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.leads4pass.com/ms-500.html

100% Passing Guarantee
100% Money Back Assurance

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

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

HOTSPOT

You have a Microsoft 365 E5 subscription.

From Microsoft Azure Active Directory (Azure AD), you create a security group named Group1. You add 10 users to Group1.

You need to apply app enforced restrictions to the members of Group1 when they connect to Microsoft Exchange Online from non-compliant devices, regardless of their location.

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 Azure portal, create a conditional access policy and configure:

Users and groups, Cloud apps, and Session settings Users and groups, Cloud apps, and Conditions settings Users and groups, Conditions, and Session settings	V

From an Exchange Online Remote PowerShell session, run:

New-OwaMailbox Policy and Set-OwaMailboxPolicy New-ClientAccessRule and Test-ClientAccessRule Get-CASMailbox and Set-CASMailbox	V

Correct Answer:

Answer Area

From the Azure portal, create a conditional access policy and configure:

Users and groups, Cloud apps, and Session settings Users and groups, Cloud apps, and Conditions settings Users and groups, Conditions, and Session settings	V

From an Exchange Online Remote PowerShell session, run:

New-OwaMailbox Policy and Set-OwaMailboxPolicy New-ClientAccessRule and Test-ClientAccessRule Get-CASMailbox and Set-CASMailbox	V

Reference: https://docs.microsoft.com/en-us/azure/active-directory/conditional-access/app-based-conditional-access

QUESTION 3

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.

-

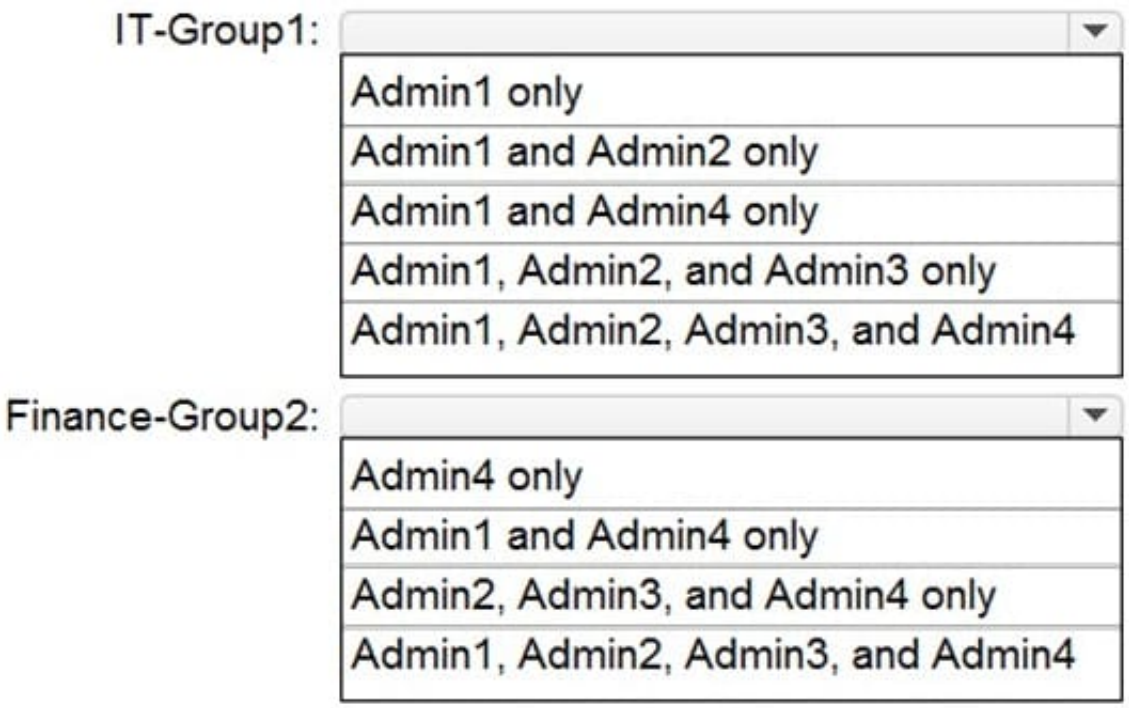
You plan to create the groups shown in the following table.

