

# Microsoft

## Exam Questions SC-401

Administering Information Security in Microsoft 365



**NEW QUESTION 1**

HOTSPOT - (Topic 1)

How many files in Site2 can User1 and User2 access after you turn on DLPpolicy1? To answer, select the appropriate options in the answer area.

NOTE: Each correct selection is worth one point.

## Answer Area

Number of files that User1 can access:

▼

1

2

3

4

Number of files that User2 can access:

▼

1

2

3

4

- A. Mastered
- B. Not Mastered

**Answer:** A

**Explanation:**

Understanding DLP Policy Impact on File Access

The DLP policy (DLPpolicy1) applies to Site2 and restricts access when: Content contains SWIFT Codes.

Instance count is 2 or more.

File Analysis (Based on SWIFT Codes Count)

File Name	SWIFT Codes Count	DLP Policy Restricts Access?
File1.docx	1	<input type="checkbox"/> No restriction (SWIFT codes < 2)
File2.bmp	4	<input type="checkbox"/> Restricted (SWIFT codes ≥ 2)
File3.txt	3	<input type="checkbox"/> Restricted (SWIFT codes ≥ 2)
File4.xlsx	7	<input type="checkbox"/> Restricted (SWIFT codes ≥ 2)

Files that remain accessible (not restricted by DLP):

File1.docx (Contains only 1 SWIFT Code Below restriction threshold) User access after DLP policy is applied:

User	Role in Site2	Access Rights	Can Access Files?
User1	Site Owner	Full Access	File1.docx, plus override access to another file
User2	Site Visitor	Read-only	File1.docx only

User1 (Site Owner):

Has higher privileges and can override DLP restrictions (through admin intervention). Can access 2 files (File1.docx + override access to another file).

User2 (Site Visitor):

Has read-only access but DLP blocks access to restricted files. Can only access 1 file (File1.docx), since all others are restricted.

**NEW QUESTION 2**

HOTSPOT - (Topic 2)

You have a Microsoft 365 E5 subscription that contains three DOCX files named File1, File2, and File3.

You create the sensitivity labels shown in the following table.

Name	Permission	Apply content marking
Label1	Any authenticated users: Viewer	Disabled
Label2	None	Enabled

You apply the labels to the files as shown in the following table.

File	Label
File1	None
File2	Label1
File3	Label2

You ask Microsoft 365 Copilot to summarize the files, and you receive the results shown in the following table.

Name	Based on content of
Summary1	File1, File3
Summary2	File2
Summary3	File1, File2, File3

For each of the following statements, select Yes if the statement is true. Otherwise, select No.

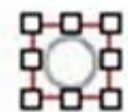
NOTE: Each correct selection is worth one point.

**Answer Area**

**Statements**

Summary1 has a sensitivity label applied.

Yes



No



Summary2 has a sensitivity label applied.



Summary3 has a sensitivity label applied.



- A. Mastered
- B. Not Mastered

Answer: A

Explanation:

## Answer Area

### Statements

Summary1 has a sensitivity label applied.

Yes

No



Summary2 has a sensitivity label applied.



Summary3 has a sensitivity label applied.



### NEW QUESTION 3

HOTSPOT - (Topic 2)

You have a Microsoft 365 E5 subscription.

You need to implement a compliance solution that meets the following requirements:

Captures clips of key security-related user activities, such as the exfiltration of sensitive company data.

Integrates data loss prevention (DLP) capabilities with insider risk management.

What should you use for each requirement? To answer, select the appropriate options in the answer area.

NOTE: Each correct selection is worth one point.

