# MS-101 Q&As

Microsoft 365 Mobility and Security

## Pass Microsoft MS-101 Exam with 100% Guarantee

**QUESTION 1**

You have a Microsoft 365 E5 subscription.

You need to be alerted when Microsoft 365 Defender detects high-severity incidents.

What should you use?

A. a threat policy

B. a custom detection rule

C. an alert policy

D. a notification rule

Correct Answer: C

Explanation:

Alert policy settings

An alert policy consists of a set of rules and conditions that define the user or admin activity that generates an alert, a list of users who trigger the alert if they perform the activity, and a threshold that defines how many times the activity has to

occur before an alert is triggered. You also categorize the policy and assign it a severity level.

Note:

You can also define user tags as a condition of an alert policy. This results in the alerts triggered by the policy to include the context of the impacted user. You can use system user tags or custom user tags.

*

When the alert is triggered.

*

Alert category.

*

Alert severity. Similar to the alert category, you assign a severity attribute (Low, Medium, High, or Informational) to alert policies.

Reference: https://learn.microsoft.com/en-us/microsoft-365/compliance/alert-policies

**QUESTION 2**

Note: The question is included in a number of questions that depicts the identical set-up. However, every question has a distinctive result. Establish if the solution satisfies the requirements.

Your company has a Microsoft 365 subscription, with a data loss prevention (DLP) policy configured.

You have been informed that

You discover that users are erroneously flagging content as false positive and circumventing the DLP policy.

You want to make sure that the DLP policy is not circumvented.

Solution: You configure user overrides.

Does the solution meet the goal?

