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

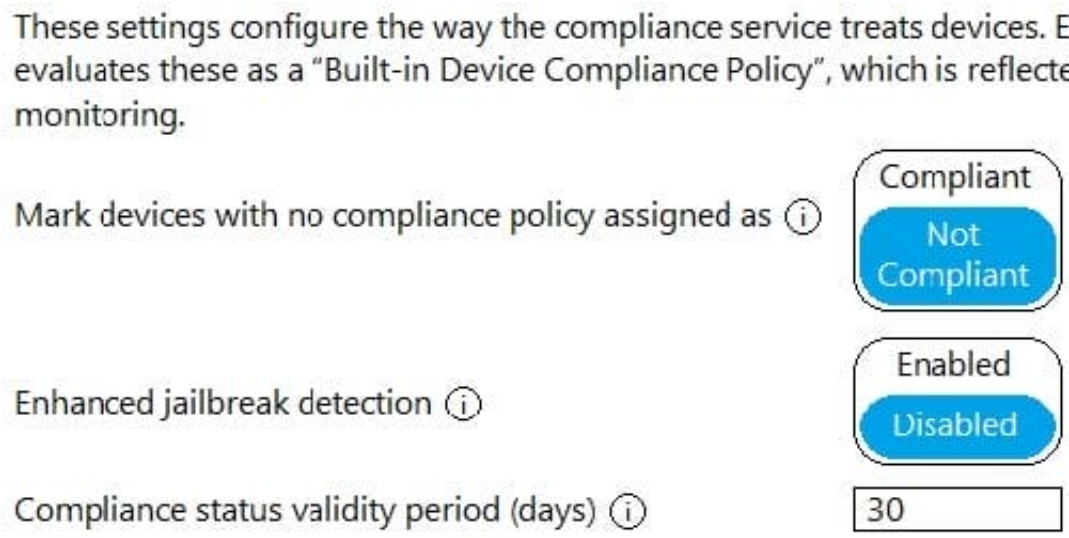
Following Questions and Answers are all new published by Microsoft Official Exam Center

QUESTION 1

HOTSPOT

You have a Microsoft 365 E5 subscription that uses Microsoft Endpoint Manager.

The Compliance policy settings are configured as shown in the following exhibit.



On February 25, 2020, you create the device compliance policies shown in the following table.

Name	Require BitLocker Drive Encryption (BitLocker)	Require Secure Boot	Mark device as not compliant	Assigned to
Policy1	Yes	No	5 days after noncompliance	Group1
Policy2	No	Yes	10 days after noncompliance	Group1, Group2

On March 1. 2020, users enroll Windows 10 devices in Microsoft Endpoint Manager as shown in the following table

Name	BitLocker enabled	Secure Boot enabled	Member of
Device1	Yes	No	Group1
Device2	No	No	Group2

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
On March 2, 2020, Device2 is marked as compliant.	○	○
On March 6, 2020, Device1 is marked as compliant.	○	○
On March 12, 2020, Device1 is marked as compliant.	○	○

Correct Answer:

Answer Area

Statements	Yes	No
On March 2, 2020, Device2 is marked as compliant.	○	○
On March 6, 2020, Device1 is marked as compliant.	○	○
On March 12, 2020, Device1 is marked as compliant.	○	○

Box 1: Yes

Device2 is in Group2 so Policy2 applies.

Device2 is not compliant with Policy2. However, the device won\\'t be marked as non-compliant until 10 days after the device was enrolled.

Box 2: Yes

Device1 is in Group1 and Group2 so both Policy1 and Policy2 apply.

Device1 is compliant with Policy1 but non-compliant with Policy2. However, the device won\\'t be marked as non-

compliant until 10 days after the device was enrolled.

Box 3: No

Device1 is in Group1 and Group2 so both Policy1 and Policy2 apply.

Device1 is compliant with Policy1 but non-compliant with Policy2.

March 12th is more than 10 days after the device was enrolled so it will now be marked as non-compliant by Policy2.

QUESTION 2

You have a Microsoft 365 subscription.

Some users access Microsoft SharePoint Online from unmanaged devices.

You need to prevent the users from downloading, printing, and syncing files.

What should you do?