## Answer Area

Captures clips of key security-related user activities:

▼

- Adaptive scopes
- Classifiers
- Forensic evidence
- Search

Integrates DLP capabilities with insider risk management:

▼

- Adaptive Protection
- eDiscovery (Premium)
- Records management
- Trainable classifiers

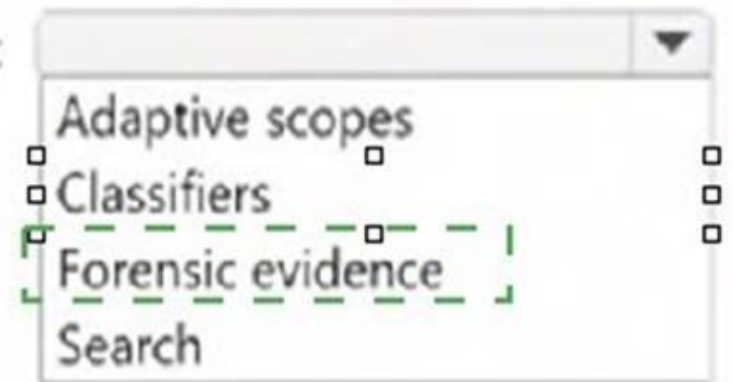
- A. Mastered
- B. Not Mastered

Answer: A

Explanation:

## Answer Area

Captures clips of key security-related user activities:



Integrates DLP capabilities with insider risk management:



### NEW QUESTION 4

- (Topic 2)

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 have a Microsoft 365 tenant and 500 computers that run Windows 11. The computers are onboarded to Microsoft Purview.

You discover that a third-party application named Tailspin\_scanner.exe accessed protected sensitive information on multiple computers. Tailspin\_scanner.exe is installed locally on the computers.

You need to block Tailspin\_scanner.exe from accessing sensitive documents without preventing the application from accessing other documents.

Solution: From Microsoft Defender for Cloud Apps, you create an app discovery policy. Does this meet the goal?

- A. Yes
- B. No

**Answer:** B

#### Explanation:

Creating an app discovery policy in Microsoft Defender for Cloud Apps is used for detecting and monitoring cloud application usage, but it does not prevent a locally installed application (Tailspin\_scanner.exe) from accessing sensitive files on Windows 11 devices.

To block Tailspin\_scanner.exe from accessing sensitive documents while allowing it to access other files, the correct solution is to use Microsoft Purview Endpoint Data Loss Prevention (Endpoint DLP) and add Tailspin\_scanner.exe to the Restricted Apps list.

Endpoint DLP allows you to block specific applications from accessing sensitive files while keeping general access available. Restricted Apps List in Endpoint DLP ensures that Tailspin\_scanner.exe cannot open, copy, or process protected documents, but it can still function normally for non-sensitive content.

### NEW QUESTION 5

- (Topic 2)

Your company has offices in multiple countries.

The company has a Microsoft 365 E5 subscription that uses Microsoft Purview insider risk management.

You plan to perform the following actions:

In a new country, open an office named Office1. Create a new user named User1.

Deploy insider risk management to Office1.

Add User1 to the Insider Risk Management Admins role group.

You need to ensure that User1 can perform insider risk management tasks for only the users and the devices in Office1.

What should you create first?

- A. a dynamic device group
- B. a dynamic user group
- C. an administrative unit
- D. a management group

**Answer:** C

#### Explanation:

To ensure User1 can perform insider risk management tasks only for the users and devices in Office1, the first step is to create an administrative unit in Microsoft Entra ID (formerly Azure AD).

Administrative units allow you to scope permissions to specific users, devices, and locations. By creating an administrative unit for Office1 and assigning User1 to the Insider Risk Management Admins role group within that unit, User1 will only have access to users and devices in Office1.

### NEW QUESTION 6

DRAG DROP - (Topic 2)

You have a Microsoft 365 E5 subscription that uses Microsoft Defender for Cloud Apps.

You plan to deploy a Defender for Cloud Apps file policy that will be triggered when the following conditions are met:

A file is shared externally.

A file is labeled as internal only.

Which filter should you use for each condition? To answer, drag the appropriate filters to the correct conditions. Each filter may be used once, more than once, or not at all. You may need to drag the split bar between panes or scroll to view content.

NOTE: Each correct selection is worth one point.

**Filters**

- 0 Access level
- 0 Collaborators
- 0 Matched policy
- 0 Sensitivity label

**Answer Area**

When a file is shared externally.

When a file is labelled as Internal only.

