MS-500 Q&As

Microsoft 365 Security Administration

Pass Microsoft MS-500 Exam with 100% Guarantee

Free Download Real Questions & Answers **PDF** and **VCE** file from:

https://www.pass4itsure.com/ms-500.html

100% Passing Guarantee
100% Money Back Assurance

Following Questions and Answers are all new published by Microsoft Official Exam Center

- **Instant Download** After Purchase
- **100% Money Back** Guarantee
- **365 Days** Free Update
- **800,000+** Satisfied Customers

QUESTION 1

You have a Microsoft 365 subscription.

You need to be notified by email whenever an administrator starts an eDiscovery search.

What should you do from the Microsoft 365 Compliance center?

A. From Policies, create an alert policy.

B. From Content search, create a new search.

C. From eDiscovery, create an eDiscovery case.

D. From Records management, create event type.

Correct Answer: A

Reference: https://docs.microsoft.com/en-us/office365/securitycompliance/alert-policies

QUESTION 2

You have a Microsoft 165 ES subscription that contains users named User 1 and User2? You have the audit log retention requirements shown in the following table.

User	Action	Retention period
User1	Rename a Microsoft SharePoint Online site.	12 months
User1	Perform all actions in Microsoft Dynamics 365.	6 months
User2	Create a Microsoft SharePoint Online site collection.	12 months
User2	Perform all Microsoft Exchange Online administrative actions.	10 years

You need to create audit retention policies to meet the requirements. The solution must minimize cost and the number of policies. What is the minimum number of audit retention policies that you should create?

A. 1

B. 2

C. 3

D. 4

Correct Answer: C

QUESTION 3

You have a Microsoft 365 subscription.

You create and run a content search from the Security and Compliance admin center.

You need to download the results of the content search.

What should you obtain first?

A. an export key

B. a password

C. a certificate

D. a pin

Correct Answer: A

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

QUESTION 4

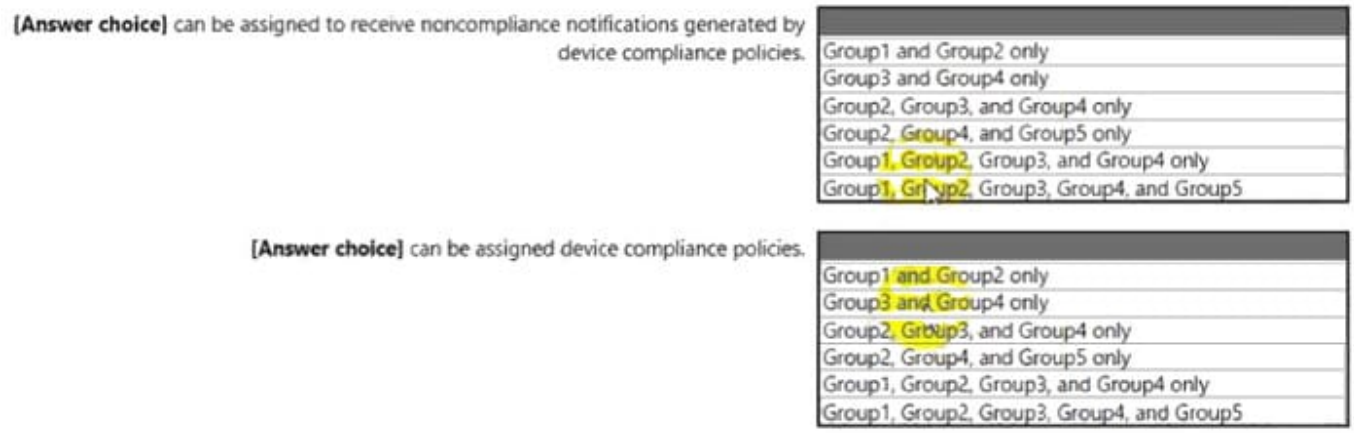
HOTSPOT

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

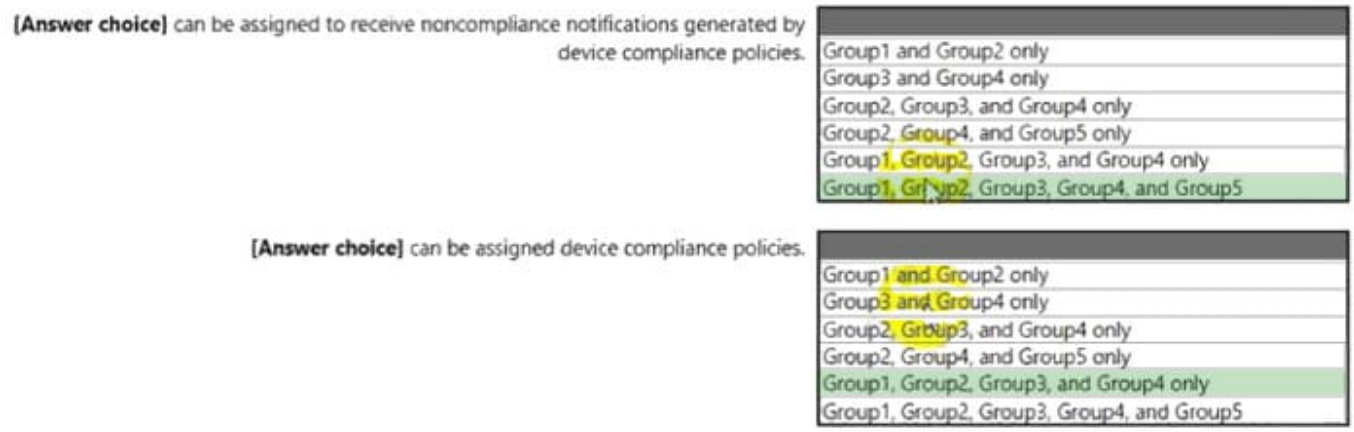
Name	Group type	Membership type	Email	Security enabled
Group1	Microsoft 365	Assigned	Group1@sk220130.onmicrosoft.com	No
Group2	Microsoft 365	Assigned	Group2@sk220130.onmicrosoft.com	Yes
Group3	Distribution	Assigned	Group3@sk220130.onmicrosoft.com	No
Group4	Mail enabled security	Assigned	Group4@sk220130.onmicrosoft.com	Yes
Group5	Security	Assigned		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:



QUESTION 5

HOTSPOT

You have a Microsoft Sentinel workspace that has an Azure Active Directory (Azure AD) connector and an Office 365 connector.

From the workspace, you plan to create an analytics rule that will be based on a custom query and will run a security play.

You need to ensure that you can add the security playbook and the custom query to the rule.

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

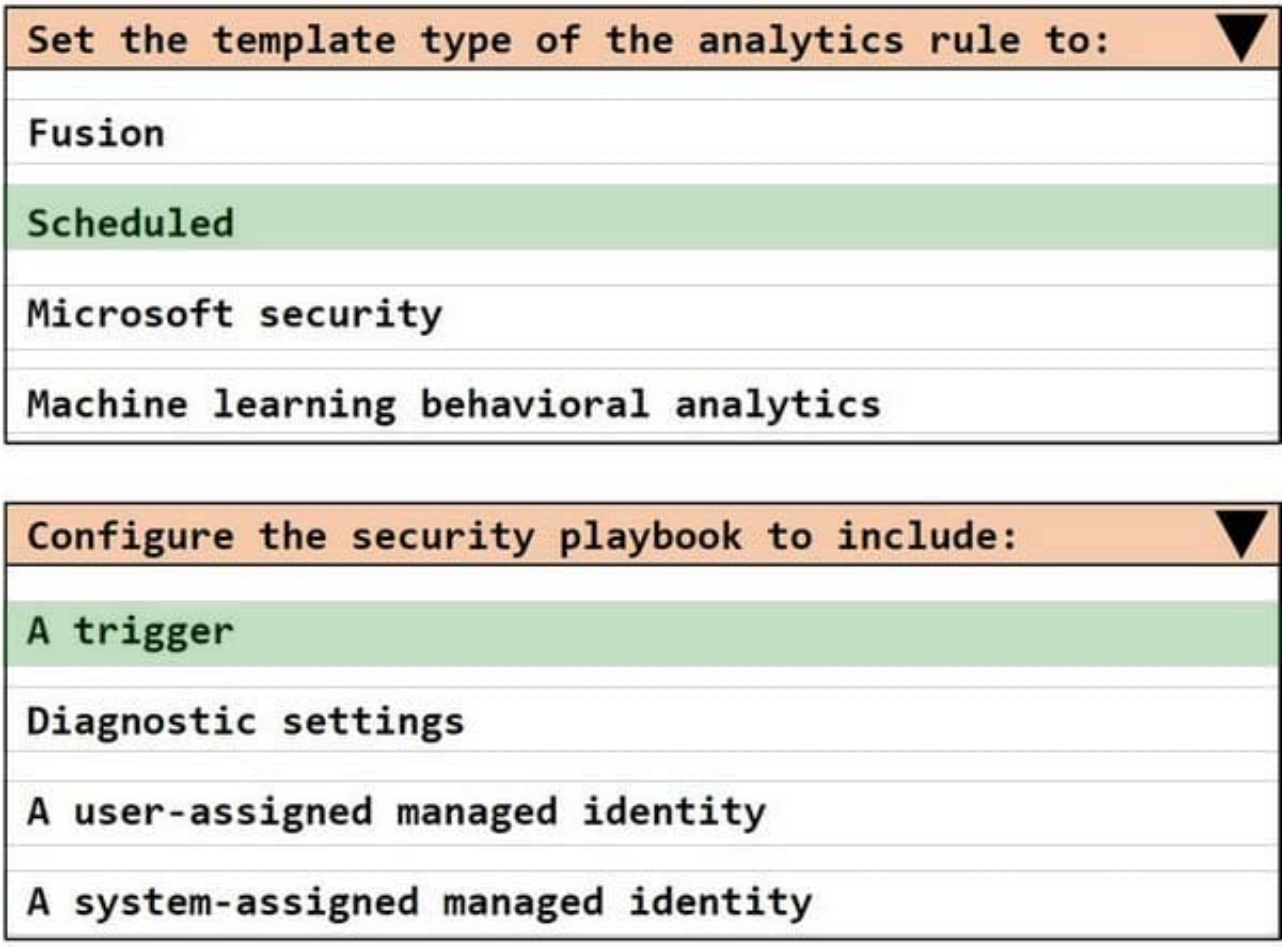
NOTE: Each correct selection is worth one point.

