DUMPSQUEEN

Microsoft 365 Security Administration

Microsoft MS-500

Version Demo

Total Demo Questions: 20

Total Premium Questions: 638

Buy Premium PDF

https://dumpsqueen.com

support@dumpsqueen.com

Topic Break Down

Topic	No. of Questions
Topic 2, New Update	268
Topic 3, Case Study 1	5
Topic 4, Case Study 2	4
Topic 5, Case Study 3	5
Topic 6, Case Study 4	2
Topic 7, Case Study 5	2
Topic 8, Case Study 6	2
Topic 9, Mixed Questions	350
Total	638

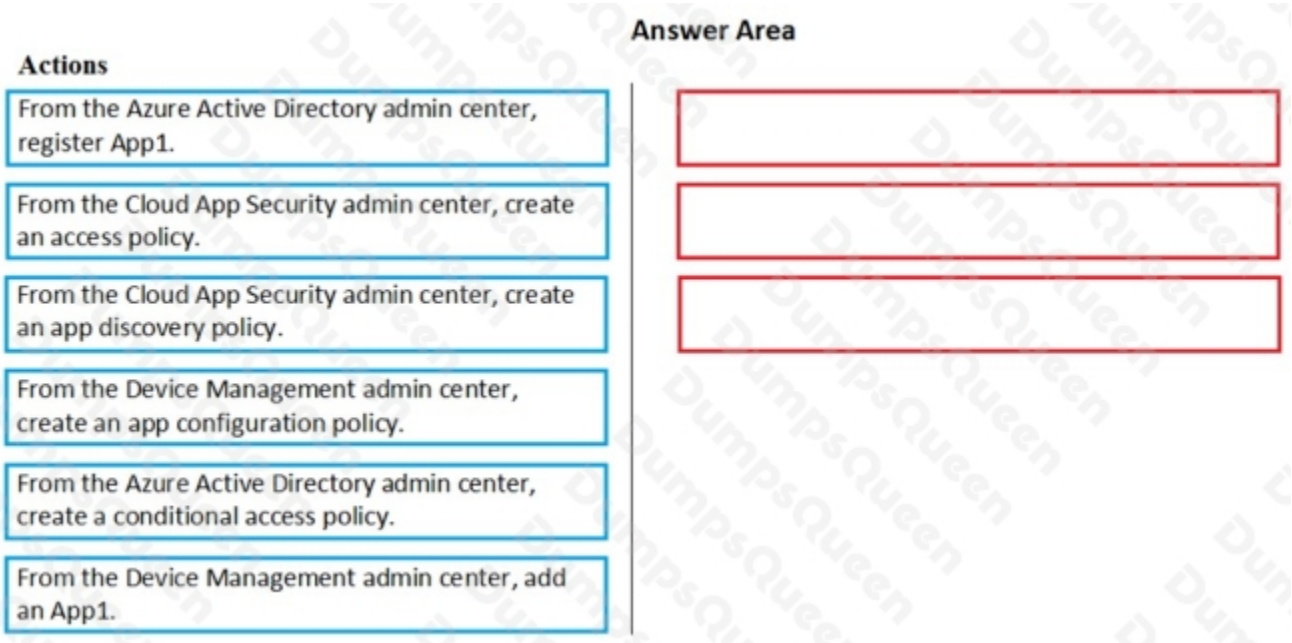
QUESTION NO: 1 - (DRAG DROP)

You have a Microsoft 365 subscription that uses an Azure Active Directory (Azure AD) tenant named contoso.com. All the devices in the tenant are managed by using Microsoft Intune.

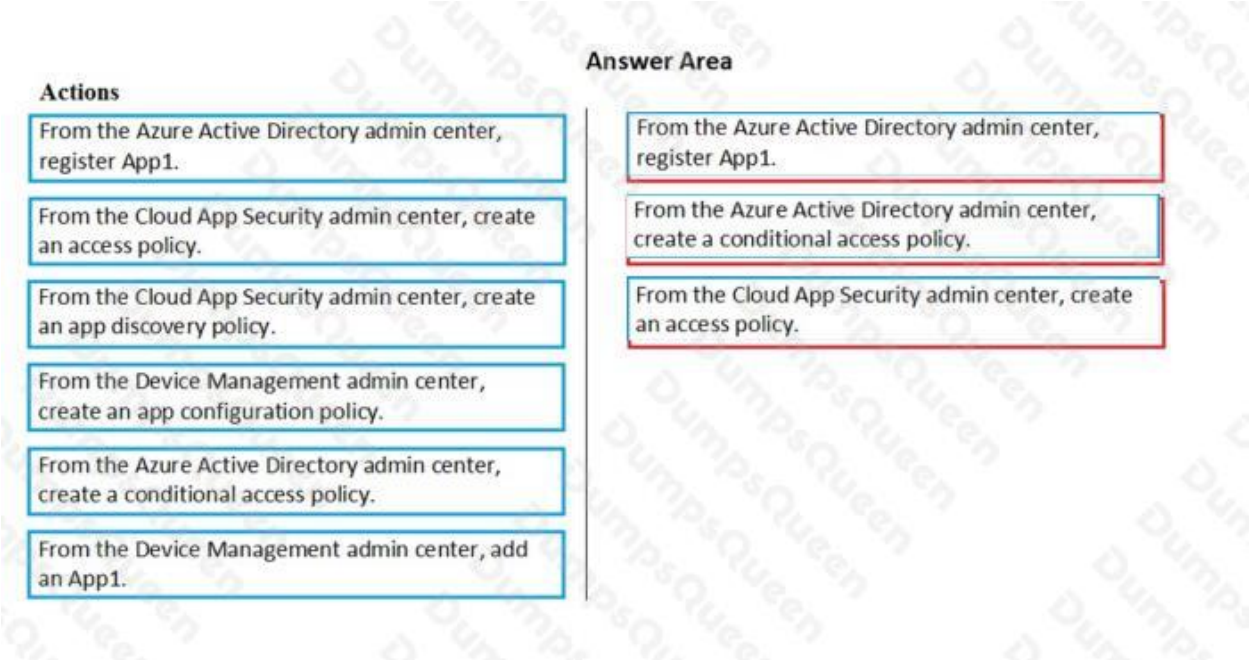
You purchase a cloud app named App1 that supports session controls.