Name	Type
IT-Group1	Microsoft 365
Finance-Group2	Security

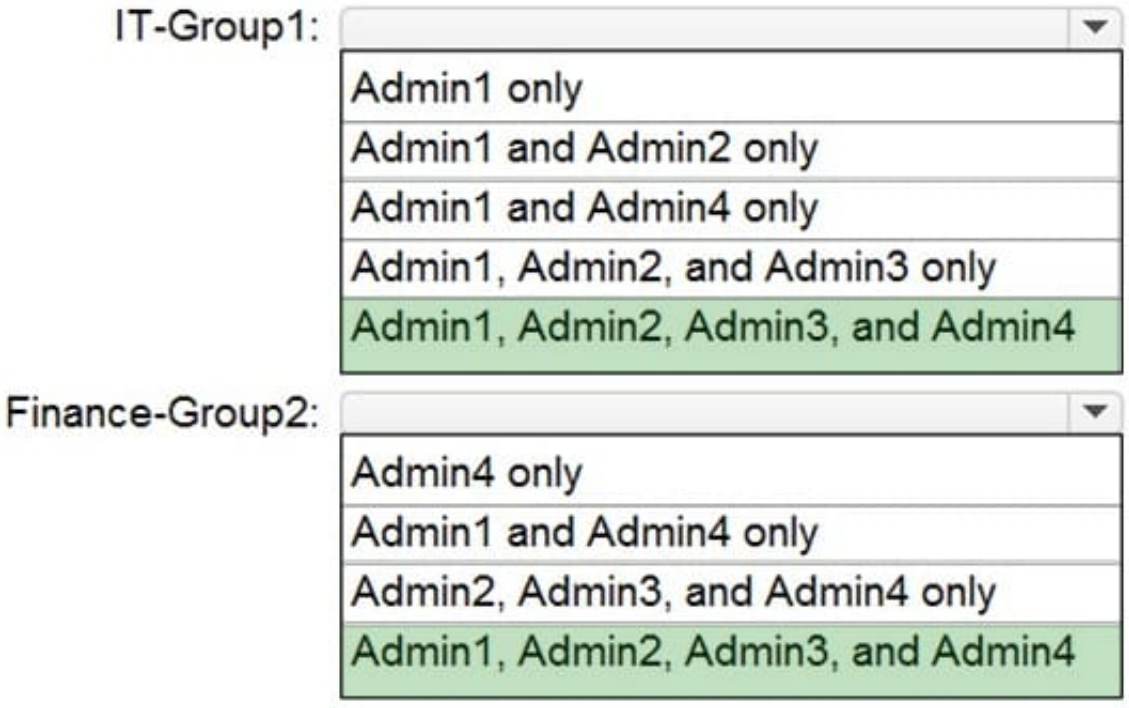
Which users can be used to create each group? To answer, select the appropriate options in the answer area.

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 4

HOTSPOT

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

User	Security group	Azure Active Directory (Azure AD)role
User1	ADGroup1	Security administrator
User2	ADGroup2	Application administrator
User3	ADGroup3	User administrator

You have the devices shown in the following table.

User	Operating system	Onboarded to Microsoft Defender for Endpoint
Device1	Windows 10	Yes
Device2	Windows 8.1	Yes
Device3	Windows 10	Yes

You have the Microsoft Defender for Endpoint portal roles shown in the following table.

