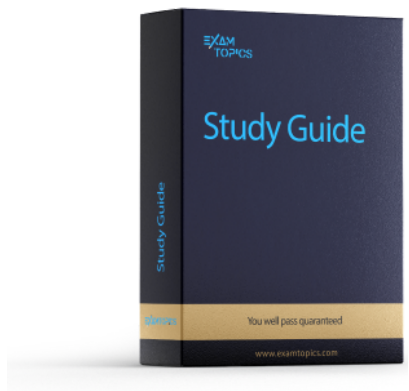
EXAMTOPICS
- Expert Verified, Online, **Free**.

Prepare for your SC-400 exam with additional products

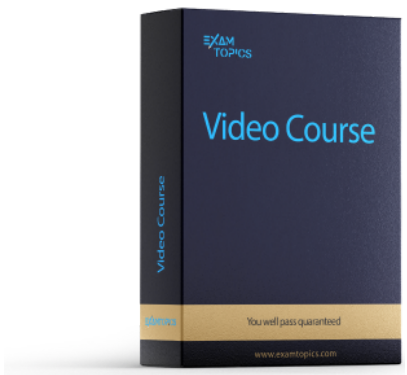


Study Guide

427 PDF Pages

$19.99

Buy Now



Video Course

58 Lectures

$19.99

Buy Now

Custom View Settings

Question #1 *Topic 1*

You create three sensitivity labels named Sensitivity1, Sensitivity2, and Sensitivity3 and perform the following actions:
- Publish Sensitivity1.
- Create an auto-labeling policy for Sensitivity2.

You plan to create a file policy named Policy1 in Microsoft Cloud App Security.
Which sensitivity labels can you apply to Microsoft SharePoint Online in Policy1?

A. Sensitivity1 only

B. Sensitivity1, Sensitivity2, and Sensitivity3

C. Sensitivity2 only

D. Sensitivity1 and Sensitivity2 only

Correct Answer: *D*
Reference:
https://docs.microsoft.com/en-us/microsoft-365/compliance/apply-sensitivity-label-automatically?view=o365-worldwide
https://docs.microsoft.com/en-us/cloud-app-security/azip-integration

Community vote distribution
A (100%)

DeeJayU Highly Voted 1 year, 11 months ago
Selected Answer: A
Tested.
"For Defender for Cloud Apps to apply sensitivity labels, they must be published as part of a sensitivity label policy in the Microsoft 365 compliance center." does not mention auto-labeling policy as an option.
upvoted 20 times

Mdwro 1 year, 10 months ago
I think it is correct
upvoted 2 times

UWSFish 1 year, 10 months ago
Agree DeeJayU, tried myself as well just now. auto-label policy does not make sensitivity label available in MDCA (MCAS) file policy.
upvoted 5 times

UWSFish 1 year, 9 months ago
exclude the NOT, you need an auto-label policy for it to surface in MDCA
upvoted 1 times

cng Highly Voted 2 years, 6 months ago
I believe the answer provided is correct for the following reasons:
1. You cannot add an empty sensitivity label to a policy, and because no information about 'Sensitivity3' is provided we have to assume that it is empty
2. 'Sensitivity1' has already been published so it is not empty
3. Information about 'Sensitivity2' is provided so it is not empty

https://docs.microsoft.com/en-us/microsoft-365/compliance/create-sensitivity-labels?view=o365-worldwide
upvoted 19 times

Davidf Most Recent 3 months, 3 weeks ago
Selected Answer: A
Tested in a sandbox tenant, only sensitivity1 is available
upvoted 2 times

TeeKay_From_the_South 5 months, 1 week ago
D. is correct.
Sensitivity labels need to be published in order to work and Sensitivity2 is already working now you just need to create an auto-label policy.
Microsoft was sneaky with the wording here.
upvoted 2 times

doori88 6 months ago
just tested it, its Sensitivity label 1 only so answer is A

upvoted 1 times

dmoorthy 7 months, 1 week ago

Selected Answer: A

upvoted 1 times

xswe 7 months, 3 weeks ago

Selected Answer: A

A, since you can only apply sensitivty labels that has been published and the other one has been used in an auto-labeling policy which means that it wont be available in this file policy that you are creating.

"For Defender for Cloud Apps to apply sensitivity labels, they must be published as part of a sensitivity label policy in the Microsoft Purview compliance portal."

upvoted 1 times

Bluebaron520 1 year ago

valid 24/11/2022

upvoted 1 times

mcas 1 year, 1 month ago

Selected Answer: A

For Defender for Cloud Apps to apply sensitivity labels, they must be published as part of a sensitivity label policy in the Microsoft Purview compliance portal.

https://learn.microsoft.com/en-us/defender-cloud-apps/azip-integration#prerequisites

upvoted 1 times

mandragon 1 year, 5 months ago

Selected Answer: A

You (the user) cannot apply Sensitivity2. It is published with an auto-labeling policy. An auto-labeling policy is server-side labeling (meaning automatic not manual). Because server-side labeling is applied by services rather than by applications, you cannot set an MCAS filter your data based on Sensitivity2.

https://docs.microsoft.com/en-us/microsoft-365/compliance/apply-sensitivity-label-automatically?view=o365-worldwide - See where it says server-side labeling

upvoted 3 times

JamesM9 1 year, 7 months ago

I have just tested this in my test tenant - I was able to create an auto-labelling policy for a custom sensitivity label and then auto-assign this to SharePoint sites only or indeed specific SharePoint sites only.

Therefore, the answer here is D - Sensitivity 1 and 2.

upvoted 2 times

Holii 1 year, 6 months ago

Re-read the question.
It asks you which Sensitivity labels can you apply to SharePoint Online within the MCAS File Policy.

Theoretically, yes it would apply an auto-label to all documents within SharePoint- but it will never surface as an option for a Sensitivity Label within Policy1 of MCAS. That is only for Published Sensitivity Labels.

Once again, ambiguous question from Microsoft.
Either A or D up to your interpretation.

upvoted 3 times

flashflo 1 year, 10 months ago

at https://docs.microsoft.com/en-us/defender-cloud-apps/file-filters#file-filters is written for the Sensitivity label: "- Search for files with specific labels set."
so a lable must be able to apply to a file. This is true for published lables (manual) but also for auto-labeling policy. so Answer D is correct

upvoted 2 times

Holii 1 year, 6 months ago

...? You've linked information on how to filter for File information- not how to construct a File Policy within MCAS.

Within the Governance Actions inside MCAS File Policy, you can only select Published Sensitivity Labels.
MCAS will assume any DLP Auto-Policy doesn't have to be managed by MCAS (since it's already applied automatically)...but in regards to the question, it seems to be asking "Which can be selected within MCAS" which would be Answer A.

upvoted 1 times

Der_97 2 years, 2 months ago

Correct answer

upvoted 2 times

MahmoudEldeep 2 years, 3 months ago

I think correct anser is B. As you can use any created sensitivity labels even if it is not published.

upvoted 1 times

pheb 2 years, 3 months ago

No, you can't. Just tried it in MCAS with a new file policy. If you created labels, but never published them, they can not be used.

upvoted 10 times

Question #2 *Topic 1*

You have a Microsoft OneDrive for Business folder that contains the files shown in the following table.

Type	Number of files
.jpg	50
.docx	300
.txt	50
.zip	20

In Microsoft Cloud App Security, you create a file policy to automatically apply a classification.
What is the effect of applying the policy?

A. The policy will apply to only the .docx and .txt files. The policy will classify the files within 24 hours.

B. The policy will apply to all the files. The policy will classify only 100 files daily.

C. The policy will apply to only the .docx files. The policy will classify only 100 files daily.

D. The policy will apply to only the .docx and .txt files. The policy will classify the files immediately.

Correct Answer: *C*

Reference:

https://docs.microsoft.com/en-us/cloud-app-security/azip-integration

Community vote distribution

C (67%) B (33%)

jcgonzalez1978 Highly Voted 2 years, 3 months ago

Cloud App Security currently supports applying Azure Information Protection classification labels for the following file types:
- Word: docm, docx, dotm, dotx
- Excel: xlam, xlsm, xlsx, xltx
- PowerPoint: potm, potx, ppsx, ppsm, pptm, pptx
- PDF

The ability to automatically apply an Azure Information Protection label through file policy is a powerful capability. To protect customers from mistakenly applying a label to a large number of files, as a safety precaution there is a daily limit of 100 Apply label actions per app, per tenant. After the daily limit is reached, the apply label action pauses temporarily and continues automatically the next day (after 12:00 UTC). To raise the limit for your tenant, open a support ticket.
When a policy is disabled, all pending labeling tasks for that policy are suspended.
https://docs.microsoft.com/en-us/cloud-app-security/azip-integration

upvoted 21 times

sergioandreslq 1 year, 11 months ago

Yeap, That is correct for MCAS (new named Defender for Cloud Apps).
As addition, there are other 2 services for auto-labeling:
Client-side Auto-labeling and Service-side Auto-labeling.
In these other auto-labeling services the format supported are greather than MCAS.
Adobe Portable Document Format: .pdf
Microsoft Project: .mpp, .mpt
Microsoft Publisher: .pub
Microsoft XPS: .xps .oxps
Images: .jpg, .jpe, .jpeg, .jif, .jfif, .jfi. png, .tif, .tiff
Autodesk Design Review 2013: .dwfx
Adobe Photoshop: .psd
Digital Negative: .dng
Microsoft Office: The following file types, including 97-2003 file formats and Office Open XML formats for Word, Excel, and PowerPoint:
.doc
.docm
.docx
.dot
.dotm
.dotx
.potm
.potx
.pps
.ppsm
.ppsx
.ppt
.pptm
.pptx
.vdw
.vsd

.vsdm
.vsdx
.vss
.vssm
.vst
.vstm
.vssx
.vstx
.xls
.xlsb
.xlt
.xlsm
.xlsx
.xltm
.xltx

Reference:
https://docs.microsoft.com/en-us/azure/information-protection/rms-client/clientv2-admin-guide-file-types#file-types-supported-for-classification-only

upvoted 2 times

Davidf Most Recent 3 months, 3 weeks ago

Selected Answer: C

C is correct, only files which can hold meta data can contain a sensitivity labels, zip, jpg and txt do not support meta data

upvoted 1 times

lmedeiros_69 6 months, 1 week ago

Qual e a resposta correta? rsrsrs Eu vou de C

upvoted 1 times

xswe 7 months, 3 weeks ago

Selected Answer: B

Auto applying sensitivity labels in Cloud Apps only sorts the following file types,

Word: docm, docx, dotm, dotx
Excel: xlam, xlsm, xlsx, xltx
PowerPoint: potm, potx, ppsx, ppsm, pptm, pptx
PDF

And for safety reason you can ONLY auto-apply sensitivity labels to 100 files per day

upvoted 1 times

xswe 7 months, 3 weeks ago

I mean ---- C

upvoted 1 times

wooyourdaddy 1 year, 6 months ago

Selected Answer: C

Ref links: https://docs.microsoft.com/en-us/azure/information-protection/rms-client/clientv2-admin-guide-file-types#file-types-supported-for-classification-only

Ref link: https://docs.microsoft.com/en-us/cloud-app-security/azip-integration

upvoted 1 times

ultrakicks 1 year, 8 months ago

The answer is correct as of today.

upvoted 1 times

MahmoudEldeep 2 years, 3 months ago

Seems Correct as the supported file types for classification (Word, Excel,PowerPoint,PDF).

upvoted 4 times

Eltooth 2 years, 5 months ago

Answer appears to be correct.

upvoted 3 times

HOTSPOT -

You have a Microsoft 365 tenant named contoso.com that contains two users named User1 and User2. The tenant uses Microsoft Office 365 Message Encryption
(OME).

User1 plans to send emails that contain attachments as shown in the following table.

Subject	To	Attachment type	Message size
Mail1	User2@contoso.com	.docx	40 MB
Mail2	User4@outlook.com	.doc	3 MB
Mail3	User3@gmail.com	.xlsx	7 MB

User2 plans to send emails that contain attachments as shown in the following table.

Subject	To	Attachment type	Message size
Mail4	User1@contoso.com	.pptx	4 MB
Mail5	User4@outlook.com	.jpg	6 MB
Mail6	User3@gmail.com	.docx	3 MB

For which emails will the attachments be protected? To answer, select the appropriate options in the answer area.

NOTE: Each correct selection is worth one point.

