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.pass2lead.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 need to create a retention policy that contains a data label. The policy must delete all Microsoft Office 365 content that is older than six months.

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

Correct Answer: See explanation below.

Creating Office 356 labels is a two-step process. The first step is to create the actual label which includes the name, description, retention policy, and classifying the content as a record. Once this is completed, the second step requires the deployment of a label using a labelling policy which specifies the specific location to publish and applying the label automatically.

To create an Office 365 label, following these steps:

1.

Open Security and Compliance Centre;

2.

Click on Classifications;

3.

Click on Labels;

4.

The label will require configuration including: name your label (Name), add a description for the admins (Description for Admins), add a description for the users (Description for Users);

5.

Click Next once the configuration is completed;

6.

Click Label Settings on the left-hand side menu;

7.

The Label Settings will need to be configured. On this screen, you can toggle the Retention switch to either “on” or “off”. If you choose “on”, then you can answer the question “When this label is applied to content” with one of two options. The first option is to Retain the Content. From the pick boxes, you can choose the length of retention and upon the end of the retention, the action that will take place. The three actions are to delete the data, trigger an approval flow for review, or nothing can be actioned. The second option is to not retain the data after a specified amount of time or based on the age of the data; and

8.

The label has now been created.

To create a label policy, follow these steps:

1.

Open Security and Compliance Centre;

2.

Click on Data Governance, Retention;

3.

Choose Label Policies box at the top of the screen; and

4.

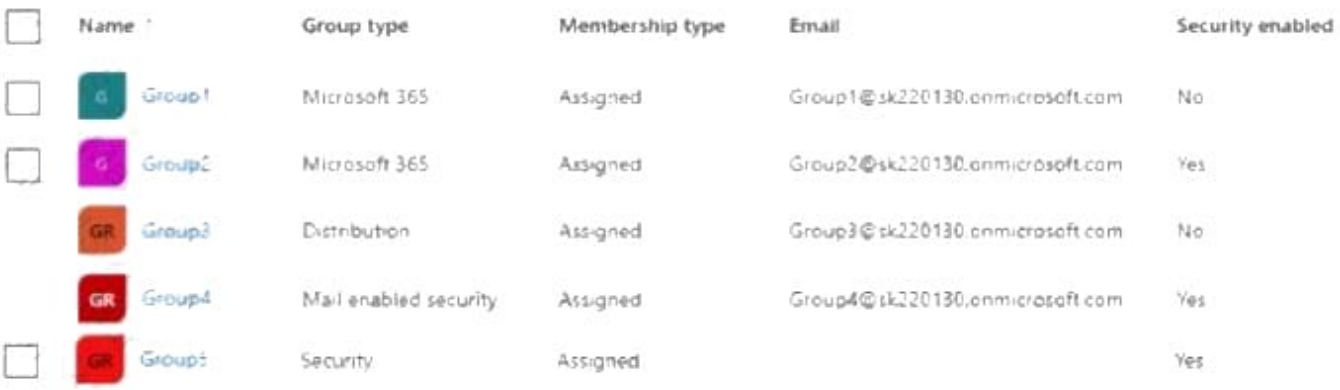
There are now two options. The first is to Publish Labels. If your organization wants its end users to apply the label manually, then this is the option you would choose. Note that this is location based. The second option is to Auto-apply Labels. With Auto-apply, you would have the ability to automatically apply a label when it meets the specified criteria.

References: https://www.maadarani.com/office-365-classification-and-retention-labels/

QUESTION 2

HOTSPOT

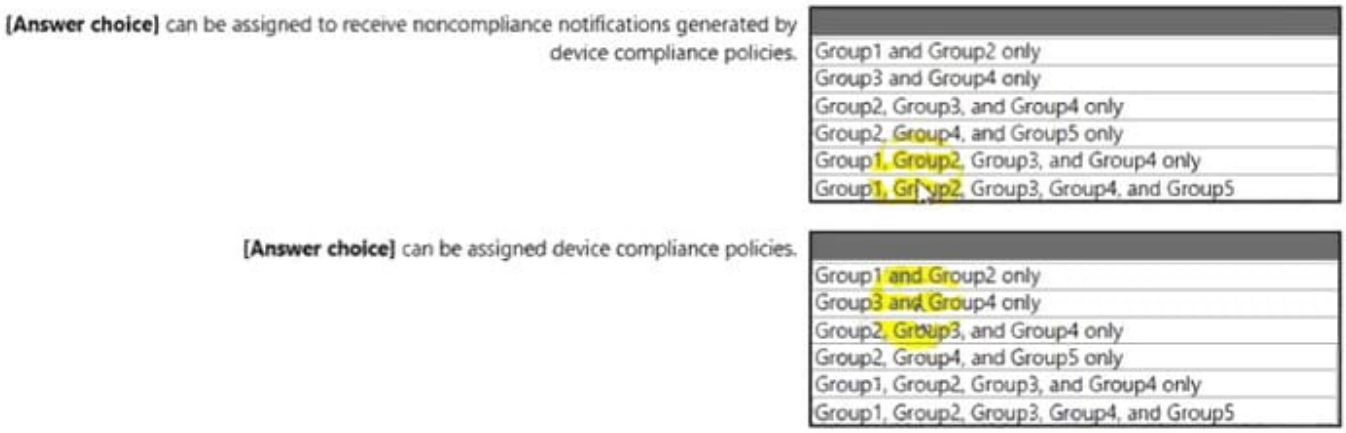
You have a Microsoft 365 subscription that contains the groups shown in the following exhibit.



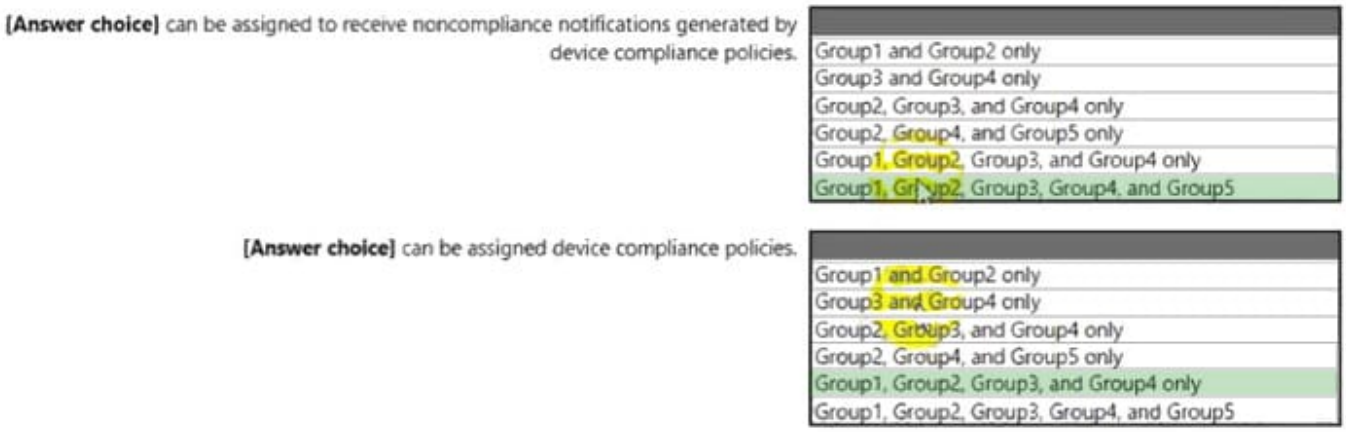
Name	Group type	Membership type	Email	Security enabled
Group1	Microsoft 365	Assigned	Group1@sk220130.onmicrosoft.com	No
Group2	Microsoft 365	Assigned	Group2@sk220130.onmicrosoft.com	Yes
Group3	Distribution	Assigned	Group3@sk220130.onmicrosoft.com	No
Group4	Mail enabled security	Assigned	Group4@sk220130.onmicrosoft.com	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 3

