Leads4Pass

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.leads4pass.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

HOTSPOT

You have a Microsoft 365 E5 subscription that contains the devices shown in the following table.
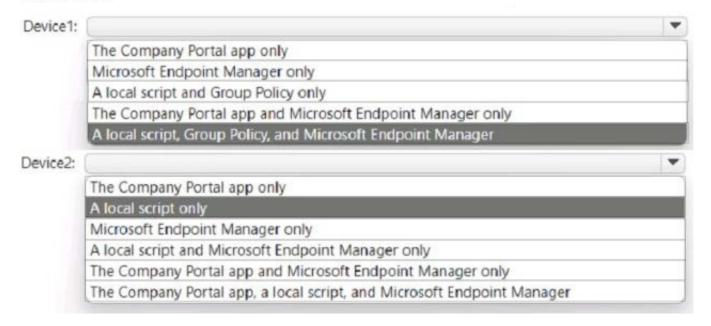
Name	Platform	Microsoft Intune
Device1	Windows 11	Not enrolled
Device2	macOS	Enrolled

You need to onboard the devices to Microsoft Purview. The solution must ensure that you can apply Endpoint data loss prevention (Endpoint DLP) policies to the devices. What can you use to onboard each device? To answer, select the appropriate options in the answer area.

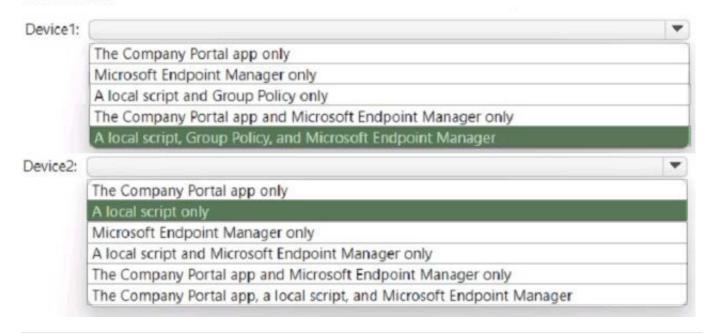NOTE: Each correct selection is worth one point.

Hot Area:

Answer Area

Device1:

| The Company Portal app only |
| Microsoft Endpoint Manager only |
| A local script and Group Policy only |
| The Company Portal app and Microsoft Endpoint Manager only |
| A local script, Group Policy, and Microsoft Endpoint Manager |

Device2:

| The Company Portal app only |
| A local script only |
| Microsoft Endpoint Manager only |
| A local script and Microsoft Endpoint Manager only |
| The Company Portal app and Microsoft Endpoint Manager only |
| The Company Portal app, a local script, and Microsoft Endpoint Manager |

Correct Answer:

Answer Area

Device1:

| The Company Portal app only |
| Microsoft Endpoint Manager only |
| A local script and Group Policy only |
| The Company Portal app and Microsoft Endpoint Manager only |
| **A local script, Group Policy, and Microsoft Endpoint Manager** |

Device2:

| The Company Portal app only |
| **A local script only** |
| Microsoft Endpoint Manager only |
| A local script and Microsoft Endpoint Manager only |
| The Company Portal app and Microsoft Endpoint Manager only |
| The Company Portal app, a local script, and Microsoft Endpoint Manager |

QUESTION 2

HOTSPOT

You have a Microsoft 365 tenant that uses a domain named canstoso.com.

A user named User1 leaves your company. The mailbox of User1 is placed on Litigation Hold, and then the account of User1 is deleted from Azure Active Directory (Azure AD).

You need to copy the content of the User1 mailbox to a folder in the existing mailbox of another user named User2.

How should you complete the PowerShell command? To answer, select the appropriate options in the answer area.

NOTE: Each correct selection is worth one point.

