deploy an Azure ATP standalone sensor, and then configure port mirroring.

**Correct Answer:** D
**Section: [none]**
**Explanation**

**Explanation/Reference:**
References:
https://docs.microsoft.com/en-us/azure-advanced-threat-protection/install-atp-step5

**QUESTION 17**
DRAG DROP

You create a Microsoft 365 subscription.

You need to create a deployment plan for Microsoft Azure Advanced Threat Protection (ATP).

Which five 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:**

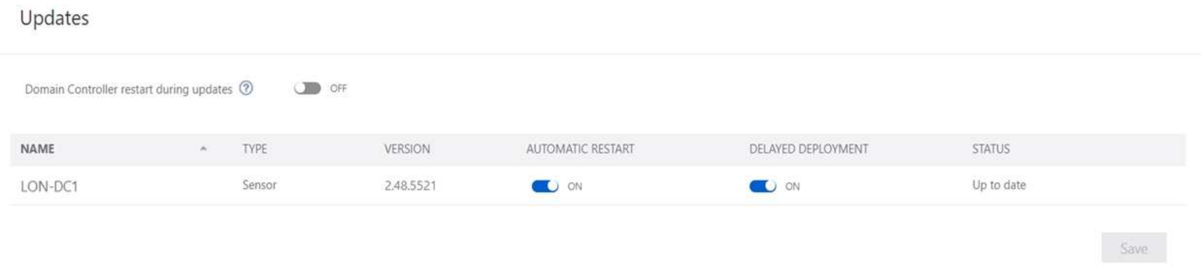
**Correct Answer:**

**Section: [none]**
**Explanation**

**Explanation/Reference:**
References:
https://blog.ahasayen.com/azure-advanced-threat-protection-deployment/

**QUESTION 18**
You implement Microsoft Azure Advanced Threat Protection (Azure ATP).

You have an Azure ATP sensor configured as shown in the following exhibit.



Updates

Domain Controller restart during updates ⓘ OFF

| NAME | TYPE | VERSION | AUTOMATIC RESTART | DELAYED DEPLOYMENT | STATUS |
|---|---|---|---|---|---|
| LON-DC1 | Sensor | 2.48.5521 | ON | ON | Up to date |

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

A. 1 hour
B. 12 hours
C. 48 hours
D. 7 days
E. 24 hours

**Correct Answer:** E
**Section: [none]**
**Explanation**

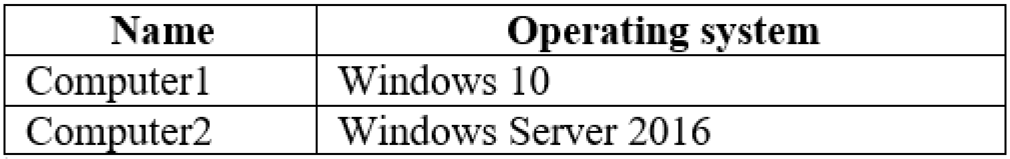
**Explanation/Reference:**
References:
https://docs.microsoft.com/en-us/azure-advanced-threat-protection/atp-whats-new

**QUESTION 19**
HOTSPOT

Your company uses Windows Defender Advanced Threat Protection (ATP). Windows 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 Windows Defender ATP as shown in the following table.

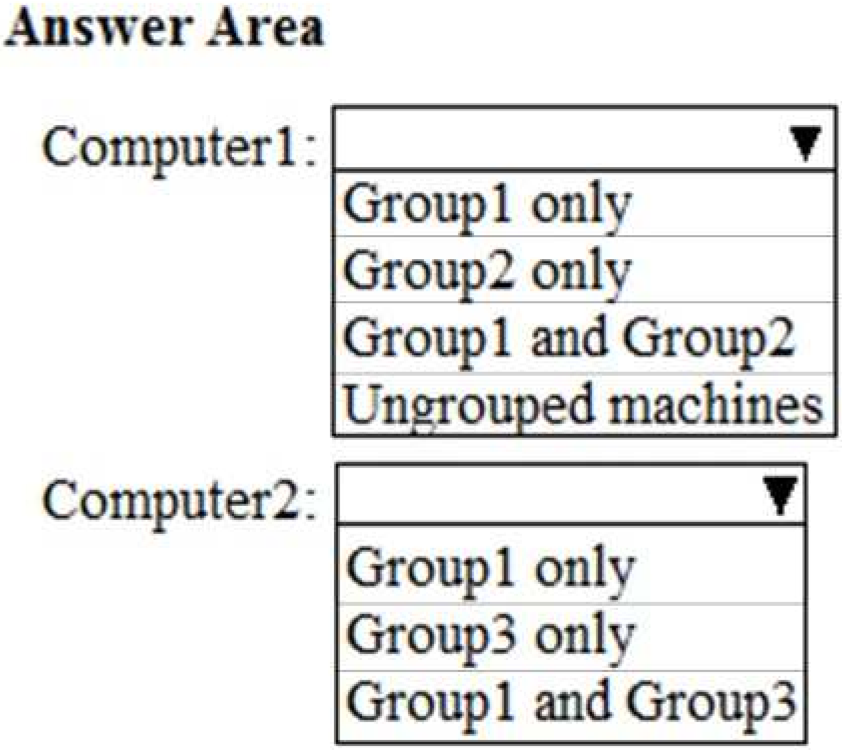


| Name | Operating system |
|---|---|
| Computer1 | Windows 10 |
| Computer2 | Windows Server 2016 |

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

**NOTE**: Each correct selection is worth one point.

**Hot Area:**



**Answer Area**

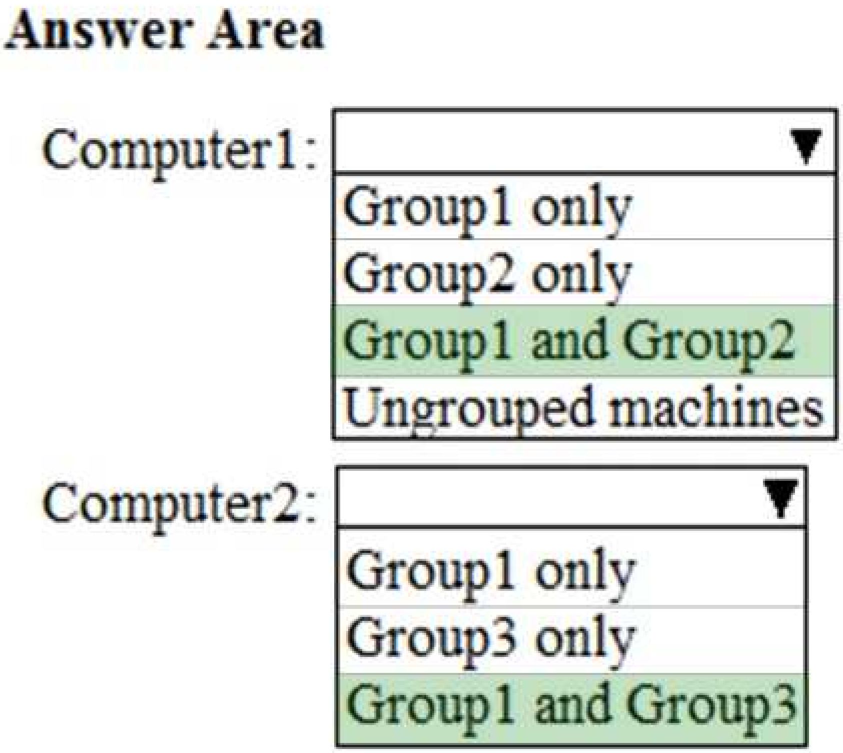
Computer1: ▼

- Group1 only
- Group2 only
- Group1 and Group2
- Ungrouped machines

Computer2: ▼

- Group1 only
- Group3 only
- Group1 and Group3

**Correct Answer:**



Answer Area

Computer1: ▼

- Group1 only
- Group2 only
- [✓ Group1 and Group2]
- Ungrouped machines

Computer2: ▼

- Group1 only
- Group3 only
- [✓ Group1 and Group3]

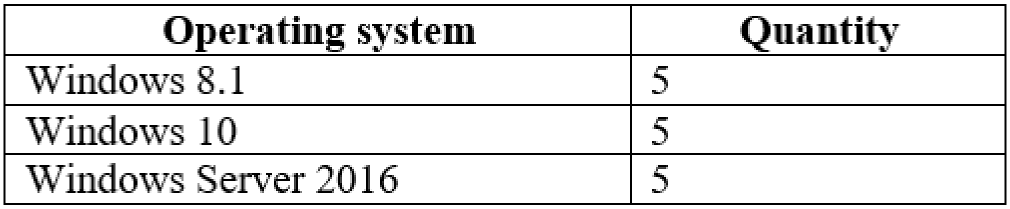
**Section: [none]**
**Explanation**

**Explanation/Reference:**

**QUESTION 20**
DRAG DROP

You have a Microsoft 365 subscription.

You have the devices shown in the following table.



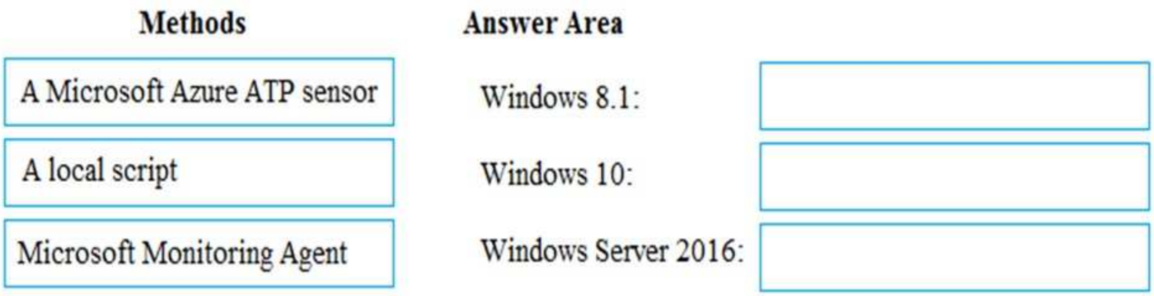
| Operating system | Quantity |
|---|---|
| Windows 8.1 | 5 |
| Windows 10 | 5 |
| Windows Server 2016 | 5 |

You need to onboard the devices to Windows Defender Advanced Threat Protection (ATP). 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.

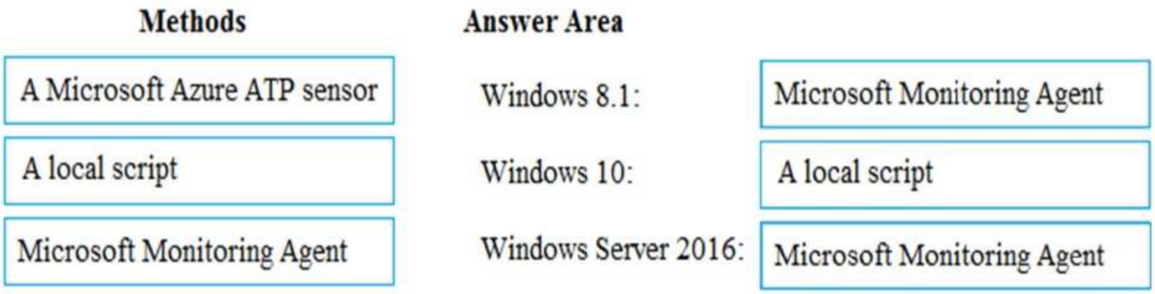
**NOTE**: Each correct selection is worth one point.

**Select and Place:**



| Methods | Answer Area | |
|---|---|---|
| A Microsoft Azure ATP sensor | Windows 8.1: | |
| A local script | Windows 10: | |
| Microsoft Monitoring Agent | Windows Server 2016: | |

**Correct Answer:**



| Methods | Answer Area | |
|---|---|---|
| A Microsoft Azure ATP sensor | Windows 8.1: | Microsoft Monitoring Agent |
| A local script | Windows 10: | A local script |
| Microsoft Monitoring Agent | Windows Server 2016: | Microsoft Monitoring Agent |

**Section: [none]**
**Explanation**

**Explanation/Reference:**
References:
https://docs.microsoft.com/en-us/windows/security/threat-protection/windows-defender-atp/onboard-downlevel-windows-defender-advanced-threat-protection

https://docs.microsoft.com/en-us/windows/security/threat-protection/windows-defender-atp/configure-endpoints-windows-defender-advanced-threat-protection

https://docs.microsoft.com/en-us/windows/security/threat-protection/windows-defender-atp/configure-server-endpoints-windows-defender-advanced-threat-protection

**QUESTION 21**
The users at your company use Dropbox to store documents. The users access Dropbox by using the MyApps portal.

You need to ensure that user access to Dropbox is authenticated by using a Microsoft 365 identity. The documents must be protected if the data is downloaded to an untrusted device.

What should you do?

A. From the Intune admin center, configure the Conditional access settings.
B. From the Azure Active Directory admin center, configure the Organizational relationships settings.
C. From the Azure Active Directory admin center, configure the Application proxy settings.
D. From the Azure Active Directory admin center, configure the Devices settings.

**Correct Answer:** B
**Section: [none]**
**Explanation**

**Explanation/Reference:**

**QUESTION 22**
**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 discover that some external users accessed content on a Microsoft SharePoint site. You modify the SharePoint sharing policy to prevent sharing outside your organization.

You need to be notified if the SharePoint sharing policy is modified in the future.

Solution: From the SharePoint admin center, you modify the sharing settings.

Does this meet the goal?

A. Yes
B. No

**Correct Answer:** B
**Section: [none]**
**Explanation**

**Explanation/Reference:**

**QUESTION 23**
**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

**Correct Answer:** B
**Section: [none]**
**Explanation**

**Explanation/Reference:**
Explanation:

Conditional Access in SharePoint Online can be configured to use an IP Address white list to allow access.

References:
https://techcommunity.microsoft.com/t5/Microsoft-SharePoint-Blog/Conditional-Access-in-SharePoint-Online-and-OneDrive-for/ba-p/46678

**QUESTION 24**
**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

**Correct Answer:** B
**Section: [none]**
**Explanation**

**Explanation/Reference:**
Explanation:
Conditional Access in SharePoint Online can be configured to use an IP Address white list to allow access.

References:
https://techcommunity.microsoft.com/t5/Microsoft-SharePoint-Blog/Conditional-Access-in-SharePoint-Online-and-OneDrive-for/ba-p/46678A

**QUESTION 25**
**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

**Correct Answer:** B
**Section: [none]**
**Explanation**

**Explanation/Reference:**
Explanation:
This solution applies to users accessing Azure Active Directory, not to users accessing SharePoint Online. Conditional Access in SharePoint Online can be configured to use an IP Address white list to allow access.

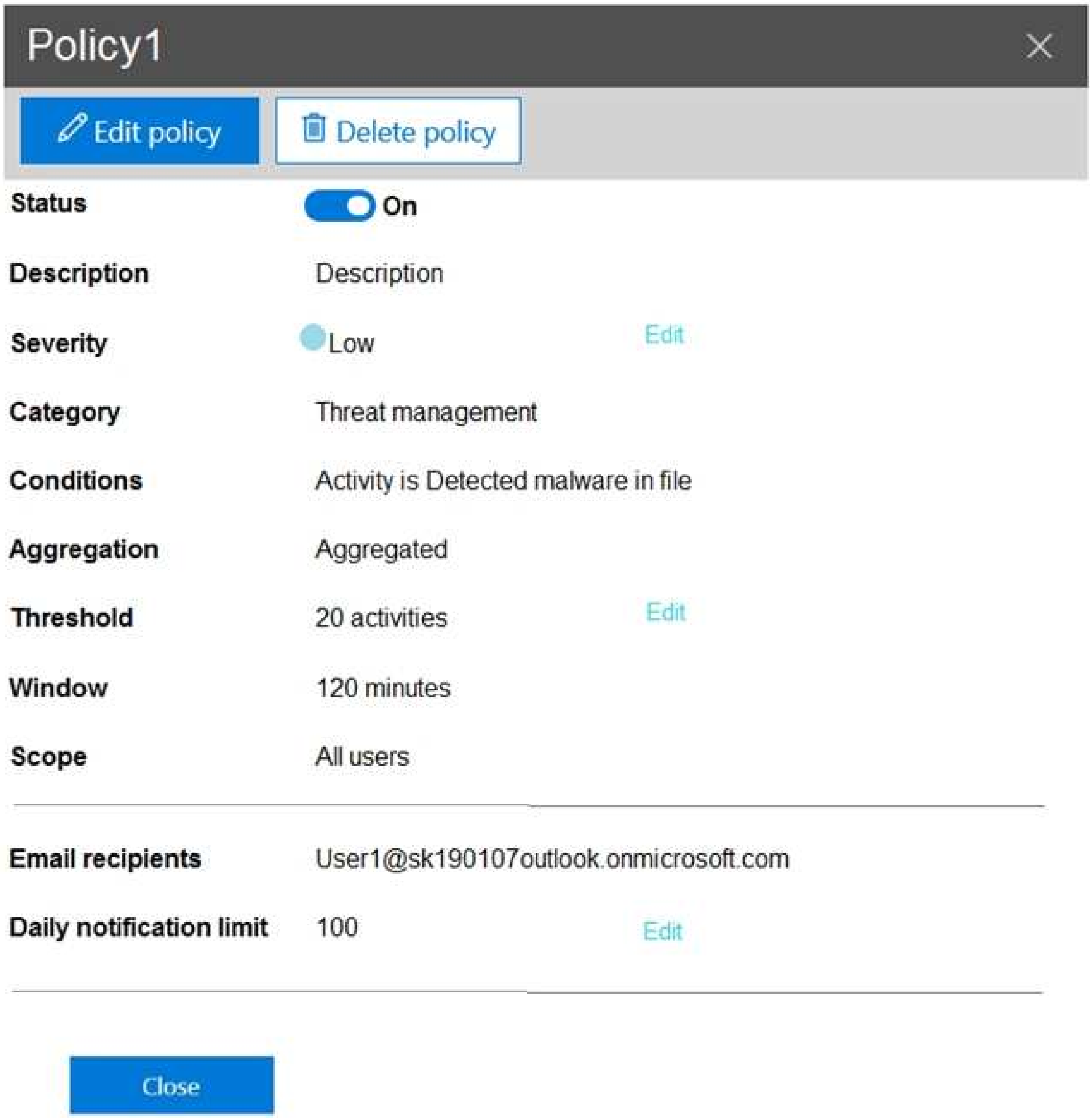
References:
https://docs.microsoft.com/en-us/azure/active-directory/conditional-access/location-condition

https://techcommunity.microsoft.com/t5/Microsoft-SharePoint-Blog/Conditional-Access-in-SharePoint-Online-and-OneDrive-for/ba-p/46678

**QUESTION 26**
HOTSPOT

You have Microsoft 365 subscription.

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

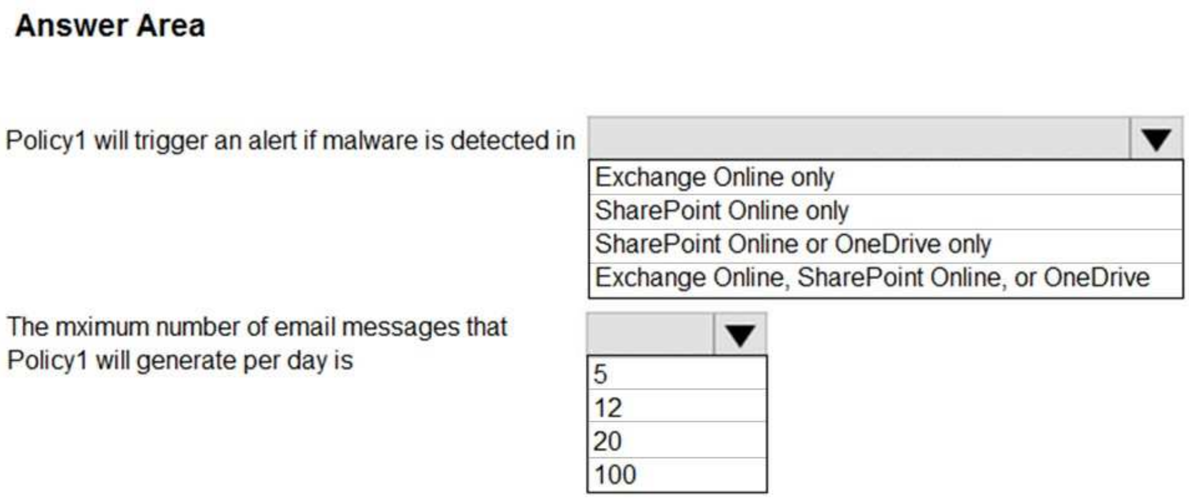


| | |
|---|---|
| Status | On |
| Description | Description |
| Severity | ● Low |
| Category | Threat management |
| Conditions | Activity is Detected malware in file |
| Aggregation | Aggregated |
| Threshold | 20 activities |
| Window | 120 minutes |
| Scope | All users |
| Email recipients | User1@sk190107outlook.onmicrosoft.com |
| Daily notification limit | 100 |

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.

