



SC-400^{Q&As}

Microsoft Information Protection Administrator

Pass Microsoft SC-400 Exam with 100% Guarantee

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

<https://www.pass4itsure.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 a data loss prevention (DLP) policy named DLP1.

DLP1 has a rule that triggers numerous alerts.

You need to reduce the number of alert notifications that are generated. The solution must maintain the sensitivity of DLP1.

What should you do?

- A. Change the mode of DLP1 to Test without notifications.
- B. Modify the rule and increase the instance count.
- C. Modify the rule and configure an alert threshold.
- D. Modify the rule and set the priority to the highest value.

Correct Answer: C

Reference: <https://learn.microsoft.com/en-us/microsoft-365/compliance/alert-policies?view=o365-worldwide>

QUESTION 2

HOTSPOT

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

| Name | Email address | Distribution group |
|-------|-------------------|--------------------|
| User1 | user1@contoso.com | Finance |
| User2 | user2@contoso.com | Sales |

You create the data loss prevention (DLP) policies shown in the following table.



| Name | Order | Apply policy to | Conditions | Actions | Exceptions | User notifications | Additional options |
|---------|-------|---|--|---|--------------------|---|--|
| Policy1 | 0 | Exchange email for the Finance distribution group | Content shared with people outside my organization. Content contains five or more credit card numbers. | Encrypt the message by using the Encrypt email messages option. | user4@fabrikam.com | Send an incident report to the administrator. | If there's a match for this rule, stop processing additional DLP policies and rules. |
| Policy2 | 1 | All locations of Exchange email | Content shared with people outside my organization. Content contains five or more credit card numbers. | Restrict access or encrypt the content in Microsoft 365 locations. Block only people outside your organization. | None | Send an incident report to the administrator. | None |

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:

Statements

Yes

No

If User1 sends an email message that contains five credit card numbers to user4@fabrikam.com, the message will be encrypted.

If User1 sends an email message that contains five credit card numbers to orders@adatum.com, the message will be encrypted and delivered.

If User2 sends an email message that contains five credit card numbers to orders@adatum.com, the message will be encrypted and delivered.

Correct Answer:



| Statements | Yes | No |
|---|----------------------------------|----------------------------------|
| If User1 sends an email message that contains five credit card numbers to user4@fabrikam.com, the message will be encrypted. | <input type="radio"/> | <input checked="" type="radio"/> |
| If User1 sends an email message that contains five credit card numbers to orders@adatum.com, the message will be encrypted and delivered. | <input checked="" type="radio"/> | <input type="radio"/> |
| If User2 sends an email message that contains five credit card numbers to orders@adatum.com, the message will be encrypted and delivered. | <input type="radio"/> | <input checked="" type="radio"/> |

QUESTION 3

You have a Microsoft 365 tenant that has data loss prevention (DLP) policies.

You need to review DLP policy matches for the tenant.

What should you use?

- A. Content explorer
- B. Activity explorer
- C. Compliance Manager
- D. records management events

Correct Answer: B

Using Endpoint data loss prevention (DLP), Activity explorer gathers *DLP policy matches* events from Exchange, SharePoint, OneDrive, Teams Chat and Channel, on-premises SharePoint folders and libraries, on-premises file shares, and devices running Windows 10, Windows 11, and any of the three most recent major macOS versions.

Note: Activity explorer The data classification overview and content explorer tabs give you visibility into what content has been discovered and labeled, and where that content is. Activity explorer rounds out this suite of functionality by allowing you to monitor what's being done with your labeled content. Activity explorer provides a historical view of activities on your labeled content. The activity information is collected from the Microsoft 365 unified audit logs, transformed, and then made available in the Activity explorer UI. Activity explorer reports on up to 30 days worth of data.

There are more than 30 different filters available for use, some are:

Date range Activity type Location User Sensitivity label Retention label File path *-> DLP policy

Incorrect:

* Content explorer



Content explorer shows a current snapshot of the items that have a sensitivity label, a retention label or have been classified as a sensitive information type in your organization.

How to use content explorer:

Open Microsoft Purview compliance portal > Data classification > Content explorer.

If you know the name of the label, or the sensitive information type, you can type that into the filter box.

Alternately, you can browse for the item by expanding the label type and selecting the label from the list.

Select a location under All locations and drill down the folder structure to the item.

Double-click to open the item natively in content explorer.