You have a Microsoft 365 subscription named contoso.com.

You need to configure Microsoft OneDrive for Business external sharing to meet the following requirements:

1.

Enable file sharing for users that have a Microsoft account.

2.

Block file sharing for anonymous users. What should you do?

A. From Advanced settings for external sharing, select Allow or block sharing with people on specific domains and add contoso.com.

B. From the External sharing settings for OneDrive, select Only people in your organization.

C. From the External sharing settings for OneDrive, select Existing external users.

D. From the External sharing settings for OneDrive, select New and existing external users.

Correct Answer: D

Reference: https://www.sharepointdiary.com/2020/09/enable-external-sharing-in-onedrive-for-business.html

QUESTION 4

Which role should you assign to User1?

A. Global administrator

B. User administrator

C. Privileged role administrator

D. Security administrator

Correct Answer: C

This role grants the ability to manage assignments for all Azure AD roles including the Global Administrator role. This role does not include any other privileged abilities in Azure AD like creating or updating users. However, users assigned to this role can grant themselves or others additional privilege by assigning additional roles.
https://docs.microsoft.com/en-us/azure/active-directory/privileged-identity-management/pim-how-to-give-access

QUESTION 5

You have a Microsoft 365 subscription that contains 100 users and a Microsoft 365 group named Group1.

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

A sensitivity label named Label1 is published as the default label for Group1.

You add two sublabels named Sublabel1 and Sublabel2 to Label1.

You need to ensure that the settings in Sublabel1 are applied by default to Group1.

What should you do?

A. Change the order of Sublabel1.

B. Modify the policy of Label1.

C. Duplicate all the settings from Sublabel1 to Label1.

D. Delete the policy of Label1 and publish Sublabel1.

Correct Answer: B

To ensure that the settings in Sublabel1 are applied by default to Group1, you need to modify the policy of Label1. As Label1 is the default label for Group1, any changes made to the policy of Label1 will be applied by default to Group1.

Therefore, modifying the policy of Label1 to include the settings in Sublabel1 will ensure that these settings are applied by default to Group1.

Option A, changing the order of Sublabel1, will not have any effect on which settings are applied by default to Group1.

Option C, duplicating all the settings from Sublabel1 to Label1, is unnecessary and will not ensure that the settings in Sublabel1 are applied by default to Group1.

Option D, deleting the policy of Label1 and publishing Sublabel1, will remove Label1 as the default label for Group1, and it will not ensure that the settings in Sublabel1 are applied by default to Group1.

Reference:

https://docs.microsoft.com/en-us/microsoft-365/compliance/sensitivity-labels?view=o365-worldwide

QUESTION 6

HOTSPOT

You have a Microsoft 365 E5 tenant that contains a published sensitivity label named Sensitivity1.

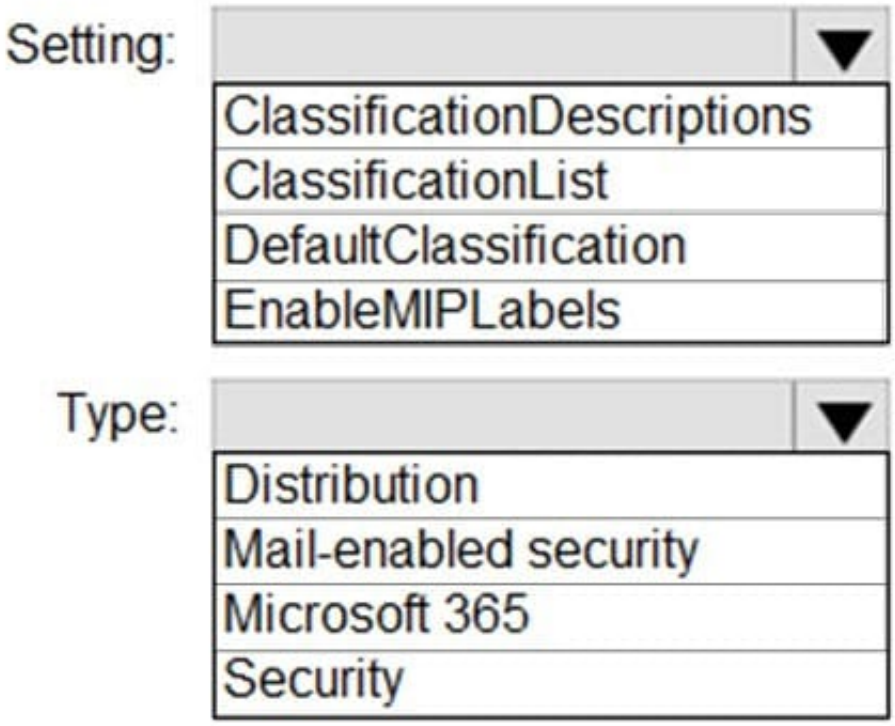
You plan to create an Azure Active Directory group named Group1 and assign Sensitivity1 to Group1.

How should you configure Group1? To answer, select the appropriate options in the answer area.

NOTE: Each correct selection is worth one point.

