



Up-to-date Questions and Answers from authentic resources to improve knowledge and pass the exam at very first attempt. ---- Guaranteed.



SC-400 MCQs
SC-400 TestPrep
SC-400 Study Guide
SC-400 Practice Test
SC-400 Exam Questions



Microsoft

SC-400

Microsoft Information Protection Administrator



Question: 103

You need to be alerted when users share sensitive documents from Microsoft OneDrive to any users outside your company.

What should you do?

- A. From the Microsoft 365 compliance center, create a data loss prevention (DLP) policy.
- B. From the Azure portal, create an Azure Active Directory (Azure AD) Identity Protection policy.
- C. From the Microsoft 365 compliance center, create an insider risk policy.
- D. From the Microsoft 365 compliance center, start a data investigation.

Answer: B

Question: 104

You have a Microsoft 365 tenant.

All Microsoft OneDrive for Business content is retained for five years.

A user named User1 left your company a year ago, after which the account of User 1 was deleted from Azure Active Directory (Azure AD)

You need to recover an important file that was stored in the OneDrive of User1.

What should you use?

- A. Deleted users in the Microsoft 365 admin center
- B. the Restore-SPODeletedSite- PowerShell cmdlet
- C. the Restore-ADObject PowerShell cmdlet
- D. the OneDrive recycle bin

Answer: D

Question: 105

You are configuring a data loss prevention (DLP) policy to report when credit card data is found on a Windows 10 device joined to Azure Active Directory (Azure AD).

You plan to use information from the policy to restrict the ability to copy the sensitive data to the clipboard.

What should you configure in the policy rule?

- A. the incident report
- B. an action
- C. user notifications
- D. user overrides

Answer: D

Explanation:

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

Question: 106

You plan to implement sensitivity labels for Microsoft Teams.

You need to ensure that you can view and apply sensitivity labels to new Microsoft Teams sites.

What should you do first?

- A. Run the Set-sposite cmdlet.
- B. Configure the EnableMTPLabels Azure Active Directory (Azure AD) setting.
- C. Create a new sensitivity label scoped to Groups & sites.
- D. Run the Execute-AzureAdLabelSync cmdlet.

Answer: A

Question: 107

DRAG DROP

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

You have a custom employee information form named Template 1.docx.

You need to create a classification rule package based on the document fingerprint of Templatel.docx.

Which three actions should you perform in sequence? To answer, move the appropriate actions from the list of actions to the answer area and arrange them in the correct order.

Actions	Answer Area
Create a variable that contains the result of the get-Content cmdlet.	
Run the New-DlpSensitiveInformationType cmdlet.	
Create a variable that contains the result of the New-DlpFingerprint cmdlet.	
Run the Set-DlpSensitiveInformationType cmdlet.	
Create a variable that contains the result of the get-ContentFilterPhrase cmdlet.	

Answer:

Actions	Answer Area
Create a variable that contains the result of the Get-Content cmdlet.	Create a variable that contains the result of the New-DlpFingerprint cmdlet.
Run the New-DlpSensitiveInformationType cmdlet.	Run the Set-DlpSensitiveInformationType cmdlet.
Create a variable that contains the result of the New-DlpFingerprint cmdlet.	Create a variable that contains the result of the Get-ContentFilterPhrase cmdlet.
Run the Set-DlpSensitiveInformationType cmdlet.	
Create a variable that contains the result of the Get-ContentFilterPhrase cmdlet.	

Question: 108

You have a new Microsoft 365 tenant.

You need to ensure that custom trainable classifiers can be created in the tenant.

To which role should you be assigned to perform the configuration?

- A. Security administrator
- B. Security operator
- C. Global administrator
- D. Compliance administrator

Answer: D

Explanation:

Reference: <https://docs.microsoft.com/en-us/microsoft-365/compliance/classifier-get-started-with?view=o365-worldwide>

Question: 109

You have a data loss prevention (DLP) policy that applies to the Devices location. The policy protects documents that contain States passport numbers.

Users reports that they cannot upload documents to a travel management website because of the policy.

You need to ensure that the users can upload the documents to the travel management website. The solution must prevent the protected content from being uploaded to other locations.

Which Microsoft 365 Endpoint data loss prevention (Endpoint DLP) setting should you configure?

- A. Unallowed apps
- B. File path exclusions
- C. Service domains
- D. Unallowed browsers

Answer: A

Question: 110

You need to create a retention policy to delete content after seven years from the following locations:

Exchange email SharePoint sites

OneDrive accounts Office 365 groups

Teams channel messages Teams chats

What is the minimum number of retention policies that you should create?