Hot Area:

Answer Area

User1:

- Mail1 only
- Mail3 only
- Mail1 and Mail2 only
- Mail2 and Mail3 only
- Mail1, Mail2, and Mail3

User2:

- Mail5 only
- Mail6 only
- Mail4 and Mail5 only
- Mail4 and Mail6 only
- Mail4, Mail5, and Mail6

Answer Area

Correct Answer:

User1:

- Mail1 only
- Mail3 only
- Mail1 and Mail2 only
- Mail2 and Mail3 only
- Mail1, Mail2, and Mail3

User2:

- Mail5 only
- Mail6 only
- Mail4 and Mail5 only
- Mail4 and Mail6 only
- Mail4, Mail5, and Mail6

Reference:
https://support.microsoft.com/en-gb/office/introduction-to-irm-for-email-messages-bb643d33-4a3f-4ac7-9770-fd50d95f58dc?ui=en-us&rs=en-gb&ad=gb#FileTypesforIRM https://docs.microsoft.com/en-us/microsoft-365/compliance/ome?view=o365-worldwide https://docs.microsoft.com/en-us/office365/servicedescriptions/exchange-online-service-description/exchange-online-limits#message-limits-1

jarihd1 Highly Voted 2 years, 7 months ago
Mail1 Size is bigger than supported and JPG is not supported format
upvoted 26 times

sergioandreslq 1 year, 11 months ago
The files .doc are protected by Azure Information Right management but not encrypted. meaning that the email from user1 with extension .doc will be protected by Azure
Information Right management, however, the email with extesion .doc won't be encrypted.
OME does not support the 97-2003 versions of the following Office programs: Word (.doc), Excel (.xls), and PowerPoint (.ppt)
https://docs.microsoft.com/en-us/azure/information-protection/rms-client/client-admin-guide-file-types#footnote-1

It is correct for the file size encrypted, the maximum is 25MB
https://docs.microsoft.com/en-us/azure/information-protection/rms-client/client-admin-guide-file-types#footnote-1
upvoted 5 times

BTAB 1 year, 6 months ago
Correct also verified here

https://docs.microsoft.com/en-us/microsoft-365/compliance/ome-faq?view=o365-worldwide#what-file-types-are-supported-as-attachments-in-protected-emails--do-attachments-inherit-the-protection-policies-associated-with-protected-emails-
upvoted 2 times

Brox Highly Voted 2 years, 5 months ago
User1 should be mail3 only. .doc files are not supported, it is in the link eriksrocha posted.

You can attach any file type to a protected mail. With one exception, protection policies are applied only on the file formats mentioned in File types supported by the Azure Information Protection client. OME does not support the 97-2003 versions of the following Office programs: Word (.doc), Excel (.xls), and PowerPoint (.ppt).
upvoted 18 times

test123123 2 years, 5 months ago
Na dude, even .doc works. Have a look at
https://mn.gov/admin/assets/Office%20365%20Outlook%20Email%20Encryption%20Instructions_tcm36-426033.pdf
upvoted 4 times

MahmoudEldeep 2 years, 3 months ago

Please refer to Microsoft Docs:
https://docs.microsoft.com/en-us/microsoft-365/compliance/ome-faq?view=o365-worldwide#what-file-types-are-supported-as-attachments-in-protected-emails--do-attachments-inherit-the-protection-policies-associated-with-protected-emails-

upvoted 4 times

Topaz007 2 years, 2 months ago

This is correct indeed. The 'old' Office files will b classified only NOT protected, which is the question. Also see here: https://docs.microsoft.com/en-us/azure/information-protection/rms-client/client-admin-guide-file-types under the header 'File types supported for classification only': The supported file formats for these file types are the 97-2003 file formats and Office Open XML formats for the following Office programs: Word, Excel, and PowerPoint. That table also contains the .doc extension.

upvoted 3 times

Dhamus Most Recent 2 months, 2 weeks ago

I think this type of encryption is no longer used today.

upvoted 3 times

xswe 7 months, 3 weeks ago

The max size for the OME encryption functionality is 25 mb and all file extension are not covered by the OME encryption. You can only encrypt docx files, powerpoint files and excel files. The following are the one supported,

Old file extension such as xls, doc and ppt are not supported.

Correct answer: Mail 3, since 40mb is too big and doc are not supported
Mail 4 and Mail 6, since jpg are not supported.

upvoted 2 times

MartinSebek 10 months, 3 weeks ago

According to the documentation this answer is still valid. Maximum size of email is 25MB and 97-2003 formats of Office documents is not supported.
https://learn.microsoft.com/en-us/microsoft-365/compliance/ome-faq?view=o365-worldwide

upvoted 6 times

NinjaSchoolProfessor 11 months, 2 weeks ago

This answer is outdated and all file types from User 1 are now supported (.doc, .docx, .xlsx) with a file size maximum of 512MB. User two answer of Mail 4 and Mail 6 are still correct.

upvoted 1 times

Davidf 3 months, 3 weeks ago

Still a 25MB limit and .doc is not supported, ignore this answer

upvoted 1 times

NinjaSchoolProfessor 1 year, 4 months ago

Office 365 Message Encryption can encrypt messages of up to 25 megabytes.

https://docs.microsoft.com/en-us/microsoft-365/compliance/legacy-information-for-message-encryption

upvoted 1 times

Jahoor69 1 year, 8 months ago

User 1:
mail 1 - exceeds max 25mb limit
Mail 2 - .Doc is not supported
Mail 3 - is supported and correct

User 2:
Mail 4 - is supported and correct
Mail 5 - JPG not supported
Mail 6 - Is supported.

so the answer is

User 1 Mail 3 only
https://docs.microsoft.com/en-us/microsoft-365/compliance/ome-faq?view=o365-worldwide#:~:text=The%20maximum%20message%20size%20you,including%20attachments%2C%20is%2025%20MB.

User 2 Mail 4 and Mail 6 only

https://docs.microsoft.com/en-us/microsoft-365/compliance/ome?view=o365-worldwide#:~:text=Office%20365%20Message%20Encryption%20works%20with%20Outlook.com%2C%20Yahoo!%2C%20Gmail%2C%20and%20other%20email%20services.

upvoted 11 times

daavidsc400 1 year, 8 months ago

This article says that .doc files will be protected
https://support.microsoft.com/en-us/office/introduction-to-irm-for-email-messages-bb643d33-4a3f-4ac7-9770-fd50d95f58dc?ui=en-us&rs=en-us&ad=us#FileTypesforIRM

upvoted 1 times

iJabu 1 year, 9 months ago

As per "https://docs.microsoft.com/en-us/microsoft-365/compliance/ome-faq?view=o365-worldwide"

https://docs.microsoft.com/en-us/microsoft-365/compliance/ome-faq?view=o365-worldwide
upvoted 1 times

iJabu 1 year, 9 months ago
OME does not support the 97-2003 versions of the following Office programs: Word (.doc), Excel (.xls), and PowerPoint (.ppt).
upvoted 3 times

PrettyFlyWifi 1 year, 10 months ago
User 1 can only send Mail 3, as OME does NOT support .doc files. See https://docs.microsoft.com/en-us/microsoft-365/compliance/ome-faq?view=o365-worldwide. It says "OME does not support the 97-2003 versions of the following Office programs: Word (.doc), Excel (.xls), and PowerPoint (.ppt)."
User 2 answer looks correct to me.
upvoted 1 times

Pravda 1 year, 10 months ago
On exam 1/20/2022
upvoted 2 times

Pravda 1 year, 10 months ago
Take a look here https://docs.microsoft.com/en-us/microsoft-365/compliance/ome?view=o365-worldwide
Outlook.com, Gmail, and Yahoo accounts receive a wrapper
U1 -> 2,3 The maximum message size you can send with OME, including attachments, is 25 MB. Not to 1
U2 -> 4,6 Can't encrypt jpeg. Not to 5
upvoted 3 times

melatocaroca 1 year, 9 months ago
Check actual OME and IRM,
https://docs.microsoft.com/en-us/microsoft-365/compliance/ome-version-comparison?view=o365-worldwide
https://support.microsoft.com/en-us/office/introduction-to-irm-for-email-messages-bb643d33-4a3f-4ac7-9770-fd50d95f58dc?ui=en-us&rs=en-us&ad=us#FileTypesforIRM
upvoted 1 times

Pravda 1 year, 10 months ago
User 1 - 2,3 seems right. Not Contoso domain and file extensions are supported.
User 2 - I think 6 only. 4 is on Contoso domain. 5 is .jpg, which is not supported. 6 is .docx, supported and file size in small enough.
Why are some people saying 5 is correct?
upvoted 3 times

Sam12 1 year, 10 months ago
"With Office 365 Message Encryption, your organization can send and receive encrypted email messages between people inside and outside your organization."
upvoted 1 times

Sam12 1 year, 10 months ago
https://docs.microsoft.com/en-us/microsoft-365/compliance/ome-faq?view=o365-worldwide#what-file-types-are-supported-as-attachments-in-protected-emails--do-attachments-inherit-the-protection-policies-associated-with-protected-emails-

What file types are supported as attachments in protected emails? Do attachments inherit the protection policies associated with protected emails? You can attach any file type to a protected mail. With one exception, protection policies are applied only on the file formats mentioned in File types supported by the Azure Information Protection client. OME does not support the 97-2003 versions of the following Office programs: Word (.doc), Excel (.xls), and PowerPoint (.ppt).

If a file format is supported, such as a Word, Excel, or PowerPoint file, the file is always protected, even after the attachment has been downloaded by the recipient. For example, say an attachment is protected by Do Not Forward. The original recipient downloads the file, creates a message to a new recipient and attaches the file. When the new recipient receives the file, the recipient will not be able to open the protected file.
upvoted 1 times

kornjaca 1 year, 11 months ago
Hi fellas!
I am a bit confused with this one. I have created an OME rule and sent two (un)supported attachments. One DOC and one JPG. It appears that OME encrypts the whole message, not the individual attachments.
So, shouldn't the answer be "Mail1, Mail2 and Mail3"? At least for User2, because I did not try sending 40MB large attachment.
Am I missing something here?
upvoted 2 times

Question #4 *Topic 1*

HOTSPOT -

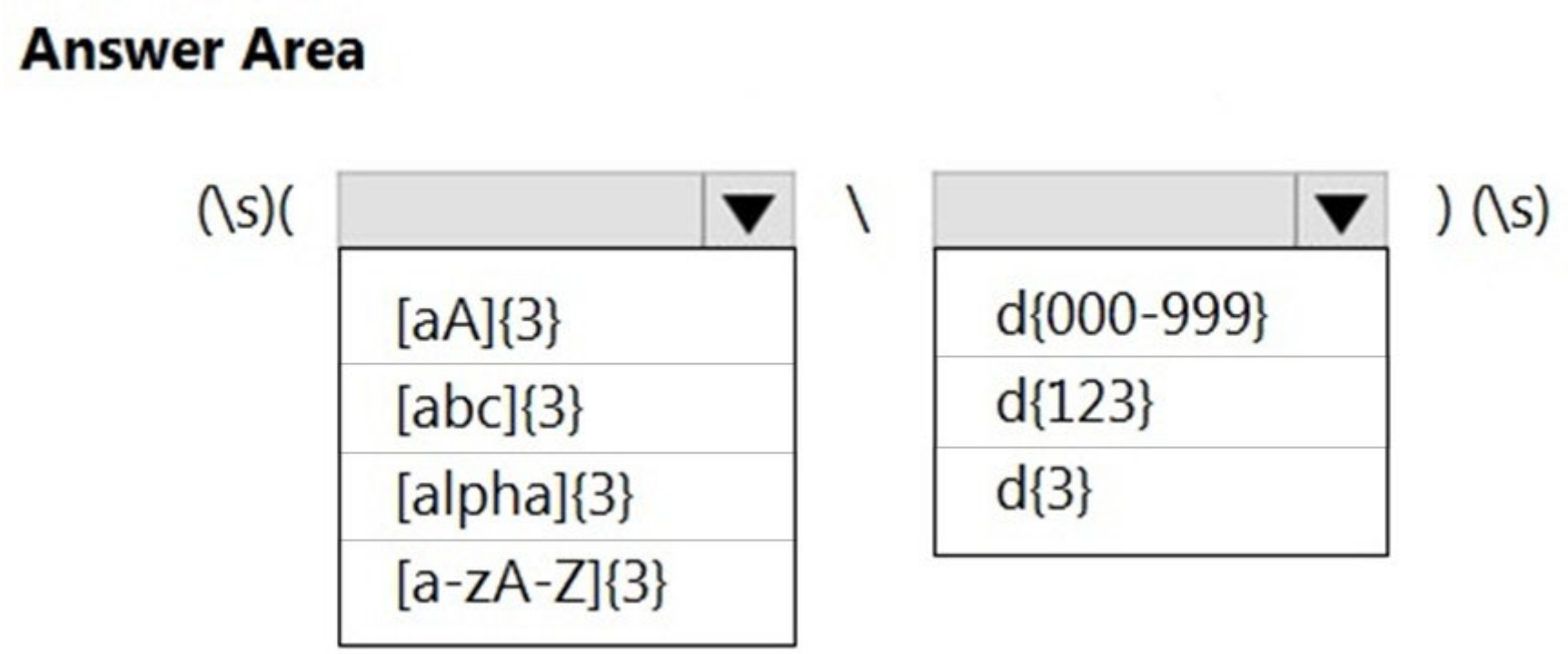
You use project codes that have a format of three alphabetical characters that represent the project type, followed by three digits, for example Abc123.

You need to create a new sensitive info type for the project codes.