A. Yes

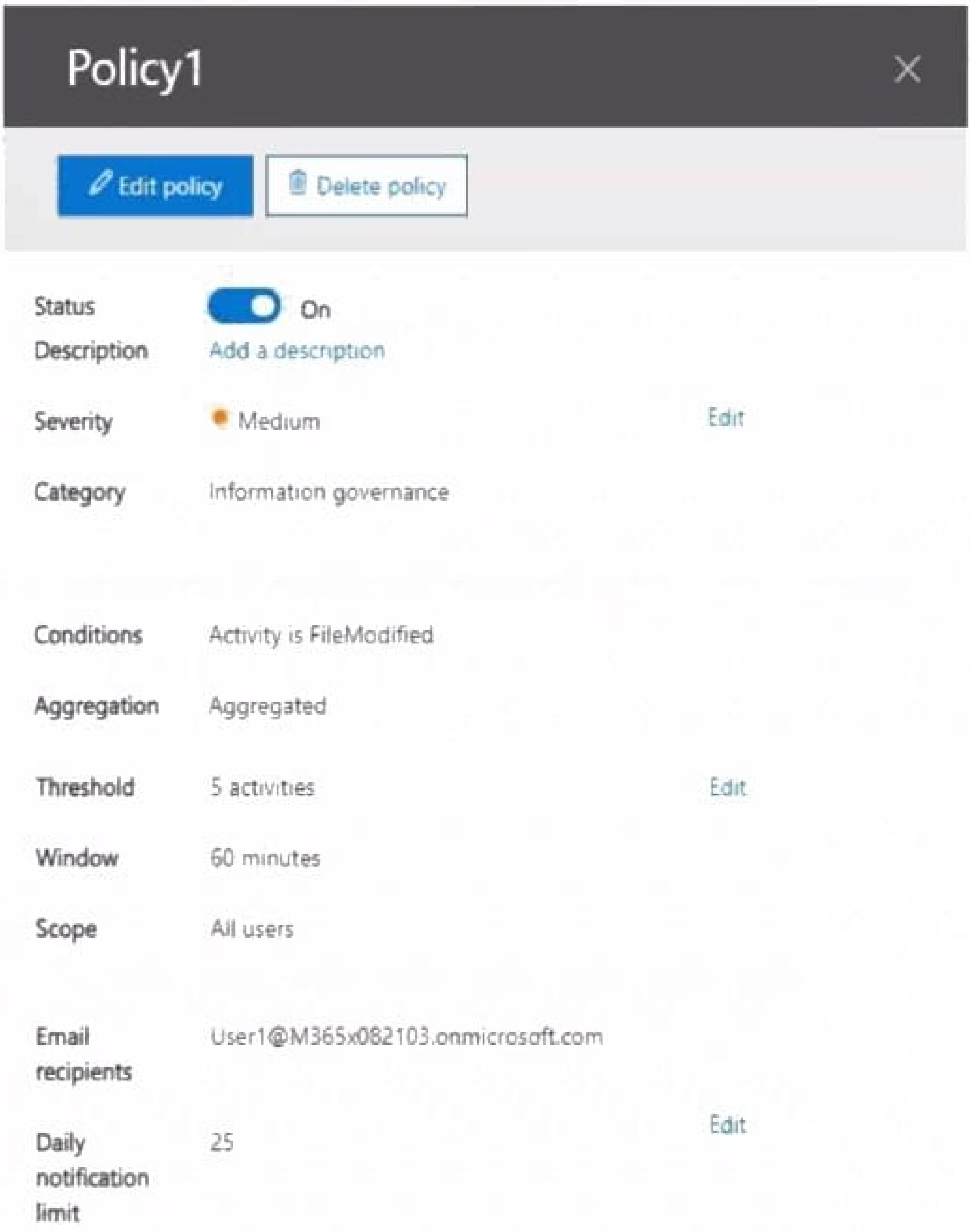
B. No

Correct Answer: A

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

**QUESTION 3**

You have a Microsoft 365 tenant that contains two users named User1 and User2. You create the alert policy shown in the following exhibit.



Policy1

| | | |
|---|---|---|
| Status | On | |
| Description | Add a description | |
| Severity | ● Medium | Edit |
| Category | Information governance | |
| Conditions | Activity is FileModified | |
| Aggregation | Aggregated | |
| Threshold | 5 activities | Edit |
| Window | 60 minutes | |
| Scope | All users | |
| Email recipients | User1@M365x082103.onmicrosoft.com | |
| Daily notification limit | 25 | Edit |

User2 runs a script that modifies a file in a Microsoft SharePoint Online library once every four minutes and runs for a period of two hours. How many alerts will User1 receive?

A. 2

B. 5

C. 10

D. 25

Correct Answer: D

**QUESTION 4**

Note: This question is part of a series of questions that present the same scenario. Each question in the series contains a unique solution that might meet the stated goals. Some question sets might have more than one correct solution, while

others might not have a correct solution.

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 are deploying Microsoft Intune.

You successfully enroll Windows 10 devices in Intune.

When you try to enroll an iOS device in Intune, you get an error.

You need to ensure that you can enroll the iOS device in Intune.

Solution: You configure the Apple MDM Push certificate.

Does this meet the goal?