A. Run the Set-SPODataConnectionSetting cmdlet and specify the AssignmentCollection parameter

B. From the SharePoint admin center, configure the Access control settings

C. From the Microsoft Azure portal, create an Azure Active Directory (Azure AD) Identity Protection sign-in risk policy

D. From the Microsoft Azure portal, create an Azure Active Directory (Azure AD) conditional access policy

Correct Answer: D

References: https://docs.microsoft.com/en-us/sharepoint/control-access-from-unmanaged-devices

---

QUESTION 3

HOTSPOT

You have a Microsoft Sentinel workspace that has an Azure Active Directory (Azure AD) connector and an Office 365 connector.

From the workspace, you plan to create an analytics rule that will be based on a custom query and will run a security play.

You need to ensure that you can add the security playbook and the custom query to the rule.

What should you do? To answer, select the appropriate options in the answer area.

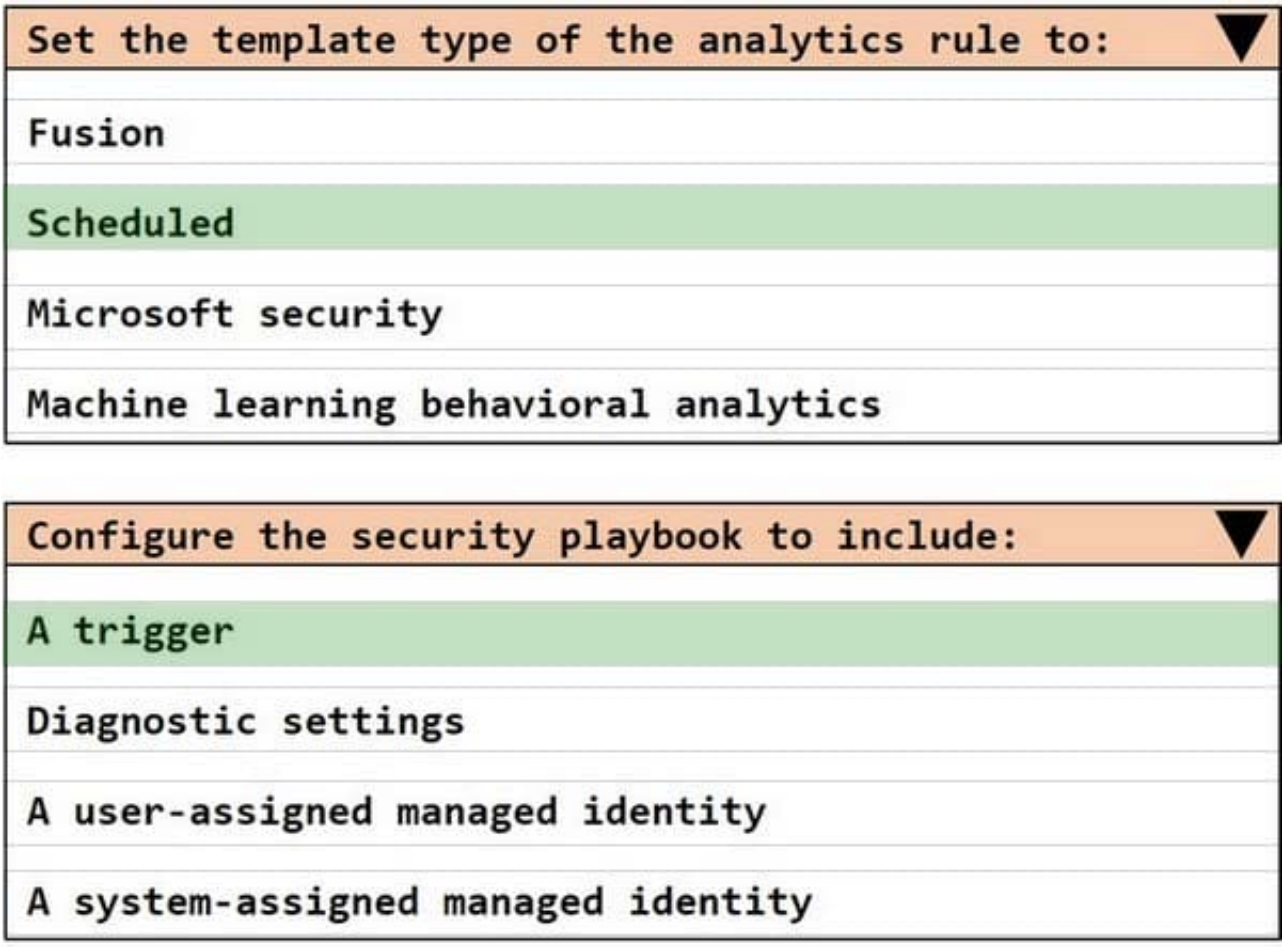
NOTE: Each correct selection is worth one point.