**Hot Area:**



Answer Area

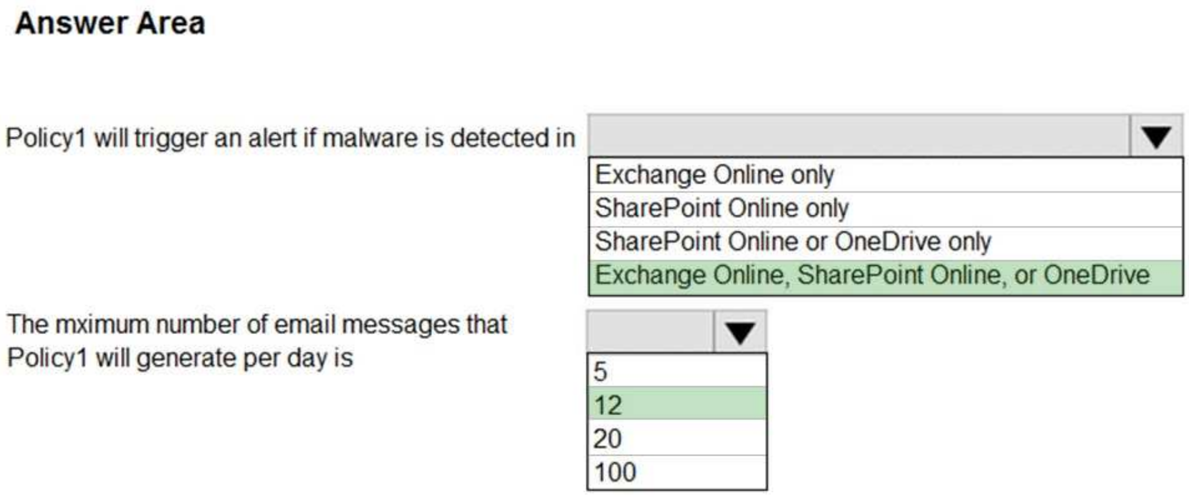
Policy1 will trigger an alert if malware is detected in

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

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

- 5
- 12
- 20
- 100

**Correct Answer:**



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 mximum number of email messages that Policy1 will generate per day is

- 5
- [✓ 12]
- 20
- 100

**Section: [none]**
**Explanation**

**Explanation/Reference:**
Explanation:
Note: The Aggregation settings has a 120 minute window

**QUESTION 27**
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.

**Correct Answer:** A
**Section: [none]**
**Explanation**

**Explanation/Reference:**
References:
https://docs.microsoft.com/en-us/azure/information-protection/configure-policy-classification

**QUESTION 28**
HOTSPOT

You have a new Microsoft 365 subscription.

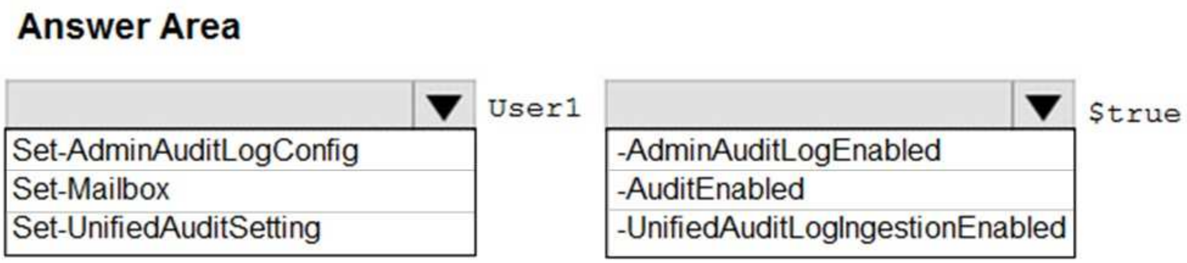
A user named User1 has a mailbox in Microsoft Exchange Online.

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.

**NOTE:** Each correct selection is worth one point.

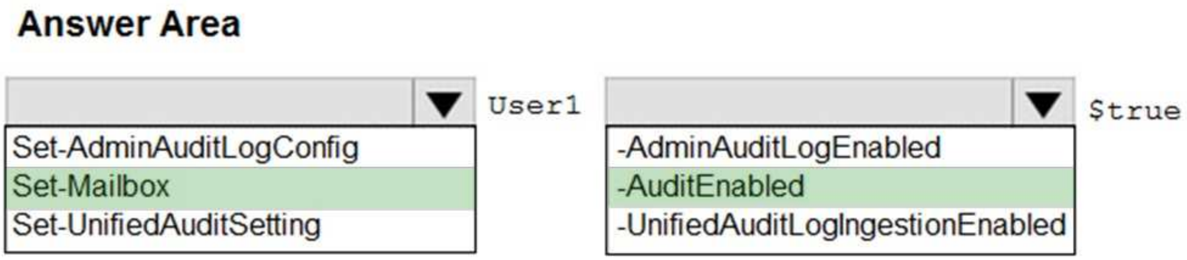
**Hot Area:**



Answer Area

| | | | |
|---|---|---|---|
| Set-AdminAuditLogConfig<br>Set-Mailbox<br>Set-UnifiedAuditSetting | User1 | -AdminAuditLogEnabled<br>-AuditEnabled<br>-UnifiedAuditLogIngestionEnabled | $true |

**Correct Answer:**



Answer Area

| | | | |
|---|---|---|---|
| Set-AdminAuditLogConfig<br>[✓ Set-Mailbox]<br>Set-UnifiedAuditSetting | User1 | -AdminAuditLogEnabled<br>[✓ -AuditEnabled]<br>-UnifiedAuditLogIngestionEnabled | $true |

**Section: [none]**
**Explanation**

**Explanation/Reference:**
Explanation:

To enable auditing for a single mailbox (in this example, belonging to Holly Sharp), use this PowerShell command: Set-Mailbox username -AuditEnabled $true

References:
https://support.microsoft.com/en-us/help/4026501/office-auditing-in-office-365-for-admins

https://docs.microsoft.com/en-us/powershell/module/exchange/mailboxes/set-mailbox?view=exchange-ps

**QUESTION 29**
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 Windows Defender Advanced Threat Protection (Windows Defender ATP)
C. Enable Microsoft Office 365 Analytics.

**Correct Answer:** B
**Section: [none]**
**Explanation**

**Explanation/Reference:**

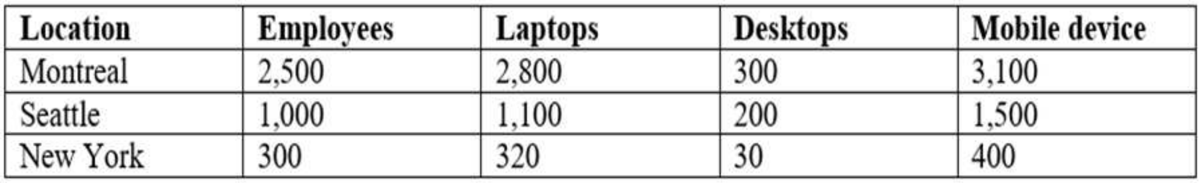
**Testlet 2**

**Case Study**

**Overview**

Contoso, Ltd. is a consulting company that has a main office in Montreal and two branch offices in Seattle and New York.

The company has the employees and devices shown in the following table.

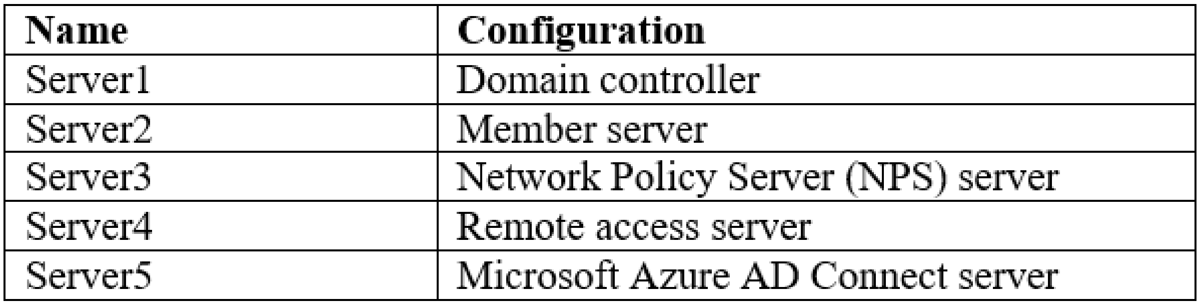


| Location | Employees | Laptops | Desktops | Mobile device |
|---|---|---|---|---|
| Montreal | 2,500 | 2,800 | 300 | 3,100 |
| Seattle | 1,000 | 1,100 | 200 | 1,500 |
| New York | 300 | 320 | 30 | 400 |

Contoso recently purchased a Microsoft 365 E5 subscription.

**Existing Environment**

The network contains an on-premises Active Directory forest named contoso.com. The forest contains the servers shown in the following table.

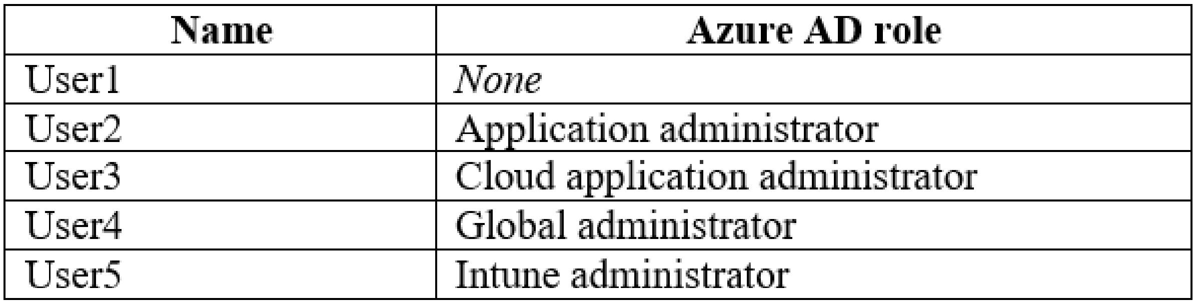


| Name | Configuration |
|---|---|
| Server1 | Domain controller |
| Server2 | Member server |
| Server3 | Network Policy Server (NPS) server |
| Server4 | Remote access server |
| Server5 | Microsoft Azure AD Connect server |

All servers run Windows Server 2016. All desktops and laptops run Windows 10 Enterprise and are joined to the domain.

The mobile devices of the users in the Montreal and Seattle offices run Android. The mobile devices of the users in the New York office run iOS.

The domain is synced to Azure Active Directory (Azure AD) and includes the users shown in the following table.



| Name | Azure AD role |
|---|---|
| User1 | *None* |
| User2 | Application administrator |
| User3 | Cloud application administrator |
| User4 | Global administrator |
| User5 | Intune administrator |

The domain also includes a group named Group1.

**Requirements**

**Planned Changes**

Contoso plans to implement the following changes:

- Implement Microsoft 365.
- Manage devices by using Microsoft Intune.
- Implement Azure Advanced Threat Protection (ATP).
- Every September, apply the latest feature updates to all Windows computers. Every March, apply the latest feature updates to the computers in the New York office only.

**Technical Requirements**

Contoso identifies the following technical requirements:

- When a Windows 10 device is joined to Azure AD, the device must enroll in Intune automatically.
- Dedicated support technicians must enroll all the Montreal office mobile devices in Intune.
- User1 must be able to enroll all the New York office mobile devices in Intune.
- Azure ATP sensors must be installed and must **NOT** use port mirroring.
- Whenever possible, the principle of least privilege must be used.
- A Microsoft Store for Business must be created.

**Compliance Requirements**

Contoso identifies the following compliance requirements:

- Ensure that the users in Group1 can only access Microsoft Exchange Online from devices that are enrolled in Intune and configured in accordance with the corporate policy.
- Configure Windows Information Protection (WIP) for the Windows 10 devices.

**QUESTION 1**
On which server should you install the Azure ATP sensor?

A. Server1
B. Server2
C. Server3
D. Server4
E. Server5

**Correct Answer:** A
**Section: [none]**
**Explanation**

**Explanation/Reference:**
References:
https://docs.microsoft.com/en-us/azure-advanced-threat-protection/atp-capacity-planning

**Testlet 3**

**Case Study**

**Overview**

ADatum Corporation is an international financial services company that has 5,000 employees.

ADatum has six offices: a main office in New York and five branch offices in Germany, the United Kingdom, France, Spain, and Italy.

All the offices are connected to each other by using a WAN link. Each office connects directly to the Internet.

**Existing Environment**

**Current Infrastructure**

ADatum recently purchased a Microsoft 365 subscription.

All user files are migrated to Microsoft 365.

All mailboxes are hosted in Microsoft 365. The users in each office have email suffixes that include the country of the user, for example, user1@us.adatum.com or user2@uk.adatum.com.

Each office has a security information and event management (SIEM) appliance. The appliance comes from three different vendors.

ADatum uses and processes Personally Identifiable Information (PII).

**Problem Statements**

ADatum entered into litigation. The legal department must place a hold on all the documents of a user named User1 that are in Microsoft 365.

**Requirements**

**Business Goals**

ADatum wants to be fully compliant with all the relevant data privacy laws in the regions where is operates.

ADatum wants to minimize the cost of hardware and software whenever possible.

**Technical Requirements**

ADatum identifies the following technical requirements:

- Centrally perform log analysis for all offices.
- Aggregate all data from the SIEM appliances to a central cloud repository for later analysis.
- Ensure that a SharePoint administrator can identify who accessed a specific file stored in a document library.
- Provide the users in the finance department with access to Service assurance information in Microsoft Office 365.
- Ensure that documents and email messages containing the PII data of European Union (EU) citizens are preserved for 10 years.
- If a user attempts to download 1,000 or more files from Microsoft SharePoint Online within 30 minutes, notify a security administrator and suspend the user's user account.
- A security administrator requires a report that shown which Microsoft 365 users signed in. Based on the

report, the security administrator will create a policy to require multi-factor authentication when a sign-in is high risk.

- Ensure that the users in the New York office can only send email messages that contain sensitive U.S. PII data to other New York office uses. Email messages must be monitored to ensure compliance. Auditors in the New York office must have access to reports that show the sent and received email messages containing sensitive U.S. PII data.

**QUESTION 1**
You need to meet the technical requirement for large-volume document retrieval.

What should you create?

A. an activity policy from Microsoft Cloud App Security

B. a data loss prevention (DLP) policy from the Security & Compliance admin center

C. a file policy from Microsoft Cloud App Security

D. an alert policy from the Security & Compliance admin center

**Correct Answer:** A
**Section: [none]**
**Explanation**

**Explanation/Reference:**
References:
https://docs.microsoft.com/en-us/office365/securitycompliance/activity-policies-and-alerts

**Question Set 1**

**QUESTION 1**
You plan to use the Security & Compliance admin center to import several PST files into Microsoft 365 mailboxes.

Which three actions should you perform before you import the data? Each correct answer presents part of the solution.

**NOTE**: Each correct selection is worth one point.

A. From the Exchange admin center, create a public folder.
B. Copy the PST files by using AzCopy.
C. From the Exchange admin center, assign admin roles.
D. From the Microsoft Azure portal, create a storage account that has a blob container.
E. From the Microsoft 365 admin center, deploy an add-in.
F. Create a mapping file that uses the CSV file format.

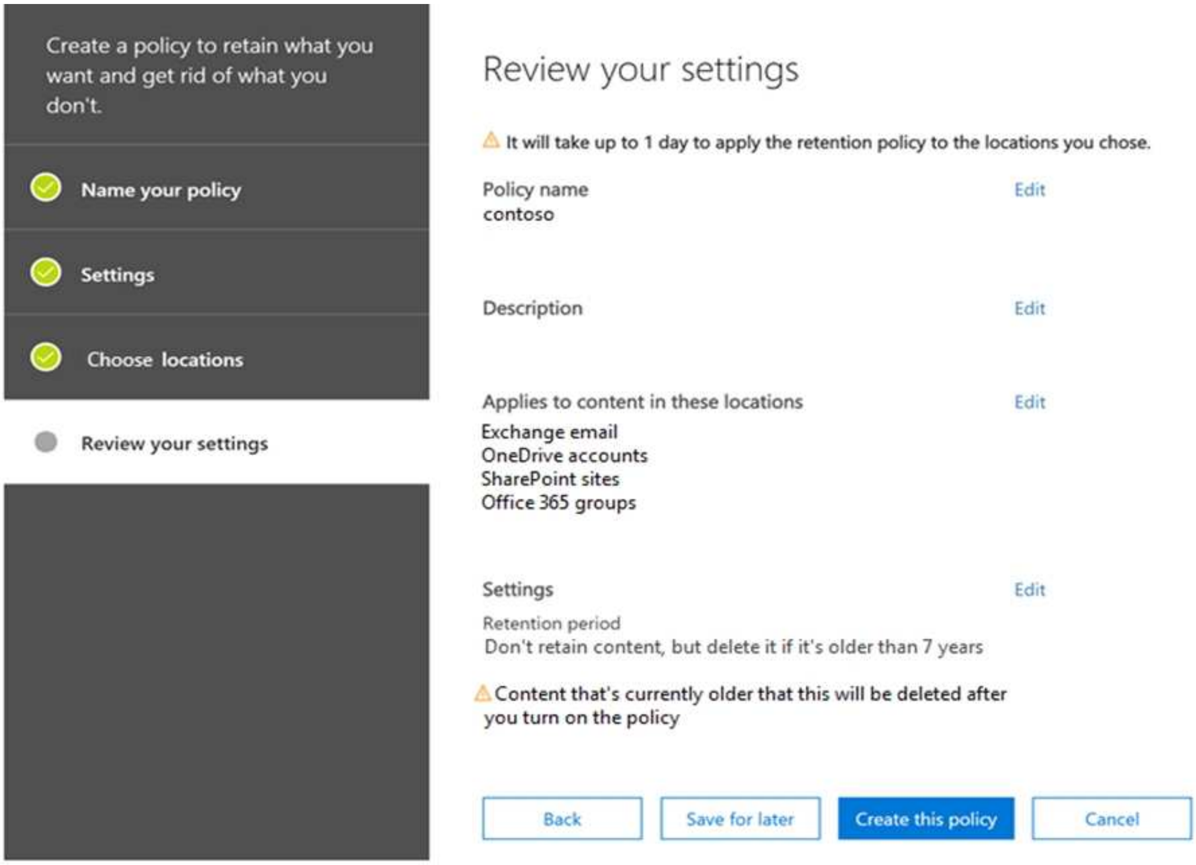
**Correct Answer:** BCF
**Section: [none]**
**Explanation**

**Explanation/Reference:**
References:
https://docs.microsoft.com/en-us/office365/securitycompliance/use-network-upload-to-import-pst-files

**QUESTION 2**
HOTSPOT

You have a Microsoft 365 tenant.

You plan to create a retention policy as shown in the following exhibit.



Create a policy to retain what you want and get rid of what you don't.
Name your policy
Settings
Choose locations
Review your settings

Review your settings

⚠ It will take up to 1 day to apply the retention policy to the locations you chose.

Policy name
contoso

Description

Applies to content in these locations
Exchange email
OneDrive accounts
SharePoint sites
Office 365 groups

Settings
Retention period
Don't retain content, but delete it if it's older than 7 years

⚠ Content that's currently older that this will be deleted after you turn on the policy

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.

**Hot Area:**

**Correct Answer:**

**Section: [none]**
**Explanation**

**Explanation/Reference:**

**QUESTION 3**
You deploy Microsoft Azure Information Protection.

You need to ensure that a security administrator named SecAdmin1 can always read and inspect data protected by Azure Rights Management (Azure RMS).

What should you do?

A. From the Security & Compliance admin center, add SecAdmin1 to the eDiscovery Manager role group.
B. From the Azure Active Directory admin center, add SecAdmin1 to the Security Reader role group.
C. From the Security & Compliance admin center, add SecAdmin1 to the Compliance Administrator role group.
D. From Windows PowerShell, enable the super user feature and assign the role to SecAdmin1.

**Correct Answer:** D
**Section: [none]**
**Explanation**

**Explanation/Reference:**
Explanation:
The super user feature of the Azure Rights Management service from Azure Information Protection ensures that authorized people and services can always read and inspect the data that Azure Rights Management protects for your organization. However, the super user feature is not enabled by default. The PowerShell cmdlet Enable-AadrmSuperUserFeature is used to manually enable the super user feature.

References:
https://docs.microsoft.com/en-us/azure/information-protection/configure-super-users

**QUESTION 4**
HOTSPOT

You have a data loss prevention (DLP) policy.

You need to increase the likelihood that the DLP policy will apply to data that contains medical terms from the International Classification of Diseases (ICD-9-CM). The solution must minimize the number of false positives.

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

**NOTE**: Each correct selection is worth one point.

**Hot Area:**

**Correct Answer:**

**Section: [none]**
**Explanation**

**Explanation/Reference:**
References:
https://docs.microsoft.com/en-us/office365/securitycompliance/data-loss-prevention-policies

https://docs.microsoft.com/en-us/office365/securitycompliance/what-the-sensitive-information-types-look-for#international-classification-of-diseases-icd-9-cm

**QUESTION 5**
HOTSPOT

From the Security & Compliance admin center, you create a retention policy named Policy1.

You need to prevent all users from disabling the policy or reducing the retention period.

Which command should you run? To answer, select the appropriate options in the answer area.

**NOTE**: Each correct selection is worth one point.

**Hot Area:**

**Correct Answer:**

**Section: [none]**
**Explanation**

**Explanation/Reference:**

References:
https://docs.microsoft.com/en-us/powershell/module/exchange/policy-and-compliance-retention/set-retentioncompliancepolicy?view=exchange-ps

**QUESTION 6**
You create a new Microsoft 365 subscription and assign Microsoft 365 E3 licenses to 100 users.

From the Security & Compliance admin center, you enable auditing.