You need to ensure that access to App can be reviewed in real time.

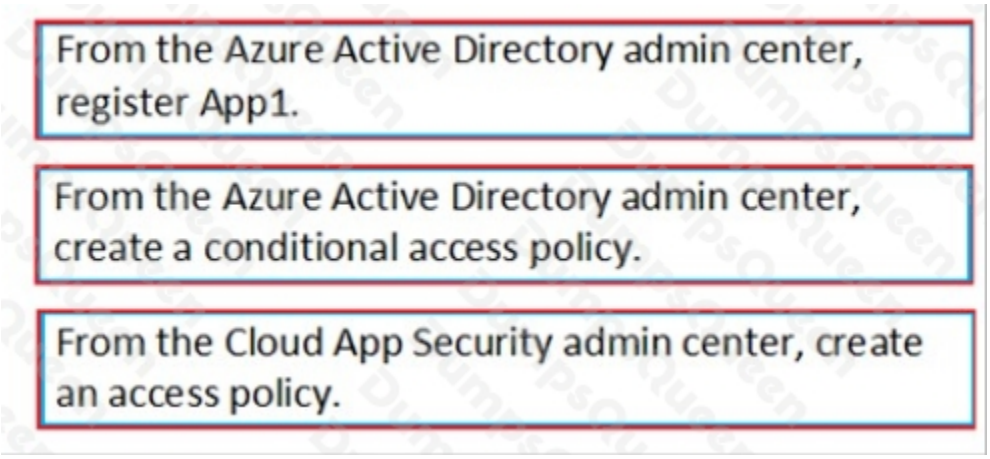
Which three actions should you perform in sequence? To answer, move the appropriate actions from the list of actions to the answer area and arrange them in the correct order.



ANSWER:



Explanation:



References:

https://docs.microsoft.com/en-us/cloud-app-security/access-policy-aad

QUESTION NO: 2

NOTE: This question is a part of a series of questions that present the same scenario. For each of the following statements, select the best response(s) to the question or statement below. Each answer is worth one point.

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 organization has a single-domain, single-forest Active Directory. You have installed Azure AD Connect with express settings. You need a new group that you want to use to manage access to a cloud application you have registered with Azure Active Directory.

What type of group will you create?

A. Security Group

B. Mail-enabled security group

C. Distribution list

D. Office 365 group

E. Any of the above

F. None of the above

ANSWER: A

Explanation:

Using express settings on AD Connect will sync users and certain groups (and other things) from on-premises to Azure AD. Creating the group on the on-premises AD will work, since it will be synchronized to the cloud. Since you are creating a group to be used to manage access to an application, a security group is best. You can only create O365 groups in AAD.

Reference:

https://docs.microsoft.com/en-us/azure/active-directory/fundamentals/active-directory-groups-create-azure-portal

QUESTION NO: 3

You have a Microsoft 365 subscription that includes a user named Admin1.

You need to ensure that Admin1 can preserve all the mailbox content of users, including their deleted items.

The solution must use the principle of least privilege.

What should you do?

A. From the Microsoft 365 admin center, assign the Exchange administrator role to Admin1.

B. From the Exchange admin center, assign the Discovery Management admin role to Admin1.

C. From the Azure Active Directory admin center, assign the Service administrator role to Admin1.

D. From the Exchange admin center, assign the Recipient Management admin role to Admin1.

ANSWER: C

Explanation:

https://docs.microsoft.com/en-us/microsoft-365/compliance/sensitivity-labels#what-label-policies-can-do

QUESTION NO: 4

Your setting up DLP policies in O365 Security & Compliance Center.

Which of the options can you choose to apply your DLP policy to? (Choose all that apply.)

A. Exchange Online

B. SharePoint Online

C. Teams chat

D. SharePoint

E. OneDrive

F. Teams Channel messages

G. Teams file libraries

ANSWER: A B C E F G

Explanation:

O365 DLP can be applied to O365 online services, not on premises services.

Teams chats and channel messages are really Exchange Online hidden mailboxes.

Teams file libraries are really just SharePoint Online sites.

Getting O365 applications to do DLP – aka detect when sensitive information types are being used – in an office document, you must configure the auto-labelling feature in the sensitivity label.

Reference:

https://docs.microsoft.com/en-us/microsoft-365/compliance/data-loss-prevention-policies?view=o365-worldwide

QUESTION NO: 5

You are configuring a 3rd party DLP solution for your organization. You need to give the DLP system the ability to decrypt any data item that has been protected by a AIP label. You want to solution to be operational immediately.

What should you do? (Choose three.)