Hot Area:

Set the template type of the analytics rule to: ▼
Fusion
Scheduled
Microsoft security
Machine learning behavioral analytics

Configure the security playbook to include: ▼
A trigger
Diagnostic settings
A user-assigned managed identity
A system-assigned managed identity

Correct Answer:



Box 1: Scheduled Create a custom analytics rule with a scheduled query

1.

From the Microsoft Sentinel navigation menu, select Analytics.

2.

In the action bar at the top, select +Create and select Scheduled query rule. This opens the Analytics rule wizard.

3.

Etc.

Box 2: A trigger

Use triggers and actions in Microsoft Sentinel playbooks.

Reference:

https://docs.microsoft.com/en-us/azure/sentinel/detect-threats-custom https://docs.microsoft.com/en-us/azure/sentinel/playbook-triggers-actions#microsoft-sentinel-triggers-summary

QUESTION 4

SIMULATION

You plan to publish a label that will retain documents in Microsoft OneDrive for two years, and then automatically delete the documents.

You need to create the label.

To complete this task, sign in to the Microsoft Office 365 portal.

Correct Answer: See explanation below.

You need to create a retention label.

1.

Go to the Security and Compliance Admin Center.

2.

Navigate to Classification > Retention labels.

3.

Click on + Create a label to create a new label.

4.

Give the label a name and click Next.

5.

On the File plan descriptors, leave all options empty. The options in this page are used for auto-applying the retention label. Click Next.

6.

Turn the Retention switch to On.

7.

Under Retain the content, set the period to 2 years.

8.

Under What do you want to do after this time?, select the Delete the content automatically option.

9.

Click Next.

10.Click the Create this label button to create the label. The label is now ready to be published to Microsoft OneDrive.

QUESTION 5

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

Name	Role
User1	Compliance Manager Contributor
User2	Compliance Manager Assessor
User3	Compliance Manager Administrator
User4	Portal Admin

You discover that all the users in the subscription can access Compliance Manager reports.

The Compliance Manager Reader role is not assigned to any users.

You need to recommend a solution to prevent a user named User5 from accessing the Compliance Manager reports.

Solution: You recommend assigning the Compliance Manager Reader role to User5.

Does this meet the goal?

A. Yes

B. No

Correct Answer: B

References: https://docs.microsoft.com/en-us/office365/securitycompliance/working-with-compliance-manager

QUESTION 6

You have a Microsoft 365 E5 subscription and an Sentinel workspace named Sentinel1. You need to launch the Guided investigation Process Alerts notebooks = in Sentinel. What should you create first?

A. a Log Analytic workspace

B. a Kusto query

C. an Azure Machine learning workspace

D. an Azure logic app

Correct Answer: C

QUESTION 7

You have a Microsoft 365 E3 subscription.

You plan to audit all Microsoft Exchange Online user and admin activities.

You need to ensure that all the Exchange audit log records are retained for one year.

What should you do?

A. Modify the retention period of the default audit retention policy.

B. Create a custom audit retention policy.

C. Assign Microsoft 365 Enterprise E5 licenses to all users.

D. Modify the record type of the default audit retention policy.

Correct Answer: C

Microsoft 365 Enterprise E5 license audit log record retention is 365 days. Microsoft 365 Enterprise E3 license audit log record retention is 90 days.

Reference: https://docs.microsoft.com/en-us/microsoft-365/compliance/audit-log-retention-policies?view=o365-worldwide

---

QUESTION 8

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

User1 needs to be able to create Data Subject Requests (DSRs) in the Microsoft 365 compliance center.

To which role or role group should you add User1?

A. the Compliance Data Administrator role

B. the Data Investigator role

C. the eDiscovery Manager role

D. the Records Management role group

Correct Answer: C

https://learn.microsoft.com/en-us/compliance/regulatory/gdpr-manage-gdpr-data-subject-requests-with-the-dsr-case-tool

---

QUESTION 9

You have a Microsoft 365 that uses Microsoft SharePOnt Online.

You need to ensure that users can only share files with users at specified partner companies. The solution must minimize administrative effort.

What should you do?

A. Allow only in specific security groups to share externally.

B. Set File and folder links to people.

C. Limit external by domain

D. Set External sharing to New and existing guest

Correct Answer: C

Limiting domains You can limit domains by allowing only the domains you specify or by allowing all domains except those you block. To limit domains at the organization level

1.