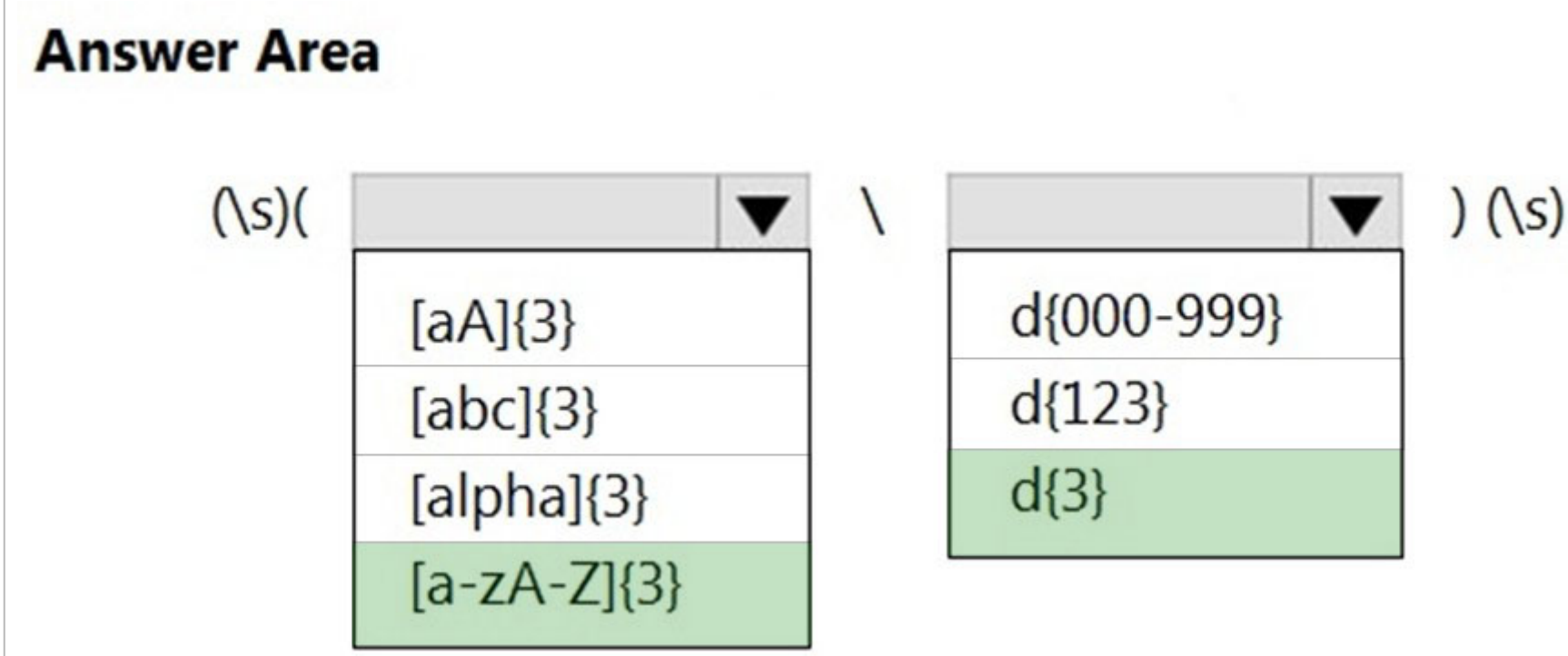
How should you configure the regular expression to detect the content? To answer, select the appropriate options in the answer area.

NOTE: Each correct selection is worth one point.

Hot Area:



Correct Answer:



Reference:

https://joannecklein.com/2018/08/07/build-and-use-custom-sensitive-information-types-in-office-365/

[Removed] Highly Voted 2 years, 6 months ago

The correct is ([a-zA-Z]{3}\d{3}). Use this site to test: http://regex101.com/

upvoted 32 times

liozuf Highly Voted 2 years, 6 months ago

\d{3} correct answer

upvoted 26 times

xswe Most Recent 7 months, 3 weeks ago

a-zA-Z = matches any 3 letters, it will be either upper or lowercase followed by

d{3} = 3 random digits

The result from this regex pattern could be: XYZ789 , MNO345 etc

upvoted 2 times

reastman66 11 months ago

Answer looks correct and it also appeared on my SC-300 exam

upvoted 3 times

HardcodedCloud 1 year, 11 months ago

([a-zA-Z]{3}\d{3}) tested & verified using regex101.
This is the result:
{3} matches the previous token exactly 3 times
a-z matches a single character in the range between a (index 97) and z (index 122) (case sensitive)
A-Z matches a single character in the range between A (index 65) and Z (index 90) (case sensitive)
\d matches a digit (equivalent to [0-9])
{3} matches the previous token exactly 3 times

upvoted 5 times

Ras1364 2 years ago

In Regex101 this one **[a-zA-Z]{3}\d{3}** is matched with any three alphabetic followed by three numbers but this one **[a-zA-Z]{3}\d{000-999}** doesn't match. I think the correct answer is the one that has a match result out of regex101.com

upvoted 4 times

klosedotorg83 2 years, 1 month ago

[a-zA-Z]{3}\d{3}

upvoted 3 times

oberte007 2 years, 1 month ago

I think given answer is correct. for the first box, they said 3 alphabetical characters i.e you can have these combinations of letters : ABC, bcE, cdf, ... so fisrt answer is [a-zA-Z]{3}. Now for the second one, they said followed by three digits it's the same thing for the alphabetical letters you'll have a combination of three digits: 123, 135, 911,... so the second box is \d{000-999}. so the full answer is [a-zA-Z]{3}\d{000-999.

upvoted 4 times

UnitedKendom 1 year, 7 months ago

\d{000-999} doesn't match using regex101, it would have to be \d{000,999} instead for option D to be correct

upvoted 1 times

jaycn67 2 years, 4 months ago

\d{3} , https://docs.microsoft.com/en-us/dotnet/api/system.text.regularexpressions.regex.ismatch?view=net-5.0

upvoted 3 times

k4d4v4r 2 years, 6 months ago

\d{3} as in this link:
https://docs.microsoft.com/en-us/dotnet/standard/base-types/quantifiers-in-regular-expressions#match-exactly-n-times-n

upvoted 4 times

Question #5 *Topic 1*

HOTSPOT -

You have a Microsoft SharePoint Online site named Site1 and a sensitivity label named Sensitivity1. Sensitivity1 adds a watermark and a header to content.

You create a policy to automatically apply Sensitivity1 to emails in Microsoft Exchange Online and Site1.

How will Sensitivity1 mark matching emails and Site1 documents? To answer, select the appropriate options in the answer area.

NOTE: Each correct selection is worth one point.

Hot Area:

Answer Area

Exchange Online emails:
- A header only
- A watermark only
- A watermark and a header

Site1 documents:
- A header only
- A watermark only
- A watermark and a header

Answer Area

Correct Answer:

Exchange Online emails:
- A header only
- A watermark only
- A watermark and a header

Site1 documents:
- A header only
- A watermark only
- A watermark and a header

Reference:

https://docs.microsoft.com/en-us/microsoft-365/compliance/sensitivity-labels?view=o365-worldwide

pheb92 Highly Voted 2 years, 6 months ago

this is correct!
outlook does not support watermarks

upvoted 15 times

xswe Most Recent 7 months, 3 weeks ago

You cannot apply watermarks to email, so the header will only get applied.
But you can for sure add both watermarks and headers to documents located at Sharepoint.

upvoted 1 times

Bluebaron520 1 year ago

valid 24/11/2022

upvoted 3 times

wooyourdaddy 1 year, 5 months ago

I wrote the exam, this question was on it, I choose these answers, 890:

Ref link: https://docs.microsoft.com/en-us/microsoft-365/compliance/sensitivity-labels?view=o365-worldwide#what-sensitivity-labels-can-do

upvoted 3 times

HardcodedCloud 1 year, 11 months ago

Mark the content when you use Office apps, by adding watermarks, headers, or footers to email or documents that have the label applied.
Watermarks can be applied to documents but not email. Example header and watermark:

upvoted 3 times

M20200713 2 years, 2 months ago

Mark the content when you use Office apps, by adding watermarks, headers, or footers to email or documents that have the label applied. Watermarks can be applied to documents but not email.

upvoted 3 times

jaycn67 2 years, 4 months ago

Answer correct, https://docs.microsoft.com/en-us/microsoft-365/compliance/sensitivity-labels?view=o365-worldwide#what-sensitivity-labels-can-do

upvoted 3 times

HOTSPOT -

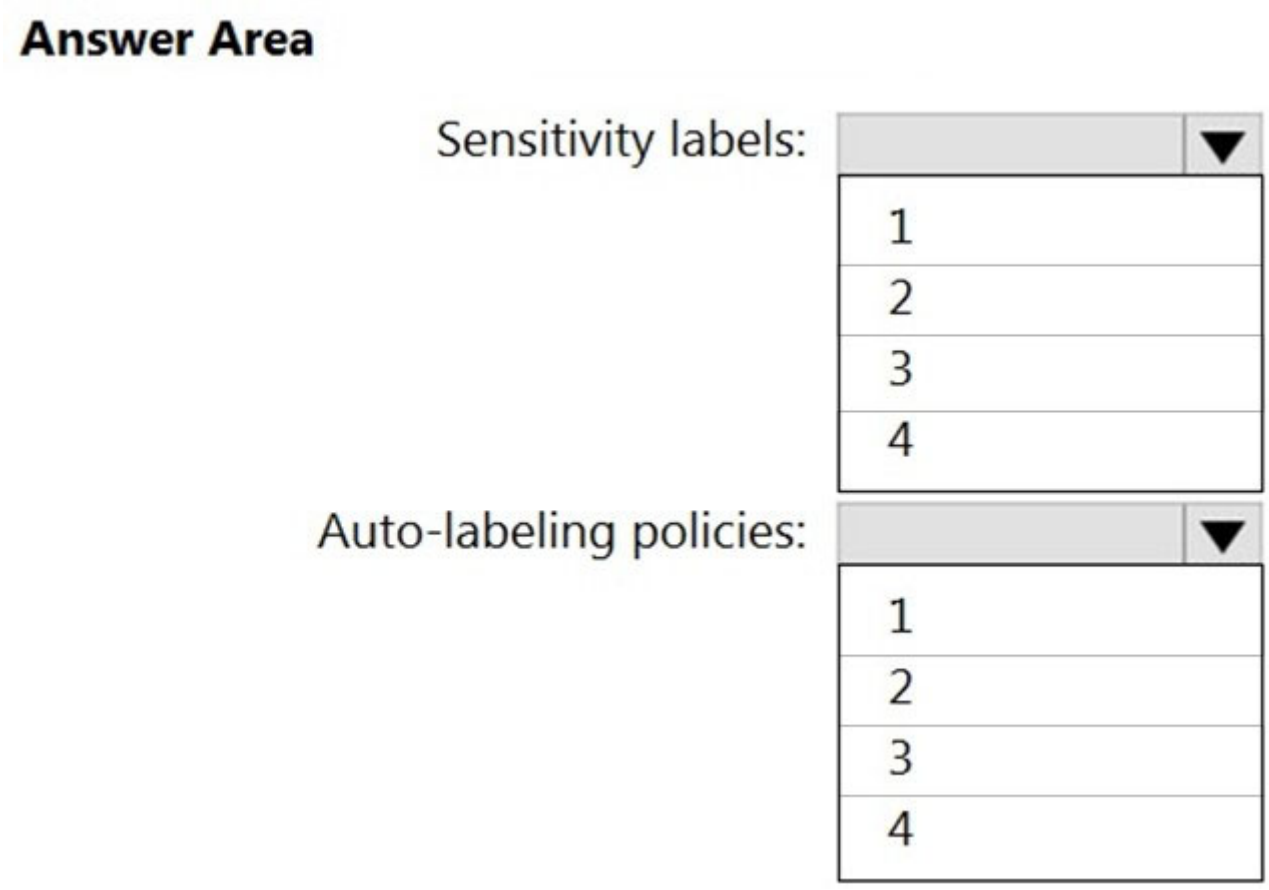
You need to implement an information compliance policy to meet the following requirements:

- Documents that contain passport numbers from the United States, Germany, Australia, and Japan must be identified automatically.
- When a user attempts to send an email or an attachment that contains a passport number, the user must receive a tooltip in Microsoft Outlook.
- Users must be blocked from using Microsoft SharePoint Online or OneDrive for Business to share a document that contains a passport number.

What is the minimum number of sensitivity labels and auto-labeling policies you should create? To answer, select the appropriate options in the answer area.

NOTE: Each correct selection is worth one point.

Hot Area:



Correct Answer:

We have four different kind of built-in sensitive information types for United States, Germany, Australia, and Japan in Data classification.

One Autolabeling policy can include all (4) passport sensitive information types in Rule-Conditions. In the same policy you choose one sensitivity label to add to files.

Reference:

https://docs.microsoft.com/en-us/microsoft-365/compliance/get-started-with-sensitivity-labels?view=o365-worldwide

shanti0091 Highly Voted 2 years, 4 months ago

Tested and trusted 1:1 is the answer. you can create 1 label and have all the PII or passport numbers for the four countries included and publish your label

upvoted 32 times

test123123 Highly Voted 2 years, 5 months ago

First of all look at the question:
What is the minimum number of sensitivity labels and auto-labeling policies you should create?

We have 4 different kind of built-inn sensitive information types for United States, Germany, Australia, and Japan in Data classification.