Reference:

<https://learn.microsoft.com/en-us/purview/data-classification-activity-explorer>

QUESTION 4



Assign sensitivity labels to Microsoft 365 groups in Microsoft Entra ID

Microsoft Entra ID supports applying sensitivity labels published by the Microsoft Purview compliance portal to Microsoft 365 groups. Sensitivity labels apply to groups across services like Outlook, Microsoft Teams, and SharePoint. F

Assign a label to an existing group in the Microsoft Entra admin center

Step 1: Sign in to the Microsoft Entra admin center as at least a Global Administrator.

Step 2: Select Microsoft Entra ID.

Step 3: Select Groups

Step 4: From the All groups page, select the group that you want to label.

Step 5: On the selected group's page, select Properties and select a sensitivity label from the list.

Select the Confidential - Finance label

The screenshot shows the Microsoft Entra admin center interface for the 'A' Project Team group. The left-hand navigation pane includes sections for Overview, Diagnose and solve problems, Manage, Activity, and Troubleshooting + Support. The 'Manage' section is expanded, and 'Properties' is selected and highlighted with a red box. The main content area displays the 'General settings' for the group, including fields for Group name, Group description, Group type, Membership type, Sensitivity label, Object id, and Group writeback state. The 'Sensitivity label' field is highlighted with a red box and shows 'Confidential, Internal only' with a 'Remove' button next to it.

Step 6: Select Save to save your changes.

Reference:

<https://learn.microsoft.com/en-us/entra/identity/users/groups-assign-sensitivity-labels>

SIMULATION

Use the following login credentials as needed:

To enter your username, place your cursor in the Sign in box and click on the username below.

To enter your password, place your cursor in the Enter password box and click on the password below.

Microsoft 365 Username: admin@123456789.onmicrosoft.com

Microsoft 365 Password: *****



If the Microsoft 365 portal does not load successfully in the browser, press CTRL-K to reload the portal in a new browser tab.

The following information is for technical support purposes only:

Lab Instance: 12345678

You need to provide users with the ability to manually classify files that contain product information that are stored in SharePoint Online sites. The solution must meet the following requirements:

1.

The users must be able to apply a classification of Product1 to the files.

2.

Any authenticated user must be able to open files classified as Product1.

3.

Files classified as Product1 must be encrypted. To complete this task, sign in to the appropriate admin center.

A. Check the explanation

B. PlaceHold

C. PlaceHold

D. PlaceHold

Correct Answer: A



Restrict access to content by using sensitivity labels to apply encryption

When you create a sensitivity label, you can restrict access to content that the label will be applied to. For example, with the encryption settings for a sensitivity label, you can protect content so that:

- * Only users within your organization can open a confidential document or email.
- * Etc.

How to configure a label for encryption

Step 1: From the Microsoft Purview compliance portal, select Solutions > Information protection > Labels

Step 2: Locate and select label Product1.

Step 3: On the Define the scope for this label page, the options selected determine the label's scope for the settings that you can configure and where they'll be visible when they're published:

Define the scope for this label

Labels can be applied directly to items (such as files, emails, meetings), containers like SharePoint sites and Teams, Power BI items, schematized data assets, and more. Let us know where you want this label to be used so you can configure the applicable protection settings. [Learn more about label scopes](#)

- Items**
Be aware that restricting the scope to only files or emails might impact encryption settings and where the label can be applied. [Learn more](#)
 - Files**
Protect files created in Word, Excel PowerPoint, and more.
 - Emails**
Protect messages sent from Outlook and Outlook on the web.
 - Meetings**
Protect calendar events and meetings scheduled in Outlook and Teams.
- Groups & sites**
Configure privacy, access control, and other settings to protect labeled Teams, Microsoft 365 Groups, and SharePoint sites.
- Schematized data assets (preview)**
Apply labels to files and schematized data assets in Microsoft Purview Data Map. Schematized data assets include SQL Azure SQL, Azure Synapse, Azure Cosmos, AWS RDS, and more.

Step 4: Select Items, and Files. Deselect the other options.

Step 5: Then, on the Choose protection settings for the types of items you selected page, make sure you select Control access.

New sensitivity label

- Label details
- Scope
- Items**
- Groups & sites
- Schematized data assets (preview)
- Finish

Choose protection settings for the types of items you selected

The protection settings you configure will be enforced when the label is applied to items in Microsoft 365.