Hot Area:

Set the template type of the analytics rule to: ▼
Fusion
Scheduled
Microsoft security
Machine learning behavioral analytics

Configure the security playbook to include: ▼
A trigger
Diagnostic settings
A user-assigned managed identity
A system-assigned managed identity

Correct Answer:



Box 1: Scheduled Create a custom analytics rule with a scheduled query

1.

From the Microsoft Sentinel navigation menu, select Analytics.

2.

In the action bar at the top, select +Create and select Scheduled query rule. This opens the Analytics rule wizard.

3.

Etc.

Box 2: A trigger

Use triggers and actions in Microsoft Sentinel playbooks.

Reference:

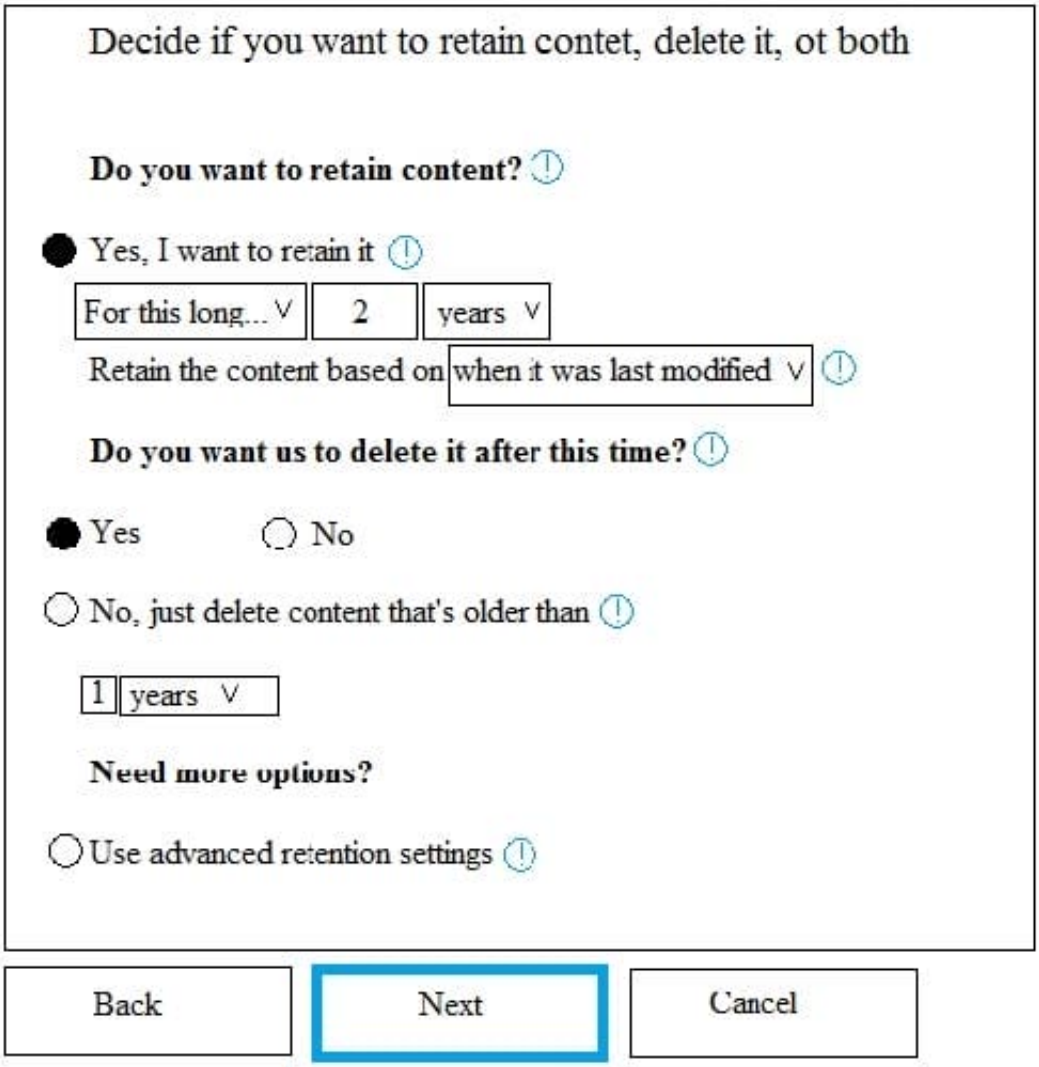
https://docs.microsoft.com/en-us/azure/sentinel/detect-threats-custom https://docs.microsoft.com/en-us/azure/sentinel/playbook-triggers-actions#microsoft-sentinel-triggers-summary

QUESTION 6

HOTSPOT

You have a Microsoft 365 subscription.

You are creating a retention policy named Retention1 as shown in the following exhibit.



You apply Retention1 to SharePoint sites and OneDrive accounts.