Hot Area:

$InactiveMailebox - Get-Mailbox InactiveMailebox - Identity <distingusished name>

New-Mailbox		-InactiveMailbox		$InactiveMailebox.DistinguishedName
New-MailboxRestoreRequest	-	-LitigationHoldEnabled		
Restore-Recoverableitems		-RetentionHoldEnabled		-TargetRootFolder "User1 Mailbox"
Set-Mailbox		-SourceMailbox		

Correct Answer:

```
$InactiveMailebox - Get-Mailbox InactiveMailebox - Identity <distingusished name>
```

New-Mailbox	-InactiveMailbox	$InactiveMailebox.DistinguishedName
New-MailboxRestoreRequest	-LitigationHoldEnabled	-TargetRootFolder "User1 Mailbox"
Restore-Recoverableitems	-RetentionHoldEnabled	
Set-Mailbox	-SourceMailbox	

References: https://docs.microsoft.com/en-us/microsoft-365/compliance/restore-an-inactive-mailbox?view=o365-worldwide

QUESTION 3

HOTSPOT

You need to meet the technical requirements for the confidential documents.

What should you created first, and what should you use for the detection method? To answer, select the appropriate options in the answer area.

NOTE: Each correct selection is worth one point.

Hot Area:

Create first	5 / 18
A Compliance Manager assessment	
A content search	
A DLP policy	
A sensitive info type	
A sensitivity label	

Use for detection method
Dictionary
File type
Keywords
Regular expression

Correct Answer:

Create first
A Compliance Manager assessment
A content search
A DLP policy
A sensitive info type
A sensitivity label

Use for detection method
Dictionary
File type
Keywords
Regular expression

QUESTION 4

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 compliance 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-Mailbox -Identity "User1" -AuditEnabled $true command.

Does that meet the goal?

A. Yes

B. No

Correct Answer: A

Set-Mailbox

This cmdlet is available in on-premises Exchange and in the cloud-based service. Some parameters and settings may be exclusive to one environment or the other.

Use the Set-Mailbox cmdlet to modify the settings of existing mailboxes.

The AuditEnabled parameter must be set to $true to enable mailbox audit logging.

-AuditEnabled

The AuditEnabled parameter specifies whether to enable or disable mailbox audit logging for the mailbox. If auditing is enabled, actions specified in the AuditAdmin, AuditDelegate, and AuditOwner parameters are logged. Valid values are:

$true: Mailbox audit logging is enabled.

$false: Mailbox audit logging is disabled. This is the default value.

Reference:

QUESTION 5

You create a retention label that has a retention period of seven years.

You need to ensure that documents containing a credit card number are retained for seven years. Other documents must not be retained.

What should you create?

A. a retention label policy of type publish

B. a retention policy that retains file automatically

C. a retention policy that deletes files automatically

D. a retention label policy of type auto-apply

Correct Answer: D

Reference: https://docs.microsoft.com/en-us/microsoft-365/compliance/apply-retention-labels-automatically?view=o365-worldwide

QUESTION 6

You have a Microsoft 365 subscription that contains a Microsoft SharePoint Online site named Site1.

You need to create a data loss prevention (DLP) policy to prevent the sharing of files that contain source code. The solution must minimize administrative effort.

What should you include in the solution?

A. an exact data match (EDM) data classification

B. a sensitive info type that uses a keyword dictionary

C. a sensitive info type that uses regular expressions

D. a trainable classifier

Correct Answer: D

Support for trainable classifiers as a condition in your DLP policy

We are excited to share that you can now use trainable classifiers (out-of-the-box as well as custom) as conditions in your DLP policies to detect and prevent sensitive business contexts (e.g., financial statements, contracts, legal and HR

documents, etc.) as well as behavioral context data (e.g., discrimination, profanity, and more) from unauthorized use, sharing, or transfer.

See below for a chart of business content and behavior classifiers supported in DLP policies today. We will be adding additional classifiers to this list in the coming months.

* Source Code

detects items that contain a set of instructions and statements written in the top 25 used computer programming languages on GitHub.

Reference: https://techcommunity.microsoft.com/t5/security-compliance-and-identity/announcing-machine-learning-features-in-microsoft-purview-data/ba-p/3583916

QUESTION 7

You have a Microsoft 365 E3 subscription.