A. Run the Enable-AipServiceSuperUserFeature PowerShell cmdlet

B. Run the Add-AipServiceSuperUser PowerShell cmdlet

C. Run the Set-AipServiceSuperUserGroup PowerShell cmdlet

D. Run the New-AzureADUser PowerShell cmdlet

E. Run the Add-AzureADGroupMember PowerShell cmdlet

ANSWER: A B D

Explanation:

Enable the feature; create a user; add the user to the feature

You can also create a group, add the user to the group and assign the group to the feature, but AIP caches group membership and only updates it periodically – it won't be available immediately as is required by the question.

Reference:

https://docs.microsoft.com/en-us/powershell/module/azuread/add-azureadgroupmember?view=azureadps-2.0

QUESTION NO: 6

You have a Microsoft 365 tenant.

You have a database that stores customer details. Each customer has a unique 13-digit identifier that consists of a fixed pattern of numbers and letters. You need to implement a data loss prevention (DLP) solution that meets the following requirements:

- Email messages that contain a single customer identifier can be sent outside your company.
- Email messages that contain two or more customer identifiers must be approved by the company's data privacy team.

Which two components should you include in the solution? Each correct answer presents part of the solution.

NOTE: Each correct selection is worth one point.

A. a sensitive information type

B. a sensitivity label

C. a retention label

D. a DLP policy

E. a mail flow rule

ANSWER: A D

Explanation:

Reference: https://docs.microsoft.com/en-us/microsoft-365/compliance/sensitive-information-type-entity-definitions?view=o365-worldwide

QUESTION NO: 7

Which of these are O365 ATP attack simulator capabilities? (Choose three.)

A. Malware outbreak

B. Spam overrun

C. Spear phishing

D. Brute force password

E. Rainbow table password

F. Password spray

ANSWER: C D F

Explanation:

Reference:

https://docs.microsoft.com/en-us/microsoft-365/security/office-365-security/attack-simulator

QUESTION NO: 8 - (SIMULATION)

SIMULATION

You need to ensure that a global administrator is notified when a document that contains U.S. Health Insurance Portability and Accountability Act (HIPAA) data is identified in your Microsoft 365 tenant.

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

ANSWER: See explanation below.

Explanation:

1. In the Security & Compliance Center > left navigation > Data loss prevention > Policy > + Create a policy.

2. Choose the U.S. Health Insurance Portability and Accountability Act (HIPAA) template > Next.

3. Name the policy > Next.

4. Choose All locations in Office 365 > Next.

5. At the first Policy Settings step just accept the defaults,

6. After clicking Next, you'll be presented with an additional Policy Settings page

- Deselect the Show policy tips to users and send them an email notification option.

- Select the Detect when content that's being shared contains option, and decrease the number of instances to 1. - Select the Send incident reports in email option.

7. > Next

8. Select the option to turn on the policy right away > Next.

9. Click Create to finish creating the policy.

References: https://docs.microsoft.com/en-us/microsoft-365/compliance/create-test-tune-dlp-policy?view=o365-worldwide
https://docs.microsoft.com/en-us/microsoft-365/compliance/data-loss-prevention-policies?view=o365-worldwide
https://docs.microsoft.com/en-us/microsoft-365/compliance/what-the-dlp-policy-templates-include?view=o365-worldwide

QUESTION NO: 9

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

Name	Role
User1	Application administrator
User2	Security administrator
User3	Security operator
User4	User administrator

You need to identify which user can enable Microsoft Defender Advanced Threat Protection (Microsoft Defender ATP) roles.

Which user should you identify?

A. User1

B. User4

C. User3

D. User2

ANSWER: D

Explanation:

Reference:

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

QUESTION NO: 10

Which of the following Windows 10 Enterprise features provides identity protection?

A. Windows Hello

B. Credential Guard

C. Device Guard

D. Defender Antivirus

E. Defender ATP

ANSWER: B

Explanation:

Reference:

https://docs.microsoft.com/en-us/windows/security/identity-protection/

QUESTION NO: 11

You have a hybrid deployment of Azure Active Directory (Azure AD) that contains two users named User1 and User2.

You need to assign Role Based Access Control (RBAC) roles to User1 and User2 to meet the following requirements:

Which two roles should you assign?

A. The Monitoring Readers role in Azure AD Connect Health to User1

B. The Security reader role in Azure AD to User 1

C. The Reports reader role in Azure AD to User 1

D. The Contributor role in Azure AD Connect Health to User 2

E. The Monitoring Contributor role in Azure Connect Health to User 2

F. The Security operator role in Azure AD to User2

ANSWER: B D

QUESTION NO: 12

You have a Microsoft 365 subscription.

From the Microsoft 365 admin center, you create a new user.

You plan to assign the Reports reader role to the user.

You need to view the permissions of the Reports reader role.

Which admin center should you use?