You are planning the auditing strategy.

Which three activities will be audited by default? Each correct answer presents a complete solution.

**NOTE**: Each correct selection is worth one point.

A. An administrator creates a new Microsoft SharePoint site collection.
B. An administrator creates a new mail flow rule.
C. A user shares a Microsoft SharePoint folder with an external user.
D. A user delegates permissions to their mailbox.
E. A user purges messages from their mailbox.

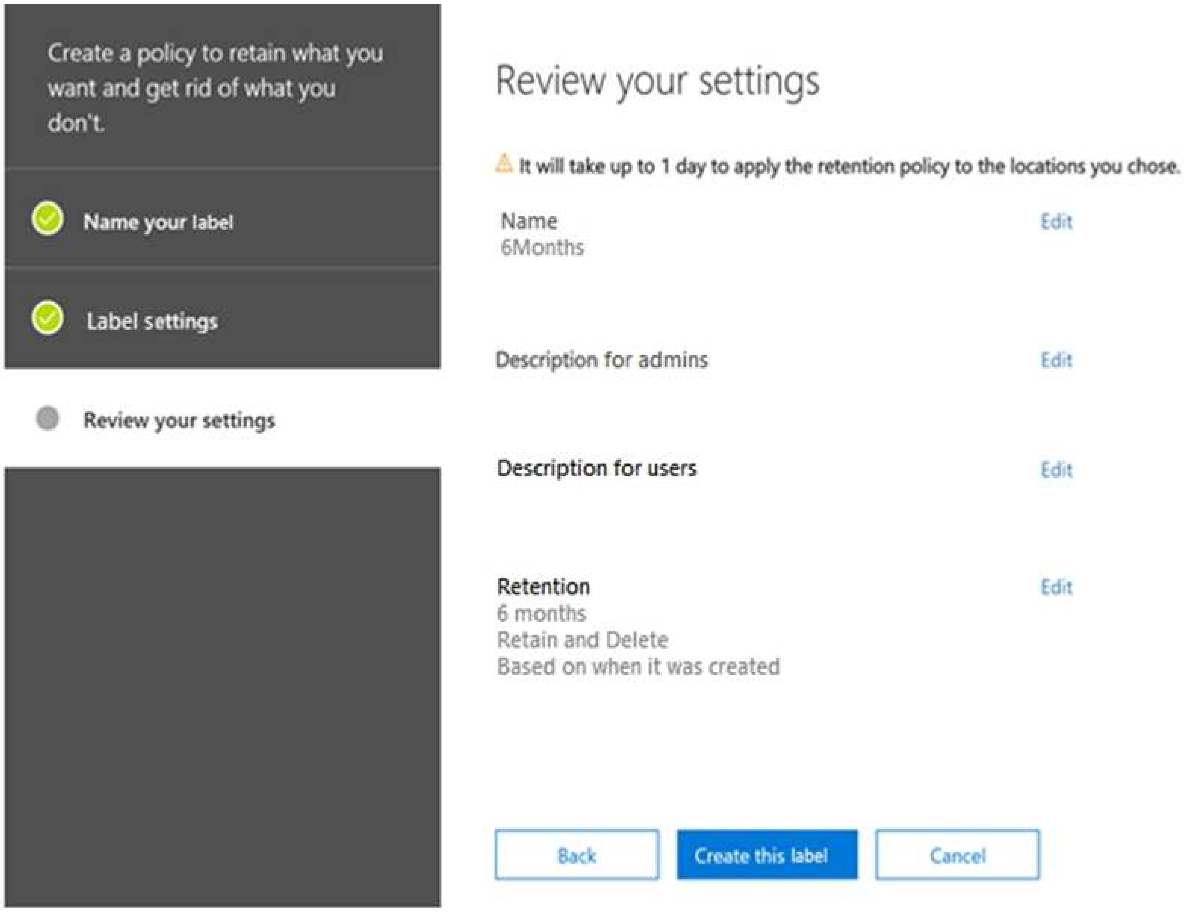
**Correct Answer:** ABC
**Section: [none]**
**Explanation**

**Explanation/Reference:**
References:
https://docs.microsoft.com/en-us/office365/securitycompliance/search-the-audit-log-in-security-and-compliance?redirectSourcePath=%252farticle%252f0d4d0f35-390b-4518-800e-0c7ec95e946c

**QUESTION 7**
HOTSPOT

You have a Microsoft 365 tenant.

You create a retention label as shown in the Retention Label exhibit. (Click the **Retention Label** tab.)



Review your settings

⚠ It will take up to 1 day to apply the retention policy to the locations you chose.

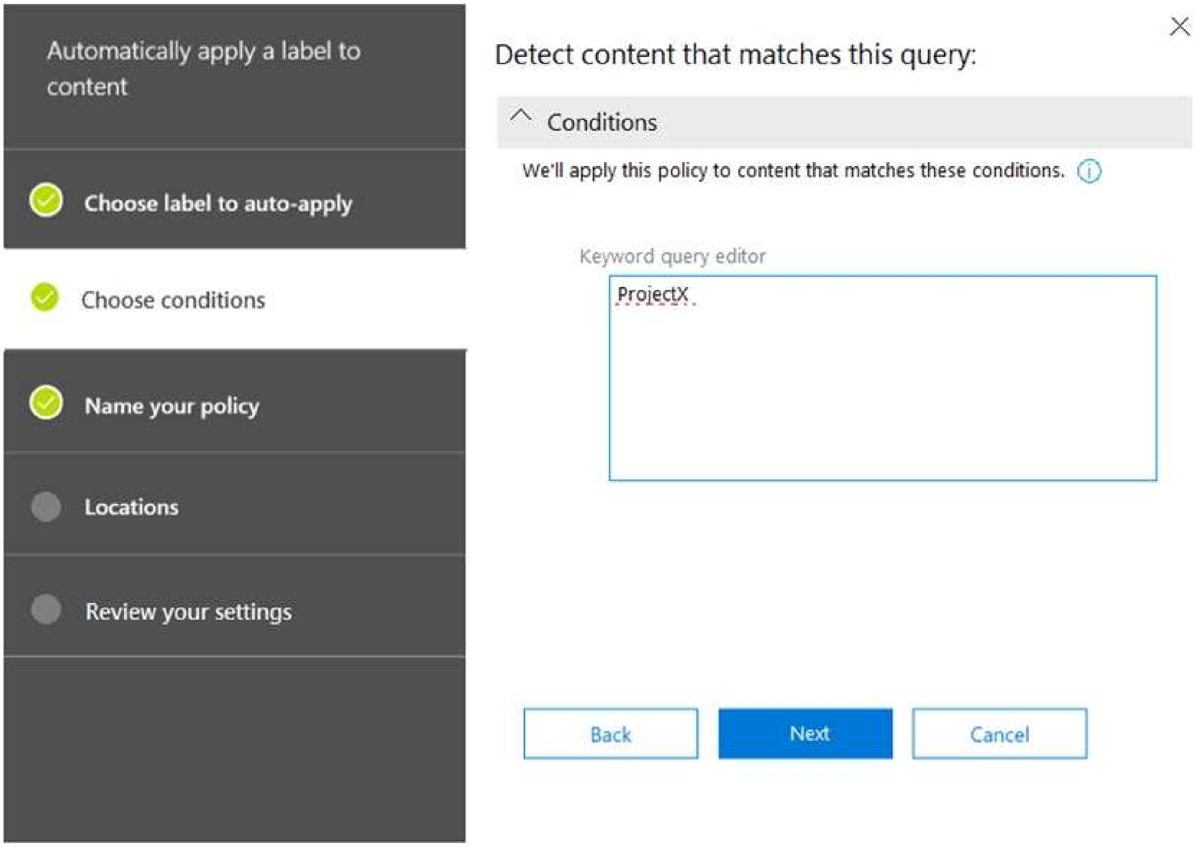
Name
6Months

Description for admins

Description for users

Retention
6 months
Retain and Delete
Based on when it was created

You create a label policy as shown in the Label Policy Exhibit. (Click the **Label Policy** tab.)



Detect content that matches this query:

Conditions

We'll apply this policy to content that matches these conditions.

Keyword query editor

ProjectX.

The label policy is configured as shown in the following table.

| Configuration | Value |
|---|---|
| Label to auto-apply | 6Months |
| Locations | Exchange email |

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:**

**Correct Answer:**

**Section: [none]**
**Explanation**

**Explanation/Reference:**
References:
https://docs.microsoft.com/en-us/office365/securitycompliance/retention-policies

**QUESTION 8**
HOTSPOT

You purchase a new Microsoft 365 subscription.

You create 100 users who are assigned Microsoft 365 E3 licenses.

From the Security & Compliance admin center, you enable auditing.

Six months later, a manager sends you an email message asking the following questions:

- Question1: Who created a team named Team1 14 days ago?
- Question2: Who signed in to the mailbox of User1 30 days ago?
- Question3: Who changed the site collection administrators of a site 60 days ago?

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:**

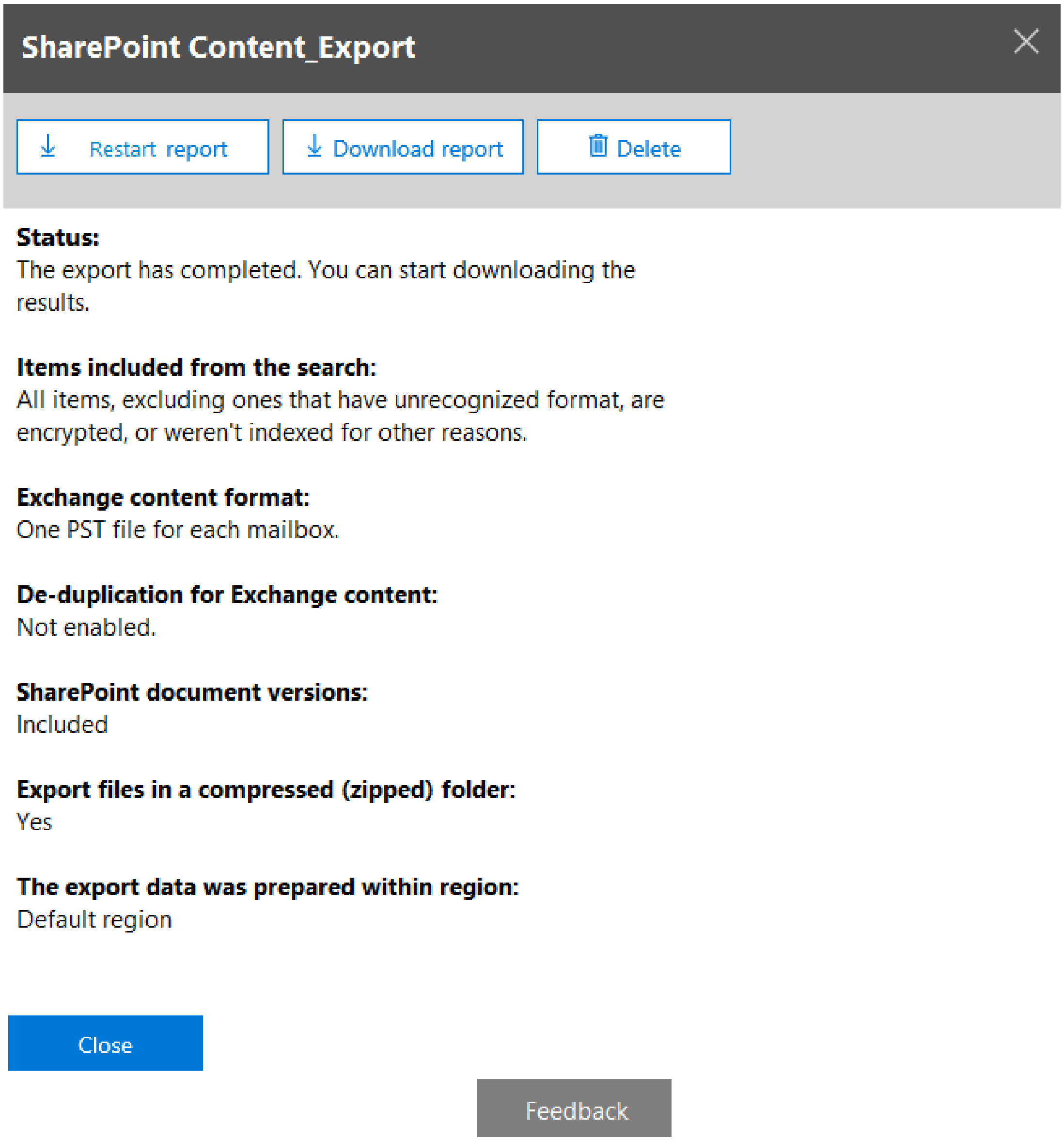
**Correct Answer:**

**Section: [none]**
**Explanation**

**Explanation/Reference:**
References:
https://docs.microsoft.com/en-us/office365/securitycompliance/search-the-audit-log-in-security-and-compliance?redirectSourcePath=%252farticle%252f0d4d0f35-390b-4518-800e-0c7ec95e946c

https://docs.microsoft.com/en-us/office365/securitycompliance/enable-mailbox-auditing

**QUESTION 9**
From the Security & Compliance admin center, you create a content export as shown in the exhibit. (Click the **Exhibit** tab.)



**Status:**
The export has completed. You can start downloading the results.

**Items included from the search:**
All items, excluding ones that have unrecognized format, are encrypted, or weren't indexed for other reasons.

**Exchange content format:**
One PST file for each mailbox.

**De-duplication for Exchange content:**
Not enabled.

**SharePoint document versions:**
Included

**Export files in a compressed (zipped) folder:**
Yes

**The export data was prepared within region:**
Default region

What will be excluded from the export?

A. a 60-MB DOCX file
B. a 5-MB MP3 file
C. a 10-MB XLSX file
D. a 5-KB RTF file
E. an 80-MB PPTX file
F. a 100-MB VSDX file

**Correct Answer:** B
**Section: [none]**
**Explanation**

**Explanation/Reference:**
Explanation:
Unrecognized file formats are excluded from the search.

Incorrect answers:
A: DOCX is a supported Microsoft PowerPoint file format.
C: XLSX is a supported Microsoft Excel file format.
D: RTF is a supported Rich Text File format.
E: PPTX is a supported Microsoft PowerPoint file format.
F: VSDX is a supported Microsoft Visio file format.

Answer: B

References:
https://docs.microsoft.com/en-us/office365/securitycompliance/export-a-content-search-report

**QUESTION 10**
Your company has a Microsoft 365 tenant.

The company sells products online and processes credit card information.

You need to be notified if a file stored in Microsoft SharePoint Online contains credit card information. The file must be removed automatically from its current location until an administrator can review its contents.

What should you use?

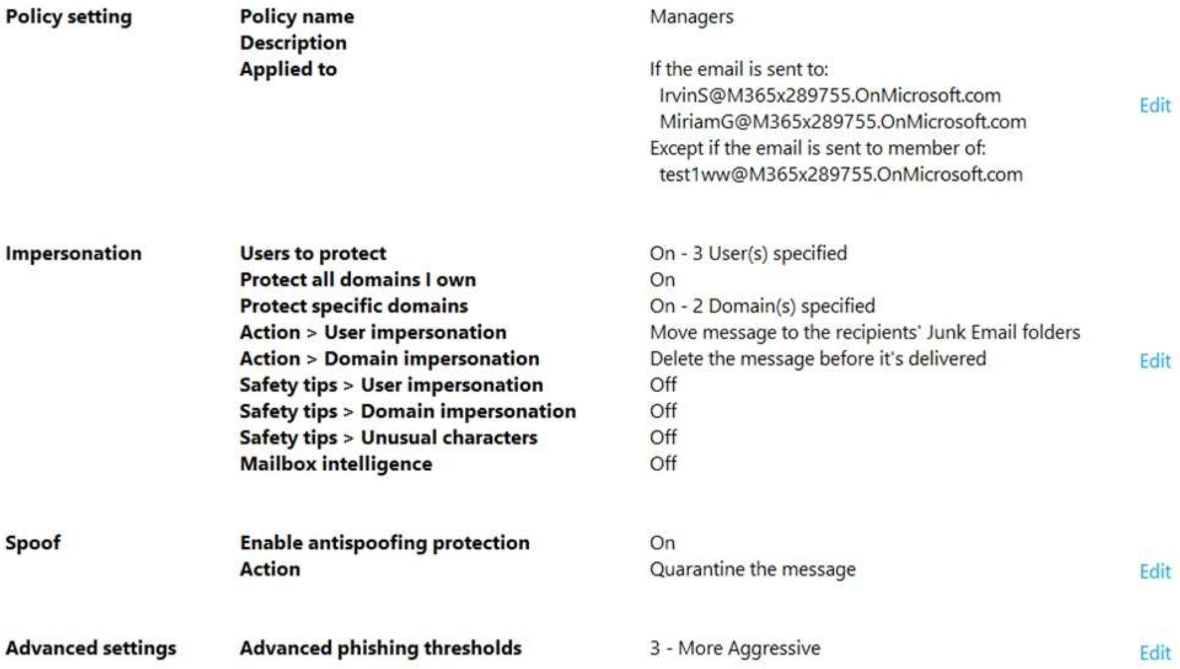
A. a Security & Compliance data loss prevention (DLP) policy
B. a Microsoft Cloud App Security access policy
C. a Security & Compliance retention policy
D. a Microsoft Cloud App Security file policy

**Correct Answer:** A
**Section: [none]**
**Explanation**

**Explanation/Reference:**
References:
https://docs.microsoft.com/en-us/office365/securitycompliance/data-loss-prevention-policies

**QUESTION 11**
HOTSPOT

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



| | | | |
|---|---|---|---|
| Policy setting | Policy name<br>Description<br>Applied to | Managers<br><br>If the email is sent to:<br>IrvinS@M365x289755.OnMicrosoft.com<br>MiriamG@M365x289755.OnMicrosoft.com<br>Except if the email is sent to member of:<br>test1ww@M365x289755.OnMicrosoft.com | Edit |
| Impersonation | Users to protect | On - 3 User(s) specified | Edit |
| | 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 | |
| | Safety tips > User impersonation | Off | |
| | Safety tips > Domain impersonation | Off | |
| | Safety tips > Unusual characters | Off | |
| | Mailbox intelligence | Off | |
| Spoof | Enable antispoofing protection | On | Edit |
| | Action | Quarantine the message | |
| 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.

**Hot Area:**

**Correct Answer:**

**Section: [none]**
**Explanation**

**Explanation/Reference:**
References:
https://docs.microsoft.com/en-us/office365/securitycompliance/set-up-anti-phishing-policies#learn-about-atp-anti-phishing-policy-options

**QUESTION 12**
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 site.

What should you do?

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

**Correct Answer:** A
**Section: [none]**
**Explanation**

**Explanation/Reference:**
References:

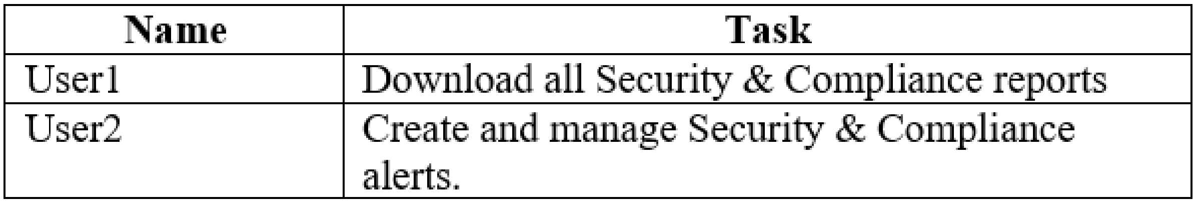
https://docs.microsoft.com/en-us/office365/securitycompliance/create-activity-alerts

**QUESTION 13**
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.

**NOTE**: Each correct selection is worth one point.

**Hot Area:**

**Correct Answer:**

**Section: [none]**
**Explanation**

**Explanation/Reference:**
References:
https://docs.microsoft.com/en-us/office365/securitycompliance/permissions-in-the-security-and-compliance-center#mapping-of-role-groups-to-assigned-roles

**QUESTION 14**
HOTSPOT

You have a Microsoft Azure Active Directory (Azure AD) tenant named contoso.onmicrosoft.com.

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:**

**Correct Answer:**

**Section: [none]**
**Explanation**

**Explanation/Reference:**
References:

https://docs.microsoft.com/en-us/windows/security/information-protection/windows-information-protection/create-wip-policy-using-intune-azure

**QUESTION 15**
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. From the AADRM PowerShell module, run the `Set-AadrmOnboardingControlPolicy` cmdlet.
B. From Azure Information Protection, create a policy.
C. From the AADRM PowerShell module, run the `Set-AadrmRoleBasedAdministrator` cmdlet.
D. From Azure Information Protection, configure the protection activation status.

**Correct Answer:** B
**Section: [none]**
**Explanation**

**Explanation/Reference:**
References:
https://blogs.technet.microsoft.com/kemckinn/2018/05/17/creating-labels-for-azure-information-protection/

**QUESTION 16**
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 Activity Directory (Azure AD) audit logs
B. Security & Compliance content search
C. Microsoft Azure Activity Directory (Azure AD) sign-ins
D. Security & Compliance audit log search

**Correct Answer:** A
**Section: [none]**
**Explanation**

**Explanation/Reference:**
References:
https://docs.microsoft.com/en-us/azure/azure-monitor/platform/activity-logs-overview

**QUESTION 17**
You have a Microsoft 365 subscription.

You have a user named User1.