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

Answer: A

Explanation:

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

Question: 111

Topic 1, Misc. Questions

You need to be alerted when users share sensitive documents from Microsoft OneDrive to any users outside your company.

What should you do?

- A. From the Microsoft 365 compliance center, create a data loss prevention (DLP) policy.
- B. From the Azure portal, create an Azure Active Directory (Azure AD) Identity Protection policy.
- C. From the Microsoft 365 compliance center, create an insider risk policy.
- D. From the Microsoft 365 compliance center, start a data investigation.

Answer: B

Question: 112

You have a data loss prevention (DLP) policy that applies to the Devices location. The policy protects documents that contain States passport numbers.

Users reports that they cannot upload documents to a travel management website because of the policy.

You need to ensure that the users can upload the documents to the travel management website. The solution must prevent the protected content from being uploaded to other locations.

Which Microsoft 365 Endpoint data loss prevention (Endpoint DLP) setting should you configure?

- A. Unallowed apps
- B. File path exclusions
- C. Service domains
- D. Unallowed browsers

Answer: A

Question: 113

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

Answer: B

Question: 114

HOTSPOT

You create a retention label policy named Contoso_policy that contains the following labels.

10 years then delete

5 years then delete

Do not retain

Contoso_Policy is applied to content In Microsoft Sharepoint Online sites.

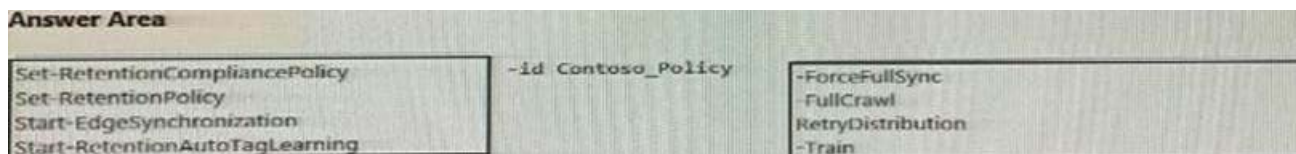
After a couple of days, you discover the following messages on the Properties page of the label policy.

* Statue Off (Error)

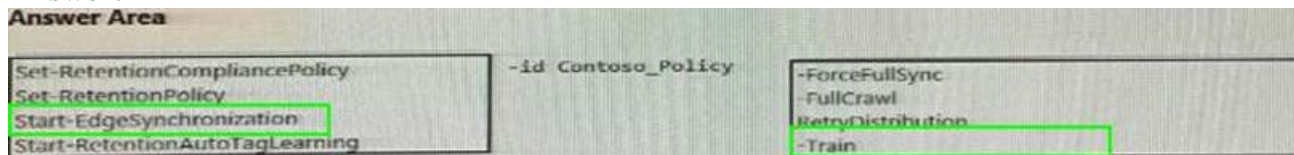
* It's taking longer than expected to deploy the policy

You need to reinitiate the policy.

How should you complete the command? To answer, select the appropriate options in the; answer area. NOTE: Each correct selection is worth one point.