A. Azure Active Directory

B. Cloud App Security

C. Security & Compliance

D. Microsoft 365

ANSWER: A

QUESTION NO: 13 - (DRAG DROP)

DRAG DROP

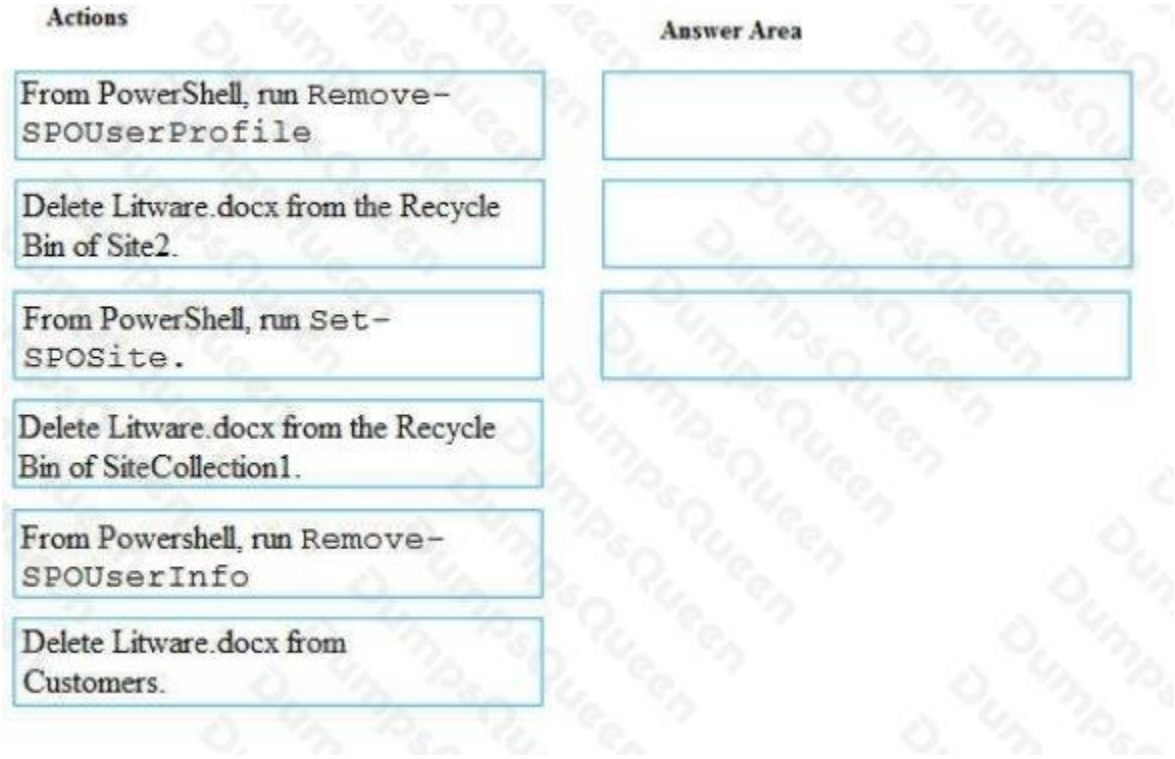
You have a Microsoft 365 subscription.

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

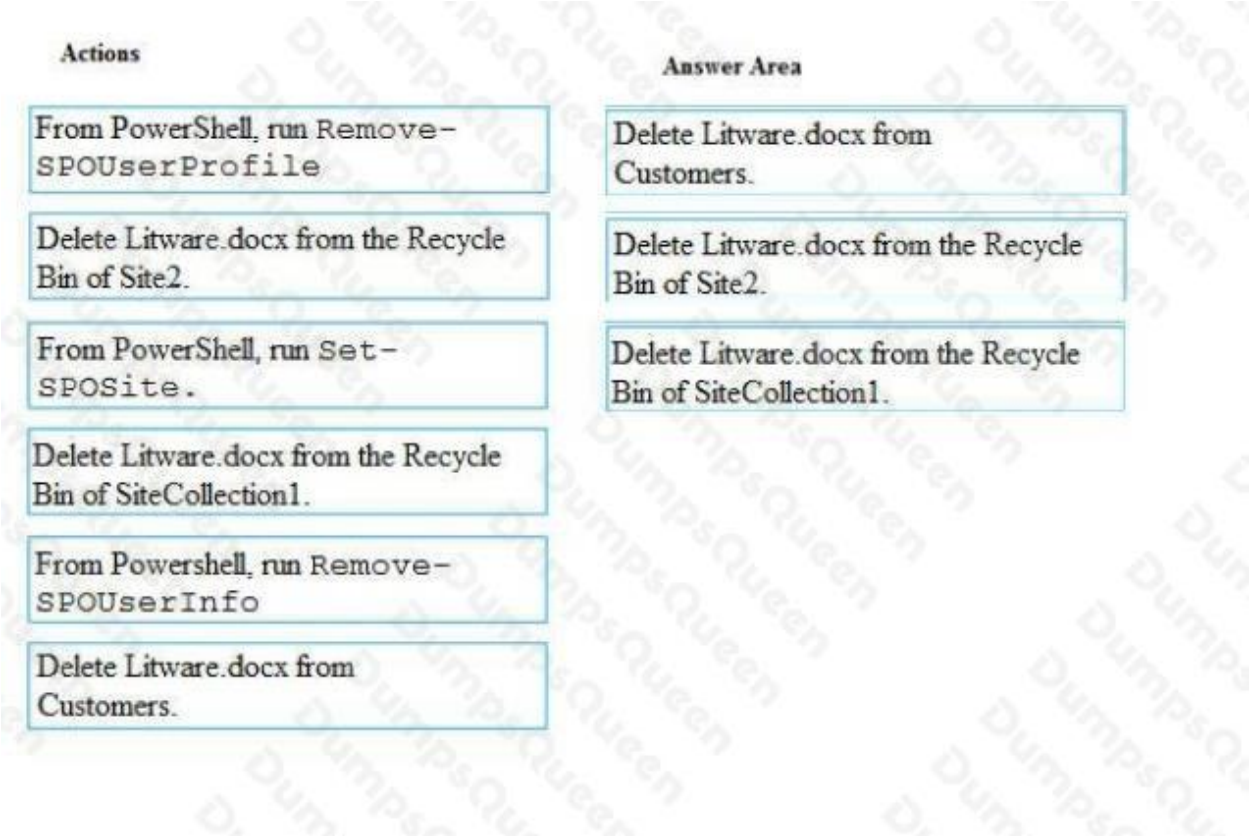
Customers contains a document named Litware.docx. You need to remove Litware.docx permanently.