1 Autolabeling policy can include all (4) passport sensitive information types in Rule-Conditions. In the same policy you choose 1 sensitivity label to add to files.
So I would say the answer is 1 and 1.

upvoted 21 times

mbhasker Most Recent 2 days, 20 hours ago

3 Sensitivty Label and 1 Auto Label Policy

upvoted 1 times

hsinchang 3 months, 1 week ago

To better illustrate:
You can create a sensitivity label named Passport Number and configure it to apply encryption and a watermark to the content. You can also choose to restrict access to specific users or groups, or block external sharing.
You can create an auto-labeling policy named Passport Number Policy and select the Passport Number label to apply automatically. You can also choose the locations where you want to apply the policy, such as Exchange Online, SharePoint Online, and OneDrive for Business. You can then define a condition to match the content that contains passport numbers from the United States, Germany, Australia, and Japan.

upvoted 2 times

xswe 7 months, 3 weeks ago

I've tested this and you only need to create a sensitivity label and auto-apply label policy to achieve this.

upvoted 2 times

Pravda 1 year, 10 months ago

On exam 1/20/2022

upvoted 2 times

klosedotorg83 2 years, 2 months ago

1 Sensitivty Label and 1 Auto Label Policy

upvoted 7 times

NW16 2 years, 4 months ago

1 Sensitivity label will cover all Passport # and One label policy can use to show tooltips.
So the answer would be 1 and 1.

upvoted 6 times

k4d4v4r 2 years, 6 months ago

I would say 1 label and 1 policy as written here:
https://docs.microsoft.com/en-us/microsoft-365/compliance/apply-sensitivity-label-automatically?view=o365-worldwide#how-to-configure-auto-labeling-policies-for-sharepoint-onedrive-and-exchange

upvoted 5 times

pheb92 2 years, 6 months ago

this is a weird one!
#Documents that contain passport numbers ... "must be identified automatically".#
Sensitive Information Types identify automatically. Since this is about Sensitivity Labels, i would say, you need to create one and apply it automatically.
#When a user attempts..."must receive a tooltip"#
This is configured in DLP: https://docs.microsoft.com/en-us/microsoft-365/compliance/use-notifications-and-policy-tips?view=o365-worldwide
#User must be blocked from...#
This is a DLP Policy as well: https://docs.microsoft.com/en-us/microsoft-365/compliance/data-loss-prevention-policies?view=o365-worldwide

upvoted 6 times

Piper 2 years, 6 months ago

So you think 1 Sensitivity label and 2 DLP policies?

upvoted 1 times

pheb 2 years, 3 months ago

1 Sensitivty Label and 1 Auto Label Policy (2 DLP would be needed for the use case, but are not available as answers)

upvoted 2 times

dasha_an 2 years, 6 months ago

for me "Documents that contain passport numbers ... " can be managed by a single label.
"When a user attempts...must receive a tooltip" + "When a user attempts..."must receive a tooltip" can be unified in 1 Label Policy
So I don't understand why do we need 3 labels in this case.

upvoted 5 times

HOTSPOT -

You have a Microsoft 365 E5 tenant.

You create sensitivity labels as shown in the Sensitivity Labels exhibit.

+ Create a label Publish labels Refresh

Name	Order	Scope
Public	0 – lowest	File, Email
General	1	File, Email
Confidential	2	File, Email
Internal	3	File, Email
External	4 – highest	File, Email

The Confidential/External sensitivity label is configured to encrypt files and emails when applied to content.

The sensitivity labels are published as shown in the Published exhibit.

Sensitivity Policy1

Edit policy Delete policy

Name

Sensitivity Policy1

Description

Published labels

Public
General
Confidential
Confidential/External
Confidential/Internal

Published to

All

Policy settings

Users must provide justification to remove a label or lower its classification

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:

Answer Area

Statements	Yes	No
The Internal sensitivity label inherits all the settings from the Confidential label.	○	○
Users must provide justification if they change the label of content from Confidential/Internal to Confidential/External.	○	○
Content that has the Confidential/External label applied will retain the encryption settings if the sensitivity label is removed from the label policy.	○	○

Answer Area

Correct Answer:

Statements	Yes	No
The Internal sensitivity label inherits all the settings from the Confidential label.	○	○
Users must provide justification if they change the label of content from Confidential/Internal to Confidential/External.	○	○
Content that has the Confidential/External label applied will retain the encryption settings if the sensitivity label is removed from the label policy.	○	○

Reference:

https://docs.microsoft.com/en-us/microsoft-365/compliance/sensitivity-labels?view=o365-worldwide

Eltooth Highly Voted 2 years, 5 months ago

No /No / Yes - correct

upvoted 20 times

fimbulvetrk Highly Voted 1 year ago

Answer is: No/No/Yes.
- Sublabels don't inherit settings from their parent label (https://learn.microsoft.com/en-us/microsoft-365/compliance/sensitivity-labels?view=o365-worldwide#sublabels-grouping-labels)
- Moving from Confidential\Internal to Confidential\External isn't lowering the label "level", it's the opposite, just check the labels order (https://learn.microsoft.com/en-us/microsoft-365/compliance/sensitivity-labels?view=o365-worldwide#label-priority-order-matters)
- Well, when you remove a label that applied encryption to a document you don't necessarily remove the encryption. You only remove the encryption when you change to a label that removes encryption (you can configure that on the label settings)

upvoted 9 times

xswe Most Recent 7 months, 3 weeks ago

No, the parent label are only there for the visualization no configuration will get inehrited.
No, since the Internal is higher in priority than the External.
Yes, the encryption will still be there even if you remove the sensitivity label.

"Sublabels don't inherit any settings from their parent label, except for their label color. When you publish a sublabel for a user, that user can then apply that sublabel to content and containers, but can't apply just the parent label."

upvoted 3 times

Bluebaron520 1 year ago

valid 24/11/2022

upvoted 3 times

prats005 1 year, 4 months ago

1.Sublabels don't inherit any settings from their parent label - No
2.f a user tries to remove a label or replace it with a label that has a lower-order number, you can require the user provides a justification to perform this action. For example, a user opens a document labeled Confidential (order number 3) and replaces that label with one named Public (order number 1) -N
3. I dont know the answer

upvoted 1 times

wooyourdaddy 1 year, 5 months ago

I wrote the exam, this question was on it, I choose these answers, 890:

I know I missed this one, I did Yes / No / No.

upvoted 1 times

JCkD4Ni3L 11 months, 2 weeks ago

Blindly using answers here is not a good idea, you should research and leverage Microsoft documentations to actually learn something. :/

upvoted 3 times

UnitedKendom 1 year, 7 months ago

Struggling with this one - I think from looking at the link the asnwer should be No/Yes/Yes: "Require a justification for changing a label.
If a user tries to remove a label or replace it with a label that has a lower-order number, you can require the user provides a justification to perform this action. For example, a user opens a document labeled Confidential (order number 3) and replaces that label with one named Public (order number 1). For Office apps, this justification prompt is triggered once per app session when you use built-in labeling, and per file when you use the Azure Information Protection unified labeling client. Administrators can read the justification reason along with the label change in activity explorer."

upvoted 1 times

Holii 1 year, 6 months ago

You just explained why it's No/No/Yes.
Confidential/External is above Confidential/Internal, which means it doesn't require justification since you are changing it to a stricter label policy.

upvoted 4 times

[Removed] 1 year, 6 months ago

Well said

upvoted 1 times

shanti0091 2 years, 4 months ago

the correct answer as justification indicates lower or remove. Very tricky

upvoted 4 times

olsi 2 years, 5 months ago

agree ...

upvoted 4 times

Question #8 *Topic 1*

You are implementing a data classification solution.
The research department at your company requires that documents containing programming code be labeled as Confidential. The department provides samples of the code from its document library. The solution must minimize administrative effort.
What should you do?

A. Create a custom classifier.

B. Create a sensitive info type that uses Exact Data Match (EDM).

C. Use the source code classifier.

D. Create a sensitive info type that uses a regular expression.

Correct Answer: *C*
Reference:
https://docs.microsoft.com/en-us/microsoft-365/compliance/classifier-learn-about?view=o365-worldwide

dasha_an Highly Voted 2 years, 6 months ago
Resumes, Source code, Harassment, Profanity, Threat are pre-trained classifiers that exist already in Microsoft 365 -> Source code is correct
upvoted 20 times

Anker 2 years, 5 months ago
The key is the "minimize administrative effort". Could you use other options on here to get to the same end result, yes... but the Source code option is built in so requires minimal effort. So that's why I'm sticking with C
upvoted 10 times

JCkD4Ni3L 11 months, 2 weeks ago
Correct, the trap here is "The department provides samples of the code from its document library"... you are not minimizing efforts if you training a new classifier.
upvoted 1 times

Gesbie Most Recent 3 months, 3 weeks ago
was on Exam August 9, 2023
upvoted 1 times

xswe 7 months, 3 weeks ago
In this case you should use a trainable classifier since you want to classify data and this can be done with the trainable classifier.
The custom classifier will demand more administrative effort than the "Source code classifier" that are already available since you are going to need to train it.

Correct answer, source code classifier.
upvoted 1 times

Fcnet 11 months ago
the exact reference here
https://learn.microsoft.com/en-us/microsoft-365/compliance/classifier-tc-definitions?view=o365-worldwide#trainable-classifiers-definitions
Source code is trained to detect when the bulk of the text is source code. It does not detect source code text that is interspersed with plain text.
upvoted 2 times

Bluebaron520 1 year ago
valid 24/11/2022
upvoted 3 times

Eltooth 2 years, 5 months ago
Agreed - C.
upvoted 4 times

k4d4v4r 2 years, 6 months ago
In a note: "Source Code is trained to detect when the bulk of the text is source code. It does not detect source code text that is interspersed with plain text."
upvoted 2 times

k4d4v4r 2 years, 6 months ago
Should be A as seen in here. Ok there is a built-in but why would we have samples for that?
https://docs.microsoft.com/en-us/microsoft-365/compliance/classifier-get-started-with?view=o365-worldwide
upvoted 2 times

jeffangel28 2 years, 5 months ago

It is option C so it mentions "The solution must minimize administrative effort." and the pre-built option has 25 programming languages.

upvoted 7 times

Question #9 *Topic 1*

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

Correct Answer: *D*
Reference:
https://docs.microsoft.com/en-us/microsoft-365/compliance/classifier-get-started-with?view=o365-worldwide

Community vote distribution
C (61%) D (39%)

[Removed] Highly Voted 2 years, 6 months ago
Well, the documentation says "Compliance Administrator role is required to train a classifier.", but I did a test and the Compliance Administrator can create Treinable Classifiers too. So, using the principle of the least privillege, the answer is D.
upvoted 25 times

MahmoudEldeep 2 years, 2 months ago
Correct, I tested it also and Compliance administrator can create a trainable classifier.
upvoted 3 times

melatocaroca 1 year, 9 months ago
https://books.google.es/books?id=5YJSEAAAQBAJ&pg=PA60&lpg=PA60&dq=Compliance+Administrator+can+create+Trainable+Classifiers&source=bl&ots=brkqVY_Aum&sig=ACfU3U2ZvAV8MPsVq4mjbweibCRdGDmlwA&hl=en&sa=X&ved=2ahUKEwi7muqU26L2AhUH3BoKHe-lBM0Q6AF6BAgYEAM#v=onepage&q=Compliance%20Administrator%20can%20create%20Trainable%20Classifiers&f=false
upvoted 1 times

dasha_an Highly Voted 2 years, 6 months ago
Correct answer is Global Admin:
https://docs.microsoft.com/en-us/microsoft-365/compliance/classifier-get-started-with?view=o365-worldwide
"the Global admin needs to opt in for the tenant to create custom classifiers.
Compliance Administrator role is required to train a classifier"
upvoted 13 times

Piper 2 years, 6 months ago
Technically you are right, but I will assume (could be wrong), that is asked on the basis that an opt in has been set. Though I dont like to have to assume anything for an exam, that makes me nervous
upvoted 6 times

Anker 2 years, 5 months ago
Agreed, I would ere on the side of minimum required permissions as well and Compliance Administrator fits that criteria.
upvoted 1 times

Eltooth 2 years, 5 months ago
Agreed and MS should always state if any changes have been made to default settings - that or you can provide feedback in exam about ambiguity of question.
I believe the answer is Compliance Admin - provided Global Admin has allowed Compliance Admins to create classifiers.
upvoted 2 times

mbhasker Most Recent 2 days, 20 hours ago
D. Compliance administrator
upvoted 1 times

Davidf 3 months, 3 weeks ago
Selected Answer: C
NEW tenant - Global admin is required to opt in
upvoted 3 times

TeeKay_From_the_South 5 months ago
Correct, Global admin's include alot of tasks. However Compliance admin is related to the exam. Its as simple as that.

upvoted 1 times

dmoorthy 7 months, 1 week ago

Correct answer is Global Admin:
https://docs.microsoft.com/en-us/microsoft-365/compliance/classifier-get-started-with?view=o365-worldwide
"the Global admin needs to opt in for the tenant to create custom classifiers.
Compliance Administrator role is required to train a classifier"