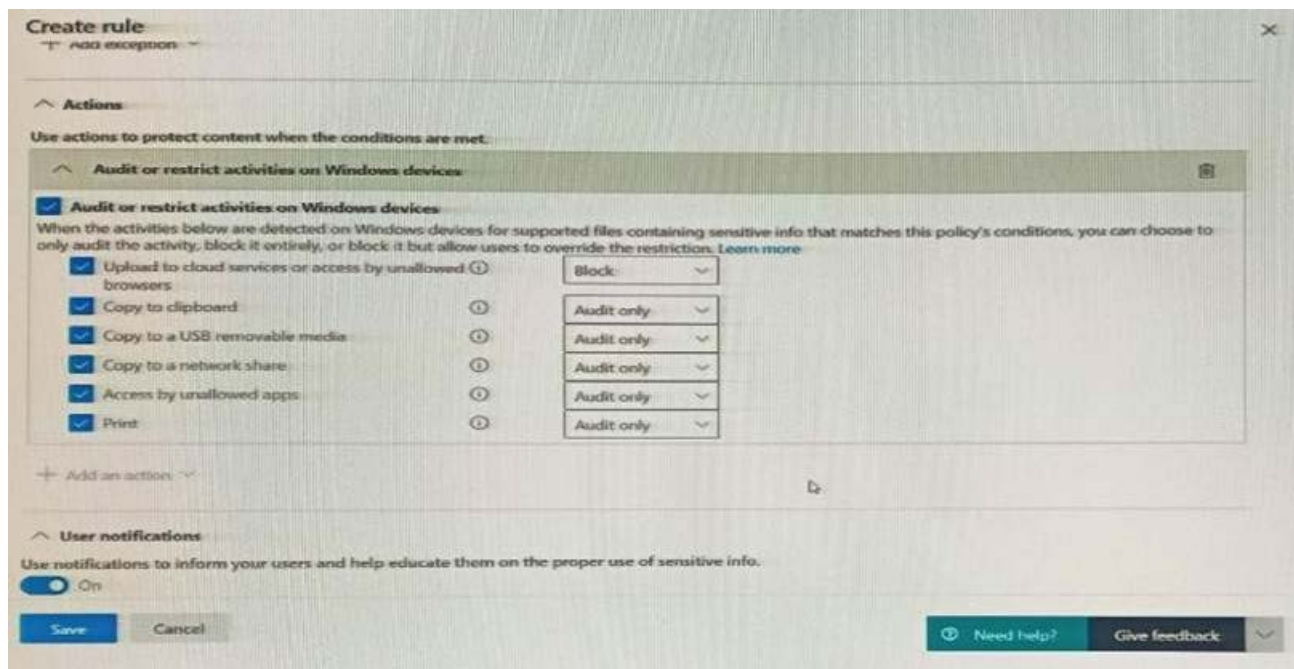


Answer:



Question: 115

You have a data loss prevention (DLP) policy configured for endpoints as shown in the following exhibit.



From a computer named Computer1, 3 user can sometimes upload files to cloud services and sometimes cannot. Other users experience the same issue.

What are two possible causes of the issue? Each correct answer presents a complete solution. NOTE: Each correct selection is worth one point.

- A. The Access by unallowed apps action is set to Audit only.
- B. The computers are NOT onboarded to the Microsoft 365 compliance center.
- C. The Copy to clipboard action is set to Audit only.
- D. There are file path exclusions in the Microsoft 365 Endpoint data loss prevention (Endpoint DIP) settings.
- E. The unallowed browsers in the Microsoft 365 Endpoint data loss prevention (Endpoint DLP) settings are NOT configured.

Answer: A,D

Question: 116

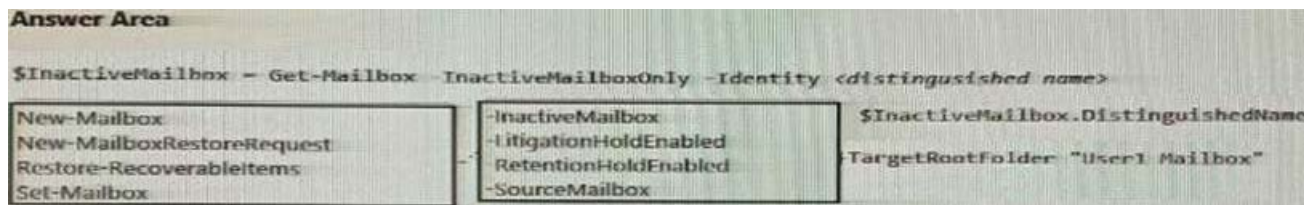
HOTSPOT

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

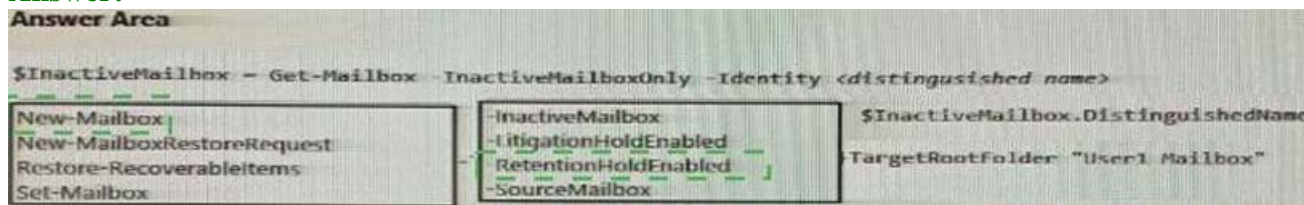
A user named User1 leaves your company. The mailbox of User1 is placed on Litigation Hold, and then the account of User1 is deleted from Azure Active Directory (Azure AD).