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:



ANSWER:



Explanation:

QUESTION NO: 14

Which of the following O365-ATP safe attachment policies does not cause a message delivery delay? (Choose two.)

A. Off

B. Monitor

C. Replace

D. Block

E. Dynamic Delivery

ANSWER: A E

Explanation:

All delivery options other than dynamic and off requires ATP to sandbox-detonate attachments before delivery – even monitor.

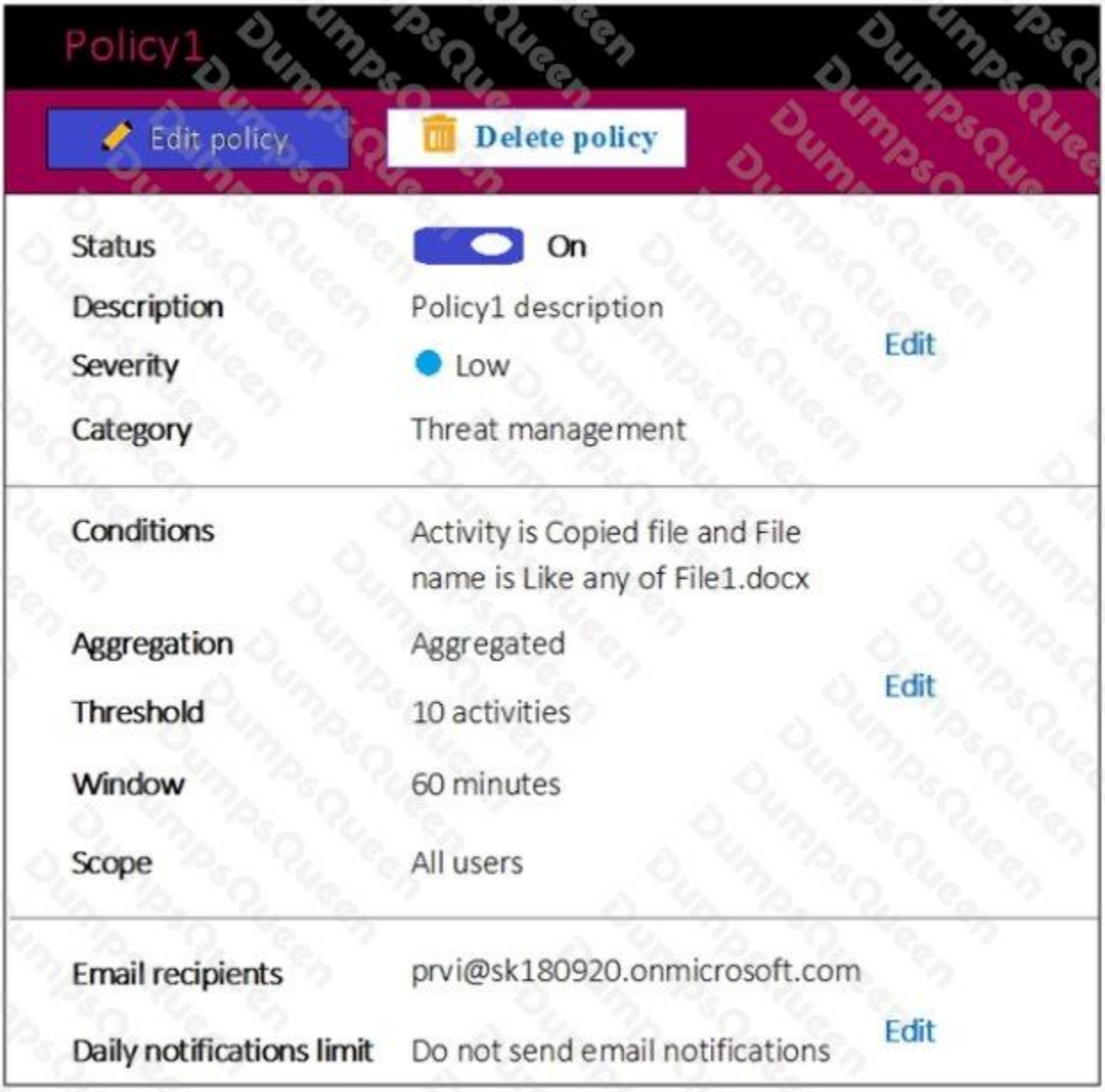
Reference: https://docs.microsoft.com/en-us/microsoft-365/security/office-365-security/set-up-atp-safe-attachments-policies?view=o365-worldwide

QUESTION NO: 15 - (HOTSPOT)

You have a Microsoft 365 subscription that include three users named User1, User2, and User3.

A file named File1.docx is stored in Microsoft OneDrive. An automated process updates File1.docx every minute.

You create an alert policy named Policy1 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.

If User1 runs a scheduled task that copies File1.docx to a local folder every five minutes. [answer choice].