**Filter**

0

0

- A. Mastered
- B. Not Mastered

**Answer:** A

**Explanation:**

**Filters**

- 0 Access level
- 0 Collaborators
- 0 Matched policy
- 0 Sensitivity label

**Answer Area**

When a file is shared externally.

When a file is labelled as Internal only.

**Filter**

0 Access level

0 Sensitivity label

**NEW QUESTION 7**

DRAG DROP - (Topic 2)

You have a Microsoft 365 subscription that contains 20 data loss prevention (DLP) policies. You need to identify the following:

Rules that are applied without triggering a policy alert The top 10 files that have matched DLP policies Alerts that are miscategorized

Which report should you use for each requirement? To answer, drag the appropriate reports to the correct requirements. Each report may be used once, more than once, or not at all. You may need to drag the split bar between panes or scroll to view content.

NOTE: Each correct selection is worth one point.

**Reports**

- 0 DLP policy matches
- 0 False positive and override
- 0 Incident reports

**Answer Area**

Rules that are applied without triggering a policy alert:

The top 10 files that have matched DLP policies:

Alerts that are miscategorized:

**Report**

0

0

0

- A. Mastered
- B. Not Mastered

**Answer:** A

**Explanation:**

The False positive and override report helps identify rules that were applied but did not generate an actual policy alert, which means they were overridden or deemed false positives.

The DLP policy matches report provides details on files that matched DLP policies, including the top 10 files.

The Incident reports report helps analyze and review alerts, including those that may have been miscategorized.

**NEW QUESTION 8**

- (Topic 2)

You are creating a data loss prevention (DLP) policy that will apply to all available locations except Fabric and Power BI workspaces.

You configure an advanced DLP rule in the policy. Which type of condition can you use in the rule?

- A. Sensitive info type
- B. Content search query
- C. Sensitive label
- D. Keywords

**Answer:** A

**Explanation:**

When configuring an advanced DLP rule in Microsoft Purview Data Loss Prevention (DLP), you can use a Sensitive Information Type (SIT) condition to detect and classify specific types of sensitive data, such as credit card numbers, Social Security numbers, or custom sensitive data patterns. This allows you to apply protection and trigger actions based on the identified content.

**NEW QUESTION 9**

HOTSPOT - (Topic 2)

You have a Microsoft 365 sensitivity label that is published to all the users in your Microsoft Entra tenant as shown in the following exhibit.

<b>Label name</b> Rebranding	<a href="#">Edit</a>
<b>Tooltip</b> Used for all documents containing information about the rebranding effort	<a href="#">Edit</a>
<b>Description</b>	<a href="#">Edit</a>
<b>Encryption</b> Advanced protection for content with this label	<a href="#">Edit</a>
<b>Content marking</b> Watermark: INTERNAL	<a href="#">Edit</a>
<b>Endpoint data loss prevention</b>	<a href="#">Edit</a>
<b>Auto labeling</b>	<a href="#">Edit</a>

For each of the following statements, select Yes if the statement is true. Otherwise, select No.

**Answer Area**

Statements	Yes	No
All the documents stored on each user's computer will include a watermark automatically.	<input type="radio"/>	<input checked="" type="radio"/>
If the sensitivity label is applied to a document, the document will have a header that contains the word "INTERNAL".	<input type="radio"/>	<input type="radio"/>
The sensitivity label can be applied only to documents that contain the word rebranding.	<input type="radio"/>	<input type="radio"/>

- A. Mastered
- B. Not Mastered

**Answer:** A

**Explanation:**

Statement 1 - No. The sensitivity label includes content marking (watermark: INTERNAL), but it only applies to documents where the label is manually or automatically applied, not to all documents by default.  
 Statement 2 - No. The sensitivity label only specifies a watermark, not a header. If a header marking was configured, it would explicitly appear in the label settings.  
 Statement 3 - No. There is no indication that auto-labeling is configured to apply the label only to documents with the word "rebranding". Auto-labeling is an optional setting that needs explicit configuration.

**NEW QUESTION 10**

HOTSPOT - (Topic 2)

You have a Microsoft 365 E5 subscription.

You need to identify documents that contain patent application numbers containing the letters PA followed by eight digits, for example, PA 12345678. The solution must minimize administrative effort.