Catch is "You have a new Microsoft 365 tenant" in the Question. New tenant need to Opt-in. So Global Administrator is the answer.

upvoted 3 times

xswe 7 months, 3 weeks ago

Since they are asking for what role you need to ENSURE that CUSTOM TRAINABLE CLASSIFIERS can be CREATED I will go for Global admin.
Global admin are needed to opt in for the tenant to create custom classifiers.
Compliance admin are required to train classifiers

"To access classifiers in the UI:
the Global admin needs to opt in for the tenant to create custom classifiers.
Compliance Administrator role is required to train a classifier."

upvoted 3 times

Azurefox79 9 months, 3 weeks ago

C is correct. The key phrase is "can be created". The compliance admin cannot do this, the GA needs to first opt-in AKA allow them to be created.
https://learn.microsoft.com/en-us/microsoft-365/compliance/classifier-get-started-with?view=o365-worldwide

upvoted 1 times

NinjaSchoolProfessor 11 months, 2 weeks ago

The GA role is required to opt in, meaning enabled it. Comp Admin is simply required to use it.

upvoted 1 times

NinjaSchoolProfessor 11 months, 2 weeks ago

To access classifiers in the UI: the "Global admin" needs to opt in for the tenant to create custom classifiers. Then the "Compliance Administrator" role is required to train a classifier. So technically someone who's a GA needs to assign the Compliance Admin role to the user.

upvoted 1 times

car10589 1 year ago

Selected Answer: D

It's correct

upvoted 4 times

Bluebaron520 1 year ago

valid 24/11/2022

upvoted 2 times

Jawad1462 1 year ago

Selected Answer: D

Is correct

upvoted 3 times

chrissempai 1 year, 2 months ago

The answer need to be C (global admin)
To access classifiers in the UI:

the Global admin needs to opt in for the tenant to create custom classifiers.
Compliance Administrator role is required to train a classifier.

upvoted 1 times

prats005 1 year, 4 months ago

the Global admin needs to opt in for the tenant to create custom classifiers.
Compliance Administrator role is required to train a classifier.

upvoted 1 times

bigwhitebeaver 1 year, 5 months ago

D - compliance admon, tested in lab.

upvoted 1 times

Kamal_SriLanka 1 year, 5 months ago

To access classifiers in the UI:
the Global admin needs to opt in for the tenant to create custom classifiers.
Compliance Administrator role is required to train a classifier.

upvoted 1 times

Question #10 *Topic 1*

You need to automatically apply a sensitivity label to documents that contain information about your company's network including computer names, IP addresses, and configuration information.
Which two objects should you use? Each correct answer presents part of the solution. (Choose two.)
NOTE: Each correct selection is worth one point.

A. an Information protection auto-labeling policy

B. a custom trainable classifier

C. a sensitive info type that uses a regular expression

D. a data loss prevention (DLP) policy

E. a sensitive info type that uses keywords

F. a sensitivity label that has auto-labeling

Correct Answer: *AB*
Reference:
https://docs.microsoft.com/en-us/microsoft-365/compliance/classifier-learn-about?view=o365-worldwide https://docs.microsoft.com/en-us/microsoft-365/compliance/apply-sensitivity-label-automatically?view=o365-worldwide

Community vote distribution

BF (96%) 4%

[Removed] Highly Voted 2 years ago

Selected Answer: BF

True, the auto-labeling policy does not support trainable classifiers. So the answer would be B and F.
upvoted 21 times

MahmoudEldeep 2 years ago

Agree and tested
upvoted 3 times

Ali_557 1 year, 11 months ago

Which answers you have tested? AB or AF?
upvoted 2 times

sergioandreslq 1 year, 11 months ago

More supporting elements:
"Once published your trainable classifier will be available as a condition in Office auto-labeling with sensitivity labels, auto-apply retention label policy based on a condition."
Step 21 on reference:
https://docs.microsoft.com/en-us/microsoft-365/compliance/classifier-get-started-with?view=o365-worldwide#how-to-create-a-trainable-classifier
upvoted 2 times

k4d4v4r Highly Voted 2 years, 6 months ago

A and B as you need custom classifiers to begin. IP Addresses are built-in so you wouldn't need a new regex or anything for that, just configure in the policy together with the custom classifier with and AND/OR operator.
upvoted 17 times

lime568 2 years, 2 months ago

what about "... and configuration information."?
upvoted 1 times

mbhasker Most Recent 2 days, 20 hours ago

correct answer: AB
upvoted 1 times

dmoorthy 7 months, 1 week ago

Answer is BF

However, if the label contains trainable classifiers as a label condition:
- When the label conditions contain just trainable classifiers, you won't see the option to automatically create an auto-labeling policy.
- When the label conditions contain trainable classifiers and sensitivity info types, an auto-labeling policy will be created for just the sensitive info types.

https://learn.microsoft.com/en-us/microsoft-365/compliance/apply-sensitivity-label-automatically?view=o365-worldwide

upvoted 2 times

xswe 7 months, 3 weeks ago

Since we want to automatically apply sensitivity labels we need "a sensitivity label that has auto-labeling".
And to detect these documents we are going to need to create a custom trainable classifier, the document provided the contains network info & computer info can be used as seeding files. Theses seeding files will be uploaded to SharePoint Online when we start the seeding process.

Tested.

upvoted 2 times

[Removed] 9 months, 2 weeks ago

Selected Answer: BF

However, if the label contains trainable classifiers as a label condition:
- When the label conditions contain just trainable classifiers, you won't see the option to automatically create an auto-labeling policy.
- When the label conditions contain trainable classifiers and sensitivity info types, an auto-labeling policy will be created for just the sensitive info types.

https://learn.microsoft.com/en-us/microsoft-365/compliance/apply-sensitivity-label-automatically?view=o365-worldwide

upvoted 1 times

NinjaSchoolProfessor 11 months, 2 weeks ago

Answer is AB. A trainable classifier is definitely needed due to the "company configuration information" requirement, but "sensitivity labels" are found under the Data Classification tab and do not have auto-labeling capabilities, rather auto-labeling is located under Information Protection so the answers AB are correct. Additionally, if scenario didn't include the "configuration information", then a SIT that uses regular expression would have been fine. Reference: https://learn.microsoft.com/en-us/microsoft-365/compliance/apply-sensitivity-label-automatically

upvoted 3 times

Bluebaron520 1 year ago

valid 24/11/2022

upvoted 2 times

fimbulvetrk 1 year ago

what was your answer? for me it's A and B, once auto-labeling policy now supports trainable classifiers

upvoted 2 times

prats005 1 year, 4 months ago

BF
Classifiers are available to use as a condition for Office auto-labeling with sensitivity labels, auto-apply retention label policy based on a condition and in communication compliance.

Sensitivity labels can use classifiers as conditions, see Apply a sensitivity label to content automatically.

either the manual or automated pattern-matching methods. This method of classification is more about using a classifier to identify an item based on what the item is, not by elements that are in the item (pattern matching). A classifier learns how to identify a type of content by looking at hundreds of examples of the content you're interested in classifying.

upvoted 1 times

wooyourdaddy 1 year, 5 months ago

Selected Answer: CF

I wrote the exam, this question was on it, I choose these answers, 890:

I got this one wrong, well half wrong, chose D instead of B.

upvoted 1 times

MahmoudEldeep 1 year, 7 months ago

Selected Answer: BF

Correct answer is B&F

upvoted 3 times

JamesM9 1 year, 7 months ago

This is a tricky question - after a lot of digging, I would say that a custom trainable classifier needs to be created in order to capture the configuration information.

Based on the link below, an information Protection auto-labelling policy does not allow the use of custom trainable classifiers, so this can only leave option F.

"Once published your classifier will be available as a condition in Office auto-labeling with sensitivity labels, auto-apply retention label policy based on a condition and in Communication compliance"

https://docs.microsoft.com/en-us/microsoft-365/compliance/classifier-get-started-with?view=o365-worldwide#how-to-create-a-trainable-classifier

Therefore, the answers here are B & F.

upvoted 4 times

fimbulvetrk 1 year ago

I think you're right, even though it's possible to use builtin trainable classifiers in auto labeling policies (which have IP and IT patterns), I'm not sure what is "configuration information" mentioned in this question. Considering that "configuration information" is a type of info not covered

by the builtin trainable classifiers, the answer would be B and F, of course... however, if it does cover, it's A and B.

upvoted 1 times

CalST 1 year, 9 months ago

Auto-labelling for files and emails (ie auto apply settings in the label creation) displays the suggested label but a user can change it (if allowed). This occurs on creation and editing. Auto-labelling applies the label and settings to content at rest and does not need user display or interaction. The question doesn't specify new content, so A is correct.
Without information about the computer names & configuration the label could be either keywords, regular expressions or trainable classifiers. Assuming there is already content with this information (the question implies it is already there) then Trainable classifiers would be easiest - but bad question

upvoted 1 times

nupagazi 1 year, 10 months ago

BF. There are ways for auto labeling: 1. Label with auto labeling (client side). 2. Auto labeling policy (service side). Service side does not support tainable classifiers https://docs.microsoft.com/en-us/microsoft-365/compliance/apply-sensitivity-label-automatically?view=o365-worldwide

upvoted 2 times

girikedar 1 year, 11 months ago

Answer is B & F
B=Custom Trainable classifier
f= Sensitivity label with auto label policy
because Auto-Labelling policy only support Sensitive info types

upvoted 3 times

Deeksix 2 years, 1 month ago

BF is correct.
1. You need a trainable classifier to classify "configuration information".
2. Info Protection auto-labeling does not support custom trainable classifiers so A is not correct.
From link provided in the answer:
Both built-in classifiers and trainable classifiers are available as a condition for Office autolabeling with sensitivity labels, auto-apply retention label policy based on a condition and in communication compliance. Sensitivity labels can use classifiers as conditions

upvoted 4 times

jkklim 2 years, 2 months ago

AB

You need to automatically apply a sensitivity label to documents ==> key word is automatically, therefore you have choose auto-labeling policy which is A

company's network including computer names, IP addresses, and configuration information. ==> computer name already indicated that u need custom trainable classifier because your company and my company computer name already different, so need custom trainable classifer

so AB is the answer

upvoted 5 times

Question #11 *Topic 1*

You are creating a custom trainable classifier to identify organizational product codes referenced in Microsoft 365 content.
You identify 300 files to use as seed content.
Where should you store the seed content?

A. a Microsoft SharePoint Online folder

B. a Microsoft OneDrive for Business folder

C. an Azure file share

D. Microsoft Exchange Online shared mailbox

Correct Answer: *A*
Reference:
https://docs.microsoft.com/en-us/microsoft-365/compliance/classifier-get-started-with?view=o365-worldwide

olsi Highly Voted 2 years, 6 months ago
correct, has to be SP Online folder
upvoted 11 times

sergioandreslq 1 year, 11 months ago
"Place the seed content in a SharePoint Online folder that is dedicated to holding the seed content only. Make note of the site, library, and folder URL."
Step 2 on reference:
https://docs.microsoft.com/en-us/microsoft-365/compliance/classifier-get-started-with?view=o365-worldwide#how-to-create-a-trainable-classifier
upvoted 3 times

xswe Most Recent 7 months, 3 weeks ago
When you create a custom trainable classifier you are going to need at least 50-500 documents that will act as seed documents to get the classifier to know what it will be looking for.
These documents has to be uploaded to SharePoint Online.
upvoted 2 times

Bluebaron520 1 year ago
valid 24/11/2022
upvoted 2 times

Pravda 1 year, 10 months ago
On exam 1/20/2022
upvoted 1 times

examkid 2 years, 1 month ago
correct:
Place the seed content in a SharePoint Online folder that is dedicated to holding the seed content only. Make note of the site, library, and folder URL.

https://docs.microsoft.com/en-us/microsoft-365/compliance/classifier-get-started-with?view=o365-worldwide#how-to-create-a-trainable-classifier
upvoted 3 times

Question #12 *Topic 1*

Each product group at your company must show a distinct product logo in encrypted emails instead of the standard Microsoft Office 365 logo. What should you do to create the branding templates?