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 a user creates a file in a Microsoft SharePoint library on January 1, 2019, and modifies the file every six months, the file will be **[answer choice]**.

retained
deleted on January 1, 2021
deleted on July 1, 2021

If a user creates a file in a Microsoft OneDrive on January 1, 2019, modifies the file on March 1, 2019, and deletes the file on May 1, 2019, the user **[answer choice]**.

can recover the file until the Recycle Bin retention period expires
can recover the file until January 1, 2021
can recover the file until March 1, 2021
can recover the file until May 1, 2021

Correct Answer:

Answer Area

If a user creates a file in a Microsoft SharePoint library on January 1, 2019, and modifies the file every six months, the file will be **[answer choice]**.

retained
deleted on January 1, 2021
deleted on July 1, 2021

If a user creates a file in a Microsoft OneDrive on January 1, 2019, modifies the file on March 1, 2019, and deletes the file on May 1, 2019, the user **[answer choice]**.

can recover the file until the Recycle Bin retention period expires
can recover the file until January 1, 2021
can recover the file until March 1, 2021
can recover the file until May 1, 2021

1.- Retained

2.- Can recover the file until the Recycle Bin retention period expired (93 days). Because the question says "the user", so the user can\\'t recover a file from the "Preservation hold library". "If the content is modified or deleted during the retention period, a copy of the original content as it existed when the retention policy was assigned is created in the Preservation Hold library. There, the timer job identifies items whose retention period has expired. Those items are moved to the second-stage Recycle Bin, where they\\'re permanently deleted at the end of 93 days. The second-stage Recycle Bin is not visible to end users (only the first-stage Recycle Bin is), but site collection admins can view and restore content from there." https://docs.microsoft.com/en-us/microsoft-365/compliance/retention-policies-sharepoint?view=o365-worldwide

QUESTION 7

You need to meet the technical requirements for User9. What should you do?

A. Assign the Privileged administrator role to User9 and configure a mobile phone number for User9

B. Assign the Compliance administrator role to User9 and configure a mobile phone number for User9

C. Assign the Security administrator role to User9

D. Assign the Global administrator role to User9

Correct Answer: A

https://learn.microsoft.com/en-us/azure/active-directory/privileged-identity-management/pim-getting-started

When a user who is active in a privileged role in an Azure AD organization with a Premium P2 license goes to Roles and administrators in Azure AD and selects a role (or even just visits Privileged Identity Management):

We automatically enable PIM for the organization Their experience is now that they can either assign a "regular" role assignment or an eligible role assignment When PIM is enabled it doesn\\'t have any other effect on your organization that you need to worry about. It gives you additional assignment options such as active vs eligible with start and end time. PIM also enables you to define scope for role assignments using Administrative Units and custom roles. If you are a Global Administrator or Privileged Role Administrator, you might start getting a few additional emails like the PIM weekly digest. You might also see MS-PIM service principal in the audit log related to role assignment. This is an expected change that should have no effect on your workflow.

QUESTION 8

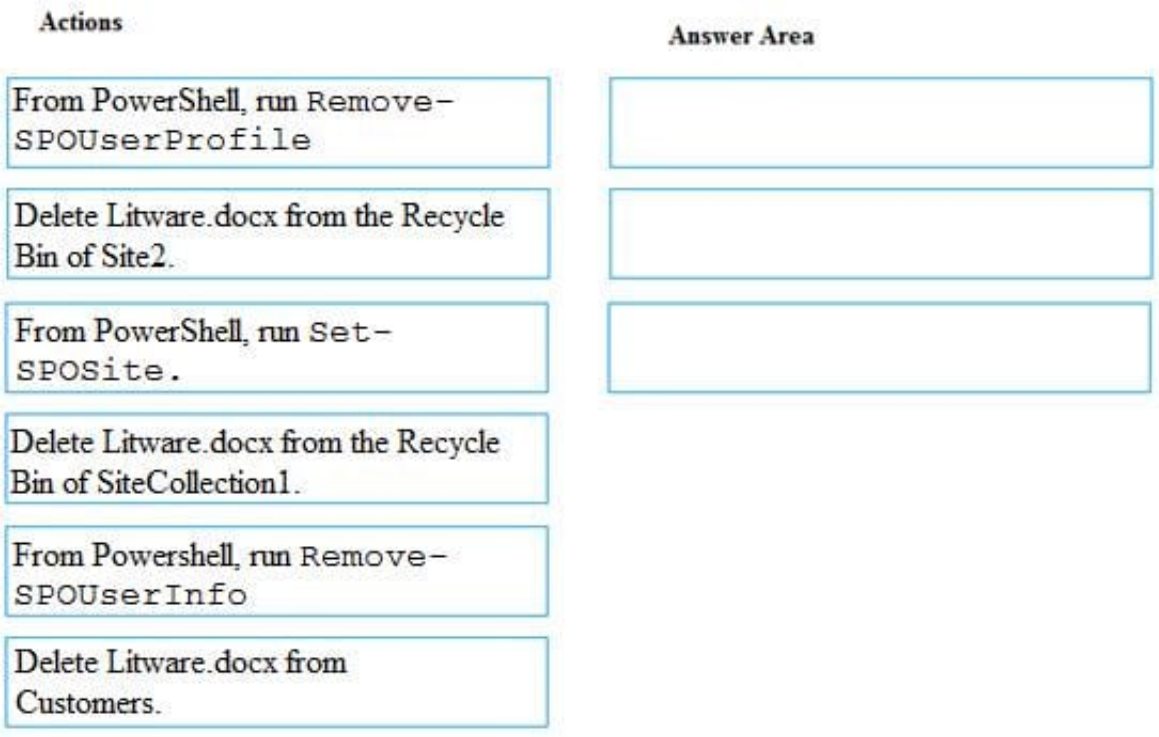
You have a Microsoft 365 subscription.