- Policy1 will not be triggered
- Policy1 will be triggered after 45 minutes
- Policy1 will be triggered after 60 minutes

If User1, User2, and User3 each run a scheduled task that copies File1.docx to a local folder every 10 minutes. [answer choice].

- Policy1 will not be triggered
- Policy1 will be triggered within 20 minutes
- Policy1 will be triggered within 45 minutes
- Policy1 will be triggered after 60 minutes

ANSWER:

If User1 runs a scheduled task that copies File1.docx to a local folder every five minutes. [answer choice].

- Policy1 will not be triggered
- Policy1 will be triggered after 45 minutes
- Policy1 will be triggered after 60 minutes

If User1, User2, and User3 each run a scheduled task that copies File1.docx to a local folder every 10 minutes. [answer choice].

- Policy1 will not be triggered
- Policy1 will be triggered within 20 minutes
- Policy1 will be triggered within 45 minutes
- Policy1 will be triggered after 60 minutes

Explanation:

Answer Area

If User1 runs a scheduled task that copies File1.docx to a local folder every five minutes. [answer choice].

- Policy1 will not be triggered
- Policy1 will be triggered after 45 minutes
- Policy1 will be triggered after 60 minutes

If User1, User2, and User3 each run a scheduled task that copies File1.docx to a local folder every 10 minutes. [answer choice].

- Policy1 will not be triggered
- Policy1 will be triggered within 20 minutes
- Policy1 will be triggered within 45 minutes
- Policy1 will be triggered after 60 minutes

References:

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

QUESTION NO: 16 - (HOTSPOT)

You have a Microsoft 365 E5 subscription that contains two users named User1 and User2.

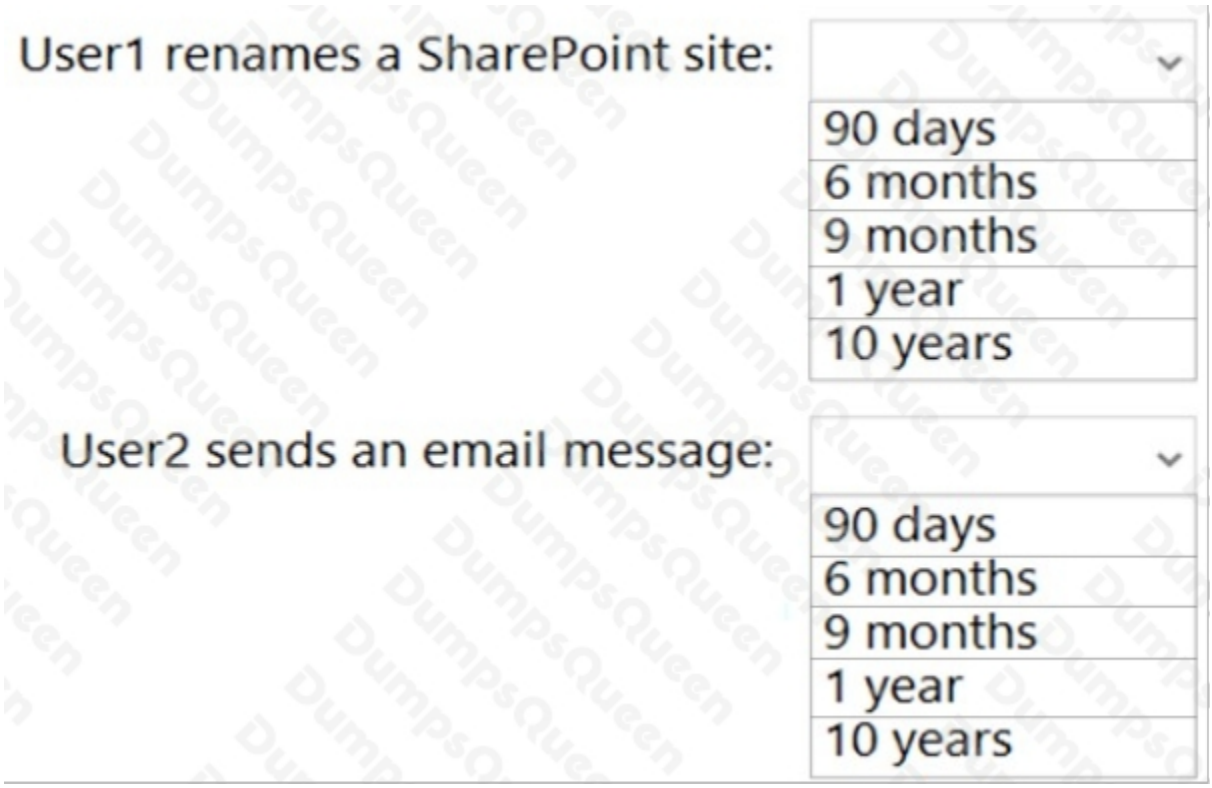
You create the audit retention policies shown in the following table.