A. Create a Transport rule.

B. Create an RMS template.

C. Run the Set-IRMConfiguration cmdlet.

D. Run the New-OMEConfiguration cmdlet.

Correct Answer: *D*
Reference:
https://docs.microsoft.com/en-us/microsoft-365/compliance/add-your-organization-brand-to-encrypted-messages?view=o365-worldwide

Community vote distribution

D (100%)

Deeksix Highly Voted 2 years, 1 month ago

D is correct. You use New-OMEConfiguration to CREATE the branding template (as the question asks). A transport rule is needed to apply it, but not to CREATE it.

upvoted 10 times

sergioandreslq 1 year, 11 months ago

To create a new branding configuration for use with a specific domain, run the New-OMEConfiguration cmdlet:
New-OMEConfiguration -Identity "Office 365 IT Pros"
You then use the Set-OMEConfiguration cmdlet to update the configuration to tweak different aspects of the notification message created using the template such as the image in the notification heading (shown instead of the Office 365 logo) and text displayed in different places in the message. For example, this command sets four different text strings, adds a different picture, and sets a 10-day expiration period for any message sent using the template. The picture should be no more than 170 x 170 pixels.
Set-OMEConfiguration -Identity "Office 365 IT Pros" -DisclaimerText "Office 365 for IT Pros takes no responsibility for this portal." -PortalText "Office 365 for IT Pros Secure Messaging" -EmailText "Good things happen when you protect email" -ExternalMailExpiryInDays 10 -IntroductionText "has sent you a secret message" -Image (Get-Content "C:\Temp\SmallBookCover.jpg" -Encoding byte)

upvoted 8 times

jcgonzalez1978 Highly Voted 2 years, 3 months ago

To create a new branding template you need to run New-OMEConfiguration and in order to use it, you must first run Set-OMEConfiguration and them create a Transport Rule. Here there is a good explanation: https://www.petri.com/advanced-ome-branding

upvoted 5 times

hsinchang Most Recent 3 months, 1 week ago

Selected Answer: D

You should run the New-OMEConfiguration cmdlet to create a new OME configuration. Then, modify the branding template using Set-OMEConfiguration cmdlet.

upvoted 1 times

xswe 7 months, 3 weeks ago

When you want to configure the your organizations emails you want to user New-OMEConfiguration cmdlet.
This cmdlet can give you the possibility to create a custom look for the emails that you send from your organization, you can do the following,
Background color of the email
Dislaimer text for recievers
Image
Introduction text
When the email will get expired
Configure the "read button" text etc

upvoted 3 times

Bluebaron520 1 year ago

valid 24/11/2022

upvoted 2 times

wooyourdaddy 1 year, 5 months ago

Selected Answer: D

I wrote the exam today, this question was on it, I choose D, scored 890. 100% right.

upvoted 3 times

Ali_557 1 year, 11 months ago

Logo
Set-OMEConfiguration -Identity "<OMEConfigurationName>" -Image <Byte[]>

Example:
Set-OMEConfiguration -Identity "Branding Template 1" -Image (Get-Content "C:\Temp\contosologo.png" -Encoding byte)
Supported file formats: .png, .jpg, .bmp, or .tiff
Optimal size of logo file: less than 40 KB
Optimal size of logo image: 170x70 pixels. If your image exceeds these dimensions, the service resizes your logo for display in the portal. The service doesn't modify the graphic file itself. For best results, use the optimal size.

upvoted 2 times

Piper 2 years, 6 months ago

I thought this would be D, then A?

upvoted 2 times

Question #13 *Topic 1*

You create a custom sensitive info type that uses Exact Data Match (EDM).
You plan to periodically update and upload the data used for EDM.
What is the maximum frequency with which the data can be uploaded?

A. twice per week

B. twice per day

C. once every six hours

D. once every 48 hours

E. twice per hour

Correct Answer: *B*
You can upload data with the EDMUploadAgent to any given data store only twice per day.
Reference:
https://docs.microsoft.com/en-us/microsoft-365/compliance/sit-get-started-exact-data-match-hash-upload?view=o365-worldwide

Community vote distribution

B (100%)

evivd Highly Voted 2 years, 4 months ago
You can upload data with the EDMUploadAgent to any given data store only twice per day. -> https://docs.microsoft.com/en-us/microsoft-365/compliance/create-custom-sensitive-information-types-with-exact-data-match-based-classification?view=o365-worldwide#links-to-edm-upload-agent-by-subscription-type
upvoted 27 times

cris_exam Highly Voted 5 months, 3 weeks ago
Old question. This was recently changed (April 2023) and now the EDMUploadAgent can be used 5 times per day.

You can upload data with the EDMUploadAgent to any given data store up to five times per day.

https://learn.microsoft.com/en-us/microsoft-365/compliance/sit-get-started-exact-data-match-hash-upload?view=o365-worldwide#links-to-edm-upload-agent-by-subscription-type
upvoted 9 times

mbhasker Most Recent 2 days, 20 hours ago
A. twice per week
upvoted 1 times

RChahal 4 days, 7 hours ago
changed to five times per day
upvoted 1 times

JacoH 3 weeks ago
It's changed to five times a day
You can upload data with the EDMUploadAgent to any given data store up to five times per day
https://learn.microsoft.com/en-us/purview/sit-get-started-exact-data-match-hash-upload
upvoted 1 times

Gesbie 3 months, 3 weeks ago
was on Exam August 9, 2023
upvoted 2 times

slick_orange 6 months, 3 weeks ago
Old Question. Supposed to be five times per day.
You can upload data with the EDMUploadAgent to any given data store up to five times per day.
Reference: https://learn.microsoft.com/en-us/microsoft-365/compliance/sit-get-started-exact-data-match-hash-upload?view=o365-worldwide#links-to-edm-upload-agent-by-subscription-type
upvoted 6 times

xswe 7 months, 3 weeks ago
The EDM Upload Agent can upload data twice per day,

"The EDMUploadAgent at the above links has been updated to automatically add a salt value to the hashed data. Alternately, you can provide your own salt value. Once you have used this version, you will not be able to use the previous version of the EDMUploadAgent.
You can upload data with the EDMUploadAgent to any given data store only twice per day."

upvoted 1 times

Bluebaron520 1 year ago

valid 24/11/2022

upvoted 3 times

hapthompson88 1 year, 2 months ago

B is correct

upvoted 3 times

prabhjot 1 year, 2 months ago

yes twice a day is correct ans - Exact Data Match (EDM) enhances an organization's ability to identify and accurately target specific data -You can upload data with the EDMUploadAgent to any given data store only twice per day.

upvoted 1 times

msoo 1 year, 3 months ago

Selected Answer: B

Correct Answer

upvoted 3 times

palciny 1 year, 3 months ago

Selected Answer: B

https://docs.microsoft.com/en-us/microsoft-365/compliance/sit-get-started-exact-data-match-hash-upload?view=o365-worldwide

You can upload data with the EDMUploadAgent to any given data store only twice per day.

upvoted 1 times

wooyourdaddy 1 year, 5 months ago

Selected Answer: B

I wrote the exam today, this question was on it, I choose B, scored 890.

upvoted 1 times

MahmoudEldeep 1 year, 7 months ago

Selected Answer: B

Correct answer is B

upvoted 1 times

Dooa 1 year, 9 months ago

B..twice per day

upvoted 2 times

Jandre 1 year, 11 months ago

Selected Answer: B

https://docs.microsoft.com/en-us/microsoft-365/compliance/create-custom-sensitive-information-types-with-exact-data-match-based-classification?view=o365-worldwide#links-to-edm-upload-agent-by-subscription-type

upvoted 3 times

Question #14 *Topic 1*

HOTSPOT -

You are implementing Microsoft Office 365 Message Encryption (OME) for a Microsoft 365 tenant named contoso.com.

You need to meet the following requirements:

- All email to a domain named fabrikam.com must be encrypted automatically.
- Encrypted emails must expire seven days after they are sent.

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

NOTE: Each correct selection is worth one point.

Hot Area:

Answer Area

All email to a domain named fabrikam.com must be encrypted automatically:

- A data connector in the Microsoft 365 compliance center
- A data loss prevention (DLP) policy in the Microsoft 365 compliance center
- A mail flow connector in the Exchange admin center
- A mail flow rule in the Exchange admin center

Encrypted emails must expire seven days after they are sent:

- A custom branding template in Microsoft Exchange Online PowerShell
- A label policy in the Microsoft 365 compliance center
- A mail flow rule in the Exchange admin center
- A sensitive info type in the Microsoft 365 compliance center

Correct Answer:

Answer Area

All email to a domain named fabrikam.com must be encrypted automatically:

- A data connector in the Microsoft 365 compliance center
- A data loss prevention (DLP) policy in the Microsoft 365 compliance center
- A mail flow connector in the Exchange admin center
- A mail flow rule in the Exchange admin center

Encrypted emails must expire seven days after they are sent:

- A custom branding template in Microsoft Exchange Online PowerShell
- A label policy in the Microsoft 365 compliance center
- A mail flow rule in the Exchange admin center
- A sensitive info type in the Microsoft 365 compliance center

Reference:

https://docs.microsoft.com/en-us/microsoft-365/compliance/email-encryption?view=o365-worldwide https://docs.microsoft.com/en-us/microsoft-365/compliance/ome-advanced-expiration?view=o365-worldwide

Bharat Highly Voted 2 years, 5 months ago

Correct answers are "A Mail Flow Rule" and "Custom Branding Template" respectively.

upvoted 48 times

ccKane 1 year, 3 months ago

"A Mail Flow Rule": see - https://docs.microsoft.com/en-us/microsoft-365/compliance/define-mail-flow-rules-to-encrypt-email?view=o365-worldwide --- /// --- "Custom Branding Template": see - https://docs.microsoft.com/en-us/microsoft-365/compliance/ome-advanced-expiration?view=o365-worldwide

upvoted 4 times

Rockalm 11 months ago

With a connector you can request to always use TLS, but not the OME encryption. So, "mail flow rule" is the right answer.

upvoted 2 times

JakubK64 Highly Voted 2 years, 5 months ago

Base on this docs article - https://docs.microsoft.com/en-us/microsoft-365/compliance/ome?view=o365-worldwide I think it will be mail flow rule (not connector) and templates for "Do not forward"

upvoted 6 times

JakubK64 2 years, 5 months ago

I mean "Expire in 7 days", not "Do not forward"

upvoted 2 times

dmoorthy Most Recent 7 months, 1 week ago

Correct answers are "A Mail Flow Rule" and "Custom Branding Template"

upvoted 1 times

xswe 7 months, 3 weeks ago

You can easily configure this if you just visit Exchange Admin Center and go to "Mail flow" then "Rules", configured a rule that encrypt all messages that goes to the given domain.

If you want the encrypted emails to get expired in x amnount of days you use a custom branding template in MS Exchange through powershell, the following command will achieve this
"New-OMEConfiguration -Identity "Expire in x days" -ExternalMailExpiryInDays X"

upvoted 2 times

fimbulvetrk 1 year ago

you don't have to use a mail flow connector in this case, once you can simply create a mail flow rule specifying the recipient domain and then apply the encryption, so I'd go for "mail flow rule" and "custom brand template"

upvoted 1 times

Bluebaron520 1 year ago

valid 24/11/2022

upvoted 1 times

wooyourdaddy 1 year, 5 months ago

I wrote the exam today, this question was on it, I choose the answers provided, scored 890!

upvoted 1 times

junior6995 1 year, 5 months ago

New-OMEConfiguration -Identity "Expire in 7 days" -ExternalMailExpiryInDays 7

upvoted 1 times

ChaBum 1 year, 10 months ago

Connector as email encryption is for a specific domain (partner)
https://docs.microsoft.com/en-us/exchange/mail-flow-best-practices/use-connectors-to-configure-mail-flow/set-up-connectors-for-secure-mail-flow-with-a-partner

upvoted 3 times

Whatsamattr81 1 year, 4 months ago

I don't think a send connector is useful in this scenario... it's gotta be a simple transport rule.

upvoted 1 times

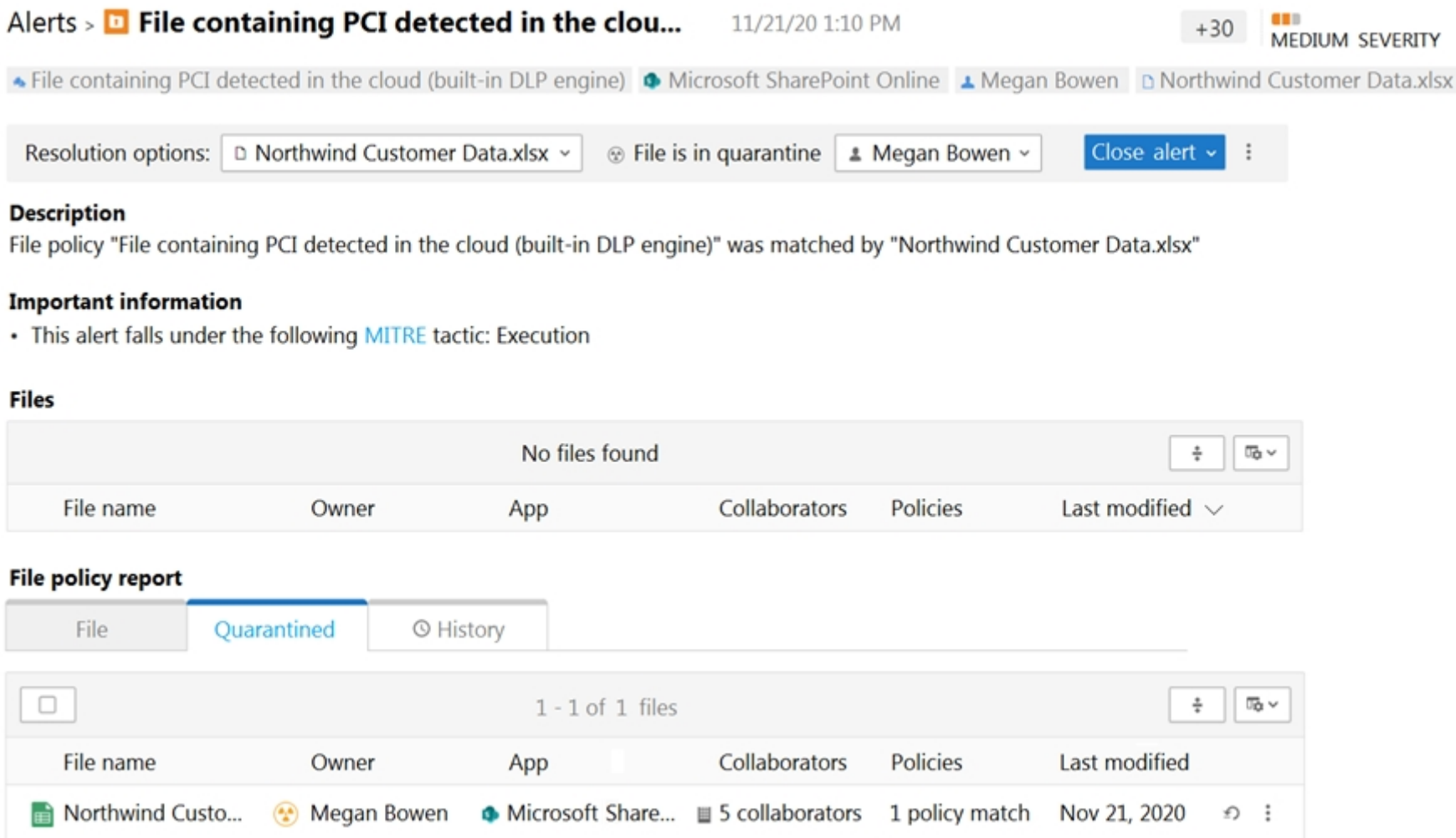
Discuss4certi 2 years, 3 months ago

Correct. for the mailflow rule go to the exchange admin center to enable it. and for the powershell follow the example in this piece of documentation: https://docs.microsoft.com/en-us/microsoft-365/compliance/ome-advanced-expiration

upvoted 3 times

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.



