



# MS-500<sup>Q&As</sup>

Microsoft 365 Security Administration

**Pass Microsoft MS-500 Exam with 100% Guarantee**

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

<https://www.geekcert.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

Your company has a main office and a Microsoft 365 subscription.

You need to enforce Microsoft Azure Multi-Factor Authentication (MFA) by using conditional access for all users who are NOT physically present in the office.

What should you include in the configuration?

- A. a user risk policy
- B. a sign-in risk policy
- C. a named location in Azure Active Directory (Azure AD)
- D. an Azure MFA Server

Correct Answer: C

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

## QUESTION 2

### HOTSPOT

You have a Microsoft 365 subscription that uses a default domain name of contoso.com. Microsoft Azure Active Directory (Azure AD) contains the users shown in the following table.

Name	Member of
User1	Group1
User2	Group1, Group2
User3	Group3

Microsoft Intune has two devices enrolled as shown in the following table:

Name	Platform
Device1	Android
Device2	Windows 10

Both devices have three apps named App1, App2, and App3 installed.

You create an app protection policy named ProtectionPolicy1 that has the following settings:

1.

Protected apps: App1

2.



Exempt apps: App2

3.

Windows Information Protection mode: Block

You apply ProtectionPolicy1 to Group1 and Group3. You exclude Group2 from ProtectionPolicy1.

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

Yes No

From Device1, User1 can copy data from App1 to App3.  
From Device2, User1 can copy data from App1 to App2.  
From Device2, User1 can copy data from App1 to App3.

<input type="radio"/>	<input type="radio"/>
<input type="radio"/>	<input type="radio"/>
<input type="radio"/>	<input type="radio"/>

Correct Answer:

### Answer Area

Yes No

From Device1, User1 can copy data from App1 to App3.  
From Device2, User1 can copy data from App1 to App2.  
From Device2, User1 can copy data from App1 to App3.

<input checked="" type="radio"/>	<input type="radio"/>
<input checked="" type="radio"/>	<input type="radio"/>
<input type="radio"/>	<input checked="" type="radio"/>

### QUESTION 3

You have a Microsoft 365 subscription linked to an Azure Active Directory (Azure AD) tenant that contains a user named User1. You need to grant User1 permission to search Microsoft 365 audit logs. The solution must use the principle of least privilege. Which role should you assign to User1?

- A. the View-Only Audit Logs role in the Security and Compliance admin center
- B. the View-Only Audit Logs role in the Exchange admin center
- C. the Compliance Management role in the Exchange admin center
- D. the Security reader role in the Azure Active Directory admin center



Correct Answer: B

There is no View-Only Audit logs role in Exchange Admin Center. The documentation for the View-Only Logs role also state that it applies to Exchange Server 2013 Reference: <https://docs.microsoft.com/en-us/microsoft-365/compliance/search-the-audit-log-in-security-and-compliance?view=o365-worldwide>  
<https://learn.microsoft.com/en-us/exchange/view-only-audit-logs-role-exchange-2013-help>

#### QUESTION 4

##### HOTSPOT

You have a Microsoft 365 subscription.

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

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... ▾ 2 years ▾

Retain the content based on when it was last modified ▾ ⓘ

**Do you want us to delete it after this time?** ⓘ

☒ Yes ☐ No

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

1 years ▾

**Need more options?**

☐ Use advanced retention settings ⓘ

Back

Next

Cancel

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 5

You need to create an eDiscovery case that places a hold on the mailbox of a user named Allan Deyoung. The hold must retain email messages that have a subject containing the word merger or the word Contoso.

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

Correct Answer: See explanation below.



1.

Navigate to eDiscovery in the Security and Compliance Center, and then click Create a case.

2.

On the New Case page, give the case a name, type an optional description, and then click Save. The case name must be unique in your organization.

The new case is displayed in the list of cases on the eDiscovery page. You can hover the cursor over a case name to display information about the case, including the status of the case (Active or Closed), the description of the case (that was created in the previous step), and when the case was changed last and who changed it.

To create a hold for an eDiscovery case:

1.

In the Security and Compliance Center, click eDiscovery > eDiscovery to display the list of cases in your organization.

2.

Click Open next to the case that you want to create the holds in.

3.

On the Home page for the case, click the Hold tab.

4.



On the Hold page, click Create.

5.

On the Name your hold page, give the hold a name. The name of the hold must be unique in your organization.

6.

(Optional) In the Description box, add a description of the hold.

7.

Click Next.

8.

Choose the content locations that you want to place on hold. You can place mailboxes, sites, and public folders on hold.

Home Hold Search Export Switch to Advanced eDiscovery

+ Create Refresh Search

Name

holdOne

HoldTwo

Name your hold

Name \*

Enter a friendly name

Description

Enter a friendly description for your policy

Next Cancel





## Choose locations

Location

Include



Exchange email

None

[Choose users, groups, or teams](#)



Office 365 group email



Skype for Business



Teams messages



To-Do



Yammer conversations



SharePoint sites

None

[Choose sites](#)



OneDrive accounts



Office 365 group sites



Teams sites



Yammer networks



Exchange public folders

None



[Back](#)

[Next](#)

[Cancel](#)



Exchange email - Click Choose users, groups, or teams and then click Choose users, groups, or teams again. to specify mailboxes to place on hold. Use the search box to find user mailboxes and distribution groups (to place a hold on

the mailboxes of group members) to place on hold. You can also place a hold on the associated mailbox for a Microsoft Team, a Yammer Group, or an Office 365 Group. Select the user, group, team check box, click Choose, and then click Done.

Note When you click Choose users, groups, or teams to specify mailboxes to place on hold, the mailbox picker that's displayed is empty. This is by design to enhance performance. To add people to this list, type a name (a minimum of 3 characters) in the search box.

9.

After configuring a query-based hold, click Next.

10.

Review your settings, and then click Create this hold.

Reference: <https://docs.microsoft.com/en-us/microsoft-365/compliance/ediscovery-cases?view=o365-worldwide#step-4-place-content-locations-on-hold>

[MS-500 PDF Dumps](#)

[MS-500 Practice Test](#)

[MS-500 Study Guide](#)