What should you do? To answer, select the appropriate options in the answer area. NOTE: Each correct selection is worth one point.

**Answer Area**

To identify the documents, use a data classification of:

Exact data match (EDM)

Sensitive info type

Trainable classifier

Configure data classifications by using a:

Keyword dictionary

Regular expression

Function

- A. Mastered
- B. Not Mastered

**Answer:** A

**Explanation:**

Box 1: Since you are looking for a specific pattern (PA followed by eight digits, e.g., PA 12345678), the best classification method is Sensitive Info Type. Sensitive Info Types allow pattern-based matching to identify structured data. Exact Data Match (EDM) is not needed because you're not comparing against a fixed dataset. Trainable classifier is not appropriate because this is a structured pattern, not an unstructured document classification.  
 Box 2: Since PA 12345678 follows a structured pattern, the most effective method is Regular Expression (Regex). A Regular Expression (Regex) can be written to match "PA" followed by exactly eight digits (e.g., PA\s\d{8}). Keyword dictionary is not ideal because it works for predefined words, not number patterns. Function is unnecessary because there is no need for checksum validation or predefined validation rules.

**NEW QUESTION 10**

- (Topic 2)

You have a Microsoft 365 E5 subscription that contains a retention policy named RP1 as shown in the following table.

Setting	Value
Location	<ul style="list-style-type: none"> <li>Exchange email (All recipients)</li> <li>SharePoint sites (All sites)</li> </ul>
Retain items for a specific period	5 years (When items were created)
At the end of the retention period	Delete items automatically

You place a preservation lock on RP1. You need to modify RP1.

Which two modifications can you perform? Each correct answer presents part of the solution.

NOTE: Each correct selection is worth one point.

- A. Add locations to the policy.
- B. Delete the policy.
- C. Remove locations from the policy.
- D. Decrease the retention period of the policy.
- E. Disable the policy.
- F. Increase the retention period of the policy.

**Answer:** AF

**Explanation:**

A Preservation Lock in Microsoft Purview Retention Policies enforces strict compliance and prevents certain modifications to ensure data is retained according to compliance requirements.

When a Preservation Lock is applied:

- \* 1. You cannot disable or delete the policy.
- \* 2. You cannot remove locations from the policy.
- \* 3. You cannot decrease the retention period.
- \* 4. You can add locations to the policy.
- \* 5. You can increase the retention period.

You can expand the retention policy to cover additional locations (e.g., more Exchange mailboxes, SharePoint sites). You can extend the retention duration (e.g., increase from 5 years to 10 years) since this aligns with stricter compliance.

**NEW QUESTION 12**

- (Topic 2)

You have a Microsoft 365 E5 subscription that uses Microsoft Purview. You are creating an exact data match (EDM) classifier named EDM1.

For EDM1, you upload a schema file that contains the fields shown in the following table.

Column name	Match mode
PP	EU Passport Number
Name	All Full Names
DateOfBirth	Single-token
AccountNumber	Multi-token

What is the maximum number of primary elements that EDM1 can have?

- A. 1
- B. 2
- C. 3
- D. 4

**Answer:** B

**Explanation:**

In Microsoft Purview Exact Data Match (EDM) classifiers, a primary element is a unique, identifying field used for data matching. EDM allows up to two primary elements per schema.

From the provided table, the Match mode indicates how data is analyzed: PP (EU Passport Number) Likely a primary element because it's unique.

Name (All Full Names) Typically not a primary element as names are common.

DateOfBirth (Single-token) Usually a secondary element, not unique. AccountNumber (Multi-token) Can be a primary element, as it's a unique identifier.

Since EDM supports a maximum of two primary elements, the correct answer is 2.

**NEW QUESTION 13**

- (Topic 2)

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 recently discovered that the developers at your company emailed Azure Storage Account keys in plain text to third parties.

You need to ensure that when Azure Storage Account keys are emailed, the emails are encrypted.

Solution: You create a data loss prevention (DLP) policy that has only the Exchange email location selected.

Does this meet the goal?