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

Community vote distribution

D (100%)

jcgonzalez1978 Highly Voted 2 years, 3 months ago

Answer is correct IMHO:
A. It's not the answers, since you cannot modify a policy template in MCAS. You can create policies from policies templates
B. Assigning that role is not going to prevent files to be quarantined
C. We don't want to exclude the file, we want to receive an alert instead of the file being sent to quarantine

upvoted 9 times

wooyourdaddy Highly Voted 1 year, 5 months ago

Selected Answer: D

I wrote the exam today, this question was on it, I choose the answers provided, scored 890!

upvoted 7 times

xswe Most Recent 7 months, 3 weeks ago

When it comes to the actions that are taking place with a policy in Cloud Apps you want to re-configure the governance action of the policy. If the "Quarintine" options is checked you ahve to uncheck this to avoid sending the file to quarantine.

upvoted 2 times

Discuss4certi 2 years, 3 months ago

correct. The wrong governance action is being executed. if you only want an alert you should not enable the quarantine option

upvoted 6 times

HOTSPOT -

You create a sensitivity label as shown in the Sensitivity Label exhibit.

Review your settings and finish

Name

Sensitivity1

Display name

Sensitivity1

Description for users

Sensitivity1

Scope

File,Email

Encryption

Content marking

Watermark: Watermark

Header: Header

Auto-labeling

Group settings

Site settings

Auto-labeling for database columns

None

You create an auto-labeling policy as shown in the Auto Labeling Policy exhibit.

Auto-labeling policy

Edit policy | Delete policy

Policy name

Auto-labeling policy

Description

Label in simulation

Sensitivity1

Info to label

IP Address

Apply to content in these locations

Exchange email All

Rules for auto-applying this label

Exchange email 1 rule

Mode

On

Comment

A user sends the following email:

From: user1@contoso.com -

To: user2@fabrikam.com -

Subject: Address List -
Message Body:
Here are the lists that you requested.
Attachments:
<<File1.docx>>
<<File2.xml>>
Both attachments contain lists of IP addresses.
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:

Answer Area

Statements	Yes	No
Sensitivity1 is applied to the email.	○	○
A watermark is added to File1.docx.	○	○
A header is added to File2.xml.	○	○

Answer Area

Correct Answer:

Statements	Yes	No
Sensitivity1 is applied to the email.	○	○
A watermark is added to File1.docx.	○	○
A header is added to File2.xml.	○	○

Box 1: Yes -

Box 2: No -
The email is labeled but not the attachment.

Box 3: No -
Reference:
https://docs.microsoft.com/en-us/microsoft-365/compliance/apply-sensitivity-label-automatically?view=o365-worldwide

slayer78 Highly Voted 2 years, 2 months ago
yes, no and no. Only the email gets a label. Specific to auto-labeling for Exchange:
Unlike manual labeling or auto-labeling with Office apps, PDF attachments as well as Office attachments are also scanned for the conditions you specify in your auto-labeling policy. When there is a match, the email is labeled but not the attachment.
https://docs.microsoft.com/en-us/microsoft-365/compliance/apply-sensitivity-label-automatically?view=o365-worldwide
upvoted 21 times

CalST 1 year, 9 months ago
Labels that have encryption settings affect supported attachments in emails but only the email gets a header (no watermark or footer)
upvoted 3 times

Topaz007 2 years, 2 months ago
This is correct indeed. A very tricking question this one.
upvoted 2 times

klosedotorg83 2 years, 1 month ago
A watermark cannot be added to an email, so in this case, the watermark is added to the file.
For me is correct, Yes, Yes and No
upvoted 2 times

Topaz007 2 years, 1 month ago
@klosedotorg83: Files in emails won't be altered (like adding a watermark), read this: https://docs.microsoft.com/en-us/microsoft-365/compliance/apply-sensitivity-label-automatically?view=o365-worldwide.

It states clearly: '...When there is a match, the email is labeled but not the attachment...'

So the answers are Yes, No and No.
upvoted 6 times

shanti0091 Highly Voted 2 years, 4 months ago
correct
upvoted 6 times

mbhasker Most Recent 2 days, 20 hours ago
yes, yes, No
upvoted 1 times

Azurefox79 9 months, 1 week ago
Only email is in scope per exhibit, answer is correct
upvoted 1 times

wooyourdaddy 1 year, 5 months ago
I wrote the exam today, this question was on it, I choose Yes / No / No, scored 890!
upvoted 2 times

Pravda 1 year, 10 months ago
Yes - No - No
Files in emails won't be altered (like adding a watermark), read this: https://docs.microsoft.com/en-us/microsoft-365/compliance/apply-sensitivity-label-automatically?view=o365-worldwide.

One or more sensitivity labels created and published (to at least one user) that you can select for your auto-labeling policies. For these labels:

It doesn't matter if the auto-labeling in Office apps label setting is turned on or off, because that label setting supplements auto-labeling policies, as explained in the introduction.
If the labels you want to use for auto-labeling are configured to use visual markings (headers, footers, watermarks), note that these are not applied to documents.

upvoted 1 times

Sam12 1 year, 10 months ago

https://docs.microsoft.com/en-us/microsoft-365/compliance/apply-sensitivity-label-automatically?view=o365-worldwide#compare-auto-labeling-for-office-apps-with-auto-labeling-policies

upvoted 1 times

examkid 2 years, 1 month ago

Regarding adding the watermark Microsoft states the following:
https://docs.microsoft.com/en-us/microsoft-365/compliance/apply-sensitivity-label-automatically?view=o365-worldwide#how-to-configure-auto-labeling-policies-for-sharepoint-onedrive-and-exchange

upvoted 3 times

nupagazi 1 year, 10 months ago

Totally afgreed. Yes, No, No:
If the labels you want to use for auto-labeling are configured to use visual markings (headers, footers, watermarks), note that these are not applied to documents.

upvoted 1 times

test123123 2 years, 5 months ago

Seems legit.

upvoted 1 times

Question #17 *Topic 1*

You receive an email that contains a list of words that will be used for a sensitive information type.
You need to create a file that can be used as the source of a keyword dictionary.
In which format should you save the list?

A. a JSON file that has an element for each word

B. an ACCDB database file that contains a table named Dictionary

C. an XML file that contains a keyword tag for each word

D. a CSV file that contains words separated by commas

Correct Answer: *D*
The keywords for your dictionary could come from various sources, most commonly from a file (such as a .csv or .txt list) imported in the service or by PowerShell cmdlet.
Note:
There are several versions of this question in the exam. The question has two possible correct answers:
1. a CSV file that contains words separated by commas
2. a text file that has one word on each line
Other incorrect answer options you may see on the exam include the following:
☞ a TSV file that contains words separated by tabs
☞ an XLSX file that contains one word in each cell of the first row
☞ a DOCX file that has one word on each line
Reference:
https://docs.microsoft.com/en-us/microsoft-365/compliance/create-a-keyword-dictionary?view=o365-worldwide

Community vote distribution
D (56%) C (44%)

pheb Highly Voted 2 years, 3 months ago
Yes, can be TXT- or a CVS-File --> the answer is correct
upvoted 11 times

luissaro Most Recent 7 months, 2 weeks ago
Selected Answer: D
"The keywords for your dictionary can come from various sources, most commonly from a file (such as a .csv or .txt list) imported in the service or via a PowerShell cmdlet, from a list you enter directly in the PowerShell cmdlet, or from an existing dictionary" in https://learn.microsoft.com/en-us/microsoft-365/compliance/create-a-keyword-dictionary?view=o365-worldwide
XML is used to create customsensitive information type using PowerShell
upvoted 1 times

xswe 7 months, 3 weeks ago
When creating a keyword dictionary for a sensitive information type you can only use .txt and .csv files.
So CSV in this case.
upvoted 1 times

Azurefox79 9 months, 1 week ago
Given answer correct, CSV or TXT file. Upload via portal or powershell
upvoted 1 times

NinjaSchoolProfessor 11 months, 1 week ago
The web GUI accepts TXT or CSV, while the PowerShell cmdlet (New-DlpKeywordDictionary) accepts only CSV.
upvoted 1 times

Abhishek1610 1 year ago
Selected Answer: D
most commonly from a file (such as a .csv or .txt list)
upvoted 1 times

chrissempai 1 year, 2 months ago
Selected Answer: D
Basic steps to creating a keyword dictionary
The keywords for your dictionary could come from various sources, most commonly from a file (such as a .csv or .txt list) imported in the service or by PowerShell cmdlet, from a list you enter directly in the PowerShell cmdlet, or from an existing dictionary.

upvoted 1 times

chrissempai 1 year, 2 months ago

Selected Answer: C

In Microsoft documentation it's XML not CSV
https://docs.microsoft.com/en-us/microsoft-365/compliance/create-a-keyword-dictionary?view=o365-worldwide

upvoted 2 times

chrissempai 1 year, 2 months ago

Sorry, finaly it's a CSV or a TXT file.
the question is which format saving for creating the keyword
ref in documentation :
Basic steps to creating a keyword dictionary
The keywords for your dictionary could come from various sources, most commonly from a file (such as a .csv or .txt list) imported in the service or by PowerShell cmdlet, from a list you enter directly in the PowerShell cmdlet, or from an existing dictionary.

upvoted 4 times

SelloLed 1 year, 3 months ago

On Microsoft ESI practice test ....option selected is C
an XML file
C

upvoted 1 times

prats005 1 year, 4 months ago

XML- You receive an email that contains a list of words that will be used for a sensitive information type.
You need to create a file that can be used as the source of a keyword dictionary.
In which format should you save the list

upvoted 1 times

prats005 1 year, 4 months ago

Although you can create keyword lists in sensitive information types, keyword lists are limited in size and require modifying XML to create or edit them

upvoted 1 times

Catsval 1 year, 5 months ago

Selected Answer: C

IMO its C because in D you cannot separate by commas in a CVS, its not gonna work. There is a similar question in the practice questions and the answer is XML

upvoted 1 times

CEAUSESCU247 1 year, 5 months ago

csv ---> comma-separated values

upvoted 1 times

Harry0300 1 year, 5 months ago

XML is for keyword list.

upvoted 1 times

JamesM9 1 year, 7 months ago

As noted in the link, the answer is D - a CSV file. However, XML is also noted. In the exam, I would go with D (CSV) purely because the link attached here specifically makes reference to using a CSV file.

Answer - D

upvoted 3 times

ccKane 1 year, 3 months ago

As mentioned, we receive a list of words via mail > copy the words into a CSV (as a source) and follow the basic steps as mentioned: with 1) Opening compliance Portal and 2) Load Keyword list from the source (.csv or txt): "...comma-separated list of keywords to create a custom keyword dictionary..."

upvoted 1 times

j_ms 1 year, 8 months ago

Selected Answer: D

D. As others note, the source list should be a CSV or TXT file. The completed dictionary will be an XML file.

upvoted 2 times

IAGirl 1 year, 8 months ago

Selected Answer: C

C is the answer, we must first create the source, on this question, we are not providing the source of keyword form, but the source for the keyword dictionary

upvoted 1 times

Pravda 1 year, 10 months ago

On exam 1/20/2022

upvoted 1 times

Ali_557 1 year, 11 months ago

The keywords for your dictionary could come from various sources, most commonly from a file (such as a .csv or .txt list) imported in the service or by PowerShell cmdlet, from a list you enter directly in the PowerShell cmdlet, or from an existing dictionary.

upvoted 1 times

HardcodedCloud 1 year, 11 months ago

The keywords for your dictionary could come from various sources, most commonly from a file (such as a .csv or .txt list) imported in the service or by PowerShell cmdlet.

upvoted 2 times

Question #18 *Topic 1*

You have a Microsoft 365 E5 tenant that uses a domain named contoso.com.
A user named User1 sends link-based, branded emails that are encrypted by using Microsoft Office 365 Advanced Message Encryption to the recipients shown in the following table.