You need to ensure that User1 can place a hold on all mailbox content.

Which role should you assign to User1?

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

**Correct Answer:** A
**Section: [none]**
**Explanation**

**Explanation/Reference:**
References:
https://docs.microsoft.com/en-us/Exchange/permissions/feature-permissions/policy-and-compliance-permissions?view=exchserver-2019

**QUESTION 18**
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

**Correct Answer:** D
**Section: [none]**
**Explanation**

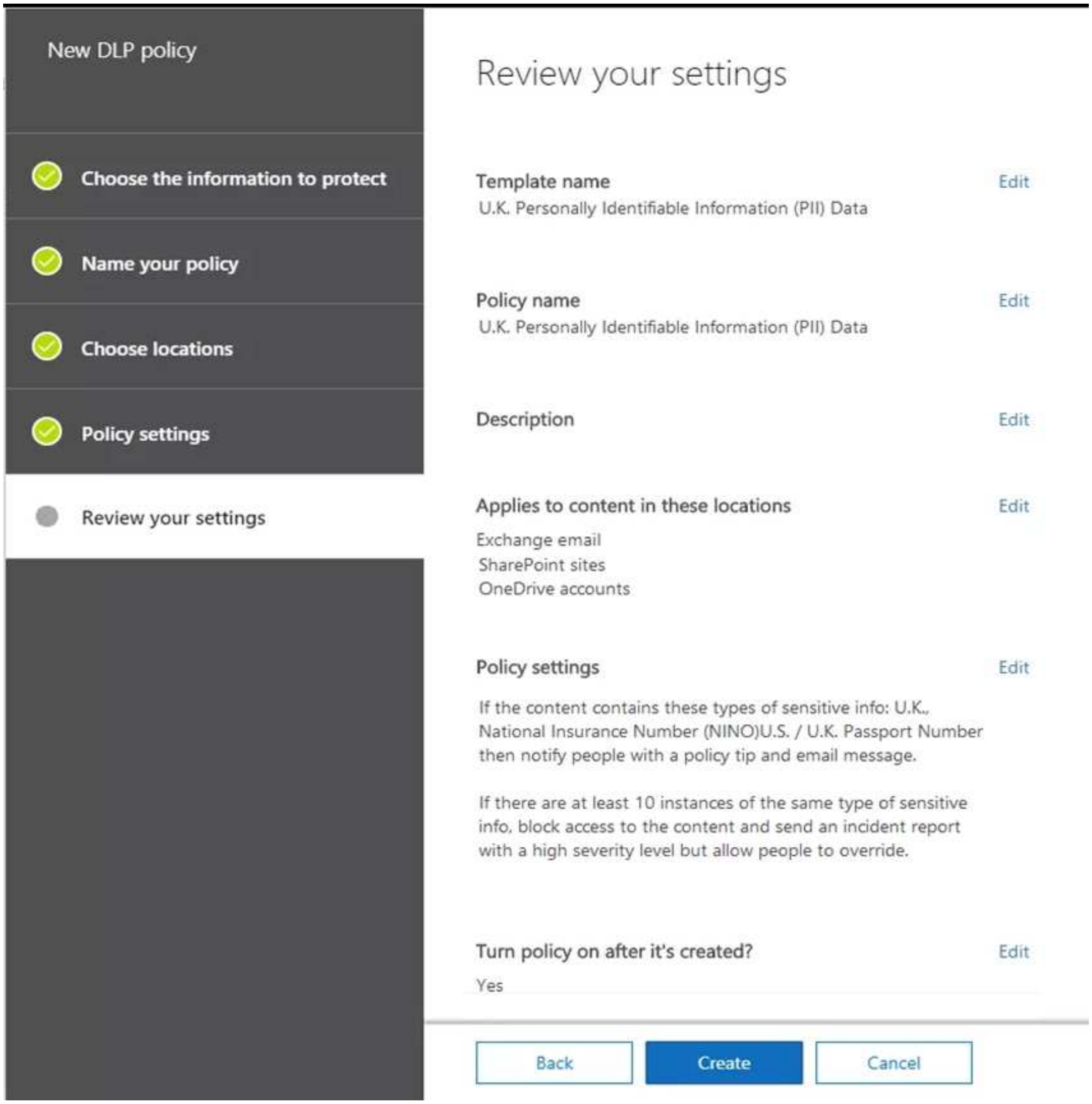
**Explanation/Reference:**
References:
https://docs.microsoft.com/en-us/office365/securitycompliance/search-the-audit-log-in-security-and-compliance

**QUESTION 19**
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.



Review your settings

Template name Edit
U.K. Personally Identifiable Information (PII) Data

Policy name Edit
U.K. Personally Identifiable Information (PII) Data

Description Edit

Applies to content in these locations Edit
Exchange email
SharePoint sites
OneDrive accounts

Policy settings Edit
If the content contains these types of sensitive info: U.K., National Insurance Number (NINO)U.S. / U.K. Passport Number then notify people with a policy tip and email message.

If there are at least 10 instances of the same type of sensitive info, block access to the content and send an incident report with a high severity level but allow people to override.

Turn policy on after it's created? Edit
Yes

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.

**Hot Area:**

**Correct Answer:**

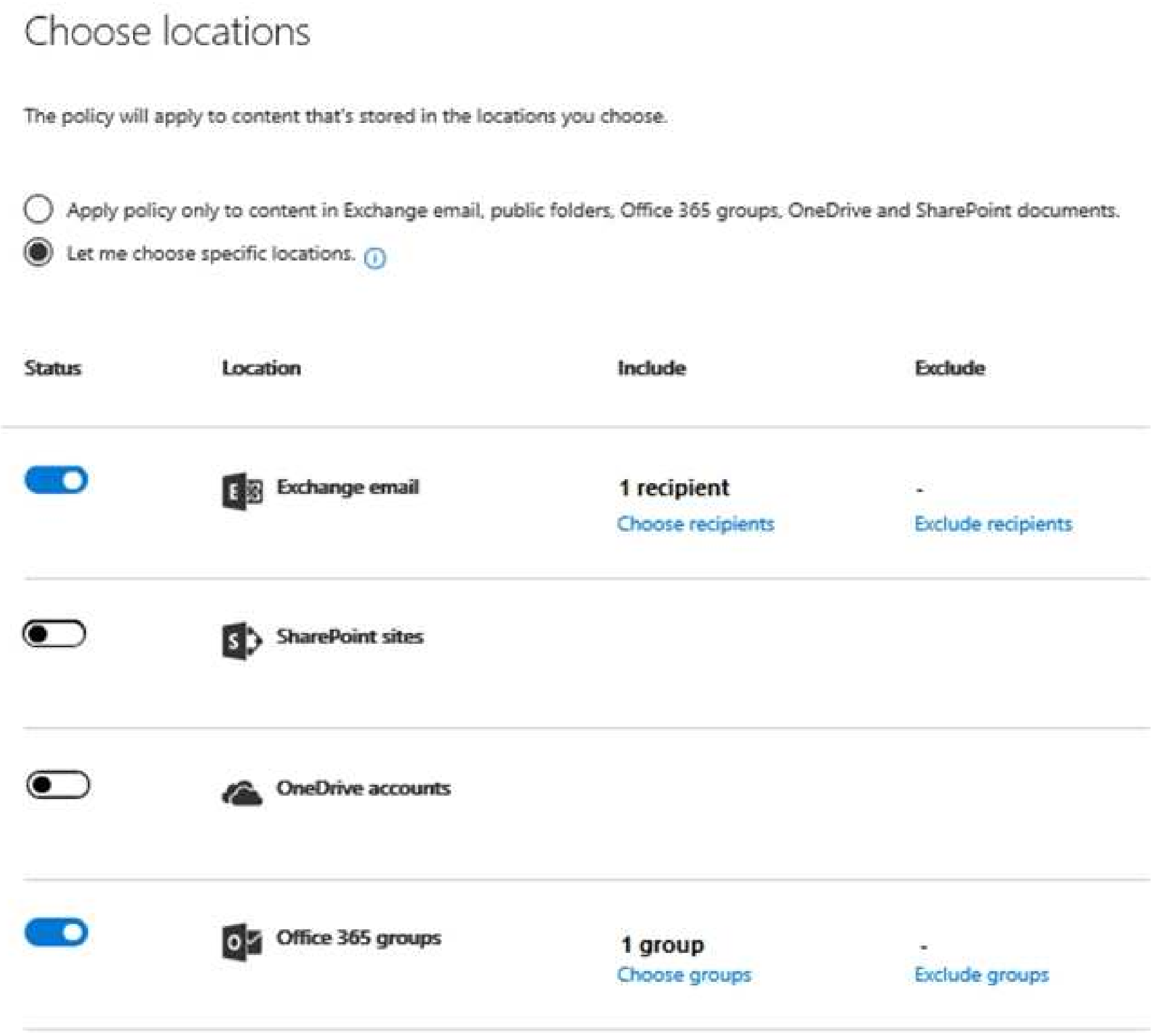
**Section: [none]**
**Explanation**

**Explanation/Reference:**
References:
https://docs.microsoft.com/en-us/office365/securitycompliance/data-loss-prevention-policies

**QUESTION 20**
HOTSPOT

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

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



## Choose locations

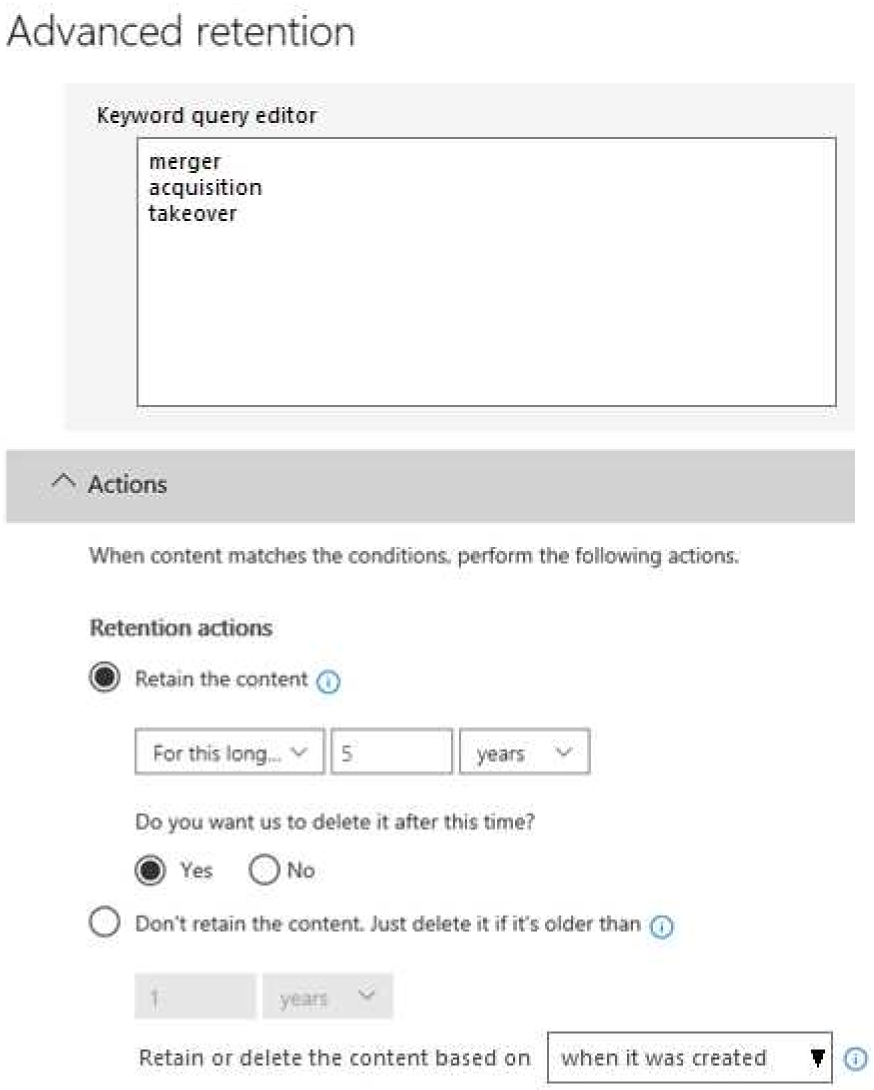
The policy will apply to content that's stored in the locations you choose.

○ Apply policy only to content in Exchange email, public folders, Office 365 groups, OneDrive and SharePoint documents.

● Let me choose specific locations. ⓘ

| Status | Location | Include | Exclude |
|---|---|---|---|
| ● | Exchange email | 1 recipient<br>Choose recipients | -<br>Exclude recipients |
| ○ | SharePoint sites | | |
| ○ | OneDrive accounts | | |
| ● | Office 365 groups | 1 group<br>Choose groups | -<br>Exclude groups |

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



Advanced retention

Keyword query editor

```
merger
acquisition
takeover
```

^ Actions

When content matches the conditions, perform the following actions.

Retention actions

● Retain the content

For this long... | 5 | years

Do you want us to delete it after this time?

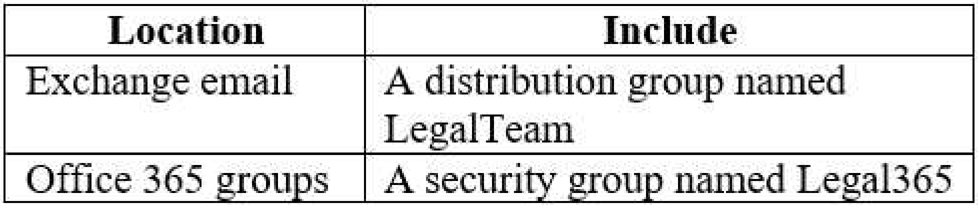
● Yes ○ No

○ Don't retain the content. Just delete it if it's older than

1 years

Retain or delete the content based on: when it was created

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



| Location | Include |
|---|---|
| Exchange email | A distribution group named LegalTeam |
| Office 365 groups | A security group named Legal365 |

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:**

**Correct Answer:**

**Section: [none]**
**Explanation**

**Explanation/Reference:**

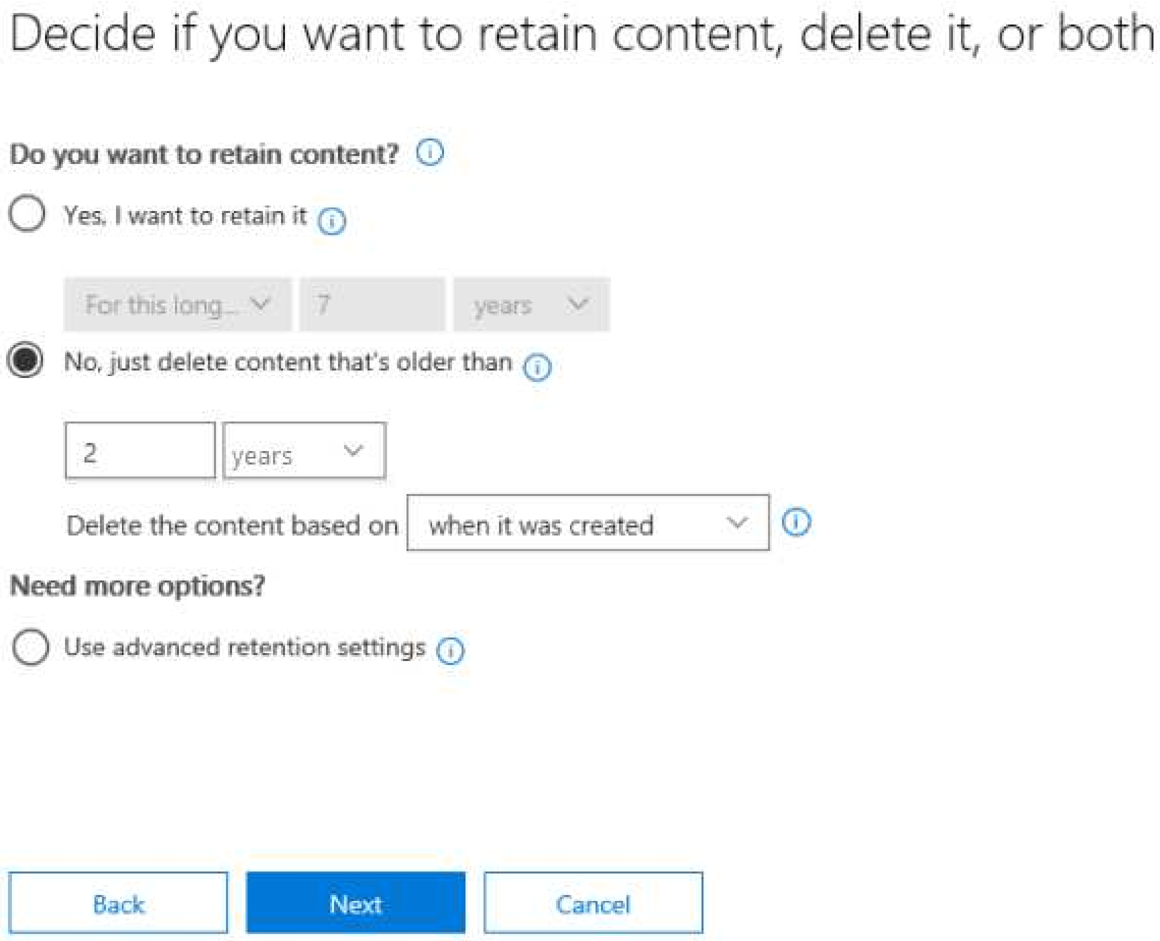
References:
https://docs.microsoft.com/en-us/office365/securitycompliance/retention-policies

**QUESTION 21**
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.)



Decide if you want to retain content, delete it, or both

Do you want to retain content?

○ Yes, I want to retain it

For this long... | 7 | years

● No, just delete content that's older than

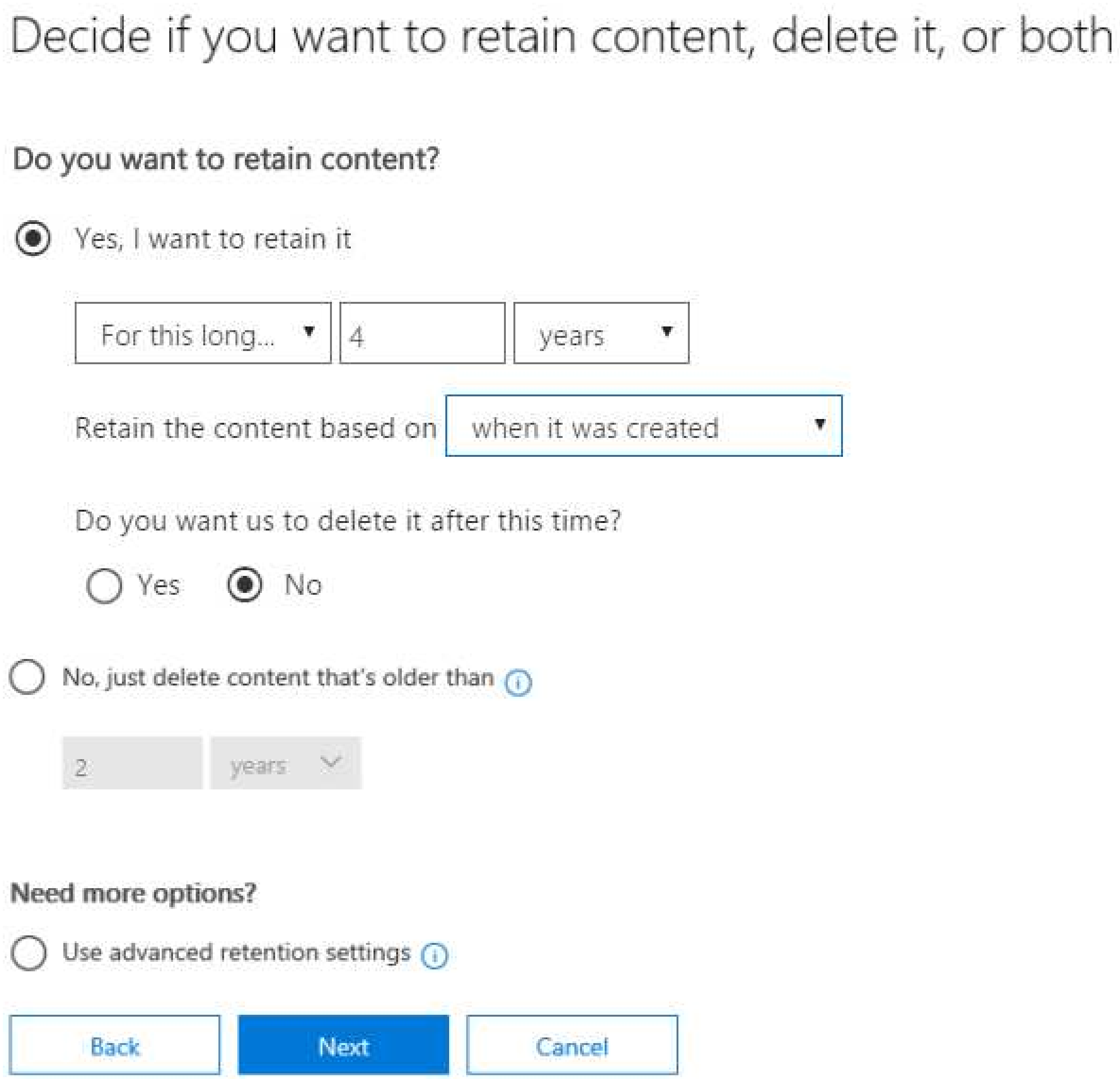
2 | years

Delete the content based on: when it was created

Need more options?