Priority	Policy name	Record type	Activities	Users	Duration
10	AuditRetention1	ExchangeItem	MailboxLogin	**None**	90 Days
20	AuditRetention2	ExchangeItem	Send, MailItemsAccessed	User1	9 Months
30	AuditRetention3	Sharepoint	**None**	User1	6 Months
40	AuditRetention4	Sharepoint	SiteRenamed	User1	9 Months
50	AuditRetention5	Sharepoint	SiteRenamed	**None**	10 Years

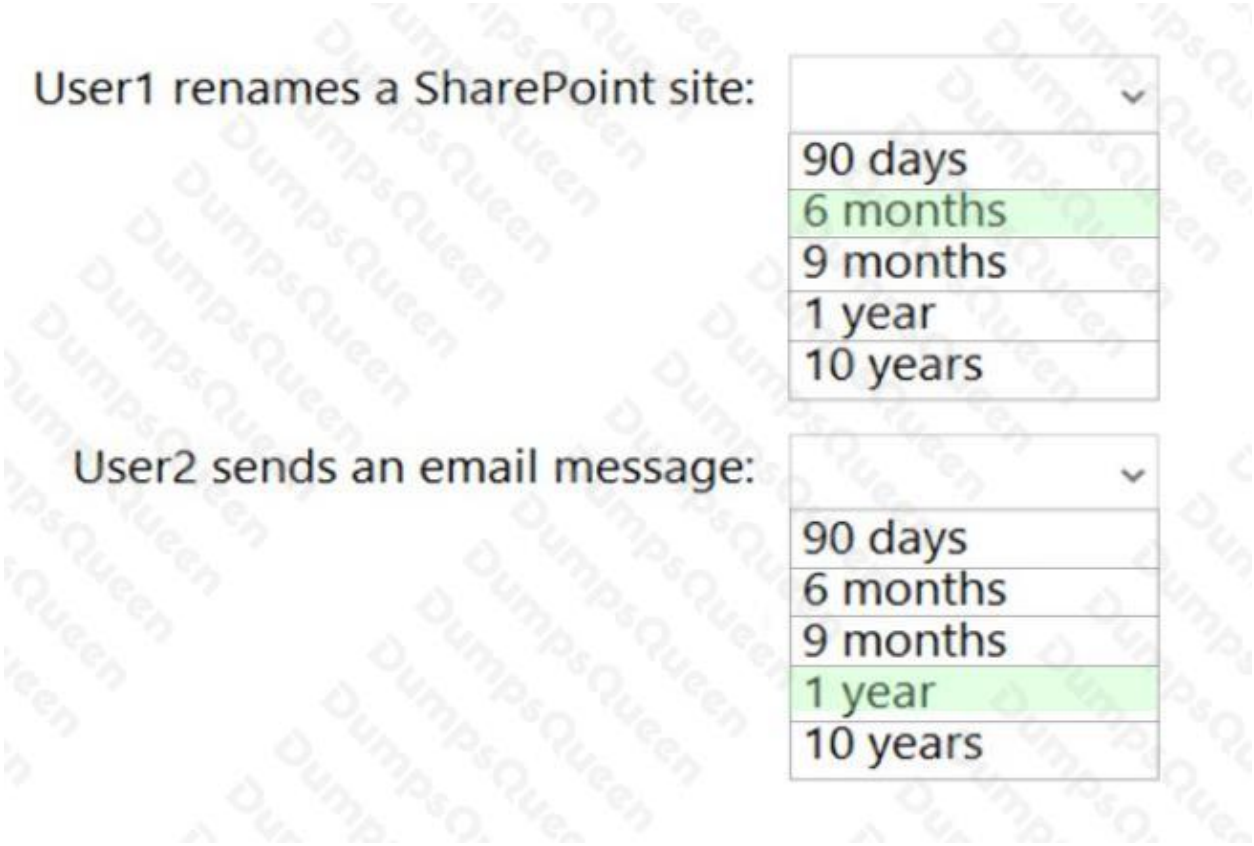
The users perform the following actions:

How long will the audit log records be retained for each action? To answer, select the appropriate options in the answer area.

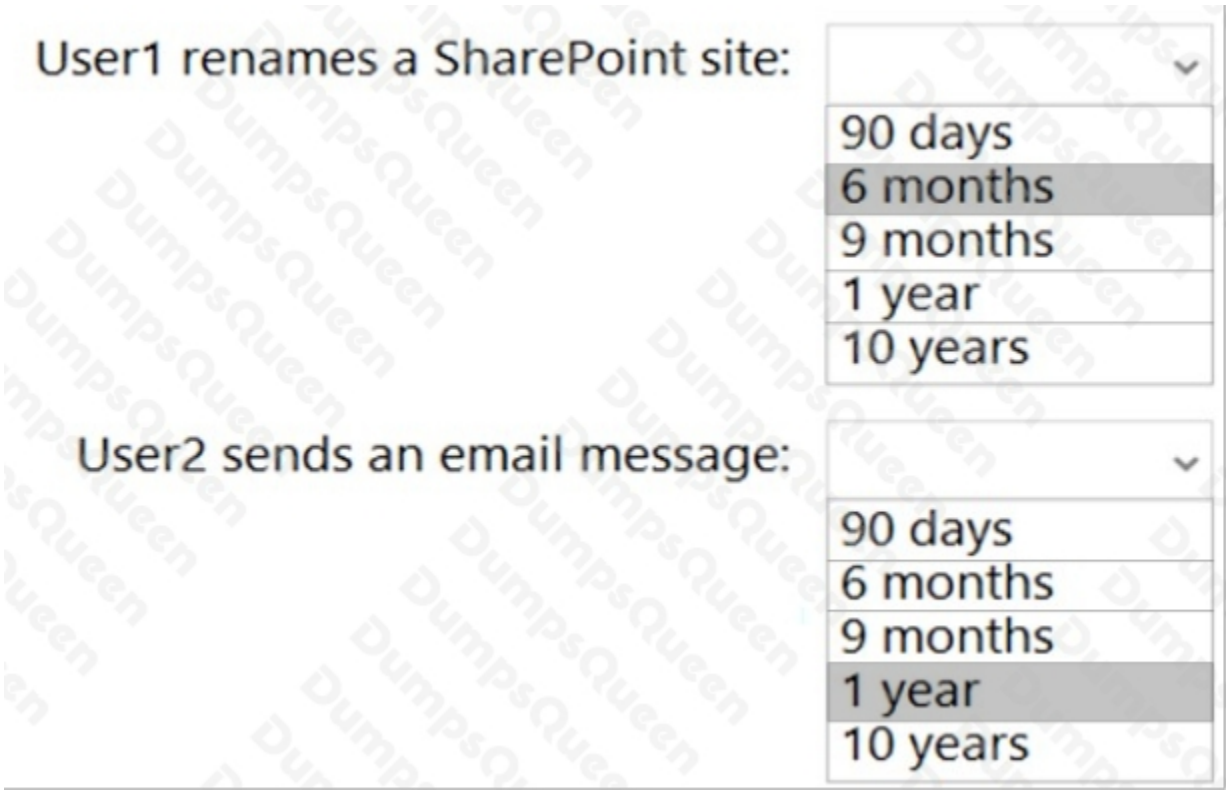
NOTE: Each correct selection is worth one point.