- Control access**
Control who can access and view labeled items.
- Apply content marking**
Add custom headers, footers, and watermarks to labeled items.
- Protect Teams meetings and chats**
Configure protection settings for Teams meetings and chats.

[To protect Teams meetings and chats, your org must have a Teams Premium license. Learn more about Teams Premium](#)

Step 6: On the Access control page, select Configure access control settings: Turns on encryption with rights management and makes the following settings visible:

Access control

Use encryption capabilities to control who can access labeled items. Depending on the scope you specified, items can include emails, Office, Fabric and Power BI files, and meeting invites. [Learn more about access control settings](#)

- Remove access control settings if already applied to items
- Configure access control settings**

Assign permissions now or let users decide?

The settings you choose will be automatically enforced when the label is applied to email and Office files.

User access to content expires ⓘ

Allow offline access ⓘ

Assign permissions to specific users and groups * ⓘ

[Assign permissions](#)

| Users and groups | Permissions | Edit | Delete |
|------------------|-------------|------|--------|
| 0 items | | | |



Step 7: Assign permissions to specific users or groups. Add users or groups

Step 7a: For users: Any authenticated users.

Step 7b: Permissions: Select View

Note: You can grant permissions to specific people so that only they can interact with the labeled content:

1. First, add users or groups that will be assigned permissions to the labeled content.
2. Then, choose which permissions those users should have for the labeled content.

Assigning permissions:

Assign permissions

Only the users or groups you choose will be assigned permissions to use the content that has this label applied. You can choose from existing permissions (such as Co-Owner, Co-Author, and Reviewer) or customize them to meet your needs.

- + Add all users and groups in your organization
- + Add any authenticated users 
- + Add users or groups
- + Add specific email addresses or domains 

Permissions assigned to

Choose permissions

Co-Author
VIEW,VIEWRIGHTSDATA,DOCEDIT,EDIT,PRINT,EXTRACT,REPLY,REPLYALL,FORWARD,OBJMODEL

Step 8: Click Save

Reference:

- <https://learn.microsoft.com/en-us/purview/trainable-classifiers-get-started-with>
- <https://learn.microsoft.com/en-us/purview/encryption-sensitivity-labels>

**QUESTION 5****HOTSPOT**

You have a Microsoft 365 E5 subscription that contains a user named User1 and the groups shown in the following table.

| Name | Type |
|-------------|-----------------------|
| Group1 | Microsoft 365 |
| Group2 | Distribution |
| Group3 | Mail-enabled security |
| Group4 | Security |

You plan to create a communication compliance policy named Policy1.

You need to identify whose communications can be monitored by Policy1, and who can be assigned the Reviewer role for Policy1.

Who should you identify? To answer, select the appropriate options in the answer area.

NOTE: Each correct selection is worth one point.

Hot Area:



Answer Area

Policy1 can monitor the communications of:

| | |
|---|---|
| | ▼ |
| User1 only | |
| User1, Group1, and Group2 only | |
| User1, Group2, and Group3 only | |
| User1, Group1, Group2, and Group3 only | |
| User1, Group1, Group2, Group3, and Group4 | |

The Reviewer role for Policy1 can be assigned to:

| | |
|---|---|
| | ▼ |
| User1 only | |
| User1 and Group4 only | |
| User1, Group3 and Group4 only | |
| User1, Group1, Group3, and Group4 only | |
| User1, Group1, Group2, Group3, and Group4 | |

Correct Answer:



Answer Area

Policy1 can monitor the communications of:

| | |
|---|---|
| | ▼ |
| User1 only | |
| User1, Group1, and Group2 only | |
| User1, Group2, and Group3 only | |
| User1, Group1, Group2, and Group3 only | |
| User1, Group1, Group2, Group3, and Group4 | |

The Reviewer role for Policy1 can be assigned to:

| | |
|---|---|
| | ▼ |
| User1 only | |
| User1 and Group4 only | |
| User1, Group3 and Group4 only | |
| User1, Group1, Group3, and Group4 only | |
| User1, Group1, Group2, Group3, and Group4 | |

Scoped users, meaning users that are targeted by the policy, has two supported groups: Distribution groups and Microsoft 365 Groups.

Reviewers does not have any supported groups.

<https://learn.microsoft.com/en-us/purview/communication-compliance-configure?view=o365-worldwide#step-3-optional-set-up-groups-for-communication-compliance>