○ Use advanced retention settings

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



Decide if you want to retain content, delete it, or both

Do you want to retain content?

● Yes, I want to retain it

For this long... ▾ 4 years ▾

Retain the content based on when it was created ▾

Do you want us to delete it after this time?

○ Yes ● No

○ No, just delete content that's older than ⓘ

2 years

Need more options?

○ Use advanced retention settings ⓘ

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:**

**Correct Answer:**

**Section: [none]**
**Explanation**

**Explanation/Reference:**
References:
https://docs.microsoft.com/en-us/office365/securitycompliance/retention-policies#the-principles-of-retention-or-what-takes-precedence

**QUESTION 22**
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

**Correct Answer:** D
**Section: [none]**
**Explanation**

**Explanation/Reference:**
References:
https://docs.microsoft.com/en-us/office365/securitycompliance/data-loss-prevention-policies

**QUESTION 23**
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.

**Correct Answer:** A
**Section: [none]**
**Explanation**

**Explanation/Reference:**
References:
https://docs.microsoft.com/en-us/office365/securitycompliance/ediscovery-cases#step-2-create-a-new-case

**QUESTION 24**
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 file 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.
C. From the Security & Compliance Center PowerShell, run the `New-DataClassification` cmdlet.

D. From the Security & Compliance Center PowerShell, run the `New-DlpComplianceRule` cmdlet.

**Correct Answer:** D
**Section: [none]**
**Explanation**

**Explanation/Reference:**
References:
https://docs.microsoft.com/en-us/powershell/module/exchange/policy-and-compliance-dlp/new-dataclassification?view=exchange-ps

**QUESTION 25**
You have a Microsoft 365 subscription.

From the Security & Compliance admin center, you create a content search of all the mailboxes that contain the work 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

**Correct Answer:** B
**Section: [none]**
**Explanation**

**Explanation/Reference:**
References:
https://docs.microsoft.com/en-us/office365/securitycompliance/export-search-results

**QUESTION 26**
HOTSPOT

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

You have three applications named App1, App2, and App3 that have the same file format.

Your company uses Windows Information Protection (WIP). WIP has the following configurations:

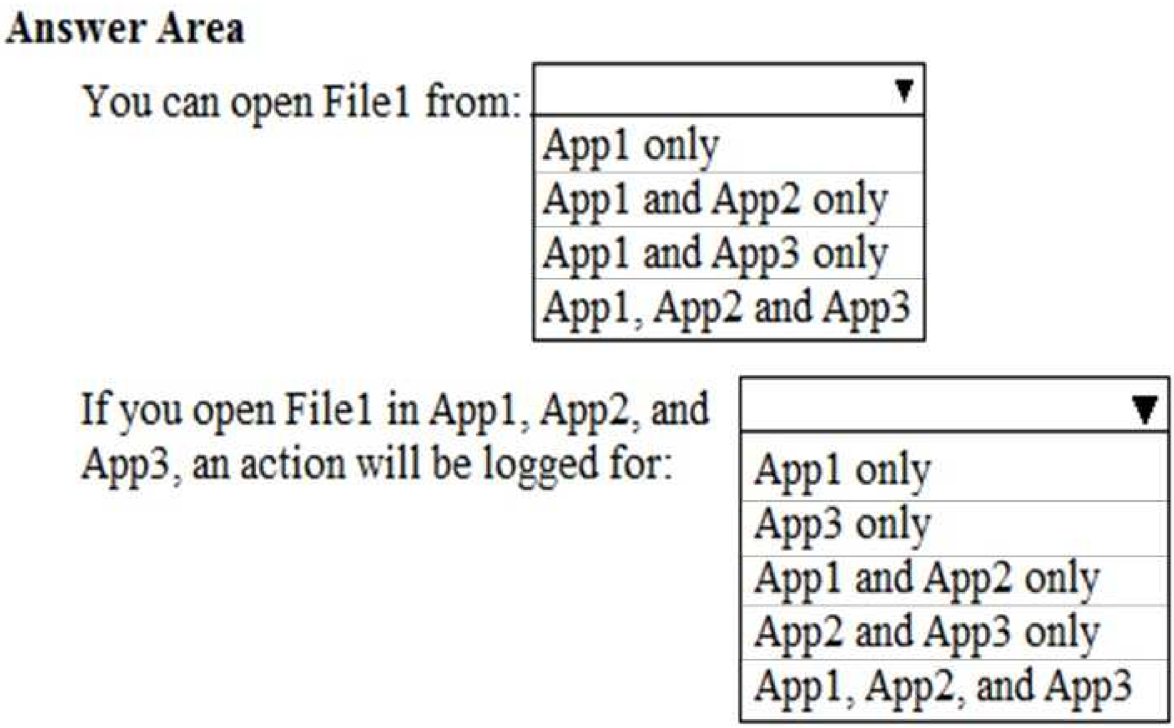
- Windows Information Protection mode: Silent
- Protected apps: App1
- Exempt apps: App2

From App1, you create a file named File1.

What is the effect of the configurations? To answer, select the appropriate options in the answer area.

**NOTE**: Each correct selection is worth one point.

**Hot Area:**



Answer Area

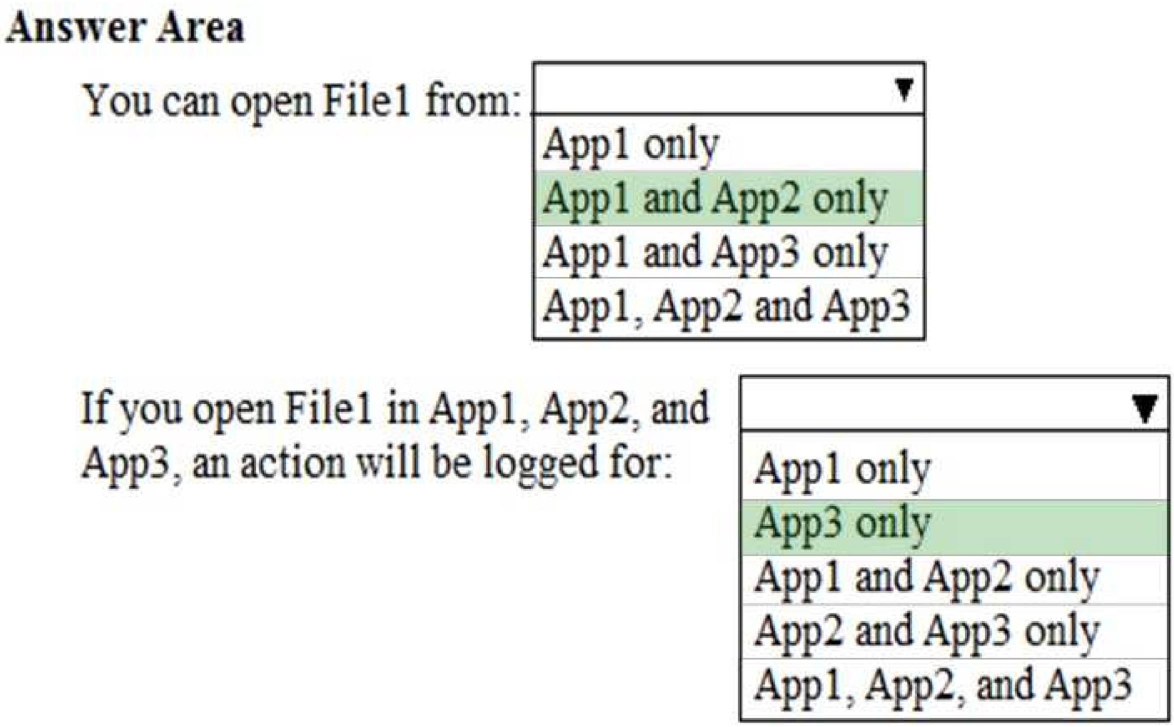
You can open File1 from: ▼

- App1 only
- App1 and App2 only
- App1 and App3 only
- App1, App2 and App3

If you open File1 in App1, App2, and App3, an action will be logged for: ▼

- App1 only
- App3 only
- App1 and App2 only
- App2 and App3 only
- App1, App2, and App3

**Correct Answer:**



Answer Area

You can open File1 from: ▼

- App1 only
- [✓ App1 and App2 only]
- App1 and App3 only
- App1, App2 and App3

If you open File1 in App1, App2, and App3, an action will be logged for: ▼

- App1 only
- [✓ App3 only]
- App1 and App2 only
- App2 and App3 only
- App1, App2, and App3

**Section: [none]**
**Explanation**

**Explanation/Reference:**
References:

https://docs.microsoft.com/en-us/windows/security/information-protection/windows-information-protection/create-wip-policy-using-intune-azure

**QUESTION 27**
HOTSPOT

You have a Microsoft 365 subscription.

You have a group named Support. Users in the Support group frequently send email messages to external users.

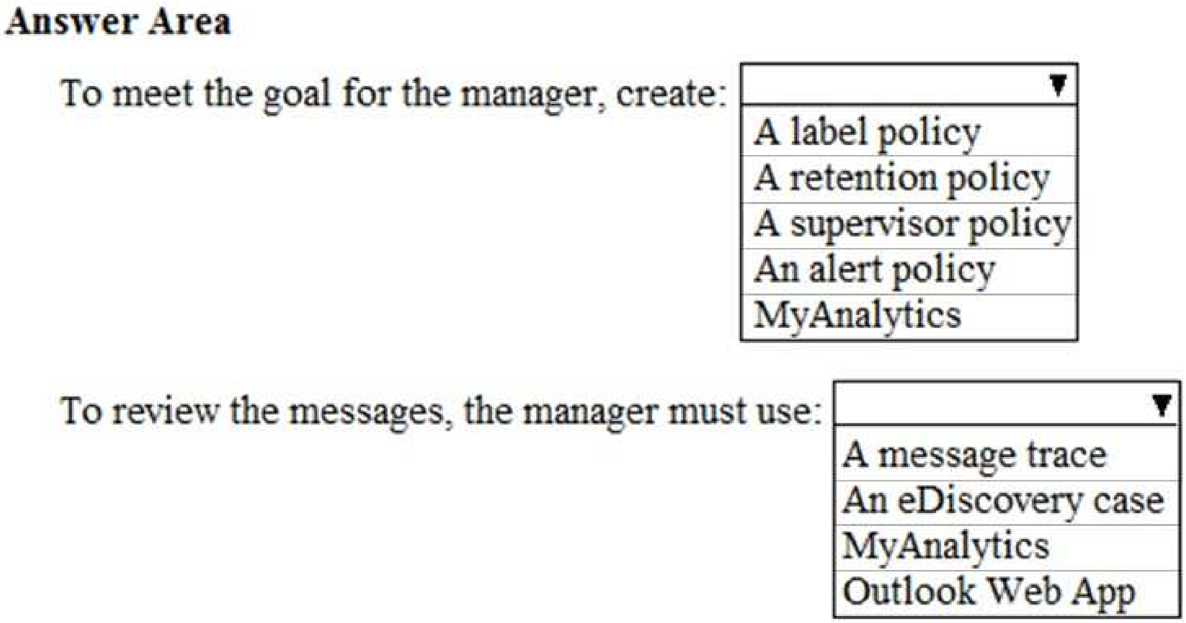
The manager of the Support group wants to randomly review messages that contain attachments.

You need to provide the manager with the ability to review messages that contain attachments sent from the Support group users to external users. The manager must have access to only 10 percent of the messages.

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**

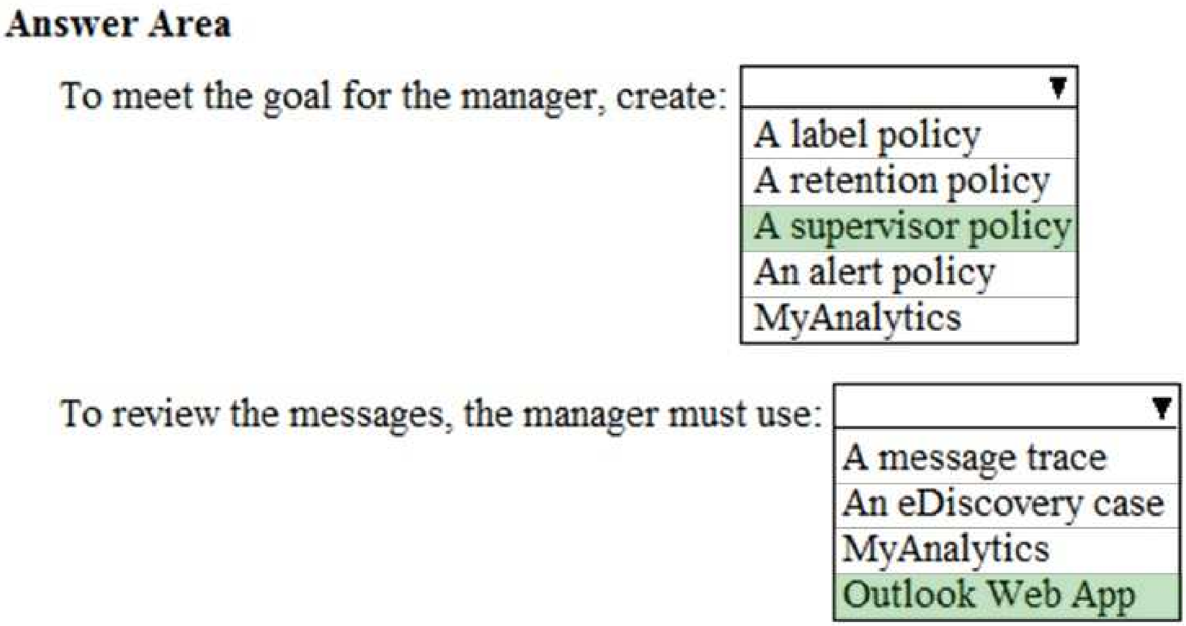
To meet the goal for the manager, create: ▼

- A label policy
- A retention policy
- A supervisor policy
- An alert policy
- MyAnalytics

To review the messages, the manager must use: ▼

- A message trace
- An eDiscovery case
- MyAnalytics
- Outlook Web App

**Correct Answer:**



Answer Area

To meet the goal for the manager, create:

- A label policy
- A retention policy
- [✓ A supervisor policy]
- An alert policy
- MyAnalytics

To review the messages, the manager must use:

- A message trace
- An eDiscovery case
- MyAnalytics
- [✓ Outlook Web App]

**Section: [none]**
**Explanation**

**Explanation/Reference:**
References:
https://docs.microsoft.com/en-us/office365/securitycompliance/supervision-policies

**QUESTION 28**
Your company has a Microsoft 365 subscription.

You implement Microsoft Azure Information Protection.

You need to automatically protect email messages that contain the word Confidential in the subject line.

What should you create?

A. a mail flow rule from the Exchange admin center
B. a message trace from the Security & Compliance admin center
C. a supervision policy from the Security & Compliance admin center
D. a sharing policy from the Exchange admin center

**Correct Answer:** A
**Section: [none]**
**Explanation**

**Explanation/Reference:**
References:
https://docs.microsoft.com/en-us/azure/information-protection/configure-exo-rules

**QUESTION 29**
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

**Correct Answer:** B
**Section: [none]**
**Explanation**

**Explanation/Reference:**
References:
https://docs.microsoft.com/en-us/office365/securitycompliance/search-the-audit-log-in-security-and-compliance

**QUESTION 30**
You are testing a data loss prevention (DLP) policy to protect the sharing of credit card information with external users.

During testing, you discover that a user can share credit card information with external users by using email. However, the user is prevented from sharing files that contain credit card information by using Microsoft SharePoint Online.

You need to prevent the user from sharing the credit card information by using email and SharePoint.

What should you configure?

A. the locations of the DLP policy
B. the user overrides of the DLP policy rule
C. the status of the DLP policy
D. the conditions of the DLP policy rule

**Correct Answer:** A
**Section: [none]**
**Explanation**

**Explanation/Reference:**
References:
https://docs.microsoft.com/en-us/office365/securitycompliance/data-loss-prevention-policies

**QUESTION 31**
You have a Microsoft 365 subscription.

You need to view the IP address from which a user synced a Microsoft SharePoint library.

What should you do?

A. From the SharePoint Online admin center, view the usage reports.
B. From the Security & Compliance admin center, perform an audit log search.
C. From the Microsoft 365 admin center, view the usage reports.
D. From the Microsoft 365 admin center, view the properties of the user's user account.

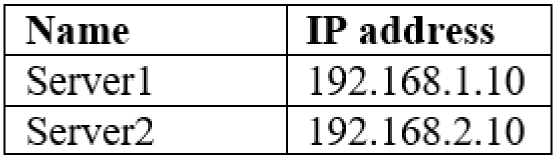
**Correct Answer:** B
**Section: [none]**
**Explanation**

**Explanation/Reference:**

References:
https://docs.microsoft.com/en-us/office365/securitycompliance/search-the-audit-log-in-security-and-compliance

**QUESTION 32**
HOTSPOT

Your network contains an Active Directory domain named contoso.com. The domain contains the file servers shown in the following table.



| Name | IP address |
|---|---|
| Server1 | 192.168.1.10 |
| Server2 | 192.168.2.10 |

A file named File1.abc is stored on Server1. A file named File2.abc is stored on Server2. Three apps named App1, App2, and App3 all open files that have the .abc file extension.

You implement Windows Information Protection (WIP) by using the following configurations:

- Exempt apps: App2
- Protected apps: App1
- Windows Information Protection mode: Block
- Network boundary: IPv4 range of: 192.168.1.1-192.168.1.255

You need to identify the apps from which you can open File1.abc.

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:**

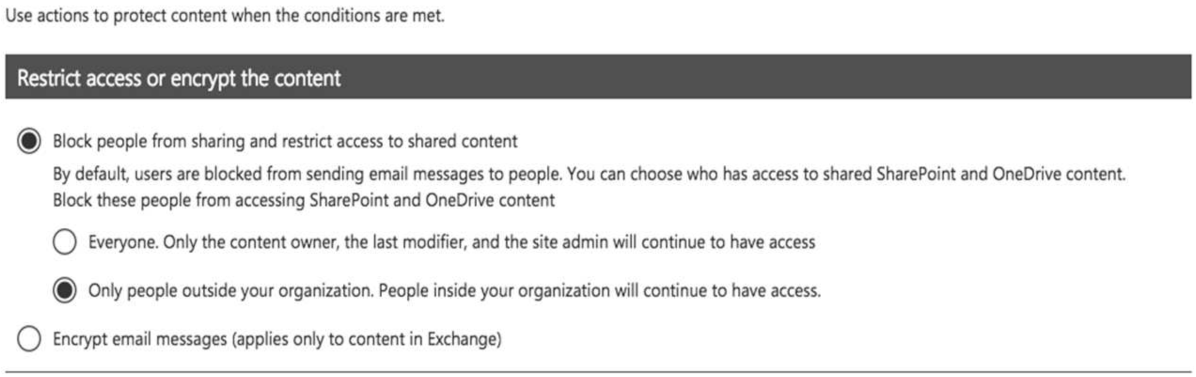
**Correct Answer:**

**Section: [none]**
**Explanation**

**Explanation/Reference:**
References:
https://docs.microsoft.com/en-us/windows/security/information-protection/windows-information-protection/create-wip-policy-using-intune-azure

**QUESTION 33**
In Microsoft 365, you configure a data loss prevention (DLP) policy named Policy1. Policy1 detects the sharing of United States (US) bank account numbers in email messages and attachments.

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



Use actions to protect content when the conditions are met.

Restrict access or encrypt the content

● Block people from sharing and restrict access to shared content

By default, users are blocked from sending email messages to people. You can choose who has access to shared SharePoint and OneDrive content.
Block these people from accessing SharePoint and OneDrive content

○ Everyone. Only the content owner, the last modifier, and the site admin will continue to have access

● Only people outside your organization. People inside your organization will continue to have access.

○ Encrypt email messages (applies only to content in Exchange)

You need to ensure that internal users can email documents that contain US bank account numbers to external users who have an email suffix of contoso.com.

What should you configure?