User1 renames a SharePoint site:
90 days
6 months
9 months
1 year
10 years
User2 sends an email message:
90 days
6 months
9 months
1 year
10 years

ANSWER:



Explanation:



Reference:

https://docs.microsoft.com/en-us/microsoft-365/compliance/audit-log-retention-policies?view=o365-worldwide

QUESTION NO: 17 - (SIMULATION)

Your on-premises network contains an Active Directory domain that syncs to Azure Active Directory (Azure AD) by using Azure AD Connect. The functional level of the domain. You need to deploy Windows Hello for Business. The solution must meet the following requirements:

• Ensure that users can access Microsoft 365 services and on-premises resources.

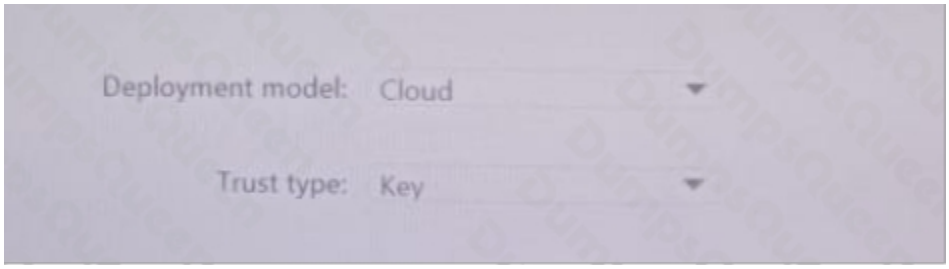
• Minimize administrative efforts

How should you deploy Windows Hello for Business, and which type of trust should you use? To answer, select the appropriate options in the answer area.

ANSWER: Seetheexplanationforanswer.

Explanation:

Answer is as below.



QUESTION NO: 18

You have a Microsoft 365 E5 subscription.

You plan to create a conditional access policy named Policy1.

You need to be able to use the sign-in risk level condition in Policy1.

What should you do first?

A. Connect Microsoft Endpoint Manager and Microsoft Defender for Endpoint.

B. From the Azure Active Directory admin center, configure the Diagnostics settings.

C. From the Endpoint Management admin center, create a device compliance policy.

D. Onboard Azure Active Directory (Azure AD) Identity Protection.

ANSWER: D

Explanation:

Reference:

https://docs.microsoft.com/en-us/azure/active-directory/conditional-access/howto-conditional-access-policy-risk

QUESTION NO: 19

You are testing the impact of Windows diagnostic data sent to Microsoft at different levels by changing the registry on your own computer.

What elements do you configure? (Choose all that apply.)

A. Registry key: HKEY_LOCAL_MACHINE\Software\Policies\Microsoft\Windows\Data Collection

B. Registry key: HKEY_LOCAL_MACHINE\Software\Policies\Microsoft\Windows\EventLog

C. Registry key: HKEY_LOCAL_MACHINE\Software\Policies\Microsoft\Windows\SettingSync

D. Value Name: (Default)

E. Value Name: EnablePeerCaching

F. Value Name: AllowTelemetry

G. Value Type: String

H. Value Type: Binary

I. Value Type: DWORD (32-bit) Value

J. Value Data: "Enhanced"

K. Value Data: 2

L. Value Data: 1

ANSWER: A F I K

Explanation:

These are also the registry entry made when Intune pushes a device configuration profile to a W10 machine.

Reference:

https://docs.microsoft.com/en-us/windows/privacy/configure-windows-diagnostic-data-in-your-organization#use-registry-editor-to-set-the-diagnostic-data-level

QUESTION NO: 20

You have a Microsoft 365 E5 subscription that contains the users shown1 in the following table.

Name	Email address	Role
Admin1	admin1@contoso.com	Global Administrator
Admin2	admin2@contoso.com	Security Administrator
Admin3	admin3@contoso.com	Security Reader
Admin4	admin4@contoso.com	User Administrator
User1	user1@contoso.com	*None*

Azure AD Identity Protection detects that the account of User1 is at risk and generates an alert. How many users will receive the alert?

A. 1

B. 2

C. 3

D. 4

E. 5

ANSWER: C