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.



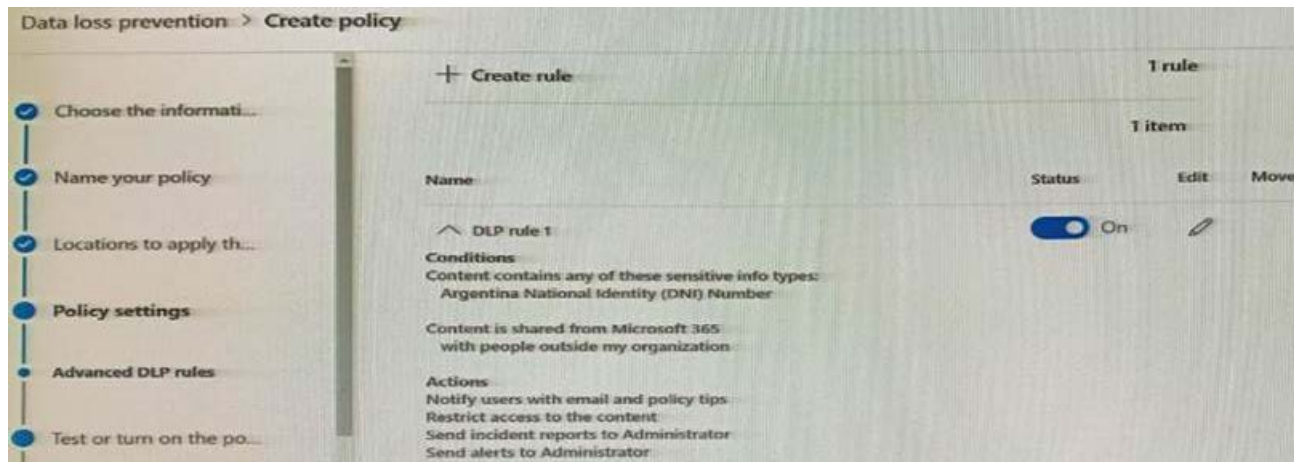
Answer:



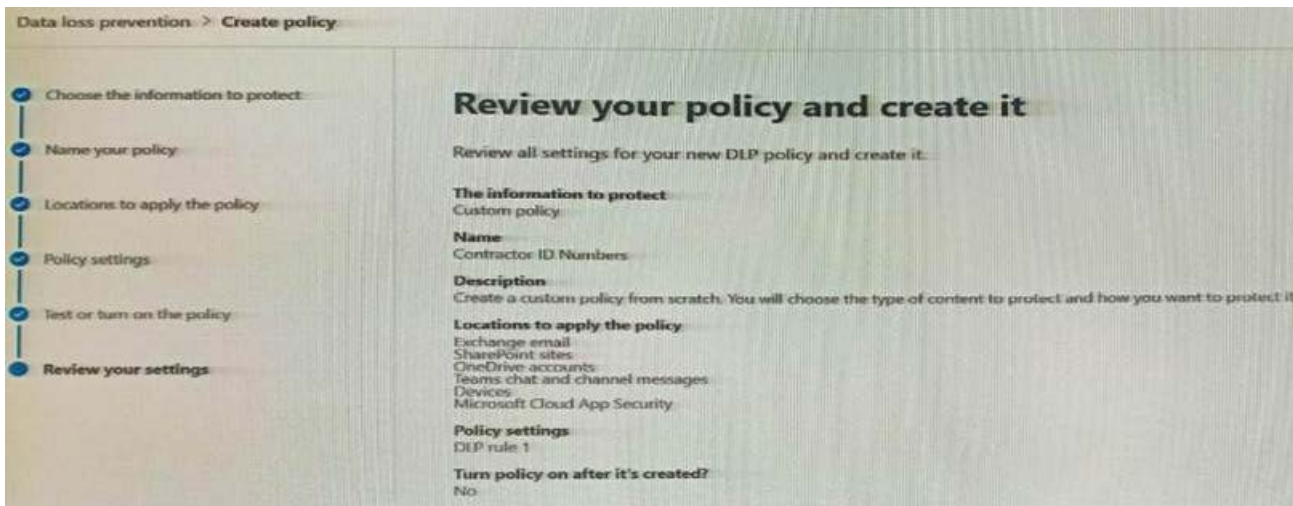
Question: 117

You create a data loss prevention (DLP) policy.

The Advanced DLP rules page is shown in the Rules exhibit.