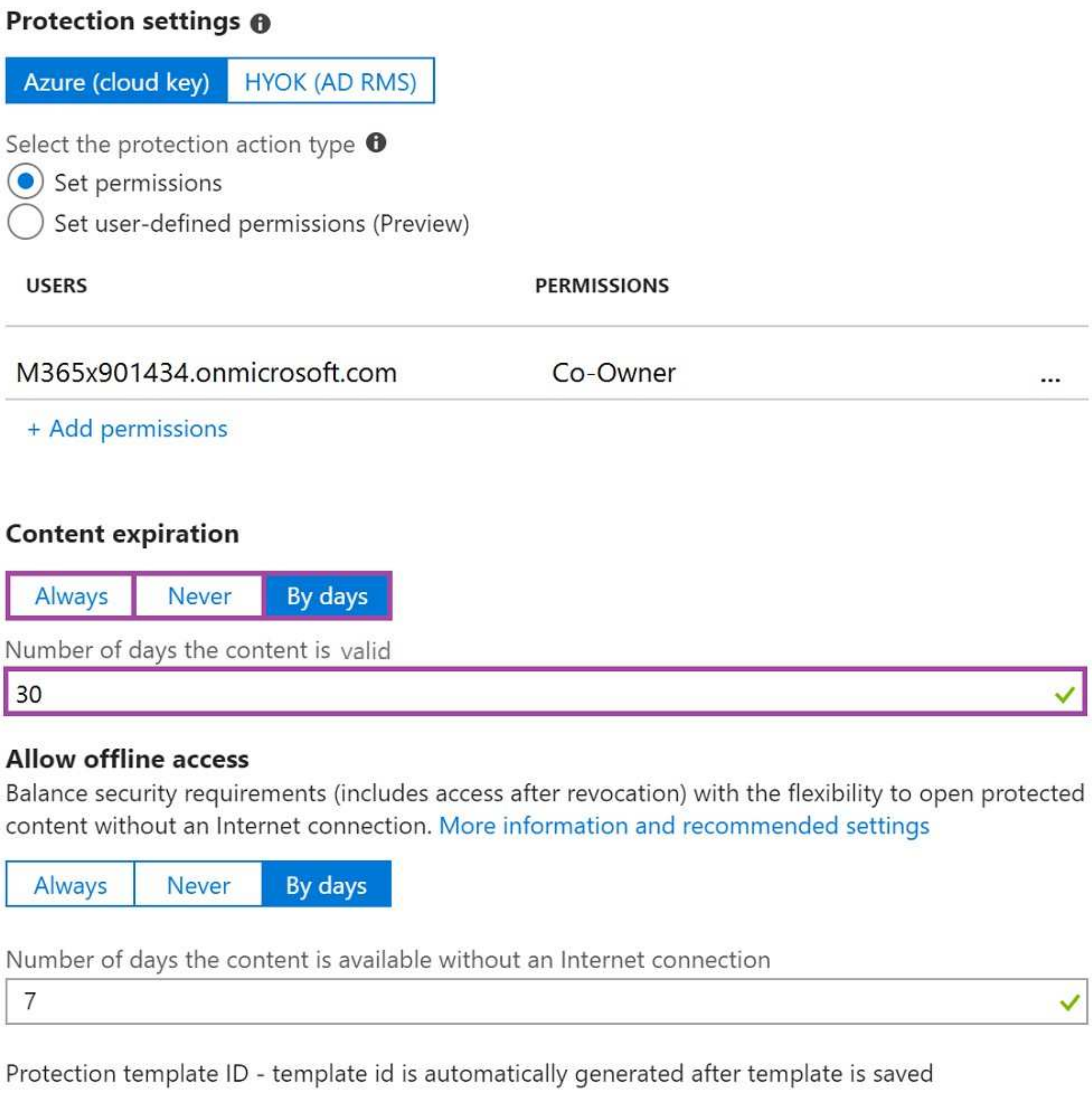
A. an exception
B. an action
C. a condition
D. a group

**Correct Answer:** B
**Section: [none]**
**Explanation**

**Explanation/Reference:**
References:
https://docs.microsoft.com/en-us/office365/securitycompliance/data-loss-prevention-policies#how-dlp-policies-work

**QUESTION 34**
HOTSPOT

You have a document in Microsoft OneDrive that is encrypted by using Microsoft Azure Information Protection as shown in the following exhibit.



**Protection settings**

Azure (cloud key) | HYOK (AD RMS)

Select the protection action type

● Set permissions

○ Set user-defined permissions (Preview)

| USERS | PERMISSIONS |
|---|---|
| M365x901434.onmicrosoft.com | Co-Owner |

+ Add permissions

**Content expiration**

Always | Never | By days

Number of days the content is valid

30 ✓

**Allow offline access**

Balance security requirements (includes access after revocation) with the flexibility to open protected content without an Internet connection. More information and recommended settings

Always | Never | By days

Number of days the content is available without an Internet connection

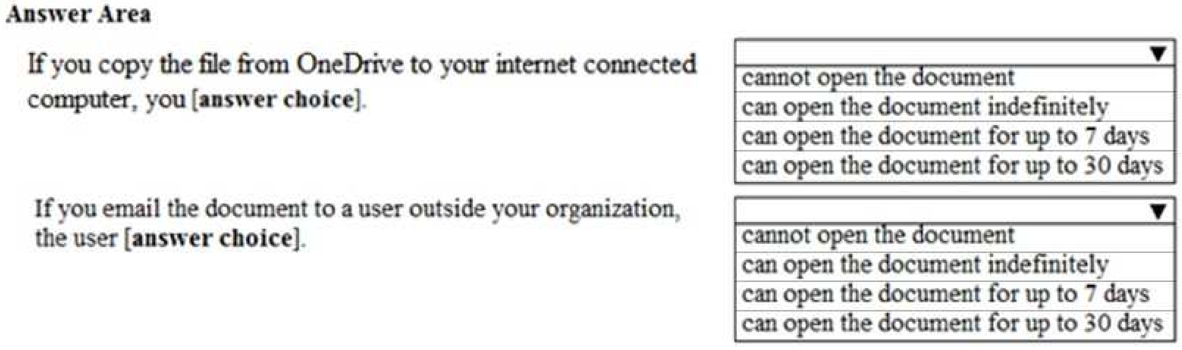
7 ✓

Protection template ID - template id is automatically generated after template is saved

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.

**Hot Area:**



**Answer Area**

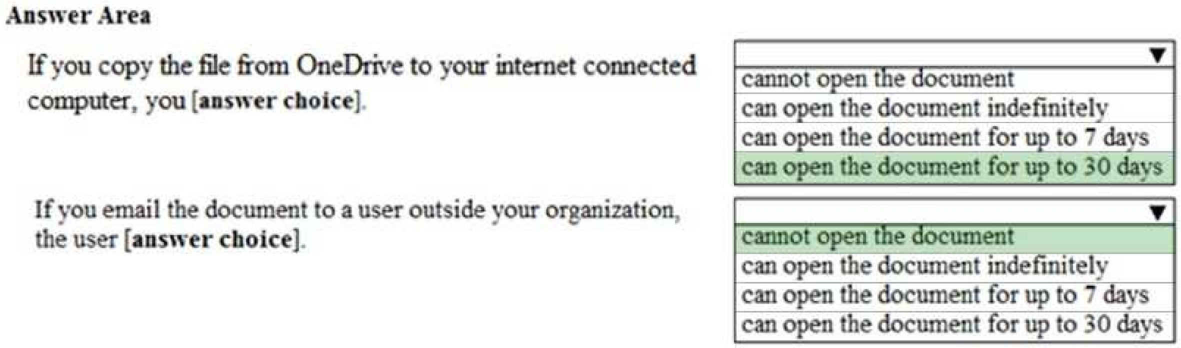
If you copy the file from OneDrive to your internet connected computer, you **[answer choice]**.

- cannot open the document
- can open the document indefinitely
- can open the document for up to 7 days
- can open the document for up to 30 days

If you email the document to a user outside your organization, the user **[answer choice]**.

- cannot open the document
- can open the document indefinitely
- can open the document for up to 7 days
- can open the document for up to 30 days

**Correct Answer:**



Answer Area

If you copy the file from OneDrive to your internet connected computer, you [answer choice].

- cannot open the document
- can open the document indefinitely
- can open the document for up to 7 days
- [✓ can open the document for up to 30 days]

If you email the document to a user outside your organization, the user [answer choice].

- [✓ cannot open the document]
- can open the document indefinitely
- can open the document for up to 7 days
- can open the document for up to 30 days

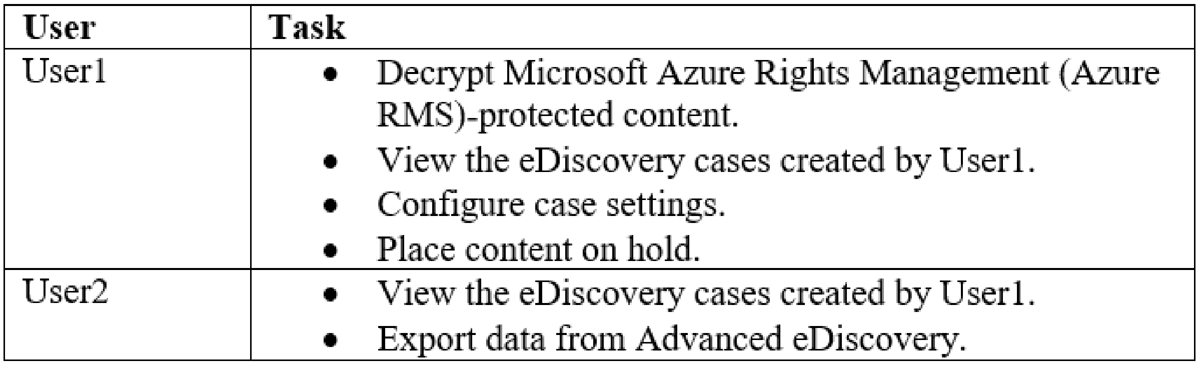
**Section: [none]**
**Explanation**

**Explanation/Reference:**
References:
https://docs.microsoft.com/en-us/azure/information-protection/configure-policy-protection

**QUESTION 35**
HOTSPOT

You have a Microsoft Office 365 subscription.

You need to delegate eDiscovery tasks as shown in the following table.



| User | Task |
|---|---|
| User1 | • Decrypt Microsoft Azure Rights Management (Azure RMS)-protected content.<br>• View the eDiscovery cases created by User1.<br>• Configure case settings.<br>• Place content on hold. |
| User2 | • View the eDiscovery cases created by User1.<br>• Export data from Advanced eDiscovery. |

The solution must follow the principle of the least privilege.

To which role group should you assign each user? To answer, select the appropriate options in the answer area.

**NOTE**: Each correct selection is worth one point.

**Hot Area:**

**Correct Answer:**

**Section: [none]**
**Explanation**

**Explanation/Reference:**
References:
https://docs.microsoft.com/en-us/office365/securitycompliance/assign-ediscovery-permissions

**QUESTION 36**

**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.

From the Security & Compliance admin center, you create a role group named US eDiscovery Managers by copying the eDiscovery Manager role group.

You need to ensure that the users in the new role group can only perform content searches of mailbox content for users in the United States.

Solution: From Windows PowerShell, you run the `New-ComplianceSecurityFilter` cmdlet with the appropriate parameters.

Does this meet the goal?

A. Yes
B. No

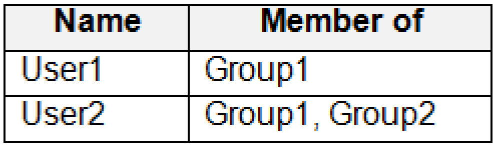
**Correct Answer:** A
**Section: [none]**
**Explanation**

**Explanation/Reference:**
References:
https://docs.microsoft.com/en-us/office365/securitycompliance/permissions-filtering-for-content-search

https://docs.microsoft.com/en-us/powershell/module/exchange/policy-and-compliance-content-search/new-compliancesecurityfilter?view=exchange-ps

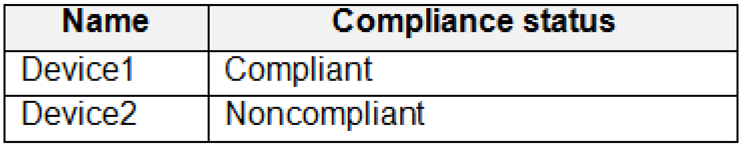
**QUESTION 37**
HOTSPOT

You have a Microsoft 365 subscription that uses a default domain named contoso.com. The domain contains the users shown in the following table.



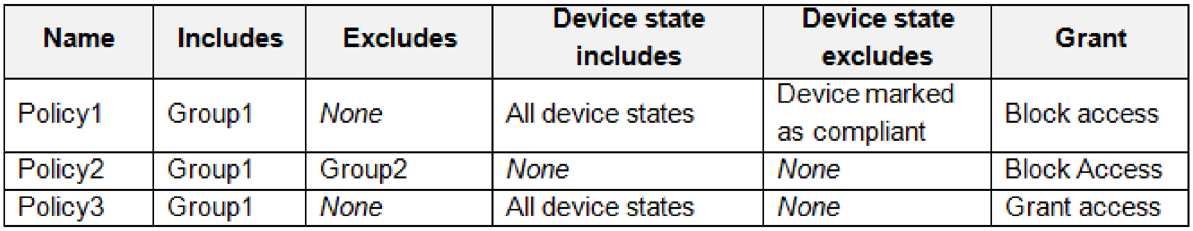
| Name | Member of |
|---|---|
| User1 | Group1 |
| User2 | Group1, Group2 |

The domain contains the devices shown in the following table.



| Name | Compliance status |
|---|---|
| Device1 | Compliant |
| Device2 | Noncompliant |

The domain contains conditional access policies that control access to a cloud app named App1. The policies are configured as shown in the following table.

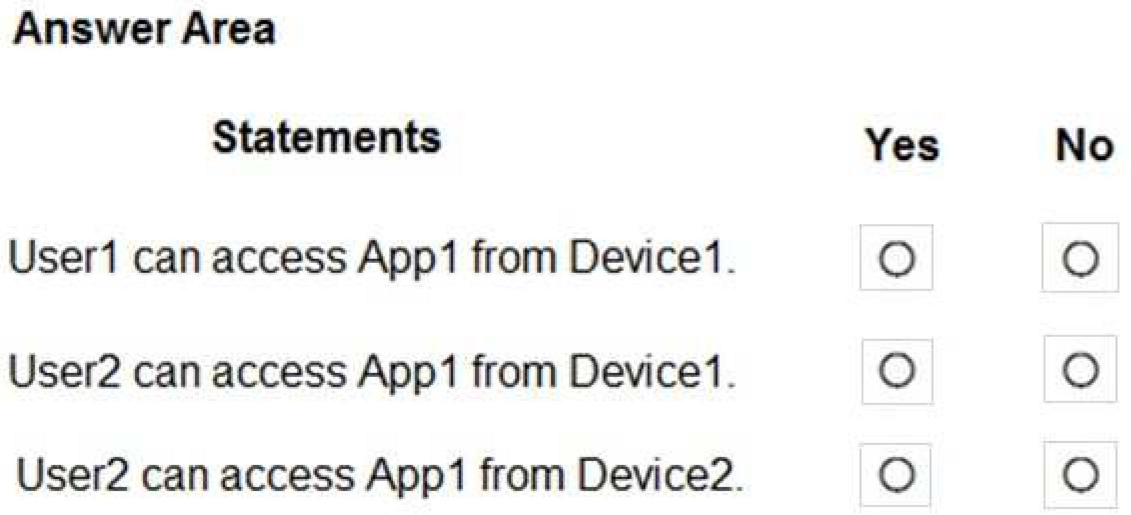


| Name | Includes | Excludes | Device state includes | Device state excludes | Grant |
|---|---|---|---|---|---|
| Policy1 | Group1 | *None* | All device states | Device marked as compliant | Block access |
| Policy2 | Group1 | Group2 | *None* | *None* | Block Access |
| Policy3 | Group1 | *None* | All device states | *None* | Grant access |

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

**NOTE:** Each correct selection is worth one point.

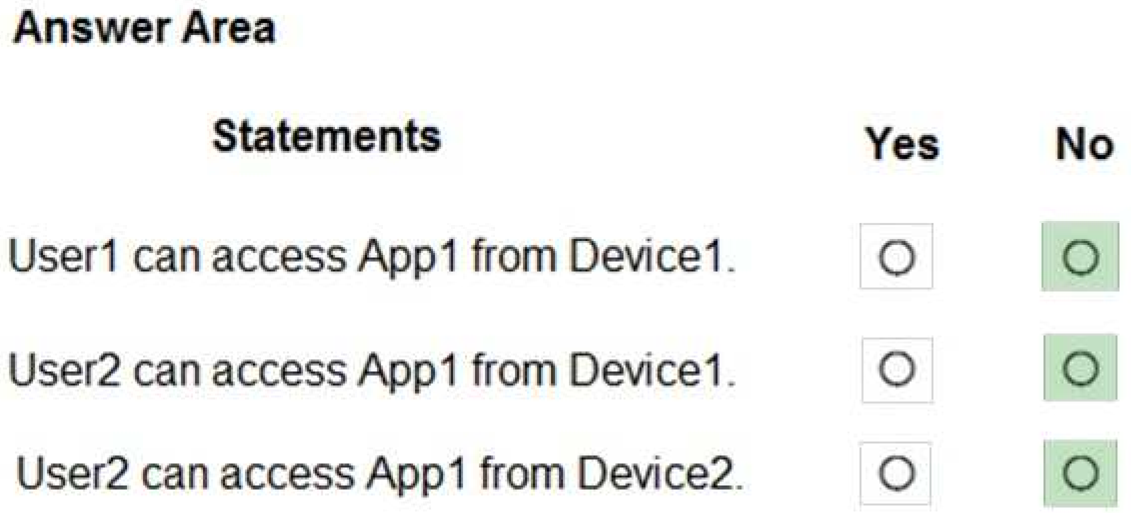
**Hot Area:**



**Answer Area**

| Statements | Yes | No |
|---|---|---|
| User1 can access App1 from Device1. | ○ | ○ |
| User2 can access App1 from Device1. | ○ | ○ |
| User2 can access App1 from Device2. | ○ | ○ |

**Correct Answer:**



**Answer Area**

| Statements | Yes | No |
|---|---|---|
| User1 can access App1 from Device1. | ○ | [✓ ○] |
| User2 can access App1 from Device1. | ○ | [✓ ○] |
| User2 can access App1 from Device2. | ○ | [✓ ○] |

**Section: [none]**
**Explanation**

**Explanation/Reference:**

Explanation:

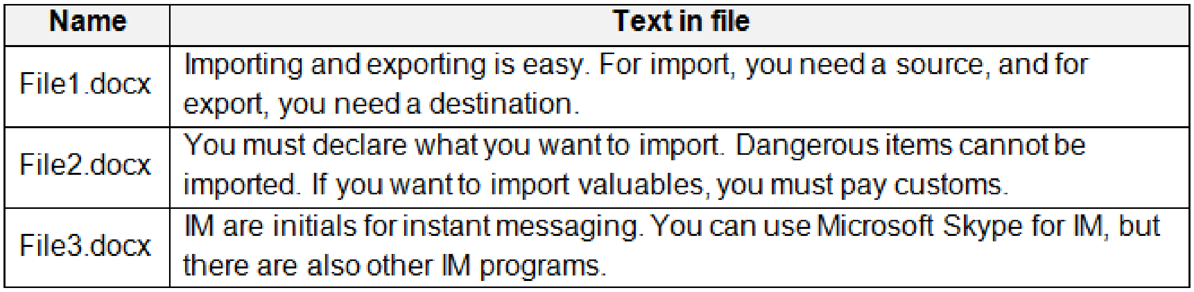
Note: Block access overrides Grant access

References:
https://docs.microsoft.com/en-us/azure/active-directory/conditional-access/plan-conditional-access

**QUESTION 38**
HOTSPOT

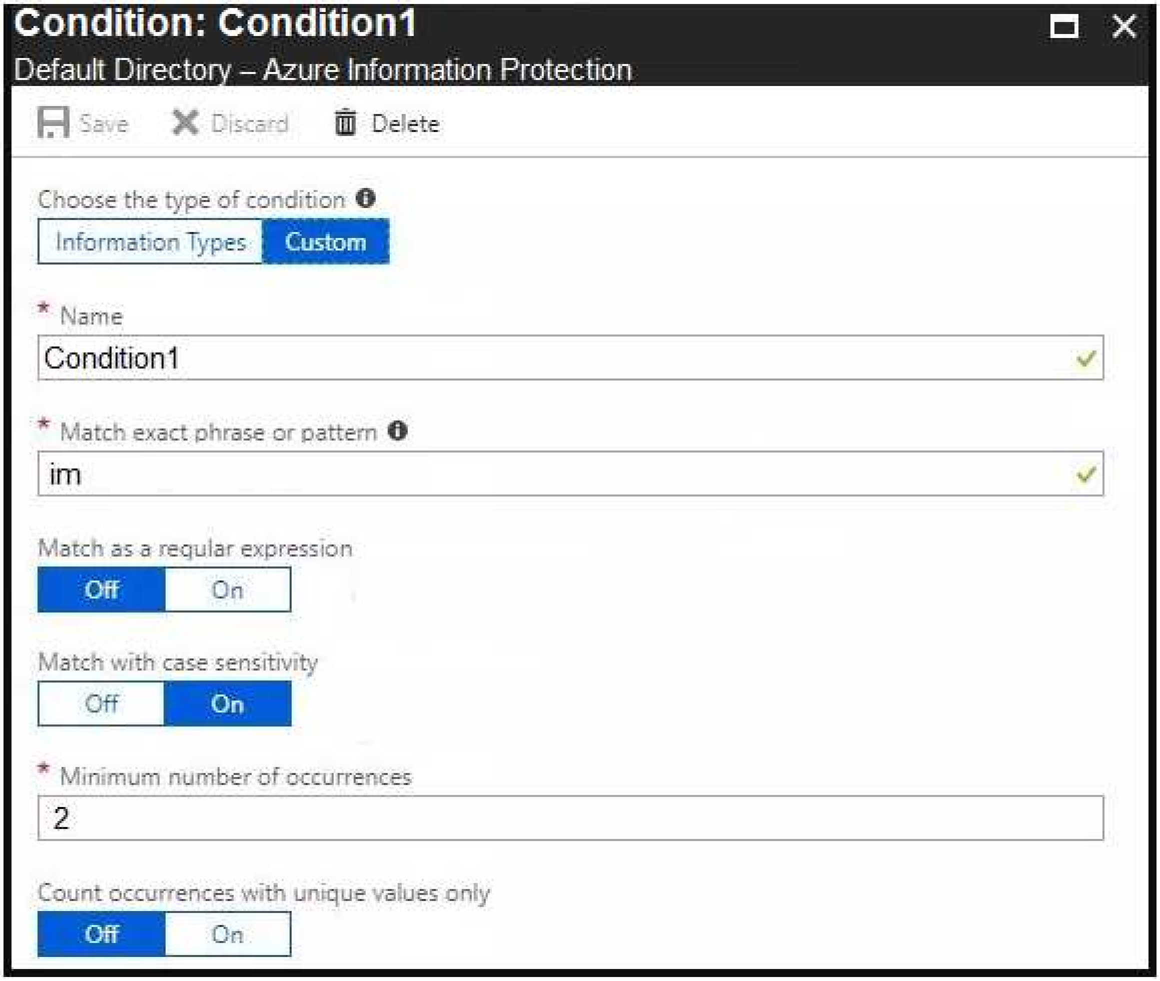
You have a Microsoft Azure Active Directory (Azure AD) tenant named contoso.com.