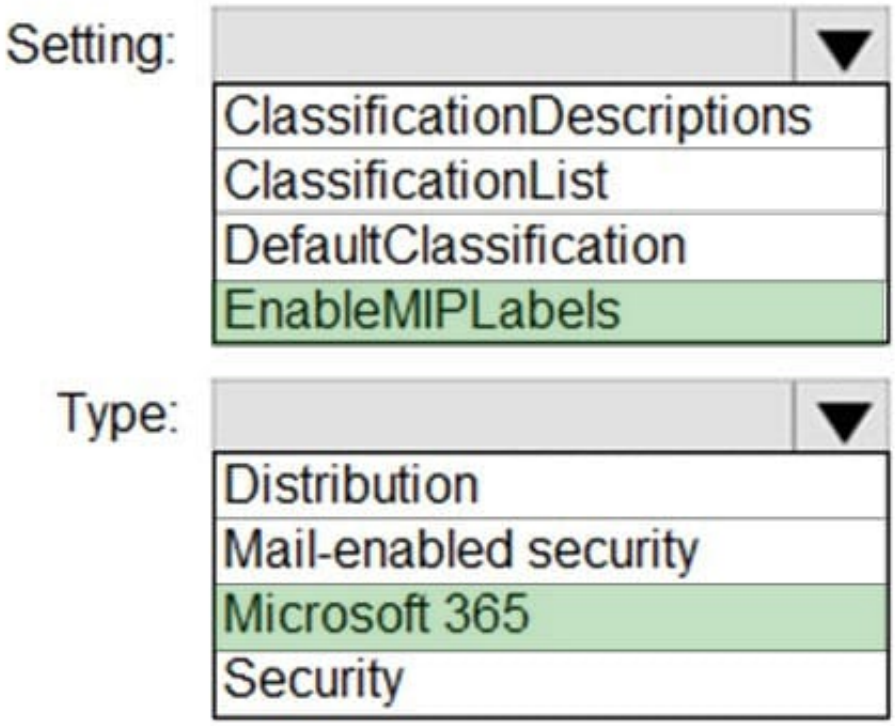
Hot Area:

Answer Area



Correct Answer:

Answer Area



Box 1: EnableMIPLabels

The sensitivity label option is only displayed for groups when all the following conditions are met:

1.

The feature is enabled, EnableMIPLabels is set to True in from the Azure AD PowerShell module.

2.

The group is a Microsoft 365 group.

3.

Etc.

Box 2: Microsoft 365 Incorrect:

* Not ClassificationList:

Classic classifications are the old classifications you set up by defining values for the ClassificationList setting in Azure AD PowerShell. When this feature is enabled, those classifications will not be applied to groups.

Reference: https://docs.microsoft.com/en-us/azure/active-directory/enterprise-users/groups-assign-sensitivity-labels

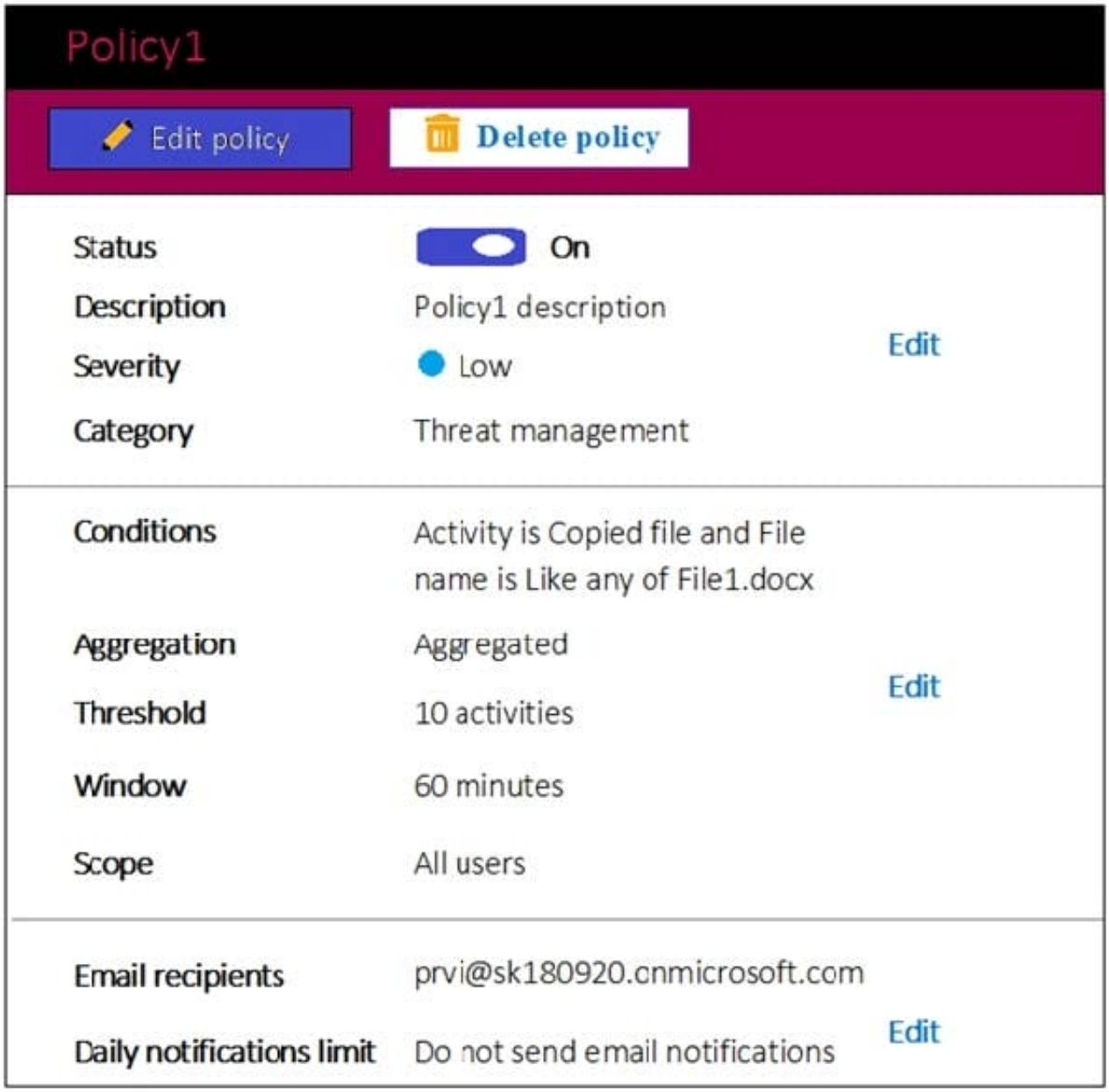
QUESTION 7

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.