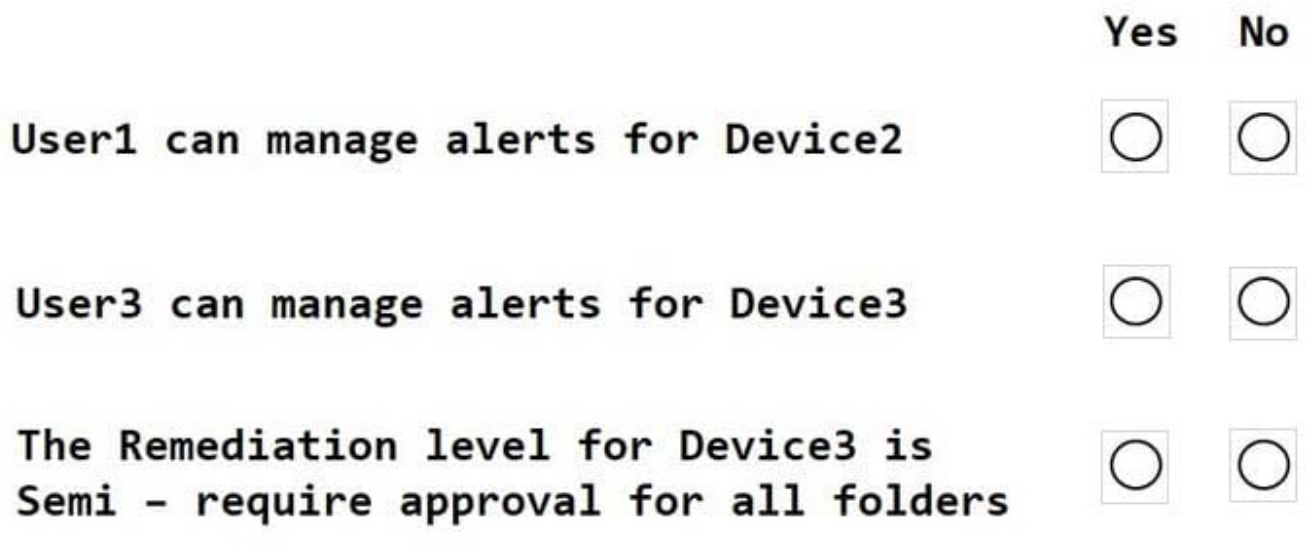
Name	Assigned to
Role1	ADGroup1
Role2	ADGroup2
Role3	ADGroup3

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

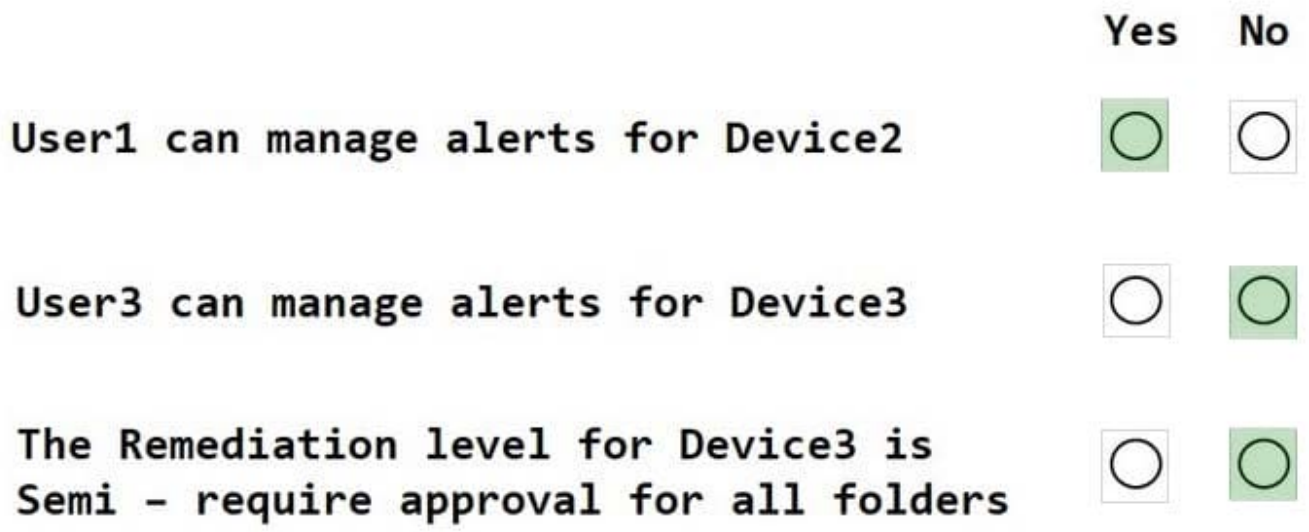
Name	Remediation level	Rank	Role	Members
Group1	Full-remediate threats automatically	1	Role1	OS:Windows 10
Group2	Semi-require approval for all folders	2	Role2	OS:Windows 8.1
Group3	Semi-require approval for all folders	3	Role3	OS:Windows 10

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:



Box1 - User1 can manage alerts for Device2 ? Yes Reason: User1 is security administrator. By default he has full access. When you first log in to the Microsoft 365 Defender portal, you\\'re granted either full access or read only access. Full access rights are granted to users with Security Administrator or Global Administrator roles in Azure AD. Box2 - User3 can manage alerts for Device3 ? No Reason: User3 (User Administrator) has no default access. He is a member of ADGroup3. Role 3 is assigned to ADGroup3. Remediation level for Group3: Semi – Require approval for all folders So user3 cannot manage alerts for Device3

Box3: Remediation level for device3: Semi – Require approval for all folders ? No

Device3 is Windows 10 device and will match Group1 (Highest Rank group)

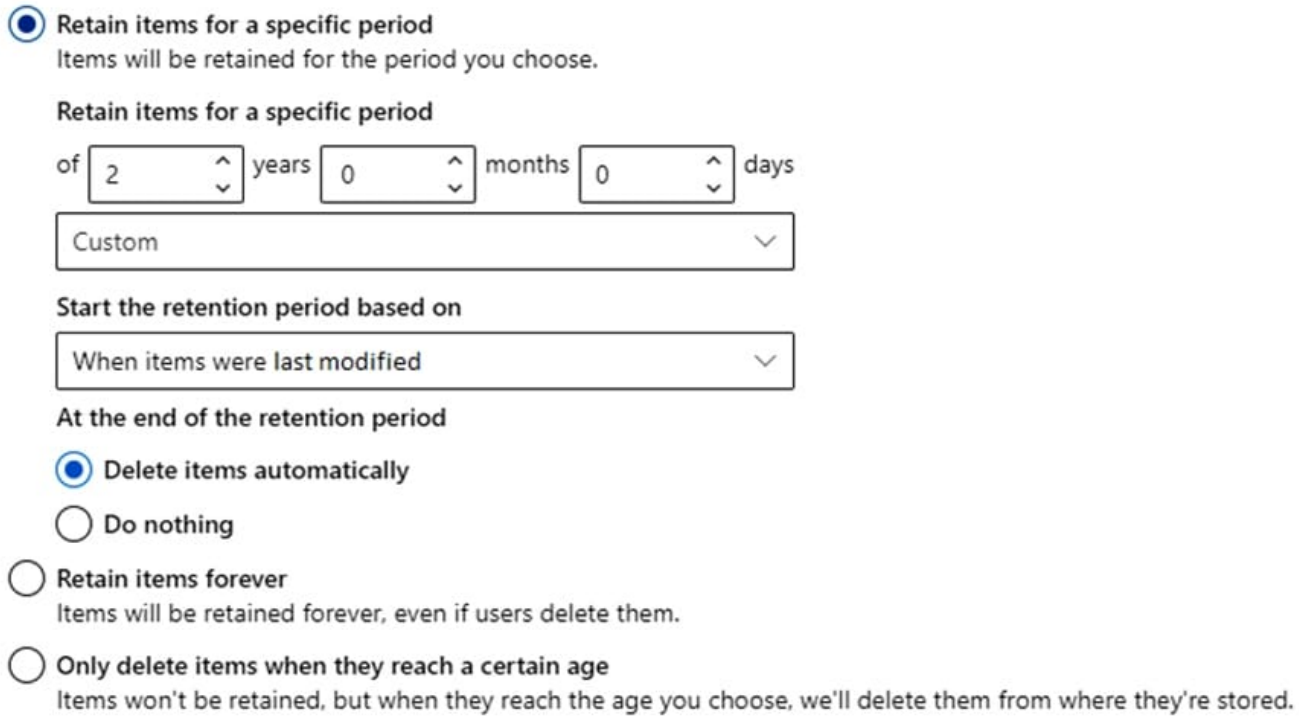
A device group with a rank of 1 is the highest ranked group. When a device is matched to more than one group, it\\'s added only to the highest ranked group.

QUESTION 5

HOTSPOT

You have a Microsoft 365 subscription.

You are creating a retention policy named Retention1 as shown in the following exhibit. (Click the Exhibit tab.)



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

Box 1: Retained Files are retained for two years and then deleted. The two-year timer resets every time the file is modified. Therefore, if a file is modified every 6 months, it will never be deleted. Box 2: The user can recover the file until the Recycle Bin retention period expires The user deleted the file so it will be removed to the Recycle Bin. The user can recover the file until the Recycle Bin retention period expires. After that time, only an administrator can recover the file and only until the file is permanently deleted after two-years from the last modification date.