Go to Sharing in the SharePoint admin center, and sign in with an account that has admin permissions for your organization.

2.

Under Advanced settings for external sharing, select the Limit external sharing by domain check box, and then select Add domains.

3.

To create an allowlist (most restrictive), select Allow only specific domains; to block only the domains you specify, select Block specific domains.

4.

List the domains (maximum of 3000) in the box provided, using the format domain.com.

5.

Etc.

Reference:

https://docs.microsoft.com/en-us/sharepoint/restricted-domains-sharing

QUESTION 10

You need to resolve the issue that targets the automated email messages to the IT team. Which tool should you run first?

A. Synchronization Service Manager

B. Azure AD Connect wizard

C. Synchronization Rules Editor

D. IdFix

Correct Answer: B

References: https://docs.microsoft.com/en-us/office365/enterprise/fix-problems-with-directory-synchronization

QUESTION 11

You have a hybrid Azure Active Directory (Azure AD) tenant that has pass- through authentication enabled.

You plan to implement Azure AD identity Protection and enable the user risk policy.

You need to configure the environment to support the user risk policy.

What should you do first?

A. Enable password hash synchronization.

B. Configure a conditional access policy.

C. Enforce the multi-factor authentication (MFA) registration policy.

D. Enable the sign-in risk policy.

Correct Answer: A

QUESTION 12

You have a Microsoft 365 E5 subscription.

You plan to create a conditional access policy named Policy1.

You need to be able to use the sign-in risk level condition in Policy1.

What should you do first?

A. Connect Microsoft Endpoint Manager and Microsoft Defender for Endpoint.

B. From the Azure Active Directory admin center, configure the Diagnostics settings.

C. From the Endpoint Management admin center, create a device compliance policy.

D. Onboard Azure Active Directory (Azure AD) Identity Protection.

Correct Answer: D

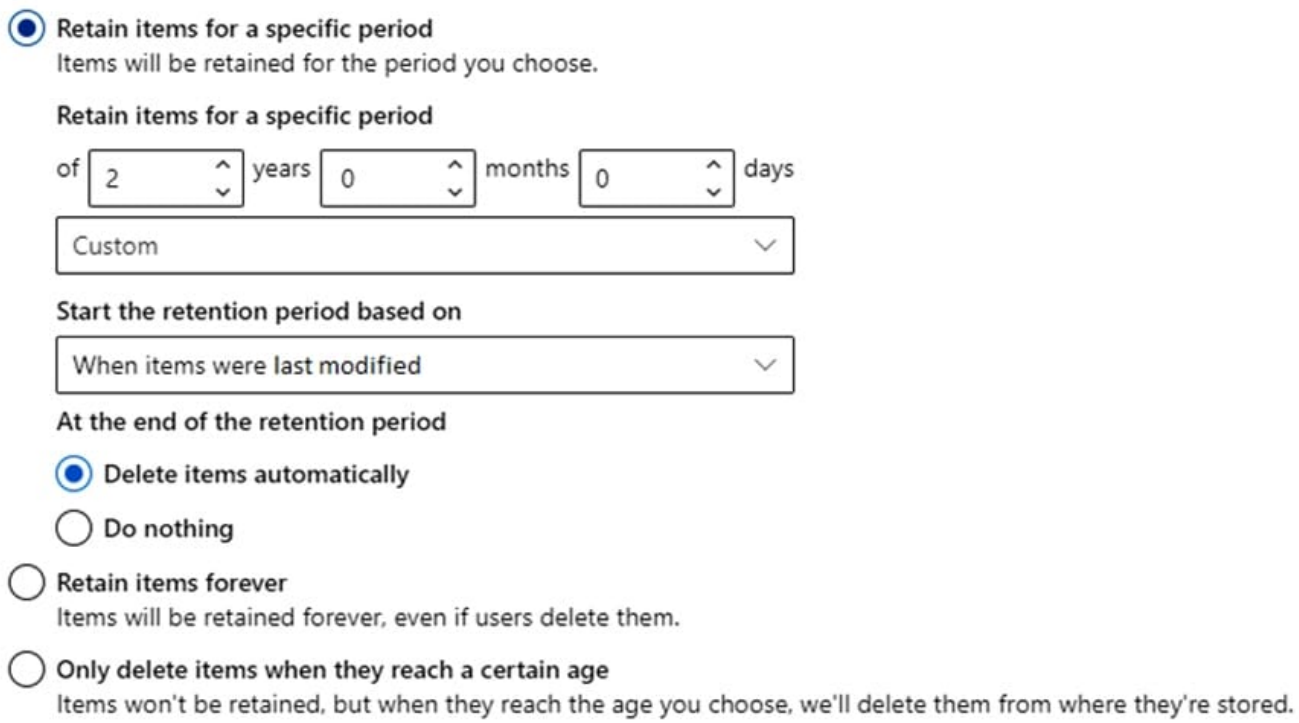
Reference: https://docs.microsoft.com/en-us/azure/active-directory/conditional-access/howto-conditional-access-policy-risk

QUESTION 13

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.