You plan to assess compliance with ISO/IEC 27001:2013.

From Compliance Manager, you discover that the ISO/IEC 27001:2013 regulatory template for Microsoft 365 is inactive.

What should you do?

A. Purchase a Microsoft 365 E5 subscription.

B. Add a data connector.

C. Add recommended assessments.

D. Create a trainable classifier.

Correct Answer: C

QUESTION 8

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 implement Microsoft 365 Endpoint data loss prevention (Endpoint DLP).

You have computers that run Windows 10 and have Microsoft 365 Apps installed. The computers are joined to Azure Active Directory (Azure AD).

You need to ensure that Endpoint DLP policies can protect content on the computers.

Solution: You deploy the unified labeling client to the computers.

Does this meet the goal?

A. Yes

B. No

Correct Answer: B

Reference: https://docs.microsoft.com/en-us/microsoft-365/compliance/endpoint-dlp-getting-started?view=o365-worldwide

QUESTION 9

HOTSPOT

You have a Microsoft 365 E5 subscription that contains a Microsoft SharePoint Online site named Site1 and the users shown in the following table.

Name	Microsoft 365 group	Site1 group
User1	Group1	Owner
User2	Group2	Member

Site1 includes a file named File1.docx.

You create two retention labels named Retention1 and Retention2.

You publish Retention1 to the following locations:

Exchange email Included: User1 Microsoft 365 Groups Included: Group2

You publish Retention2 to the following locations:

Exchange email Included: All recipients SharePoint sites Included: Site1

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
User1 can apply Retention1 or Retention2 to the email in his Exchange mailbox.	○	○
User2 can apply Retention1 to the email in his Exchange mailbox.	○	○
User2 can apply Retention2 to File1.docx.	○	○

Correct Answer:

Statements	Yes	No
User1 can apply Retention1 or Retention2 to the email in his Exchange mailbox.	●	○
User2 can apply Retention1 to the email in his Exchange mailbox.	○	●
User2 can apply Retention2 to File1.docx.	●	○

Box 1: Yes

User1 is included in Retention1.

All recipients (also User1) is included in Retention2.

Note: Advantages of using static scopes:

Simpler configuration if you want all instances automatically selected for a workload.

For "includes" and "excludes", this choice can be a simpler configuration initially if the numbers of instances that you have to specify are low and do not change. However, when these number of instances start to increase and you have

frequent changes in your organization that require you to reconfigure your policies, adaptive scopes can be simpler to configure and much easier to maintain.

Box 2: No

Only User1 is included in Retention1.

Box 3: Yes

User2 can apply Retention2.

Retention2 includes Site1.

Site1 includes a file named File1.docx.

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

QUESTION 10

Note: In-Place Hold and Litigation Hold in Exchange Online
In-Place Hold scenarios
In previous versions of Exchange, the notion of legal hold is to hold all mailbox data for a user indefinitely or until when hold is removed. In Exchange Online, In-Place Hold includes a new model that allows you to specify the following parameters:

What to hold: You can specify which items to hold by using query parameters such as keywords, senders and recipients, start and end dates, and also specify the message types such as email messages or calendar items that you want to place on hold.

How long to hold: You can specify a duration for items on hold.

Placing a mailbox on In-Place Hold
You can use the In-Place eDiscovery & Hold wizard in the Exchange admin center (EAC)
How to create an eDiscovery hold
To create an eDiscovery hold that's associated with a eDiscovery (Standard) case:

Step 1: Go to Microsoft Purview compliance portal and sign in using the credentials for user account with the appropriate eDiscovery permissions.

Step 2: In the left navigation pane, select Show all, and then select eDiscovery > Standard.