Hot Area:

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

Correct Answer:

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 8

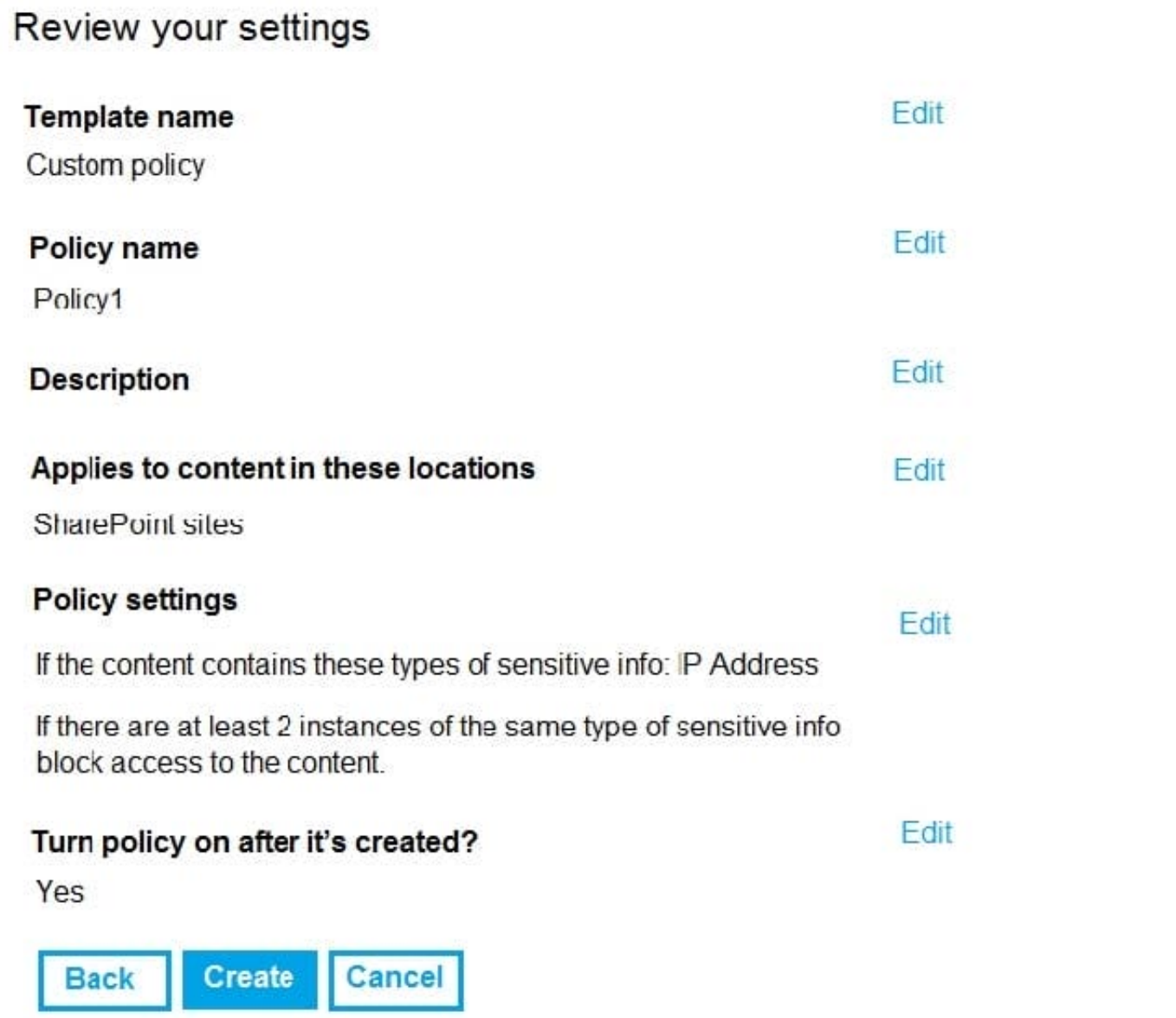
HOTSPOT

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

You have a Microsoft SharePoint site named Site1. Site1 stores files that contain IP addresses as shown in the following table.

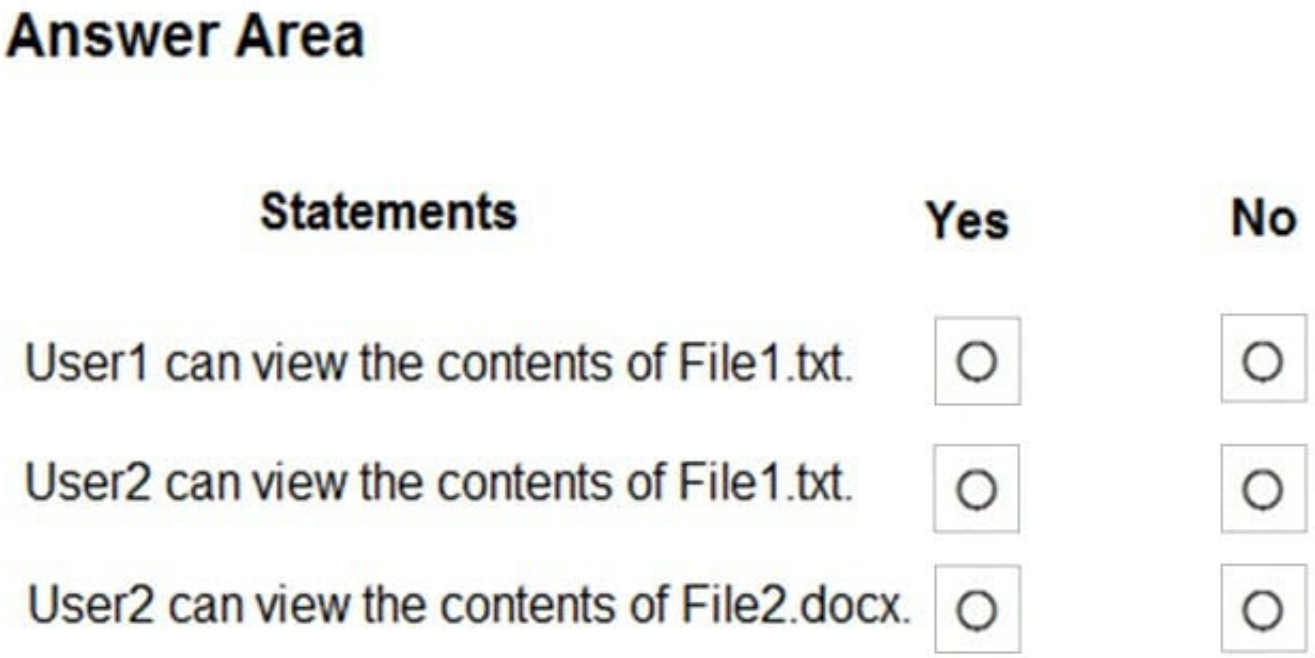
Name	Number of IP addresses
File1.txt	3
File2.docx	1

User1 is assigned the SharePoint admin role for Site1. User2 is a member of Site1. You create the data loss prevention (DLP) policy shown in the following exhibit.

