



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.passapply.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

HOTSPOT

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

<input type="checkbox"/>	Name	Group type	Membership type	Email	Security enabled
<input type="checkbox"/>	 Group1	Microsoft 365	Assigned	Group1@sk220130.onmicrosoft.com	No
<input type="checkbox"/>	 Group2	Microsoft 365	Assigned	Group2@sk220130.onmicrosoft.com	Yes
<input type="checkbox"/>	 Group3	Distribution	Assigned	Group3@sk220130.onmicrosoft.com	No
<input type="checkbox"/>	 Group4	Mail enabled security	Assigned	Group4@sk220130.onmicrosoft.com	Yes
<input type="checkbox"/>	 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:

[Answer choice] can be assigned to receive noncompliance notifications generated by device compliance policies.

- Group1 and Group2 only
- Group3 and Group4 only
- Group2, Group3, and Group4 only
- Group2, Group4, and Group5 only
- Group1, Group2, Group3, and Group4 only
- Group1, Group2, Group3, Group4, and Group5

[Answer choice] can be assigned device compliance policies.

- Group1 and Group2 only
- Group3 and Group4 only
- Group2, Group3, and Group4 only
- Group2, Group4, and Group5 only
- Group1, Group2, Group3, and Group4 only
- Group1, Group2, Group3, Group4, and Group5

Correct Answer:



[Answer choice] can be assigned to receive noncompliance notifications generated by device compliance policies.

Group1 and Group2 only
Group3 and Group4 only
Group2, Group3, and Group4 only
Group2, Group4, and Group5 only
Group1, Group2, Group3, and Group4 only
Group1, Group2, Group3, Group4, and Group5

[Answer choice] can be assigned device compliance policies.

Group1 and Group2 only
Group3 and Group4 only
Group2, Group3, and Group4 only
Group2, Group4, and Group5 only
Group1, Group2, Group3, and Group4 only
Group1, Group2, Group3, Group4, and Group5

QUESTION 2

You have an Azure Active Directory (Azure AD) tenant that has a Microsoft 365 subscription

You recently configured the tenant to require multi factor authentication (MFA) for risky sign ins

You need to review the users who required MFA.

What should you do?

- A. From the Microsoft 365 admin center, review a Security and Compliance report.
- B. From the Azure Active Directory admin center, download the sign-ins to a CSV file
- C. From the Microsoft 365 Compliance admin center, run an audit log search and download the results to a CSV file
- D. From the Azure Active Directory admin center, review the Authentication methods activities.

Correct Answer: D

Reference: <https://docs.microsoft.com/en-us/azure/active-directory/authentication/howto-mfa-reporting>

QUESTION 3

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 subscription that contains the users shown in the following table.



Name	Azure Active Directory (Azure AD) role	Security group
User1	Directory writers	Group1, Group3
User2	Security administrator	Group1, Group2
User3	Azure Information Protection administrator	Group2, Group3
User4	Cloud application administrator	Group3, Group4

You need to ensure that User1, User2, and User3 can use self-service password reset (SSPR). The solution must not affect User4.

Solution: You create a conditional access policy for User1, User2, and User3.

Does that meet the goal?

A. Yes

B. No

Correct Answer: B

Reference: <https://docs.microsoft.com/en-us/azure/active-directory/authentication/tutorial-enable-sspr>

QUESTION 4

You create a data loss prevention (DLP) policy as shown in the following exhibit:

New DLP policy

- ✓ Choose the information to protect
- ✓ Name your policy
- ✓ Choose locations
- Policy settings
- Review your settings

What do you want to do if we detect sensitive info?

We'll automatically create activity reports so you can review the content that matches this policy. What else do you want to do?

Notify users when content matches the policy settings

- ☒ Show policy tips to users and send them an email notification.
Tips appear to users in their apps (like Outlook and SharePoint) and help them learn how to use sensitive info responsibly. You can use the default tip or customize it to your liking. [Learn more about notifications and tips](#)
[Customize the tip and email](#)
- ☒ Detect when a specific amount of sensitive info is being shared at one time.
Detect when content that's being shared contains:
At least instances of the same sensitive info type.
- ☒ Send incident reports in email
By default, you and your global admin will automatically receive the email.
[Choose what to include in the report and who receives it](#)
- ☐ Restrict access or encrypt the content

Back Next Cancel

What is the effect of the policy when a user attempts to send an email messages that contains sensitive information?



- A. The user receives a notification and can send the email message
- B. The user receives a notification and cannot send the email message
- C. The email message is sent without a notification
- D. The email message is blocked silently

Correct Answer: A

Reference: <https://docs.microsoft.com/en-us/office365/securitycompliance/data-loss-prevention-policies>

QUESTION 5

You have a Microsoft 365 subscription that contains several Windows 10 devices. The devices are managed by using Microsoft Intune.

You need to enable Windows Defender Exploit Guard (Windows Defender EG) on the devices.

Which type of device configuration profile should you use?

- A. Endpoint protection
- B. Device restrictions
- C. Identity protection
- D. Windows Defender ATP

Correct Answer: A

References: <https://docs.microsoft.com/en-us/intune/endpoint-protection-windows-10>

[Latest MS-500 Dumps](#)

[MS-500 VCE Dumps](#)

[MS-500 Practice Test](#)