The Review your settings page is shown in the review exhibit.



You need to review the potential impact of enabling the policy without applying the actions.

What should you do?

- A. Edit the policy, remove all the actions in DIP rule 1, and select I'd like to test it out first
- B. Edit the policy, remove the Restrict access to the content and Send incident report to Administrator actions, and then select Yes, turn it on right away.
- C. the policy. remove all the actions in DLP rule 1, and select Yes, turn it on right away.
- D. Edit the policy, and then select I'd like to test it out first.

Answer: C

Question: 118

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

You are implementing data loss prevention (DIP).

The company's default browser in Microsoft Edge.

During a recent audit, you discover that some user use Firefox and Google Chromo browsers to upload files labeled as Confidential to a third party Microsoft SharePoint Online site that has a URL of <https://m365x076709.sharepoint>. Uses are blocked from uploading the confidential files to the site from Microsoft Edge.

You need to ensure that the users cannot upload files labels as Confidential from Firefox and Google Chrome to any cloud services. NOTE: Each correct selection is worth one point.

- A. From the Microsoft 3G5 Endpoint data loss prevention (Endpoint DLP) settings, add Firefox and Google Chrome to the unallowed browsers list.
- B. Create a DIP policy that applies to the Devices location.
- C. From the Microsoft 365 Endpoint data loss prevention (Endpoint) DLP settings, add contoso.com as an allowed service domain.
- D. From the Microsoft 365 compliance center, onboard the dcvu.es.
- E. From the Microsoft J6b Endpoint data loss prevention (Endpoint) DLP settings, add: m36Sx0767W-sharepomt.com as a blacked service domain.

Answer: A,C

Question: 119

HOTSPOT

While creating a retention label, you discover that the following options are missing:

- * Mark items as a record
- * Mark items are a regular record

You need to ensure that the options are available when you create label in the Microsoft 365 compliance center.

How should you complete the PowerShell script? To answer, select the appropriate options in the answer area. NOTE: Each correct selection is worth one point.

Answer Area

```
$UserCredential = Get-Credential

Import-Module AzureRM
                ExchangeOnlineManagement
                Microsoft.Online.SharePoint.PowerShell
                MicrosoftTeams

Connect-AadrmService
Connect-AzureAD
Connect-AzureRMAccount
Connect-IPPSSession -Credential $UserCredential

Enable-ComplianceTagStorage
New-ComplianceTag
Set-RegulatoryComplianceUI
Set-RetentionCompliancePolicy -Enabled $true
```

Answer:

Answer Area

```
$UserCredential = Get-Credential

Import-Module AzureRM
                ExchangeOnlineManagement
                Microsoft.Online.SharePoint.PowerShell
                MicrosoftTeams

Connect-AadrmService
Connect-AzureAD
Connect-AzureRMAccount
Connect-IPPSSession -Credential $UserCredential

Enable-ComplianceTagStorage
New-ComplianceTag
Set-RegulatoryComplianceUI
Set-RetentionCompliancePolicy -Enabled $true
```

Killexams.com is a leading online platform specializing in high-quality certification exam preparation. Offering a robust suite of tools, including MCQs, practice tests, and advanced test engines, Killexams.com empowers candidates to excel in their certification exams. Discover the key features that make Killexams.com the go-to choice for exam success.



Exam Questions:

Killexams.com provides exam questions that are experienced in test centers. These questions are updated regularly to ensure they are up-to-date and relevant to the latest exam syllabus. By studying these questions, candidates can familiarize themselves with the content and format of the real exam.

Exam MCQs:

Killexams.com offers exam MCQs in PDF format. These questions contain a comprehensive collection of questions and answers that cover the exam topics. By using these MCQs, candidate can enhance their knowledge and improve their chances of success in the certification exam.

Practice Test:

Killexams.com provides practice test through their desktop test engine and online test engine. These practice tests simulate the real exam environment and help candidates assess their readiness for the actual exam. The practice test cover a wide range of questions and enable candidates to identify their strengths and weaknesses.

Guaranteed Success:

Killexams.com offers a success guarantee with the exam MCQs. Killexams claim that by using this materials, candidates will pass their exams on the first attempt or they will get refund for the purchase price. This guarantee provides assurance and confidence to individuals preparing for certification exam.

Updated Contents:

Killexams.com regularly updates its question bank of MCQs to ensure that they are current and reflect the latest changes in the exam syllabus. This helps candidates stay up-to-date with the exam content and increases their chances of success.