A user named User1 has files on a Windows 10 device as shown in the following table.



| Name | Text in file |
|---|---|
| File1.docx | Importing and exporting is easy. For import, you need a source, and for export, you need a destination. |
| File2.docx | You must declare what you want to import. Dangerous items cannot be imported. If you want to import valuables, you must pay customs. |
| File3.docx | IM are initials for instant messaging. You can use Microsoft Skype for IM, but there are also other IM programs. |

In Azure Information Protection, you create a label named Label1 that is configured to apply automatically. Label1 is configured as shown in the following exhibit.



Condition: Condition1

Default Directory – Azure Information Protection

Choose the type of condition: Information Types | **Custom**

* Name: Condition1

* Match exact phrase or pattern: im

Match as a regular expression: **Off** | On

Match with case sensitivity: Off | **On**

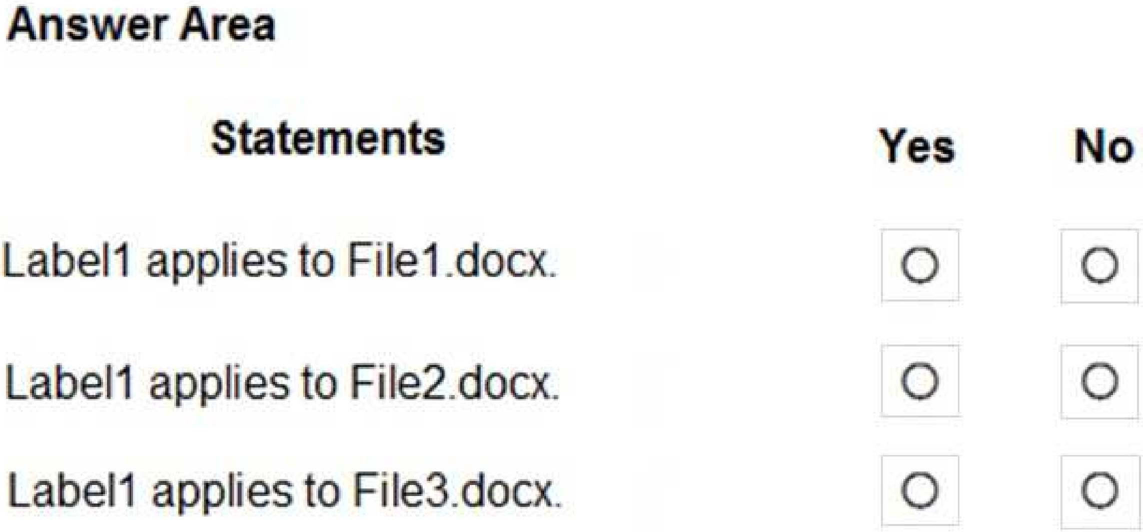
* Minimum number of occurrences: 2

Count occurrences with unique values only: **Off** | On

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

**NOTE:** Each correct selection is worth one point.

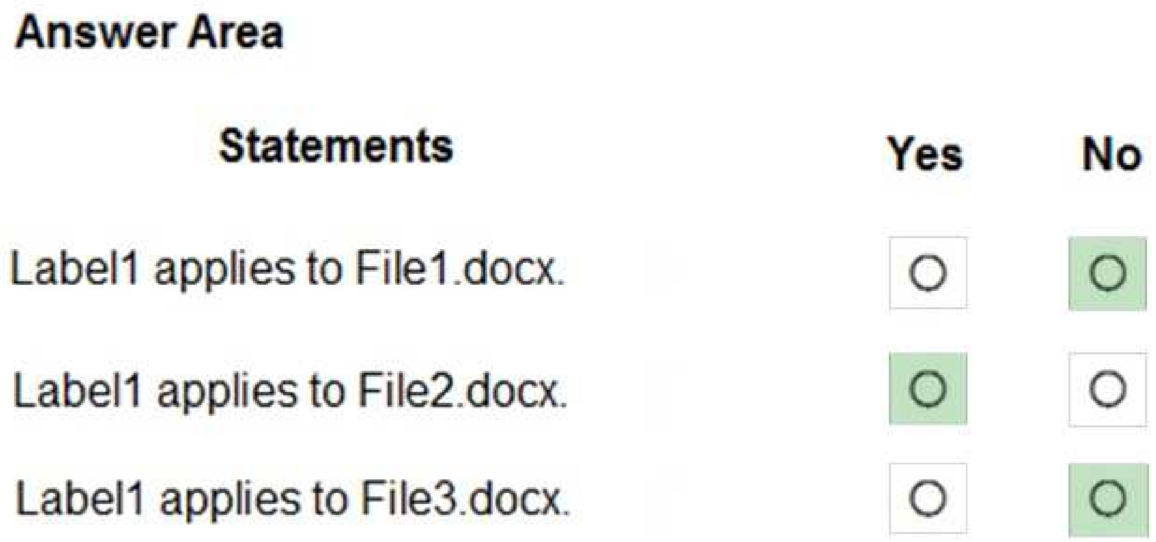
**Hot Area:**



Answer Area

| Statements | Yes | No |
|---|---|---|
| Label1 applies to File1.docx. | ○ | ○ |
| Label1 applies to File2.docx. | ○ | ○ |
| Label1 applies to File3.docx. | ○ | ○ |

**Correct Answer:**



Answer Area

| Statements | Yes | No |
|---|---|---|
| Label1 applies to File1.docx. | ○ | [✓ ○] |
| Label1 applies to File2.docx. | [✓ ○] | ○ |
| Label1 applies to File3.docx. | ○ | [✓ ○] |

**Section: [none]**
**Explanation**

**Explanation/Reference:**
Explanation:

The phrase to match is "im" and it is case sensitive. The phrase must also appear at least twice.

Box 1: No
File1.docx contain the word "import" once only

Box 2: Yes
File2.docx contains two occurrences of the word "import" as well as the word "imported"

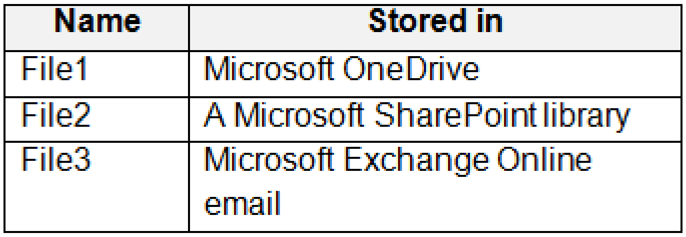
Box 3: No
File3.docx contains "IM" but his is not the correct letter case.

References:
https://docs.microsoft.com/en-us/azure/information-protection/configure-policy-classification

**QUESTION 39**
HOTSPOT

You have a Microsoft 365 subscription that uses a default domain named contoso.com.

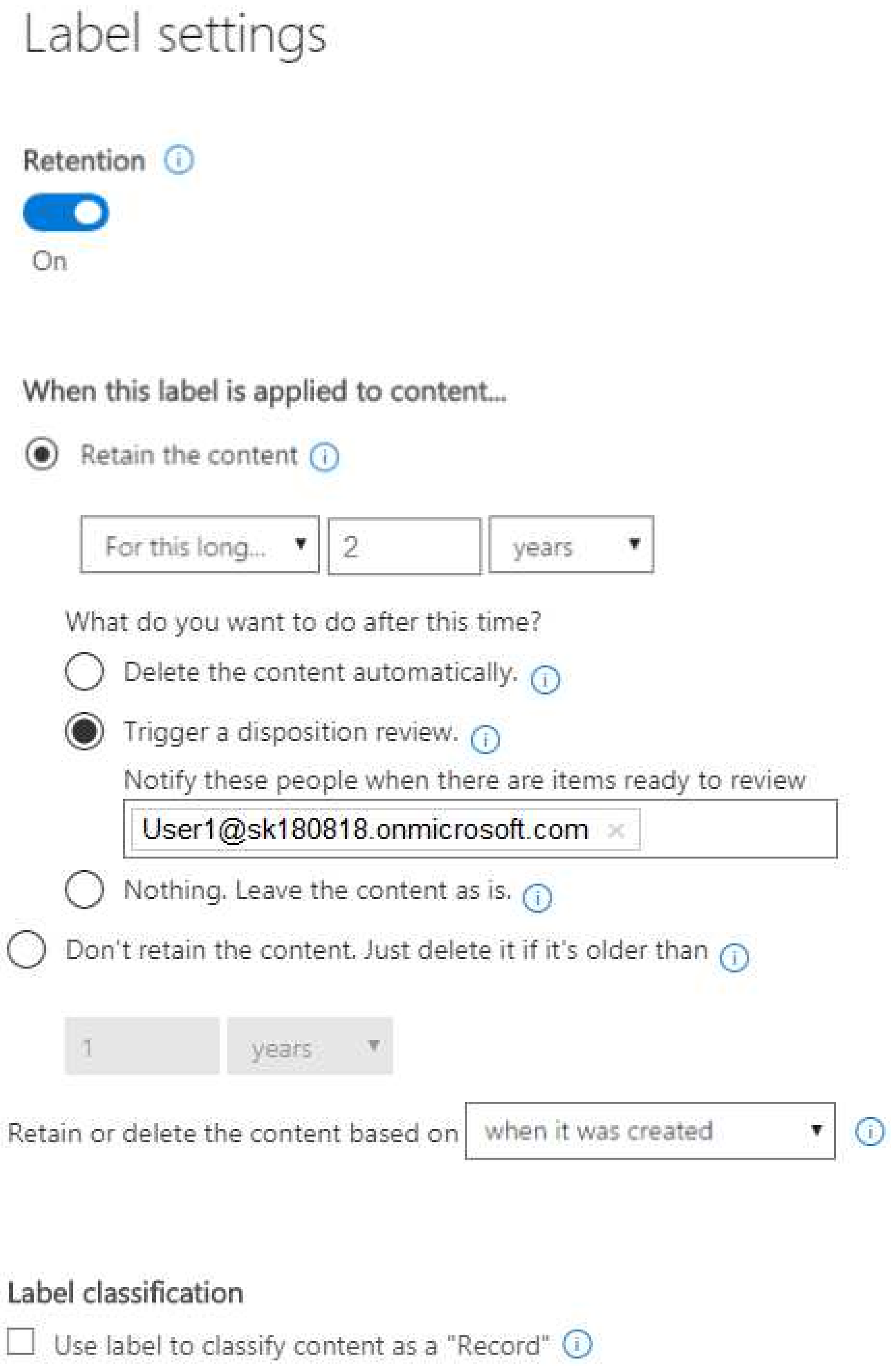
Three files were created on February 1, 2019, as shown in the following table.



| Name | Stored in |
|---|---|
| File1 | Microsoft OneDrive |
| File2 | A Microsoft SharePoint library |
| File3 | Microsoft Exchange Online email |

On March 1, 2019, you create two retention labels named Label1 and Label2.

The settings for Lable1 are configured as shown in the Label1 exhibit. (Click the **Label1** tab.)



Label settings

Retention ⓘ

On

When this label is applied to content...

● Retain the content ⓘ

For this long... ▾ | 2 | years ▾

What do you want to do after this time?

○ Delete the content automatically. ⓘ

● Trigger a disposition review. ⓘ

Notify these people when there are items ready to review

User1@sk180818.onmicrosoft.com ×

○ Nothing. Leave the content as is. ⓘ

○ Don't retain the content. Just delete it if it's older than ⓘ

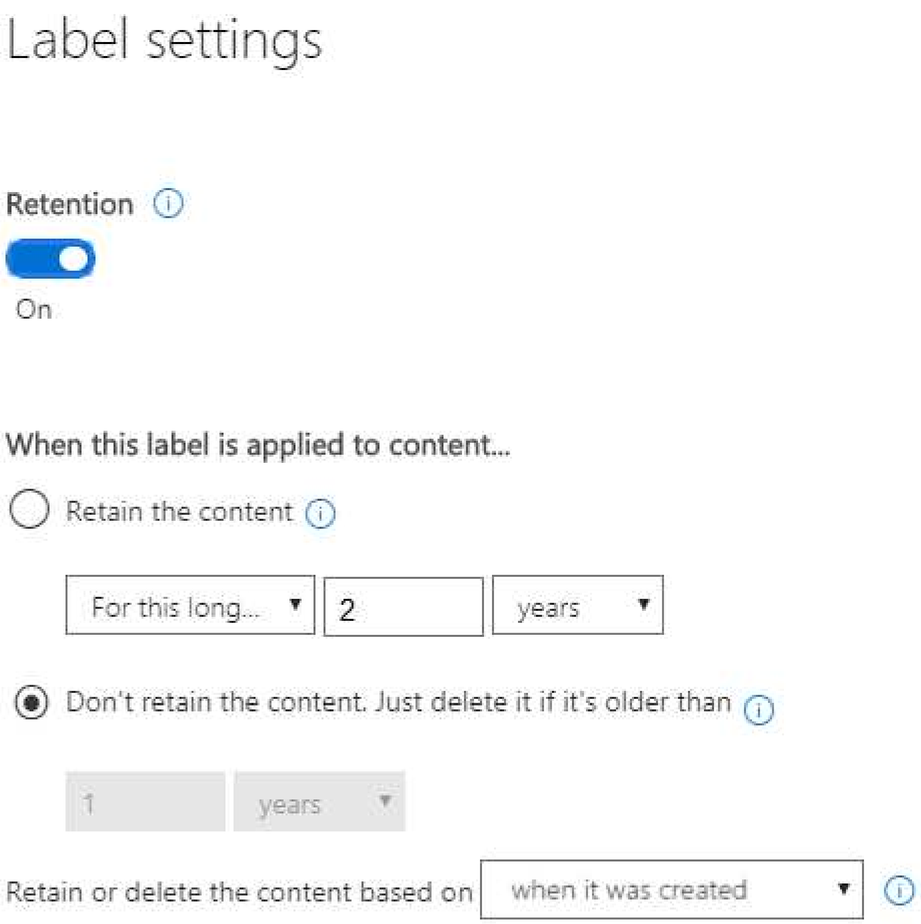
1 | years ▾

Retain or delete the content based on | when it was created ▾ ⓘ

Label classification

□ Use label to classify content as a "Record" ⓘ

The settings for Lable2 are configured as shown in the Label2 exhibit. (Click the **Label2** tab.)



Label settings

Retention

On

When this label is applied to content...

○ Retain the content

For this long... ▼ | 2 | years ▼

● Don't retain the content. Just delete it if it's older than

1 | years ▼

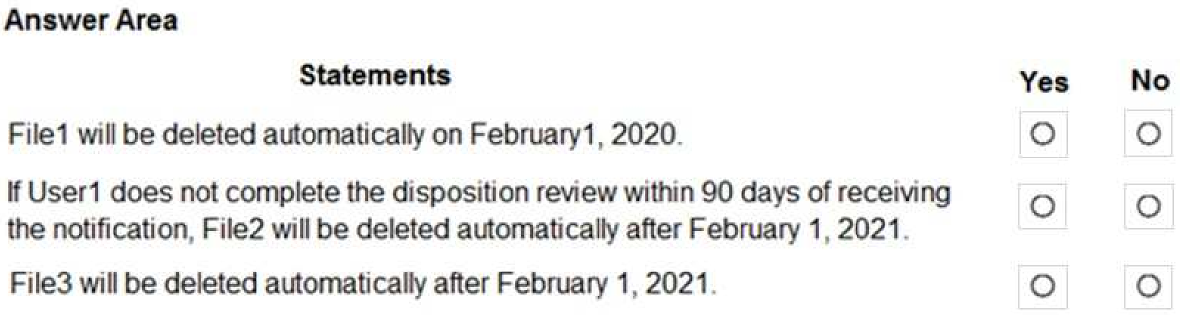
Retain or delete the content based on | when it was created ▼

You apply the retention labels to Exchange email, SharePoint sites, and OneDrive accounts.

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

**NOTE:** Each correct selection is worth one point.

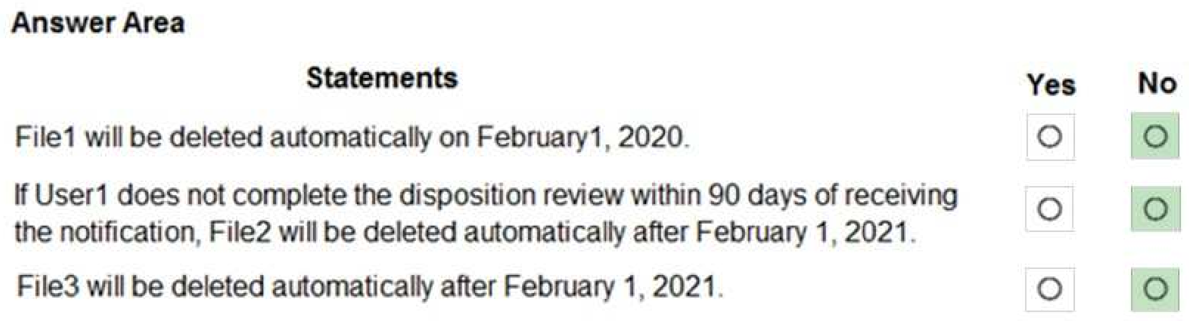
**Hot Area:**



**Answer Area**

| Statements | Yes | No |
|---|---|---|
| File1 will be deleted automatically on February1, 2020. | ○ | ○ |
| If User1 does not complete the disposition review within 90 days of receiving the notification, File2 will be deleted automatically after February 1, 2021. | ○ | ○ |
| File3 will be deleted automatically after February 1, 2021. | ○ | ○ |

**Correct Answer:**



**Answer Area**

| Statements | Yes | No |
|---|---|---|
| File1 will be deleted automatically on February1, 2020. | ○ | [✓ ○] |
| If User1 does not complete the disposition review within 90 days of receiving the notification, File2 will be deleted automatically after February 1, 2021. | ○ | [✓ ○] |
| File3 will be deleted automatically after February 1, 2021. | ○ | [✓ ○] |

**Section: [none]**
**Explanation**

**Explanation/Reference:**
Explanation:

Box 1: No
Retention overrides deletion.

Box 2: No
Content in a document library will be moved to the first-stage Recycle Bin within 7 days of disposition, and then permanently deleted another 93 days after that. Thus 100 days in total.

Box 3: No
Items in an Exchange mailbox will be permanently deleted within 14 days of disposition.

References:
https://docs.microsoft.com/en-us/office365/securitycompliance/labels

https://docs.microsoft.com/en-us/office365/securitycompliance/disposition-reviews

**QUESTION 40**
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 `Add-AadrmRoleBasedAdministrator` cmdlet.
B. Create an Azure Information Protection policy.
C. Configure the protection activation status for Azure Information Protection.
D. Run the `Set-AadrmOnboardingControlPolicy` cmdlet.

**Correct Answer:** D
**Section: [none]**
**Explanation**

**Explanation/Reference:**
Explanation:
If you don’t want all users to be able to protect documents and emails immediately by using Azure Rights Management, you can configure user onboarding controls by using the Set-AadrmOnboardingControlPolicy

References:

https://docs.microsoft.com/en-us/azure/information-protection/activate-service

**QUESTION 41**
**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.

From the Security & Compliance admin center, you create a role group named US eDiscovery Managers by copying the eDiscovery Manager role group.

You need to ensure that the users in the new role group can only perform content searches of mailbox content for users in the United States.

Solution: From Windows PowerShell, you run the `New-AzureRmRoleAssignment` cmdlet with the appropriate parameters.

Does this meet the goal?

A. Yes
B. No

**Correct Answer:** B
**Section: [none]**
**Explanation**

**Explanation/Reference:**
References:
https://docs.microsoft.com/en-us/powershell/module/azurerm.resources/new-azurermroleassignment?view=azurermps-6.13.0

**QUESTION 42**
**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.

From the Security & Compliance admin center, you create a role group named US eDiscovery Managers by copying the eDiscovery Manager role group.

You need to ensure that the users in the new role group can only perform content searches of mailbox content for users in the United States.

Solution: From the Security & Compliance admin center, you modify the roles of the US eDiscovery Managers role group.

Does this meet the goal?