A. Yes

B. No

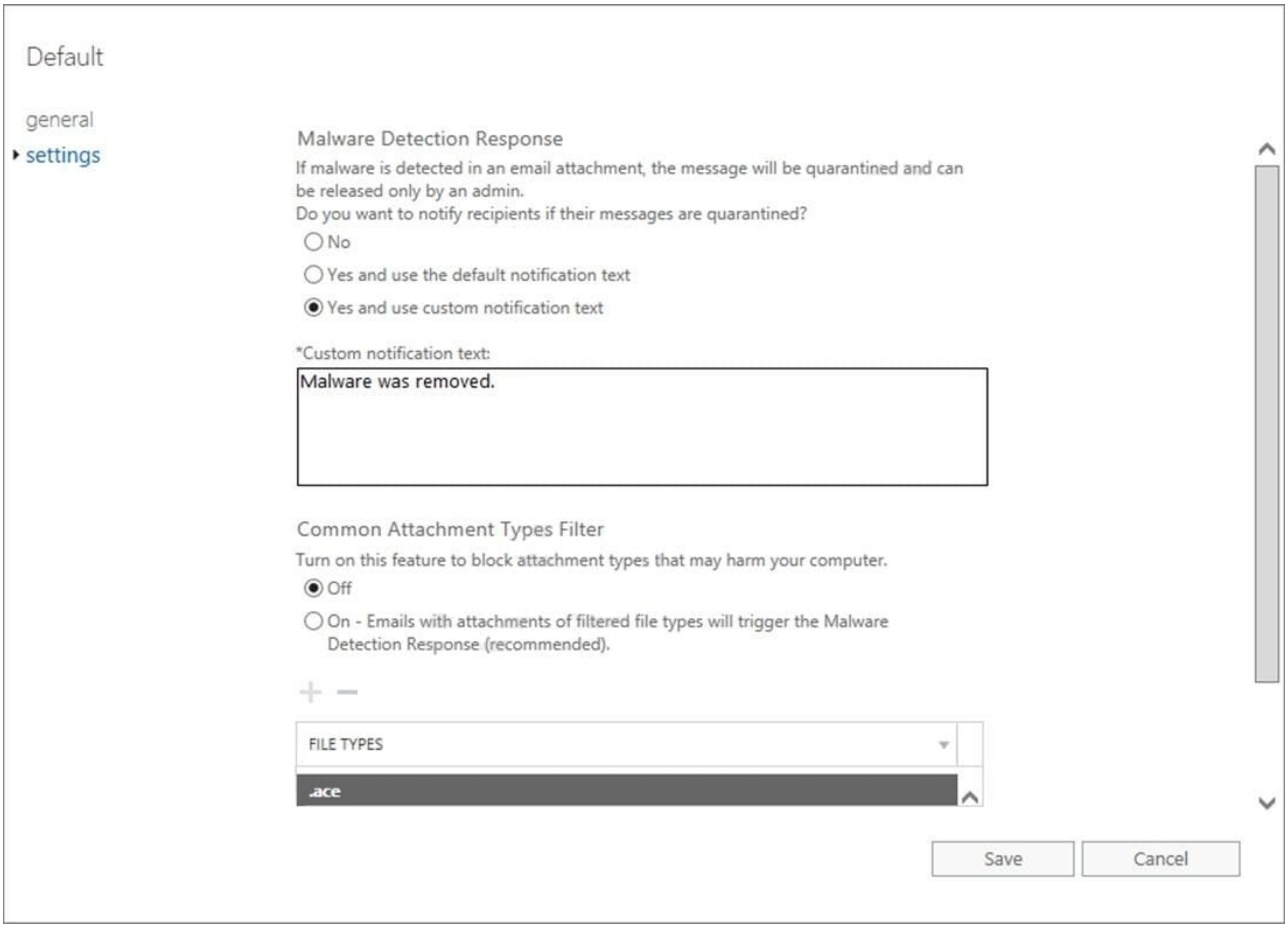
Correct Answer: A

References: https://docs.microsoft.com/en-us/intune/apple-mdm-push-certificate-get

**QUESTION 5**

You have a Microsoft 365 E5 subscription that contains a user named User1.

The subscription has a single anti-malware policy as shown in the following exhibit.



Default

general
settings

Malware Detection Response

If malware is detected in an email attachment, the message will be quarantined and can be released only by an admin.
Do you want to notify recipients if their messages are quarantined?

○ No
○ Yes and use the default notification text
● Yes and use custom notification text

*Custom notification text:
Malware was removed.

Common Attachment Types Filter

Turn on this feature to block attachment types that may harm your computer.

● Off
○ On - Emails with attachments of filtered file types will trigger the Malware Detection Response (recommended).

| FILE TYPES |
|---|
| .ace |

An email message that contains text and two attachments is sent to User1. One attachment is infected with malware. How will the email message and the attachments be processed?

A. Both attachments will be removed. The email message will be quarantined, and User1 will receive an email message without any attachments and an email message that includes the following text: “Malware was removed.”

B. The email message will be quarantined, and the message will remain undelivered.

C. Both attachments will be removed. The email message will be quarantined, and User1 will receive a copy of the message containing the original text and a new attachment that includes the following text: “Malware was removed.”

D. The malware-infected attachment will be removed. The email message will be quarantined, and User1 will receive a copy of the message containing only the uninfected attachment.

Correct Answer: C

Reference: https://docs.microsoft.com/en-us/microsoft-365/security/office-365-security/anti-malware-protection?view=o365-worldwide#anti-malware-policies

Latest MS-101 Dumps MS-101 PDF Dumps MS-101 Braindumps