Step 3: On the eDiscovery (Standard) page, select the name of the case that you want to create the hold in.
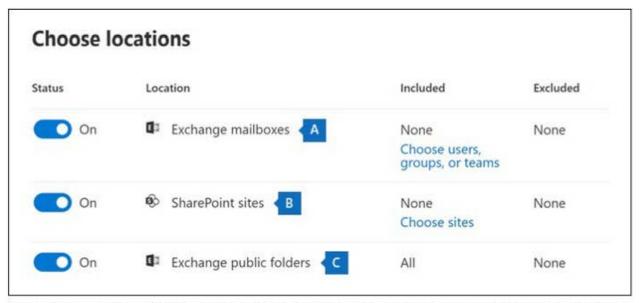
Step 4: On the Home page for the case, select the Hold tab.

Step 5: On the Hold page, select Create.

Step 6: On the Name your hold wizard page, give the hold a name and add an optional description, and then select Next. The name of the hold must be unique in your organization.

Step 7: On the Choose locations wizard page, choose the content locations that you want to place on hold. You can place mailboxes, sites, and public folders on hold.

Choose locations

Status	Location		Included	Excluded
On	📧 Exchange mailboxes A		None Choose users, groups, or teams	None
On	🌐 SharePoint sites B		None Choose sites	None
On	📧 Exchange public folders C		All	None

Step 7a: Exchange mailboxes: Set the toggle to On and then select Choose users, groups, or teams to specify the mailboxes to place on hold. Select the mailbox of Alex Wilber.

Question: You need to retain all Microsoft Exchange items in the mailbox of Alex Wilber.

Step 7b: SharePoint sites: Set the toggle to Off

Step 7c: Exchange public folders: Set to off.

Note: Set the toggle to On to put all public folders in your Exchange Online organization on hold. You can't choose specific public folders to put on hold. Leave the toggle switch off if you don't want to put a hold on public folders.

Step 8: When finished adding locations to the hold, select Next.

Step 9: To create a query-based hold using keywords or conditions, complete the following steps. To preserve all content in the specified content locations, select Next.

Query

∧ Keywords 🗑

Enter keywords A

☐ Show keyword list

＋ Add condition ∨ B

9a: add keyword: Falcon

9b: Add condition:
Specify: created in year 2021

For condition can type: created>=2021-01-01 AND created < 2022-01-01

Question: You need to retain all Microsoft Exchange items in the mailbox of Alex Wilber that contain the word Falcon and were created in the year 2021.

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 retain Microsoft SharePoint files that contain the word Falcon for two years from the date they were created, and then delete them.

To complete this task, sign in to the appropriate admin center.

A. Check the explanation

B. PlaceHold

C. PlaceHold

D. PlaceHold

Correct Answer: A

Plan:
Stage 1: Create custom sensitive information types in the Microsoft Purview compliance portal
Stage 2: Create retention policy and use the sensitive info type created in stage 1

Stage 1: Create custom sensitive information types in the Microsoft Purview compliance portal

Create a custom SIT from scratch

Step 1: Use the following procedure to fully define a brand new sensitive information type.

Step 2: In the Microsoft Purview compliance portal, navigate to Data classification > Classifiers > Sensitive info types and choose Create sensitive info type.

Step 3: Fill in values for Name and Description and choose Next.

Step 4: Choose Create pattern. You can create multiple patterns, each with different elements and confidence levels, as you define your new sensitive information type.

Step 5: Choose the default confidence level for the pattern. The values are Low confidence, Medium confidence, and High confidence.

Step 6: Choose and define the Primary element. Choose Keyword list.

Step 7: Enter: Falcon

Question: You need to retain Microsoft SharePoint files that contain the word Falcon for two years from the date they were created, and then delete them.

Step 8: Finish the wizard.

Stage 2: Create retention policy and use the sensitive info type created in stage 1

Step 1: From the Microsoft Purview compliance portal, select Data lifecycle management > Microsoft 365 > Retention Policies.

Step 2: Select New retention policy to start the Create retention policy configuration, and name your new retention policy.

Step 3: For the Assign admin units page select Full directory.
You must select Full directory for the policy to include the locations for SharePoint sites and Exchange public folders.

Step 4: For the Choose the type of retention policy to create page, select Adaptive or Static. Select Static.

Step 5: For location: Select Items, and Sharepoint

Step 6: Somehow include the sensitive information type you created in Stage 1.