You have a site collection named SiteCollection1 that contains a site named Site2. Site2 contains a document library named Customers.

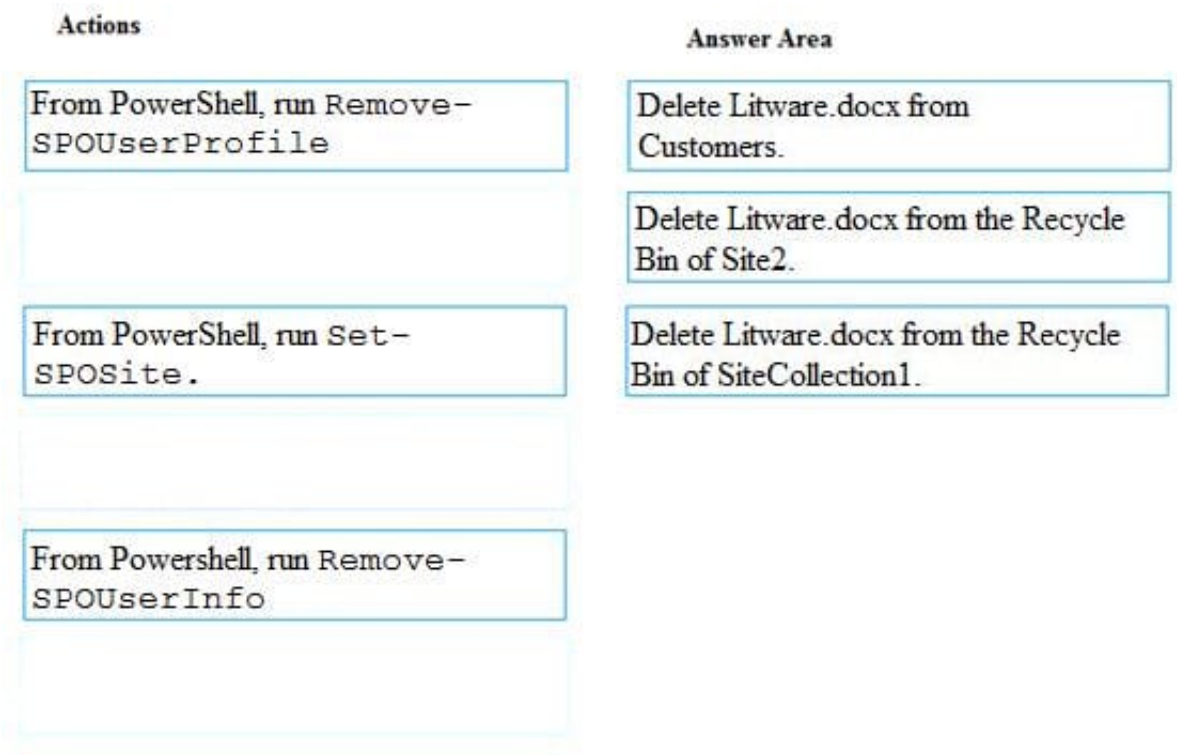
Customers contains a document named Litware.docx. You need to remove Litware.docx permanently.

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:



QUESTION 9

You have a Microsoft 365 subscription that contains a Microsoft 365 group named Group1. Group1 contains 100 users and has dynamic user membership.

All users have Windows 10 devices and use Microsoft SharePoint Online and Exchange Online.

You create a sensitivity label named Label and publish Label 1 as the default label for Group!.

You need to ensure that the users in Group1 must apply Label! to their email and documents.

Which two actions should you perform? Each correct answer presents part of the solution.

NOTE: Each correct selection is worth one point.

A. Install the Azure Information Protection unified labeling client on the Windows 10 devices.

B. From the Microsoft 365 Compliance center, modify the settings of the Label1 policy.

C. Install the Active Directory Rights Management Services (AD RMS) client on the Windows 10 devices.

D. From the Microsoft 365 Compliance center, create an auto-labeling policy.

E. From the Azure Active Directory admin center, set Membership type for Group1 to Assigned.

Correct Answer: AB

D is wrong. Auto-Labeling policy will not achieve the requirement “You need to ensure that the users in Group1 must apply Label1 to their email and documents”

This requirement is a setting in the sensitivity label policy that can be selected.

Auto-Labeling is an admin activity.

Auto-Labeling policy:

When you create a sensitivity label, you can automatically assign that label to files and emails when it matches conditions that you specify.

This ability to apply sensitivity labels to content automatically is important because:

1.

You don\\'t need to train your users when to use each of your classifications.

2.

You don\\'t need to rely on users to classify all content correctly.

3.

Users no longer need to know about your policies—they can instead focus on their work.

E is wrong. It is not a must to Membership type for Group1 to be Assigned. Label can be applied to both Assigned and Dynamic.

QUESTION 10

Note: This question is part of 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 tenant. You create a label named CompanyConfidential in Microsoft Azure Information Protection.

You add CompanyConfidential to a global policy.

A user protects an email message by using CompanyConfidential and sends the label to several external recipients. The external recipients report that they cannot open the email message.

You need to ensure that the external recipients can open protected email messages sent to them.

Solution: You create a new label in the global policy and instruct the user to resend the email message.

Does this meet the goal?