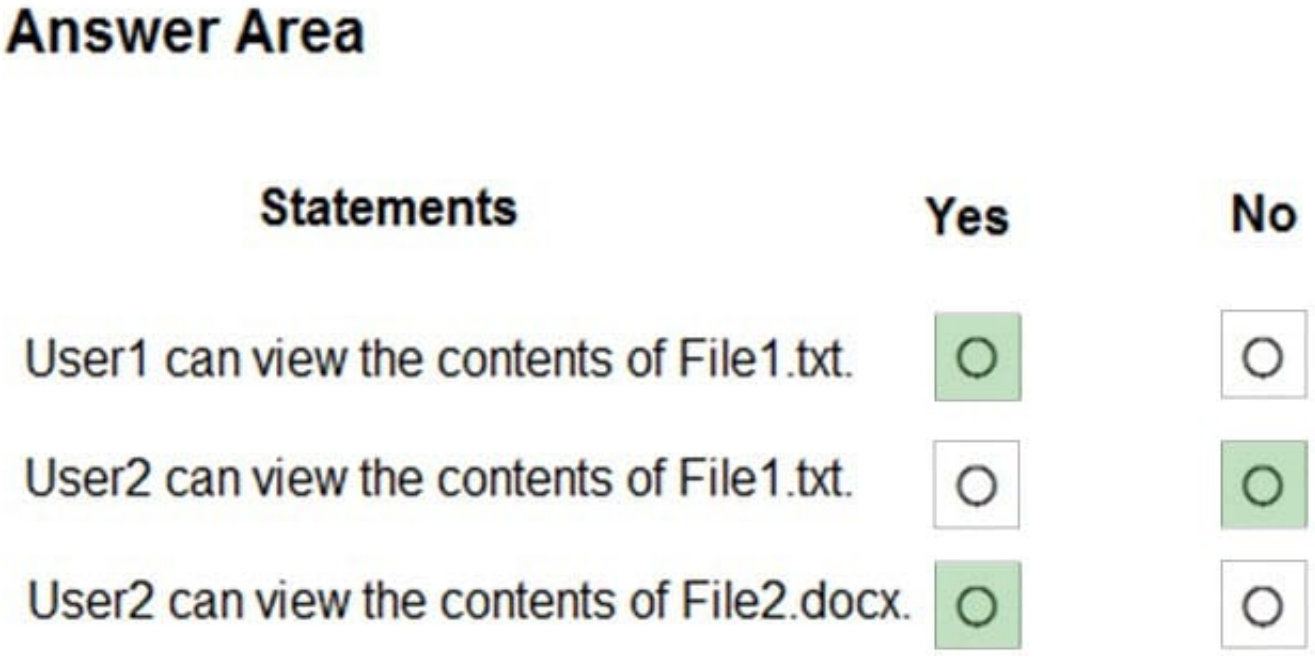


For each of the following statements, select Yes if the statement is true. Otherwise, select No. NOTE: Each correct selection is worth one point.

Hot Area:



Correct Answer:



Box 1: Yes Note: Key tasks of the SharePoint admin Here are some of the key tasks users can do when they are assigned to the SharePoint admin role:

Create sites

Delete sites

Manage sharing settings at the organization level

Add and remove site admins Manage site storage limits Box 2: No

File1.text contains 3 IP addresses.

Box 3: Yes

File2.docx contains only 1 IP address.

QUESTION 9

HOTSPOT

You have a Microsoft 365 subscription.

You configure Microsoft Defender for Endpoint as shown in the following table.

Device group	Automation level
Group1	Full – remediate threats automatically
Group2	Semi – require approval for core folders
Group3	Semi – require approval for all folders

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

Name	In device group
Device1	Group1
Device2	Group2
Device3	Group3

Microsoft Defender for Endpoint contains the incidents shown in the following table.

Name	Device	File evidence	File verdict
Case1	Device1	C:\Temp\File1.exe	Suspicious
Case2	Device2	C:\Temp\File2.exe	Malicious
Case3	Device3	C:\Temp\File3.exe	Malicious

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
C:\Temp\File1.exe will be remediated automatically.	○	○
C:\Temp\File2.exe will be remediated automatically.	○	○
C:\Temp\File3.exe will be remediated automatically.	○	○

Correct Answer:

Answer Area

Statements	Yes	No
C:\Temp\File1.exe will be remediated automatically.	○	○
C:\Temp\File2.exe will be remediated automatically.	○	○
C:\Temp\File3.exe will be remediated automatically.	○	○

Box 1: No

File1.exe on Device1 is suspicious. Device1 is in Group1. Group1 has automation level Full - remediate threats automatically.

Note: Full automation (recommended) means remediation actions are taken automatically on artifacts determined to be malicious.

Box 2: Yes

File2 on Device2 is malicious. Device2 is in Group2. Group2 has automation level Semi - require approval for core folders.

Note: Semi-automation means some remediation actions are taken automatically, but other remediation actions await approval before being taken.

Semi - require approval for core folders remediation:

With this level of semi-automation, approval is required for any remediation actions needed on files or executables that are in core folders. Core folders include operating system directories, such as the Windows (\windows*).

Remediation actions can be taken automatically on files or executables that are in other (non-core) folders.

Box 3: No

File3 on Device3 is malicious. Device3 is in Group3. Group3 has automation level Semi - require approval for all folders.

Reference:

https://docs.microsoft.com/en-us/microsoft-365/security/defender-endpoint/automation-levels

QUESTION 10

HOTSPOT

You have a Microsoft Azure Active Directory (Azure AD) tenant named contoso.com that contains the users shown in the following table.

Name	Member of	Multi-factor authentication (MFA) status
User1	Group1, Group2	Disabled
User2	Group1	Disabled

You create and enforce an Azure AD Identity Protection sign-in risk policy that has the following settings:

1.

Assignments: Include Group1, Exclude Group2

2.

Conditions: Sign in risk of Low and above

3.