QUESTION 14

You have a Microsoft 365 E5 subscription that contains a user named Use1.

You need to ensure that User1 can use the Microsoft 365 compliance center to search audit logs and identify which users were added to Microsoft 365 role groups. The solution must use the principle of least privilege.

To which role group should you add User1?

A. Security Reader

B. View-Only Organization Management

C. Organization Management

D. Compliance Management

Correct Answer: D

https://admin.exchange.microsoft.com/#/adminRoles click the roles and check permissions.

compliance management and org management have access. but compliance management is least priveliged.

not to be confused with ordinary audit logs those require reports reader.

QUESTION 15

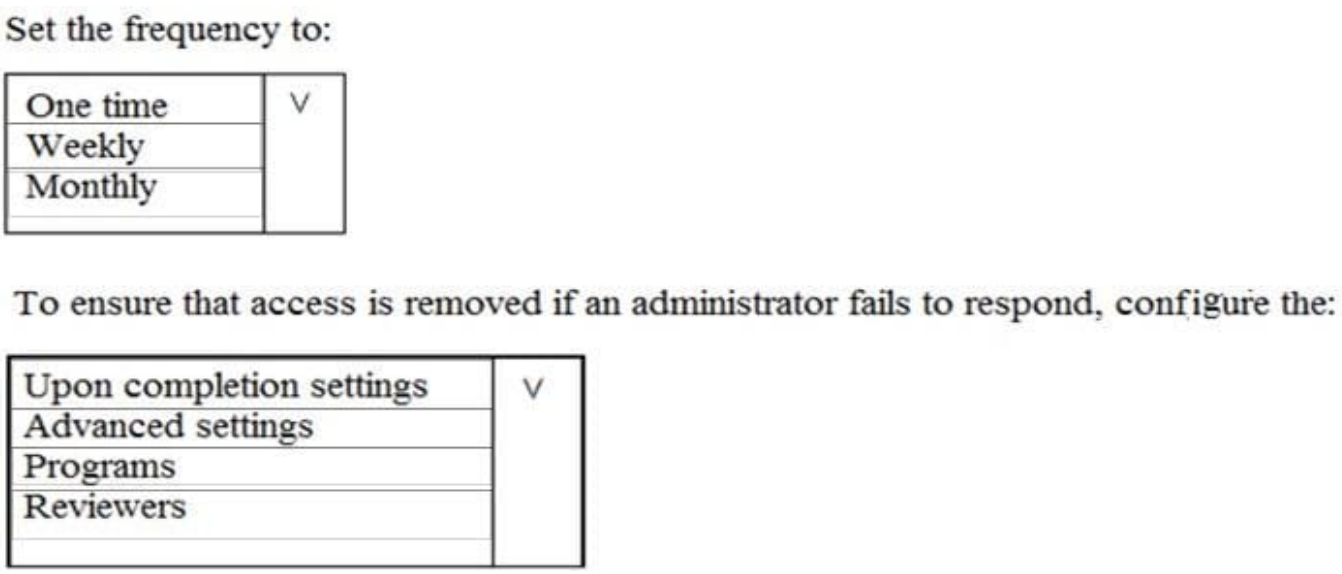
HOTSPOT

You plan to configure an access review to meet the security requirements for the workload administrators. You create an access review policy and specify the scope and a group.

Which other settings should you configure? To answer, select the appropriate options in the answer area.

NOTE: Each correct selection is worth one point.

Hot Area:



Correct Answer:

Set the frequency to:

One time	V
Weekly	
Monthly	

To ensure that access is removed if an administrator fails to respond, configure the:

Upon completion settings	V
Advanced settings	
Programs	
Reviewers	

Access to the Azure Active Directory admin center by the user administrators must be reviewed every seven days. If an administrator fails to respond to an access request within three days, access must be removed