A. Yes

B. No

Correct Answer: A

QUESTION 11

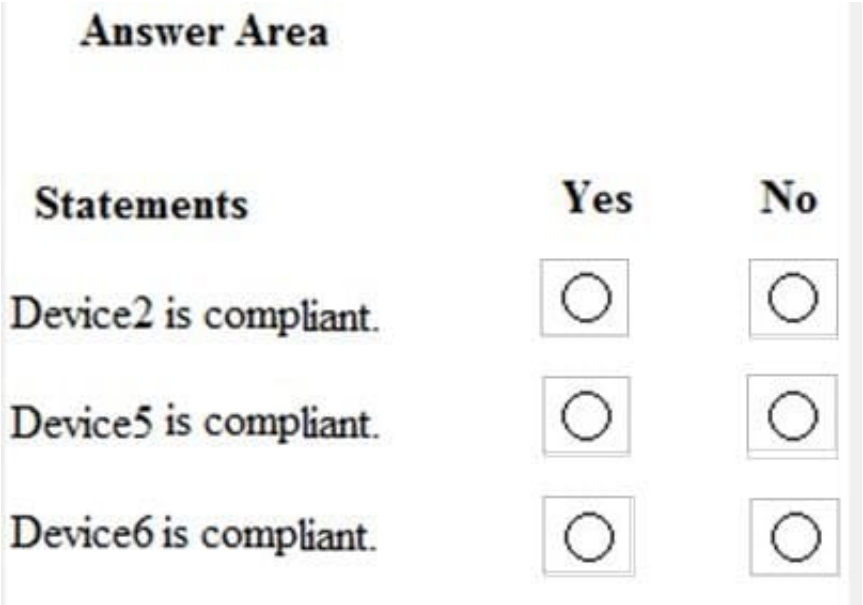
HOTSPOT

You are evaluating which devices are compliant in Intune.

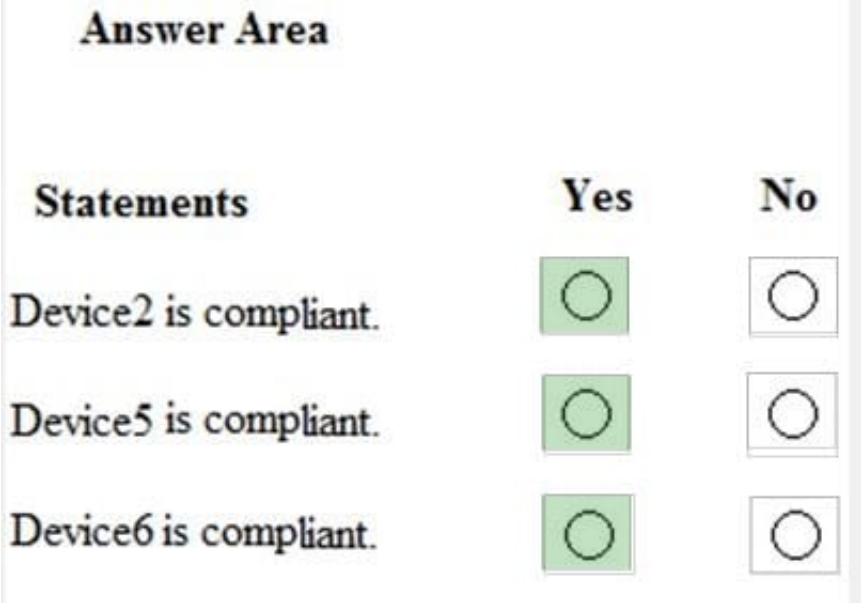
For each of the following statements, select Yes if the statement is true. Otherwise, select No.

NOTE: Each correct selection is worth one point.

Hot Area:



Correct Answer:



Device2:

Member of Group B and Group C

Group B -> DevicePolicy2

DevicePolicy2 requires Windows 10, ecryption and assignment.

Device2 meets all of these requirements.

Group C -> DevicePolicy1

Device2 is not a Androind so it is not compiant to this device policy, but thats OK because it\\'scompliant with DevicePolicy2.

Device5:

Device 5 is an IOS device, policy is for android devices so device is compliant.

Device6:

Device6 is not a part of a group and the question states that "the Mark devices with no compliane policy assigned as setting is set to Compliant." This makes Device6 compliant.

QUESTION 12

SIMULATION

Your company plans to merge with another company.

A user named Debra Berger is an executive at your company.

You need to provide Debra Berger with all the email content of a user named Alex Wilber that contains the word merger. To complete this task, sign in to the Microsoft 365 portal.

Correct Answer: See explanation below.

You need to run a content search then export the results of the search.

1.

Go to the Microsoft 365 Compliance admin center.

2.

Navigate to Content Search under the Solutions section in the left navigation pane.

3.

Click on + New Search to create a new search.

4.

In the Keywords box, type in ‘merger’.

5.

In the Locations section, select Specific locations then click the Modify link.

6.

Click on the Choose users, groups or teams link.

7.

Type Alex Wilber in the search field the select his account from the search results.

8.

Click the Choose button to add the user then click Done.

9.

Click Save to close the locations pane.

10.Click Save and run to run the search.

11.The next step is to export the results. Select the search then under Export results to a computer,click Start export.

12.On the Export the search results page, under Output options, select All items.