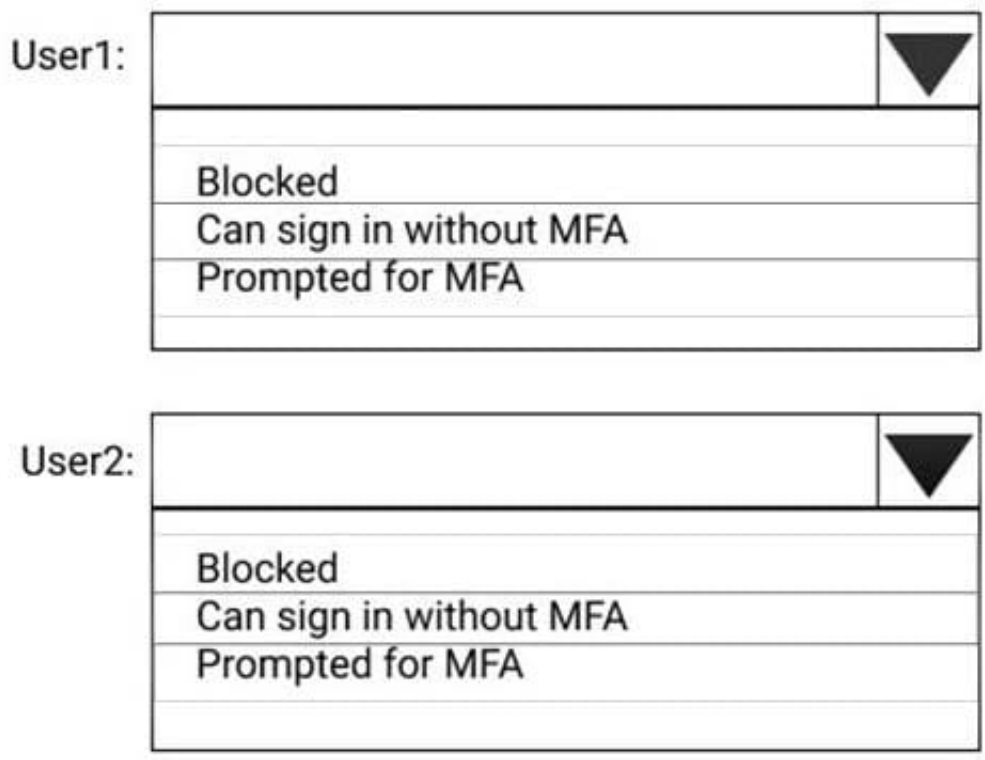
Access: Allow access, Require password multi-factor authentication

You need to identify how the policy affects User1 and User2.

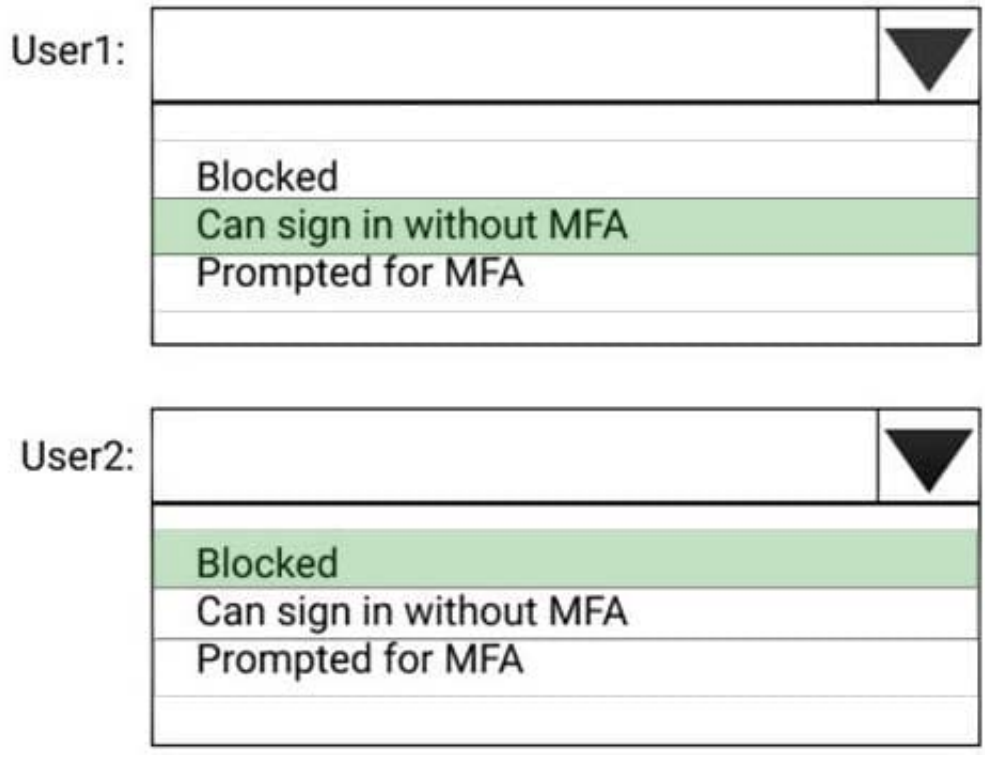
What occurs when each user signs in from an anonymous IP address? To answer, select the appropriate options in the answer area.

NOTE: Each correct selection is worth one point.

Hot Area:



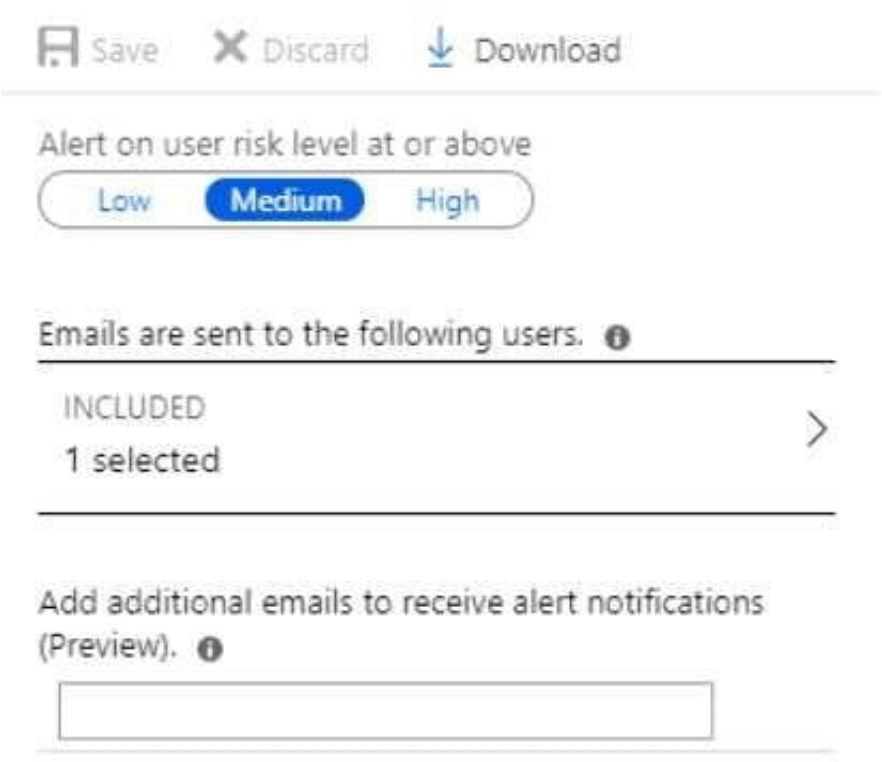
Correct Answer:



QUESTION 11

HOTSPOT

You have a Microsoft 365 E5 subscription that contains an Azure Active Directory (Azure AD) tenant named contoso.com. Azure AD Identity Protection alerts for contoso.com are configured as shown in the following exhibit.



