



# SC-400<sup>Q&As</sup>

Microsoft Information Protection Administrator

## Pass Microsoft SC-400 Exam with 100% Guarantee

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

<https://www.passapply.com/sc-400.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

You have a Microsoft 365 E5 subscription that contains multiple data loss prevention (DLP) policies.

You need to identify which DLP rules include conditions that can trigger the DLP policies.

Which report should you use from the Microsoft Purview compliance portal?

- A. DLP policy matches
- B. False positives and overrides
- C. DLP incidents
- D. Third-party DLP policy matches

Correct Answer: A

### QUESTION 2

A user reports that she can no longer access a Microsoft Excel file named Northwind Customer Data.xlsx. From the Cloud App Security portal, you discover the alert shown in the exhibit.

Alerts > **File containing PCI detected in the clou...** 11/21/20 1:10 PM +30 MEDIUM SEVERITY

File containing PCI detected in the cloud (built-in DLP engine) Microsoft SharePoint Online Megan Bowen Northwind Customer Data.xlsx

Resolution options: Northwind Customer Data.xlsx File is in quarantine Megan Bowen Close alert

**Description**  
File policy "File containing PCI detected in the cloud (built-in DLP engine)" was matched by "Northwind Customer Data.xlsx"

**Important information**  
• This alert falls under the following MITRE tactic: Execution

**Files**

No files found					
File name	Owner	App	Collaborators	Policies	Last modified
No files found					

**File policy report**

File **Quarantined** History

1 - 1 of 1 files

File name	Owner	App	Collaborators	Policies	Last modified
Northwind Custo...	Megan Bowen	Microsoft Share...	5 collaborators	1 policy match	Nov 21, 2020

You restore the file from quarantine.



You need to prevent files that match the policy from being quarantined. Files that match the policy must generate an alert.

What should you do?

- A. Modify the policy template.
- B. Assign the Global reader role to the file owners.
- C. Exclude file matching by using a regular expression.
- D. Update the governance action.

Correct Answer: D

Reference: <https://docs.microsoft.com/en-us/cloud-app-security/data-protection-policies#create-a-new-file-policy>

---

### QUESTION 3

You have a Microsoft 365 tenant that uses the following sensitivity labels:

1.  
Confidential
2.  
Internal
3.  
External

The labels are published by using a label policy named Policy1.

Users report that Microsoft Office for the web apps do not display the Sensitivity button. The Sensitivity button appears in Microsoft 365 Apps that are installed locally.

You need to ensure that the users can apply sensitivity labels to content when they use Office for the web apps.

Solution: You run the Execute-AzureAdLabelSync cmdlet.

Does this meet the goal?

- A. Yes
- B. No

Correct Answer: A

---

### QUESTION 4



Name	Role	Role group
Admin1	Global Administrator	None
Admin2	None	Compliance Administrator
Admin3	None	Records management

You have a Microsoft 365 E5 subscription that contains the users shown in the following table.

You create the retention label shown in the following exhibit.

## Create retention label

**Review and finish**

**Name**  
Name  
Retention1  
[Edit](#)

**File plan descriptors**  
**Retention settings**  
Retention period  
7 years  
[Edit](#)

**Based on**  
Based on when it was created  
[Edit](#)

**Retention action**  
Preserve, review and delete  
[Edit](#)

**Disposition stages and reviewers**  
Stage 1 name: Stage1  
Stage 1 reviewers:  
Admin1@LODSe270626.onmicrosoft.com,  
Admin2@LODSe270626.onmicrosoft.com,  
Admin3@LODSe270626.onmicrosoft.com  
[Edit](#)

**Use label to classify content as a**  
Record  
[Edit](#)

Which users can perform a disposition review of content that has Retention1 applied?

- A. Admin2 only
- B. Admin3 only
- C. Admin1 and Admin2 only
- D. Admin1 and Admin3 only
- E. Admin2 and Admin3 only
- F. Admin1, Admin2, and Admin3

Correct Answer: E



Explanation:

Permissions for disposition

\*

Admin3: To successfully access the Disposition tab in the Microsoft Purview compliance portal, users must have the Disposition Management role. From December 2020, this role is now included in the Records Management default role group.

Note:

By default, a global admin isn't granted the Disposition Management role.

\*

Admin2

Compliance Administrator - Members can manage settings for device management, data loss prevention, reports, and preservation.

The RecordManagement role is included in default roles assigned to the Compliance Administrator role. Incorrect:

\*

Not Admin1

The disposition reviewers explicitly need the Disposition Management role. This is included in the Records Management rule group

---

## QUESTION 5

Your company has a Microsoft 365 tenant that uses a domain named contoso.com.

You are implementing data loss prevention (DLP).

The company's default browser is Microsoft Edge.

During a recent audit, you discover that some users use Firefox and Google Chrome browsers to upload files labeled as Confidential to a third-party Microsoft SharePoint Online site that has a URL of <https://m365x076709.sharepoint.com>.

Users are blocked from uploading the confidential files to the site from Microsoft Edge.

You need to ensure that the users cannot upload files labeled as Confidential from Firefox and Google Chrome to any cloud services.

Which two actions should you perform? Each correct answer presents part of the solution. (Choose two.)

NOTE: Each correct selection is worth one point.

A. From the Microsoft 365 Endpoint data loss prevention (Endpoint) DLP settings, add [m365x076709.sharepoint.com](https://m365x076709.sharepoint.com) as a blocked service domain.

B. Create a DLP policy that applies to the Devices location.



C. From the Microsoft 365 Endpoint data loss prevention (Endpoint DLP) settings, add Firefox and Google Chrome to the unallowed browsers list.

D. From the Microsoft 365 compliance center, onboard the devices.

E. From the Microsoft 365 Endpoint data loss prevention (Endpoint) DLP settings, add contoso.com as an allowed service domain.

Correct Answer: CD

Reference: <https://docs.microsoft.com/en-us/microsoft-365/compliance/endpoint-dlp-learn-about?view=o365-worldwide>

[Latest SC-400 Dumps](#)

[SC-400 Exam Questions](#)

[SC-400 Braindumps](#)