- A. Yes
- B. No

**Answer:** A

**Explanation:**

To ensure Azure Storage Account keys are encrypted when sent via email, you need a Data Loss Prevention (DLP) policy that detects Azure Storage Account keys using a sensitive information type and automatically encrypts emails containing these keys.

A DLP policy with Exchange email as the only location meets this requirement because it identifies sensitive data in email messages and it applies protection actions, such as encryption, blocking, or alerts.

**NEW QUESTION 15**

HOTSPOT - (Topic 2)

You have a Microsoft 365 subscription.

You plan to deploy an audit log retention policy.

You need to perform a search to validate whether the policy will be applied to the intended entries.

Which two fields should you configure for the search? To answer, select the appropriate fields in the answer area.

NOTE: Each correct selection is worth one point.

Answer Area

# Search

Learn about audit

<b>Searches completed</b> 0	<b>Active searches</b> 0	<b>Active unfiltered searches</b> 0
<b>Date and time range (UTC) *</b>	<b>Activities - friendly names</b>	<b>Users</b>
Start <input type="text" value="Aug"/> <input type="text" value="00:00"/>	<input type="text" value="Choose which activities to search ..."/>	<input type="text" value="Add the users whose audit logs you ..."/>
End <input type="text" value="Aug"/> <input type="text" value="00:00"/>	<b>Activities - operation names ⓘ</b>	<b>File, folder, or site ⓘ</b>
	<input type="text" value="Enter operation values, separated by ..."/>	<input type="text" value="Enter all or a part of the name of a fil..."/>
<b>Keyword Search</b>	<b>Record types</b>	<b>Workloads</b>
<input type="text" value="Enter the keyword to search for"/>	<input type="text" value="Select the record types to search f..."/>	<input type="text" value="Enter the workloads to search for"/>
<b>Admin Units</b>	<b>Search name</b>	
<input type="text" value="Choose which Admin Units to se..."/>	<input type="text" value="Give the search a name"/>	

- A. Mastered
- B. Not Mastered

**Answer:** A

**Explanation:**

To validate whether an audit log retention policy will apply to the intended entries, you should configure the following fields:

Date and time range (UTC) ensures that you are searching for audit logs within the time period when the policy should be applied. Audit logs are time-sensitive, and policies affect logs based on their timestamp.

Record types allows you to filter and search for specific audit log categories (e.g., Exchange, SharePoint, Teams, etc.) that are affected by the retention policy.

Selecting the correct record type ensures that the policy is evaluated against the relevant data.

**NEW QUESTION 18**

- (Topic 2)

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 have a Microsoft 365 subscription.

You have a user named User1. Several users have full access to the mailbox of User1. Some email messages sent to User1 appear to have been read and deleted before the user viewed them.

When you search the audit log in the Microsoft Purview portal to identify who signed in to the mailbox of User1, the results are blank.

You need to ensure that you can view future sign-ins to the mailbox of User1. Solution: You run the Set-AdminAuditLogConfig -AdminAuditLogEnabled \$true -AdminAuditLogCmdlets \*Mailbox\* command. Does that meet the goal?

- A. Yes
- B. No

**Answer:** B

**Explanation:**

The Set-AdminAuditLogConfig -AdminAuditLogEnabled \$true -AdminAuditLogCmdlets

\*Mailbox\* command is incorrect. This enables admin audit logging, which tracks changes to mailbox configurations (e.g., mailbox settings updates), not user activity inside the mailbox.

**NEW QUESTION 21**

.....

## **Thank You for Trying Our Product**

### **We offer two products:**

1st - We have Practice Tests Software with Actual Exam Questions

2nd - Questions and Answers in PDF Format

### **SC-401 Practice Exam Features:**

- \* SC-401 Questions and Answers Updated Frequently
- \* SC-401 Practice Questions Verified by Expert Senior Certified Staff
- \* SC-401 Most Realistic Questions that Guarantee you a Pass on Your FirstTry
- \* SC-401 Practice Test Questions in Multiple Choice Formats and Updatesfor 1 Year

**100% Actual & Verified — Instant Download, Please Click**  
**[Order The SC-401 Practice Test Here](#)**