A user named User1 is configured to receive alerts from Azure AD Identity Protection. You create users in contoso.com as shown in the following table.

Name	Role
User2	Security reader
User3	User administrator
User4	*None*
User5	*None*

The users perform the sign-ins shown in the following table.

Time	User	Risk event type
13:00	User4	Sign-ins from infected device
14:00	User4	Sign-in from unfamiliar location
15:00	User5	Sign-ins from anonymous IP address

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:

Statements	Yes	No
User1 receives three email alerts from Azure AD Identity Protection.	○	○
User2 receives three email alerts from Azure AD Identity Protection.	○	○
User3 receives two email alerts from Azure AD Identity Protection.	○	○

Correct Answer:

Statements	Yes	No
User1 receives three email alerts from Azure AD Identity Protection.	○	○
User2 receives three email alerts from Azure AD Identity Protection.	○	○
User3 receives two email alerts from Azure AD Identity Protection.	○	○

Box 1: No

User1 will receive the two alerts classified as medium or higher. Sign-ins from infected device is classified as low. This risk detection identifies IP addresses, not user devices. If several devices are behind a single IP address, and only some

are controlled by a bot network, sign-ins from other devices my trigger this event unnecessarily, which is why this risk detection is classified as Low.

Box 2: No

User2 will receive the two alerts classified as medium or higher. Email alerts are sent to all global admins, security admins and security readers Sign-ins from infected device is classified as low. This risk detection identifies IP addresses, not

user devices. If several devices are behind a single IP address, and only some are controlled by a bot network, sign-ins from other devices my trigger this event unnecessarily, which is why this risk detection is classified as Low.

Box 3: No

User3 will not receive alters.

Email alerts are sent to all global admins, security admins and security readers.

Reference:

https://docs.microsoft.com/en-us/azure/active-directory/identity-protection/overview-identity-protection

https://docs.microsoft.com/en-us/azure/active-directory/identity-protection/howto-identity-protection-configure-risk-policies

QUESTION 12

HOTSPOT

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

Name	Department	Microsoft 365 role
Admin1	IT	Groups admin
Admin2	IT	User admin
Admin3	Research	User admin
Admin4	Finance	Groups admin

For contoso.com, you create a group naming policy that has the following configuration.

-

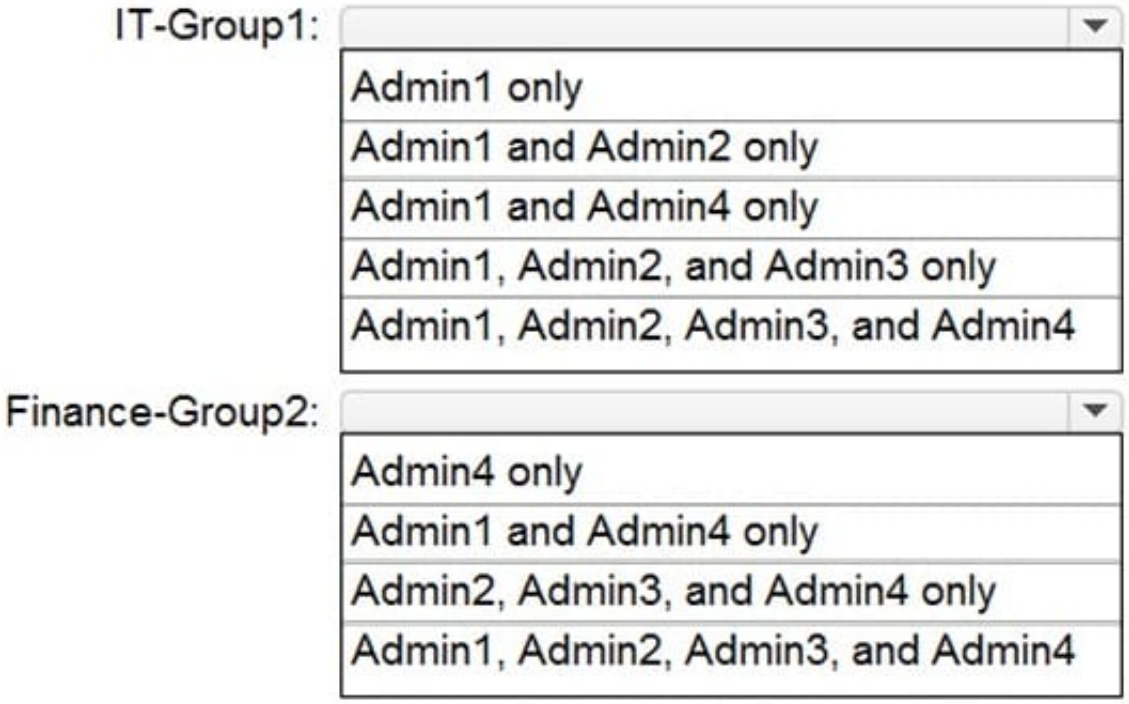
You plan to create the groups shown in the following table.

Name	Type
IT-Group1	Microsoft 365
Finance-Group2	Security

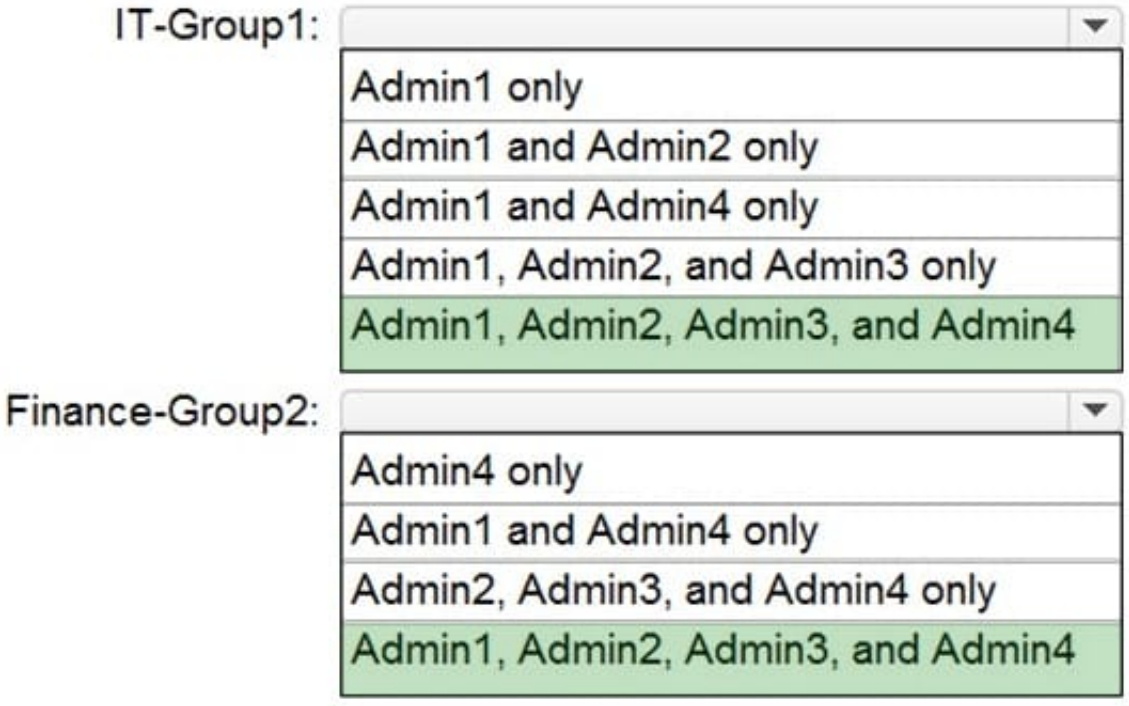
Which users can be used to create each group? To answer, select the appropriate options in the answer area.