13.Under Export Exchange content as, select One PST file for each mailbox.

14.Click on Start export. When the export has finished, there will be an option to download the exported PST file.

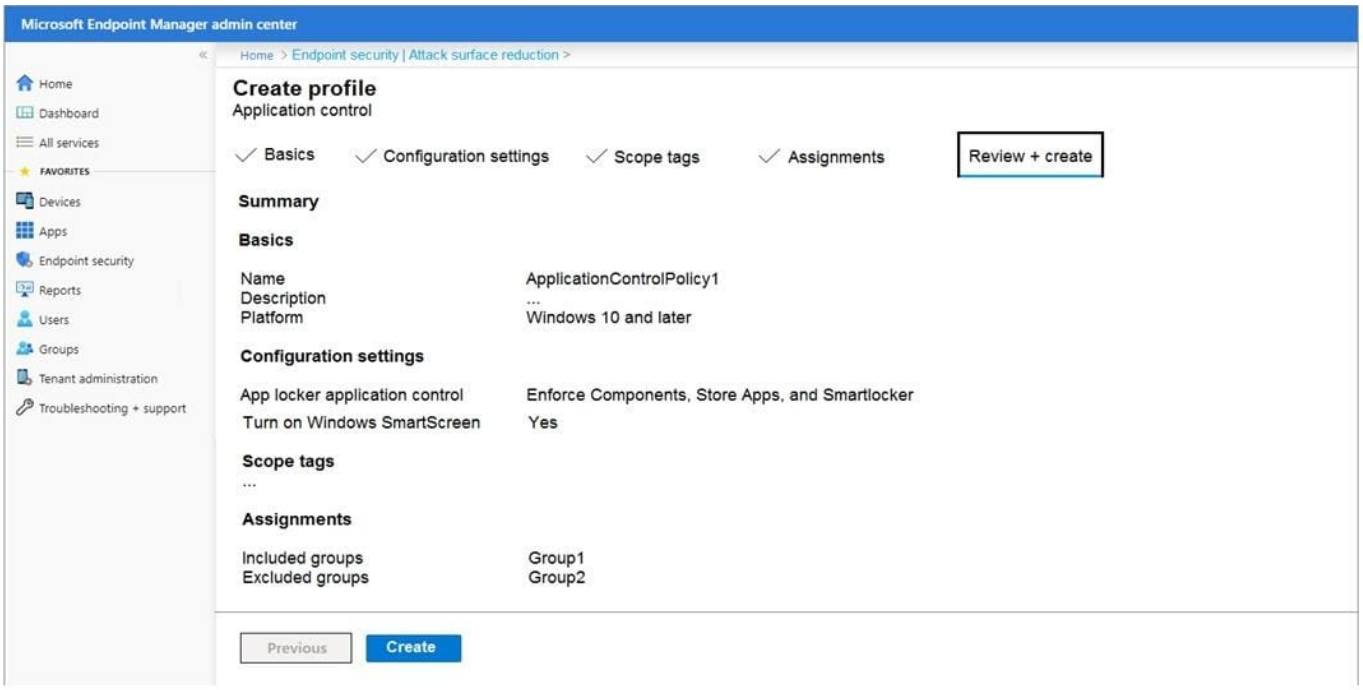
Reference: https://docs.microsoft.com/en-us/microsoft-365/compliance/content-search?view=o365-worldwide
https://docs.microsoft.com/en-us/microsoft-365/compliance/export-search-results?view=o365-worldwide

QUESTION 13

HOTSPOT

You have a Microsoft 365 tenant.

You create an attack surface reduction policy that uses an application control profile as shown in the following exhibit.



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

Hot Area:

Correct Answer:

Answer Area

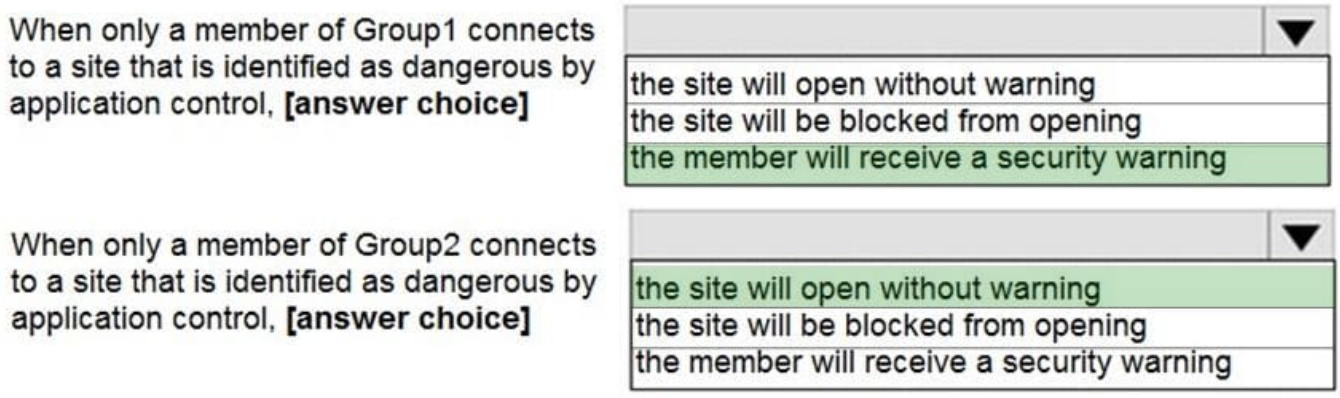
When only a member of Group1 connects to a site that is identified as dangerous by application control, **[answer choice]**

- the site will open without warning
- the site will be blocked from opening
- the member will receive a security warning

When only a member of Group2 connects to a site that is identified as dangerous by application control, **[answer choice]**

- the site will open without warning
- the site will be blocked from opening
- the member will receive a security warning

Answer Area



Box 1: the member will receive a security warning.