Step 7: For Decide if you want to retain content, delete it:
Select: On the Decide if you want to retain content, delete it, or both page, select Retain items for a specific period, specify the retention period [specify 2 years], and then for At end of the retention period select Delete items automatically.

Question: You need to retain Microsoft SharePoint files that contain the word Falcon for two years from the date they were created, and then delete them.

Decide if you want to retain content, delete it, or both

◉ Retain items for a specific period
Items will be retained for the period you choose.

Retain items for a specific period

| 7 years ⌄ |

Start the retention period based on

| When items were created ⌄ |

At the end of the retention period

◯ Delete items automatically

◉ Do nothing

◯ Retain items forever
Items will be retained forever, even if users delete them.

◯ Only delete items when they reach a certain age
Items won't be retained, but when they reach the age you choose, we'll delete them from where they're stored.

QUESTION 11

You have a Microsoft 365 subscription that contains a Microsoft 365 group named Group1. Group1 contains 100 users and has dynamic user membership.

All users have Windows 10 devices and use Microsoft SharePoint Online and Exchange Online.

You create a sensitivity label named Label1 and publish Label1 as the default label for Group1.

You need to ensure that the users in Group must apply Label1 to their email and documents.

Which two actions should you perform? Each correct answer presents part of the solution

NOTE: Each correct selection is worth one point.

A. From the Microsoft Purview compliance portal, create an auto-labeling policy.

B. Install the Active Directory Rights Management Services (AD RMS) client on the Windows 10 devices,

C. From the Microsoft Purview compliance portal, modify the settings of the Label1 policy.

D. Install the Azure Information Protection unified labeling client on the Windows 10 devices.

E. From the Microsoft Entra admin center, set Membership type for Group1 to Assigned.

Correct Answer: CD

Reference: https://learn.microsoft.com/en-us/purview/apply-sensitivity-label-automatically https://learn.microsoft.com/en-us/purview/sensitivity-labels-teams-groups-sites

---

QUESTION 12

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 are investigating a data breach.

You need to retain all Microsoft Exchange items in the mailbox of Alex Wilber that contain the word Falcon and were created in the year 2021.

To complete this task, sign in to the appropriate admin center.

A. Check the explanation

B. PlaceHold

C. PlaceHold

D. PlaceHold

Correct Answer: A

QUESTION 13

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 configuring a file policy in Microsoft Cloud App Security.

You need to configure the policy to apply to all files. Alerts must be sent to every file owner who is affected by the policy. The policy must scan for credit card numbers, and alerts must be sent to the Microsoft Teams site of the affected

---

department.

Solution: You use the Built-in DLP inspection method and send alerts to Microsoft Power Automate.

Does this meet the goal?

A. Yes

B. No

Correct Answer: A

Reference: https://docs.microsoft.com/en-us/cloud-app-security/content-inspection-built-in https://docs.microsoft.com/en-us/cloud-app-security/flow-integration

---

QUESTION 14

You have a Microsoft 365 tenant that uses 100 data loss prevention (DLP) policies.

A Microsoft Exchange administrator frequently investigates emails that were blocked due to DLP policy violations.

You need recommend which DLP report the Exchange administrator can use to identify how many messages were blocked based on each DLP policy.

Which report should you recommend?

A. Third-party DLP policy matches

B. DLP policy matches

C. DLP incidents

D. False positive and override

Correct Answer: B

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

---

QUESTION 15

You create a label that encrypts email data.

Users report that they cannot use the label in Outlook on the web to protection the email messages they send.

You need to ensure that the users can use the new label to protect their email.

What should you do?

A. Create a label policy.

B. Create a new sensitive information type.

C. Modify the priority order of label policies.

D. Wait six hours and ask the users to try again.

Correct Answer: A

Admin has to publish labels by creating label policy.

Reference: https://docs.microsoft.com/en-us/microsoft-365/compliance/sensitivity-labels#what-label-policies-can-do

Latest SC-400 Dumps   SC-400 Study Guide   SC-400 Braindumps