A. Yes
B. No

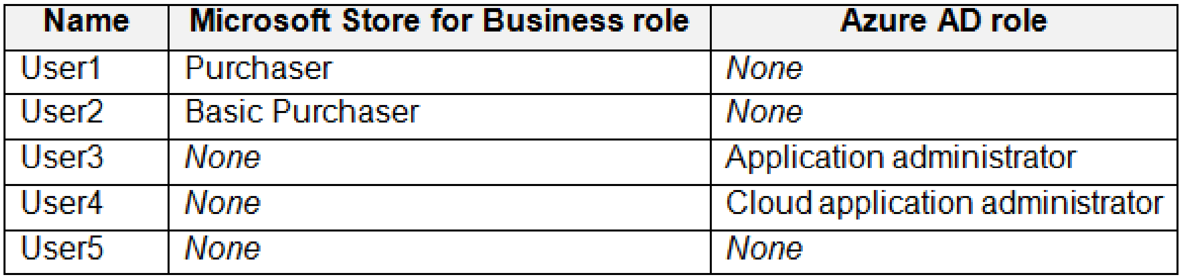
**Correct Answer:** B
**Section: [none]**
**Explanation**

**Explanation/Reference:**

**QUESTION 43**
Your company has a Microsoft Azure Active Directory (Azure AD) tenant named contoso.com.

You sign 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 |
| User5 | *None* | *None* |

Microsoft Store for Business has the following Shopping behavior settings:

- **Allow users to shop** is set to **On**
- **Make everyone a Basic Purchaser** is set to **Off**

You need to identify which users can install apps from the Microsoft for Business private store.

Which users should you identify?

A. User1, User2, User3, User4, and User5
B. User1 only
C. User1 and User2 only
D. User3 and User4 only
E. User1, User2, User3, and User4 only

**Correct Answer:** C
**Section: [none]**
**Explanation**

**Explanation/Reference:**
Explanation:
Allow users to shop controls the shopping experience in Microsoft Store for Education. When this setting is on, Purchasers and Basic Purchasers can purchase products and services from Microsoft Store for Education.

References:
https://docs.microsoft.com/en-us/microsoft-store/acquire-apps-microsoft-store-for-business

**QUESTION 44**
You have a Microsoft 365 subscription that contains a Microsoft Azure Active Directory (Azure AD) tenant named contoso.com.

In the tenant, you create a user named User1.

You need to ensure that User1 can publish retention labels from the Security & Compliance admin center. The solution must use the principle of least privilege.

To which role group should you add User1?

A. Security Administrator
B. Records Management
C. Compliance Administrator
D. eDiscovery Manager

**Correct Answer:** B
**Section: [none]**
**Explanation**

**Explanation/Reference:**
References:
https://docs.microsoft.com/en-us/office365/securitycompliance/file-plan-manager

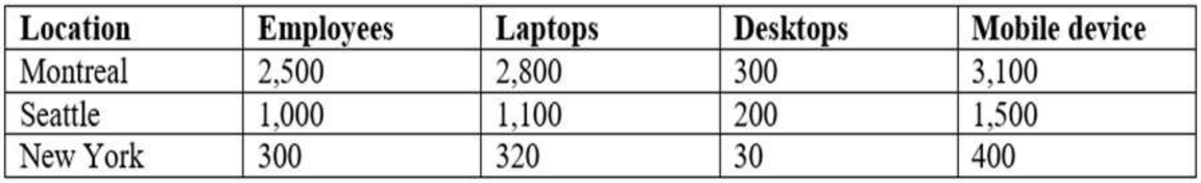
**Testlet 2**

**Case Study**

**Overview**

Contoso, Ltd. is a consulting company that has a main office in Montreal and two branch offices in Seattle and New York.

The company has the employees and devices shown in the following table.

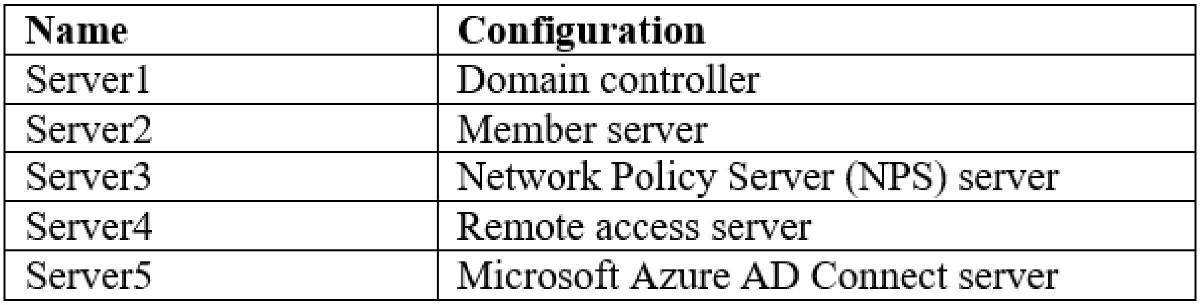


| Location | Employees | Laptops | Desktops | Mobile device |
|---|---|---|---|---|
| Montreal | 2,500 | 2,800 | 300 | 3,100 |
| Seattle | 1,000 | 1,100 | 200 | 1,500 |
| New York | 300 | 320 | 30 | 400 |

Contoso recently purchased a Microsoft 365 E5 subscription.

**Existing Environment**

The network contains an on-premises Active Directory forest named contoso.com. The forest contains the servers shown in the following table.

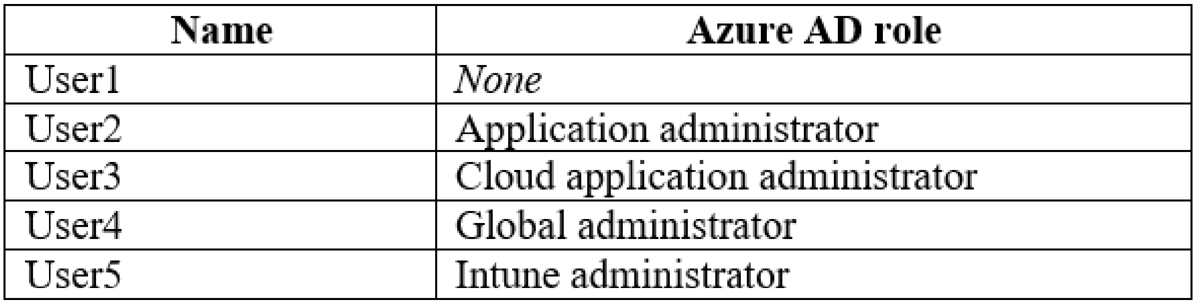


| Name | Configuration |
|---|---|
| Server1 | Domain controller |
| Server2 | Member server |
| Server3 | Network Policy Server (NPS) server |
| Server4 | Remote access server |
| Server5 | Microsoft Azure AD Connect server |

All servers run Windows Server 2016. All desktops and laptops run Windows 10 Enterprise and are joined to the domain.

The mobile devices of the users in the Montreal and Seattle offices run Android. The mobile devices of the users in the New York office run iOS.

The domain is synced to Azure Active Directory (Azure AD) and includes the users shown in the following table.



| Name | Azure AD role |
|---|---|
| User1 | *None* |
| User2 | Application administrator |
| User3 | Cloud application administrator |
| User4 | Global administrator |
| User5 | Intune administrator |

The domain also includes a group named Group1.

**Requirements**

**Planned Changes**

Contoso plans to implement the following changes:

- Implement Microsoft 365.
- Manage devices by using Microsoft Intune.
- Implement Azure Advanced Threat Protection (ATP).
- Every September, apply the latest feature updates to all Windows computers. Every March, apply the latest feature updates to the computers in the New York office only.

**Technical Requirements**

Contoso identifies the following technical requirements:

- When a Windows 10 device is joined to Azure AD, the device must enroll in Intune automatically.
- Dedicated support technicians must enroll all the Montreal office mobile devices in Intune.
- User1 must be able to enroll all the New York office mobile devices in Intune.
- Azure ATP sensors must be installed and must **NOT** use port mirroring.
- Whenever possible, the principle of least privilege must be used.
- A Microsoft Store for Business must be created.

**Compliance Requirements**

Contoso identifies the following compliance requirements:

- Ensure that the users in Group1 can only access Microsoft Exchange Online from devices that are enrolled in Intune and configured in accordance with the corporate policy.
- Configure Windows Information Protection (WIP) for the Windows 10 devices.

**QUESTION 1**
You need to meet the compliance requirements for the Windows 10 devices.

What should you create from the Intune admin center?

A. a device compliance policy

B. a device configuration profile

C. an app protection policy

D. an app configuration policy

**Correct Answer:** C
**Section: [none]**
**Explanation**

**Explanation/Reference:**
References:
https://docs.microsoft.com/en-us/windows/security/information-protection/windows-information-protection/create-wip-policy-using-intune-azure

**Testlet 3**

**Case Study**

**Overview**

ADatum Corporation is an international financial services company that has 5,000 employees.

ADatum has six offices: a main office in New York and five branch offices in Germany, the United Kingdom, France, Spain, and Italy.

All the offices are connected to each other by using a WAN link. Each office connects directly to the Internet.

**Existing Environment**

**Current Infrastructure**

ADatum recently purchased a Microsoft 365 subscription.

All user files are migrated to Microsoft 365.

All mailboxes are hosted in Microsoft 365. The users in each office have email suffixes that include the country of the user, for example, user1@us.adatum.com or user2@uk.adatum.com.

Each office has a security information and event management (SIEM) appliance. The appliance comes from three different vendors.

ADatum uses and processes Personally Identifiable Information (PII).

**Problem Statements**

ADatum entered into litigation. The legal department must place a hold on all the documents of a user named User1 that are in Microsoft 365.

**Requirements**

**Business Goals**

ADatum wants to be fully compliant with all the relevant data privacy laws in the regions where is operates.

ADatum wants to minimize the cost of hardware and software whenever possible.

**Technical Requirements**

ADatum identifies the following technical requirements:

- Centrally perform log analysis for all offices.
- Aggregate all data from the SIEM appliances to a central cloud repository for later analysis.
- Ensure that a SharePoint administrator can identify who accessed a specific file stored in a document library.
- Provide the users in the finance department with access to Service assurance information in Microsoft Office 365.
- Ensure that documents and email messages containing the PII data of European Union (EU) citizens are preserved for 10 years.
- If a user attempts to download 1,000 or more files from Microsoft SharePoint Online within 30 minutes, notify a security administrator and suspend the user’s user account.
- A security administrator requires a report that shown which Microsoft 365 users signed in. Based on the

report, the security administrator will create a policy to require multi-factor authentication when a sign-in is high risk.

- Ensure that the users in the New York office can only send email messages that contain sensitive U.S. PII data to other New York office uses. Email messages must be monitored to ensure compliance. Auditors in the New York office must have access to reports that show the sent and received email messages containing sensitive U.S. PII data.

**QUESTION 1**
Which report should the New York office auditors view?

A. DLP incidents
B. Top Senders and Recipients
C. DLP false positives and overrides
D. DLP policy matches

**Correct Answer:** A
**Section: [none]**
**Explanation**

**Explanation/Reference:**
References:
https://docs.microsoft.com/en-us/office365/securitycompliance/data-loss-prevention-policies

**QUESTION 2**
You need to meet the technical requirement for the EU PII data.

What should you create?

A. a data loss prevention (DLP) policy from the Security & Compliance admin center
B. a data loss prevention (DLP) policy from the Exchange admin center
C. a retention policy from the Exchange admin center
D. a retention policy from the Security & Compliance admin center

**Correct Answer:** D
**Section: [none]**
**Explanation**

**Explanation/Reference:**
References:
https://docs.microsoft.com/en-us/office365/securitycompliance/retention-policies

**QUESTION 3**
You need to protect the U.S. PII data to meet the technical requirements.

What should you create?

A. a data loss prevention (DLP) policy that contains a domain exception
B. a Security & Compliance retention policy that detects content containing sensitive data
C. a Security & Compliance alert policy that contains an activity
D. a data loss prevention (DLP) policy that contains a user override

**Correct Answer:** C
**Section: [none]**
**Explanation**

**Explanation/Reference:**

References:
https://docs.microsoft.com/en-us/office365/securitycompliance/create-activity-alerts

**QUESTION 4**
DRAG DROP

You need to meet the requirement for the legal department.

Which three actions should you perform in sequence from the Security & Compliance admin center? 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:**

**Correct Answer:**

**Section: [none]**
**Explanation**

**Explanation/Reference:**
References:
https://www.sherweb.com/blog/ediscovery-office-365/

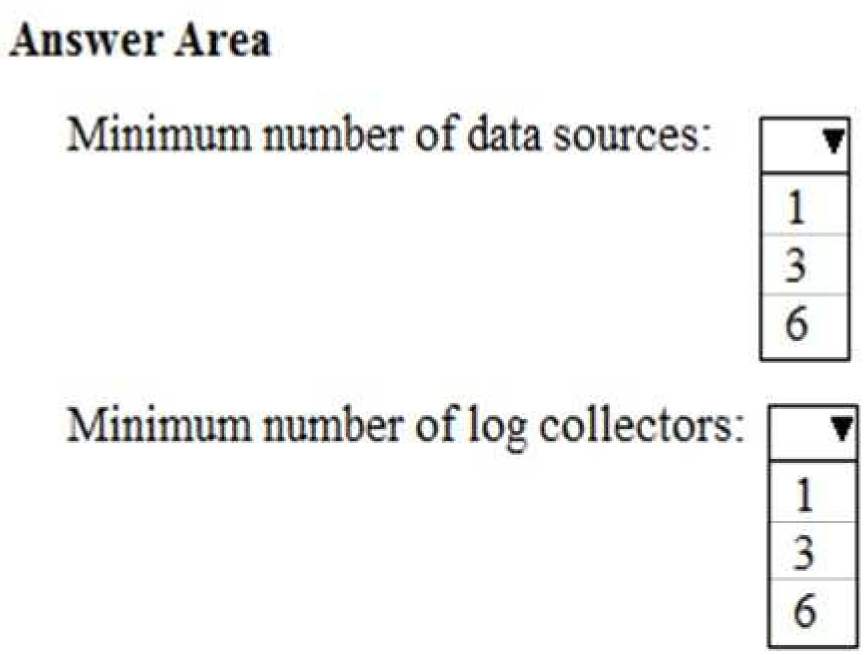
**QUESTION 5**
HOTSPOT

You need to meet the technical requirement for log analysis.

What is the minimum number of data sources and log collectors you should create from Microsoft Cloud App Security? To answer, select the appropriate options in the answer area.

**NOTE**: Each correct selection is worth one point.

**Hot Area:**

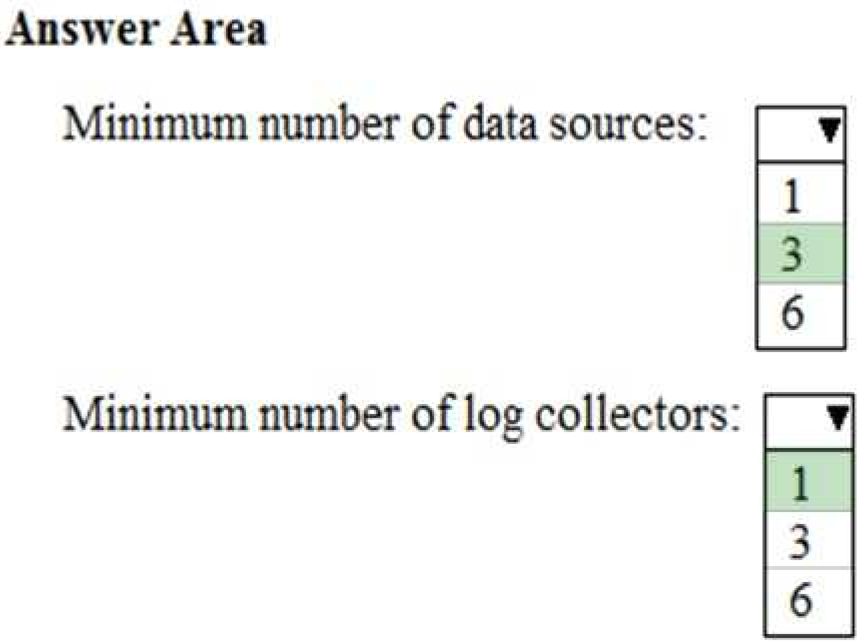


Answer Area

Minimum number of data sources: ▼
1
3
6

Minimum number of log collectors: ▼
1
3
6

**Correct Answer:**



Answer Area

Minimum number of data sources: ▼

1 [✓ 3] 6

Minimum number of log collectors: ▼

[✓ 1] 3 6

**Section: [none]**
**Explanation**

**Explanation/Reference:**
References:
https://docs.microsoft.com/en-us/cloud-app-security/discovery-docker

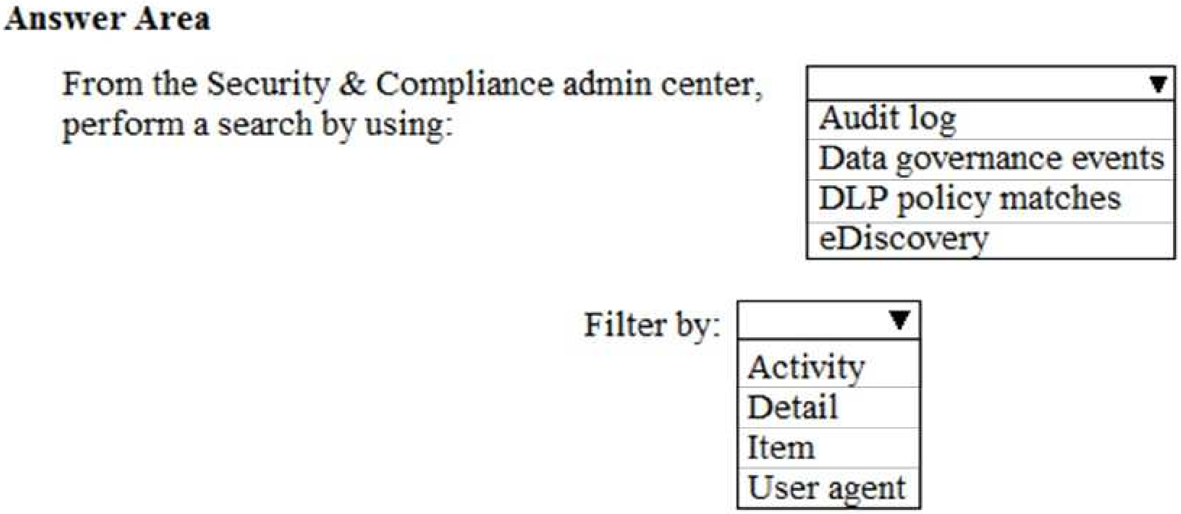
**QUESTION 6**
HOTSPOT

You need to meet the technical requirement for the SharePoint administrator.

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

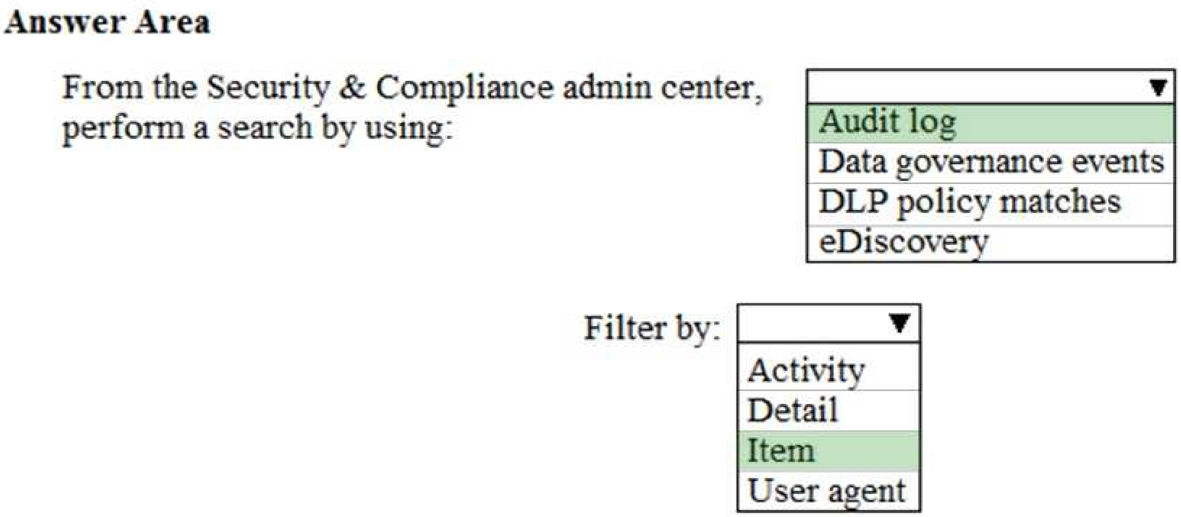
From the Security & Compliance admin center, perform a search by using: ▼

- Audit log
- Data governance events
- DLP policy matches
- eDiscovery

Filter by: ▼

- Activity
- Detail
- Item
- User agent

**Correct Answer:**



**Answer Area**

From the Security & Compliance admin center, perform a search by using:

- [✓ Audit log]
- Data governance events
- DLP policy matches
- eDiscovery

Filter by:

- Activity
- Detail
- [✓ Item]
- User agent

**Section: [none]**
**Explanation**

**Explanation/Reference:**
References:
https://docs.microsoft.com/en-us/office365/securitycompliance/search-the-audit-log-in-security-and-compliance#step-3-filter-the-search-results