Group1 is included in the policy so SmartScreen will be enabled. SmartScreen will display a warning.

Box 2: the site will open without warning.

Group2 is excluded from the policy so SmartScreen will not be enabled. Therefore, no warning will be displayed.

QUESTION 14

You need to ensure that a user named Alex Wilber can register for multifactor authentication (MFA).

To complete this task, sign in to the Microsoft Office 365 admin center.

Correct Answer: See explanation below.

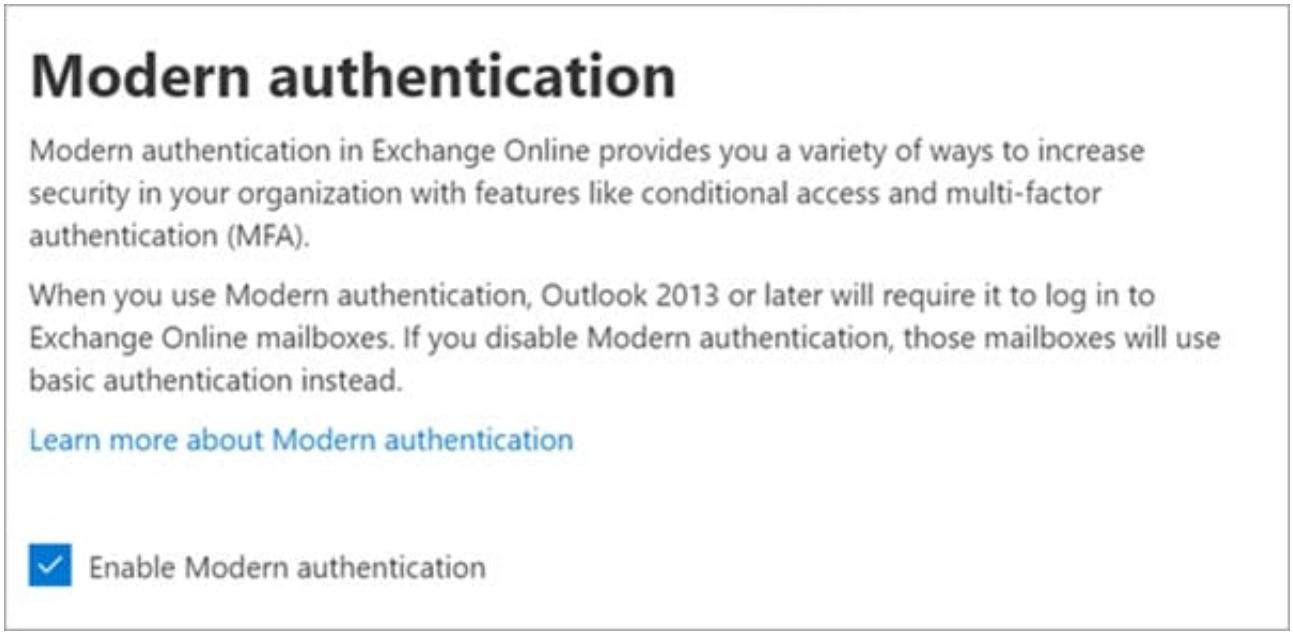
Enable Modern authentication for your organization

1.

To enable modern authentication, from the admin center, select Settings > Settings and then in the Services tab, choose Modern authentication from the list.

2.

Check the Enable modern authentication box in the Modern authentication panel.



Enable multi-factor authentication for your organization

1.

In the admin center, select Users and Active Users.

2.

In the Active Users section, Click on multi-factor authentication.

3.

On the Multi-factor authentication page, select user if you are enabling this for one user or select Bulk Update to enable multiple users.

4.

Click on Enable under Quick Steps.

5.

In the Pop-up window, Click on Enable Multi-Factor Authentication.

After you set up multi-factor authentication for your organization, your users will be required to set up two-step verification on their devices.

Reference: https://docs.microsoft.com/en-us/microsoft-365/admin/security-and-compliance/set-up-multi-factor-authentication?view=o365-worldwide

QUESTION 15

Your company has a Microsoft 365 subscription that includes a user named User1.

You suspect that User1 sent email messages to a competitor detailing company secrets.

You need to recommend a solution to ensure that you can review any email messages sent by User1 to the competitor, including sent items that were deleted.

What should you include in the recommendation?

A. Enable In-Place Archiving for the mailbox of User1

B. From the Security and Compliance, perform a content search of the mailbox of User1

C. Place a Litigation Hold on the mailbox of User1

D. Configure message delivery restrictions for the mailbox of User1

Correct Answer: C

A Litigation Hold is a feature that allows you to preserve all mailbox data, including deleted items, for a specified period of time. This means that if User1 deleted any email messages sent to the competitor, they will still be preserved and available for review.