NOTE: Each correct selection is worth one point.

Hot Area:



Correct Answer:



Reference:

https://office365itpros.com/2020/01/22/using-groups-admin-role/

https://docs.microsoft.com/en-us/azure/active-directory/roles/permissions-reference

QUESTION 13

You need to configure threat detection for Active Directory. The solution must meet the security requirements.

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.

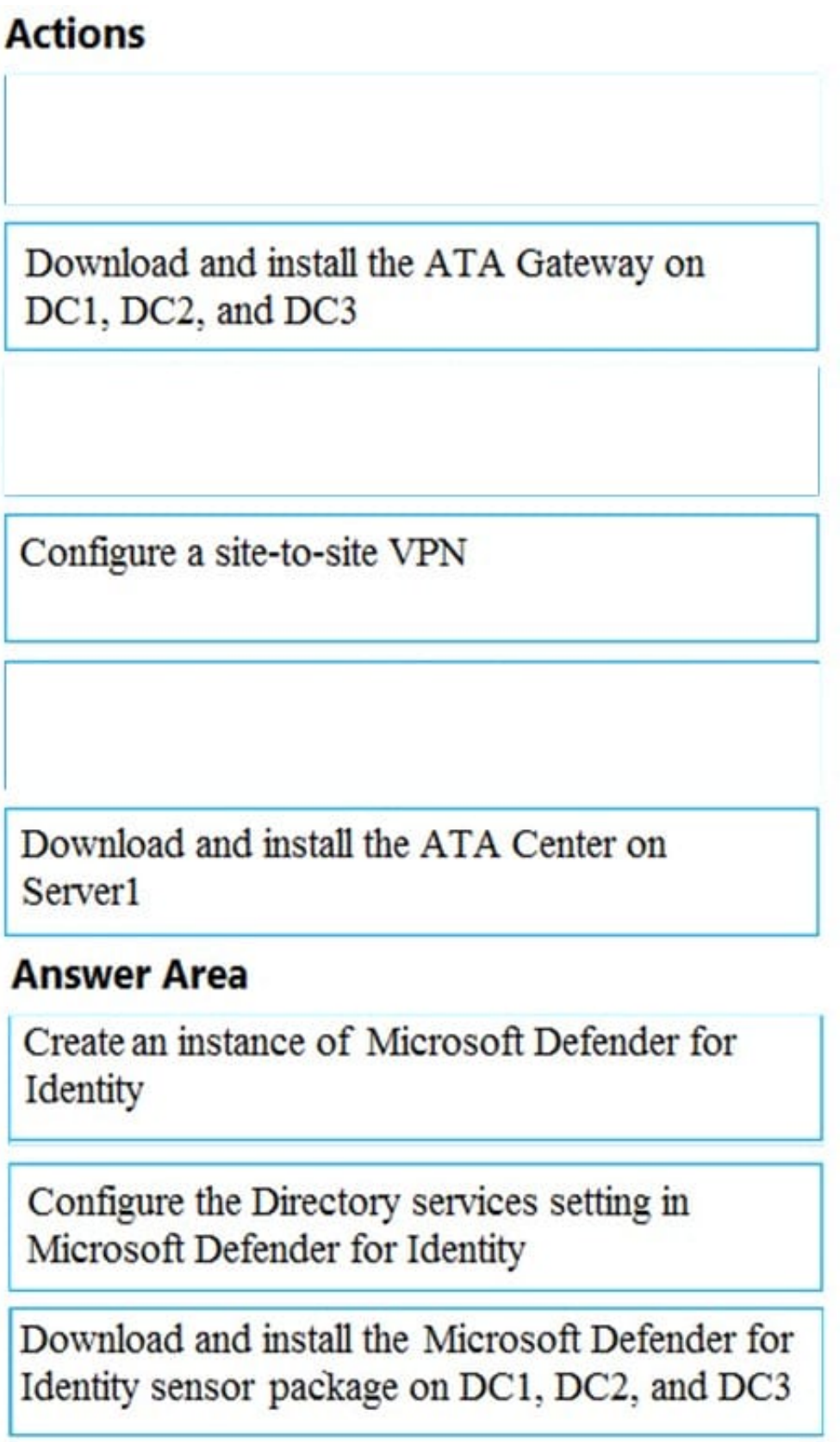
Select and Place:

Actions

- Configure the Directory services setting in Microsoft Defender for Identity
- Download and install the ATA Gateway on DC1, DC2, and DC3
- Download and install the Microsoft Defender for Identity sensor package on DC1, DC2, and DC3
- Configure a site-to-site VPN
- Create an instance of Microsoft Defender for Identity
- Download and install the ATA Center on Server1

Answer Area

Correct Answer:



Reference: https://docs.microsoft.com/en-us/defender-for-identity/install-step1

QUESTION 14

Your company uses Microsoft Azure Advanced Threat Protection (ATP).

You enable the delayed deployment of updates for an Azure ATP sensor named Sensor1.

How long after the Azure ATP cloud service is updated will Sensor1 be updated?

A. 7 days

B. 24 hours

C. 1 hour

D. 48 hours

E. 12 hours

Correct Answer: B

Note: The delay period was 24 hours. In ATP release 2.62, the 24 hour delay period has been increased to 72 hours.

QUESTION 15

You create a label that encrypts email data. Users report that they cannot use the label in Outlook on the web to protect the email messages they send.

You need to ensure that the users can use the new label to protect their email.

What should you do?

A. Modify the priority order of label policies

B. Wait six hours and ask the users to try again

C. Create a label policy

D. Create a new sensitive information type

Correct Answer: C

Admin has to publish labels by creating label policy.

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