Name	Email address
Recipient1	Recipient1@contoso.com
Recipient2	Recipient2@fabrikam.onmicrosoft.com
Recipient3	Recipient3@outlook.com
Recipient4	Recipient4@gmail.com

For which recipients can User1 revoke the emails?

A. Recipient4 only

B. Recipient1 only

C. Recipient1, Recipient2, Recipient3, and Recipient4

D. Recipient3 and Recipient4 only

E. Recipient1 and Recipient2 only

Correct Answer: *A*
Reference:
https://docs.microsoft.com/en-us/microsoft-365/compliance/revoke-ome-encrypted-mail?view=o365-worldwide

Community vote distribution
A (100%)

maxstv Highly Voted 2 years, 3 months ago
Correct answer is "A"

"You cannot revoke a mail that you sent to a recipient that uses a work or school account from Office 365 or Microsoft 365 or a user that uses a Microsoft account, for example, an outlook.com account."

https://docs.microsoft.com/en-us/microsoft-365/compliance/revoke-ome-encrypted-mail?view=o365-worldwide
upvoted 22 times

wooyourdaddy Highly Voted 1 year, 5 months ago
Selected Answer: A
I wrote the exam today, this question was on it, I choose A, scored 890!
upvoted 10 times

NidaH 3 months, 3 weeks ago
Stop commening this in every question.
upvoted 5 times

Joipanom 1 month, 2 weeks ago
I like him
upvoted 2 times

Domza 3 weeks, 2 days ago
haha :)
upvoted 1 times

Gesbie Most Recent 3 months, 3 weeks ago
was on Exam August 9, 2023
upvoted 1 times

TeeKay_From_the_South 5 months ago
Microsoft doesn't play with google.
upvoted 3 times

xswe 7 months, 3 weeks ago

When using OME encryption you have be aware that you cannot revoke any email that is sent to a reciepient that uses a work or school account from Office 365 or Microsoft 365, for example outlook.com / hotmail.com.

So the correct answer in this question will be the "gmail" reciepient will we be able to revoke the email from.

upvoted 2 times

NinjaSchoolProfessor 11 months, 1 week ago

Answer is A - The phrase to focus on here is "link-based" as link-based e-mails can be revoked. Those which are NOT link-based which include work or school account from O365 / M365 or a user that has a Microsoft account (such as Outlook.com) do cannot as they will not receive the link-based e-mail, but rather the full encrypted email.

upvoted 2 times

j_ms 1 year, 8 months ago

Selected Answer: A

A. "Whether a recipient receives a link-based experience or an inline experience depends on the recipient identity type: Office 365 and Microsoft account recipients (for example, outlook.com users) get an inline experience in supported Outlook clients. All other recipient types, such as Gmail and Yahoo recipients, get a link-based experience."
https://docs.microsoft.com/en-us/microsoft-365/compliance/revoke-ome-encrypted-mail?view=o365-worldwide

upvoted 4 times

Batman160591 1 year, 8 months ago

The answer is : Recipient 4 Only.
"You can revoke a mail that you sent to a single recipient that uses a social account such as gmail.com or yahoo.com. In other words, you can revoke an email sent to a single recipient that received the link-based experience.

You cannot revoke a mail that you sent to a recipient that uses a work or school account from Office 365 or Microsoft 365 or a user that uses a Microsoft account, for example, an outlook.com account."

https://docs.microsoft.com/en-us/microsoft-365/compliance/revoke-ome-encrypted-mail?view=o365-worldwide

upvoted 2 times

Batman160591 1 year, 8 months ago

The answer is Recipient 3 and 4.
"You can revoke a mail that you sent to a single recipient that uses a social account such as gmail.com or yahoo.com. In other words, you can revoke an email sent to a single recipient that received the link-based experience.

You cannot revoke a mail that you sent to a recipient that uses a work or school account from Office 365 or Microsoft 365 or a user that uses a Microsoft account, for example, an outlook.com account."
https://docs.microsoft.com/en-us/microsoft-365/compliance/revoke-ome-encrypted-mail?view=o365-worldwide

upvoted 2 times

Pravda 1 year, 10 months ago

On exam 1/20/2022

upvoted 1 times

jkklim 2 years, 2 months ago

Admins and message senders can revoke encrypted emails if the recipient received a link-based, branded encrypted email. If the recipient received a native inline experience in a supported Outlook client, then you can't revoke the message.

All other recipient types, such as Gmail and Yahoo recipients, get a link-based experience.

so gmail is linked based which is recipient4 - Answer A

upvoted 4 times

SuperMax 1 year, 11 months ago

Correct
Whether a recipient receives a link-based experience or an inline experience depends on the recipient identity type: Office 365 and Microsoft account recipients (for example, outlook.com users) get an inline experience in supported Outlook clients. All other recipient types, such as Gmail and Yahoo recipients, get a link-based experience.

upvoted 1 times

Eltooth 2 years, 4 months ago

Correct answer is D - Recipient 3 & Recipient 4.
Admins and message senders can revoke encrypted emails if the recipient received a link-based, branded encrypted email. If the recipient received a native inline experience in a supported Outlook client, then you can't revoke the message.
Whether a recipient receives a link-based experience or an inline experience depends on the recipient identity type: Office 365 and Microsoft account recipients (for example, outlook.com users) get an inline experience in supported Outlook clients. All other recipient types, such as Gmail and Yahoo recipients, get a link-based experience.

You can revoke a mail that you sent to a single recipient that uses a social account such as gmail.com or yahoo.com. In other words, you can revoke an email sent to a single recipient that received the link-based experience.
You cannot revoke a mail that you sent to a recipient that uses a work or school account from Office 365 or Microsoft 365 or a user that uses a Microsoft account, for example, an outlook.com account.

https://docs.microsoft.com/en-us/microsoft-365/compliance/revoke-ome-encrypted-mail?view=o365-worldwide#how-to-revoke-an-encrypted-message-that-you-sent

upvoted 3 times

xofowi5140 2 years, 4 months ago

As you said.
"You cannot revoke a mail that you sent to a recipient that uses a... Microsoft account, for example, an outlook.com account."
So Recipient4 only .

upvoted 7 times

shanti0091 2 years, 4 months ago

This is correct, inline experience cannot be revoked (office365 tenant and outlook.com)
https://docs.microsoft.com/en-us/microsoft-365/compliance/revoke-ome-encrypted-mail?view=o365-worldwide#:~:text=Whether%20a%20recipient,link-based%20experience.

upvoted 4 times

Question #19 *Topic 1*

You need to test Microsoft Office 365 Message Encryption (OME) capabilities for your company. The test must verify the following information:

- The acquired default template names
- The encryption and decryption verification status

Which PowerShell cmdlet should you run?

A. Test-ClientAccessRule

B. Test-Mailflow

C. Test-OAuthConnectivity

D. Test-IRMConfiguration

Correct Answer: *D*

Reference:

https://docs.microsoft.com/en-us/microsoft-365/compliance/set-up-new-message-encryption-capabilities?view=o365-worldwide

McAlec Highly Voted 2 years ago

The answer is definitely D.
You will get all required info by running the Test-IRMConfiguration cmdlet

Results : Acquiring RMS Templates ...
- PASS: RMS Templates acquired. Templates available: Contoso - Confidential View Only, Contoso - Confidential, Do Not Forward.
Verifying encryption ...
- PASS: Encryption verified successfully.
Verifying decryption ...
- PASS: Decryption verified successfully.
Verifying IRM is enabled ...
- PASS: IRM verified successfully.
OVERALL RESULT: PASS

upvoted 15 times

xswe Most Recent 7 months, 3 weeks ago

Test-IRMConfiguration is used to test the IRM functionality, remember that IRM is a function that helps with the encryption of messages. Just what MS are asking for.

upvoted 4 times

Question #20 *Topic 1*

You have a Microsoft 365 tenant that uses trainable classifiers.

You are creating a custom trainable classifier.

You collect 300 sample file types from various geographical locations to use as seed content. Some of the file samples are encrypted.

You organize the files into categories as shown in the following table.

Category	Type	Encryption status
Category1	.docx	Encrypted
Category2	.xlsx	Encrypted
Category3	.docx	Not encrypted
Category4	.mht	Not encrypted
Category5	.htm	Not encrypted

Which file categories can be used as seed content?

A. Category2, Category3, and Category5 only

B. Category3 and Category5 only

C. Category1 and Category3 only

D. Category3 only

E. Category1, Category2, Category3, Category4, and Category5

Correct Answer: *B*

Classifiers only work with items that are not encrypted and have file name extensions that are supported by SharePoint Online.

Note: SharePoint Online does not support .eml and .mht files.

Reference:

https://docs.microsoft.com/en-us/microsoft-365/compliance/classifier-learn-about?view=o365-worldwide https://docs.microsoft.com/en-us/microsoft-365/compliance/classifier-get-started-with?view=o365-worldwide https://docs.microsoft.com/en-us/sharepoint/technical-reference/default-crawled-file-name-extensions-and-parsed-file-types

[Removed] Highly Voted 9 months, 2 weeks ago

Should be 3,4,5
https://learn.microsoft.com/en-us/sharepoint/technical-reference/default-crawled-file-name-extensions-and-parsed-file-types

upvoted 6 times

Rohit_Panchal Most Recent 4 months, 3 weeks ago

Should be 3, 4, 5 since mht is supported, however 3,4,5 is not under answer options so the given answer is correct.

upvoted 1 times

217f3c9 6 months, 2 weeks ago

mht is supported (now)

upvoted 3 times

xswe 7 months, 3 weeks ago

When you want to use documents as seed content you cant use encrypted documents and all file extension wont work.
Both docx and xlsx will not work since they are encrypted.
Seems like all the unencrypted files are supported so both MHT, DOCX and HTM.
https://learn.microsoft.com/en-us/sharepoint/technical-reference/default-crawled-file-name-extensions-and-parsed-file-types

upvoted 2 times

MartinSebek 10 months, 3 weeks ago

I would say that the answer is correct. But also .mht files are now supported according to the links provided. But category 3, 4 and 5 is not in options.

upvoted 1 times

NinjaSchoolProfessor 11 months, 1 week ago

Answer = D - Classifiers only work with items that are not encrypted, and out of that list only .docx files are supported - Reference: https://learn.microsoft.com/en-us/microsoft-365/compliance/classifier-learn-about?view=o365-worldwide&viewFallbackFrom=o365-worldwide%20https%3A%2F%2Fdocs.microsoft.com%2Fen-us%2Fmicrosoft-365%2Fcompliance%2Fclassifier-get-started-with%3Fview%3Do365-worldwide%20https%3A%2F%2Fdocs.microsoft.com%2Fen-us%2Fsharepoint%2Ftechnical-reference%2Fdefault-crawled-file-name-extensions-and-parsed-file-types

upvoted 1 times

Harry008 1 year ago

Answer is correct .htm and docx

upvoted 2 times

Harry008 1 year ago

How to create a trainable classifier
Collect between 50-500 seed content items. These must be only samples that strongly represent the type of content you want the trainable classifier to positively identify as being in the category. See, Default crawled file name extensions and parsed file types in SharePoint Server for the supported file types.
https://learn.microsoft.com/en-us/sharepoint/technical-reference/default-crawled-file-name-extensions-and-parsed-file-types

upvoted 1 times

Question #21 *Topic 1*

You have a Microsoft 365 tenant that uses Microsoft Office 365 Message Encryption (OME).
You need to ensure that any emails containing attachments and sent to user1@contoso.com are encrypted automatically by using OME.
What should you do?

A. From the Exchange admin center, create a new sharing policy.

B. From the Microsoft 365 security center, create a Safe Attachments policy.

C. From the Exchange admin center, create a mail flow rule.

D. From the Microsoft 365 compliance center, configure an auto-apply retention label policy.

Correct Answer: *C*
You can create mail flow rules to help protect email messages you send and receive. You can set up rules to encrypt any outgoing email messages and remove encryption from encrypted messages coming from inside your organization or from replies to encrypted messages sent from your organization.
Reference:
https://docs.microsoft.com/en-us/microsoft-365/compliance/define-mail-flow-rules-to-encrypt-email?view=o365-worldwide

Community vote distribution

C (100%)

kpatllegar Highly Voted 2 years, 1 month ago
Option C - Right Answer
upvoted 10 times

heshmat2022 Most Recent 1 month, 1 week ago
IT WAS ON EXAM OCTOBER 18 2023
upvoted 1 times

xswe 7 months, 3 weeks ago
To create a rule that ensures that all email containing attachment & is sent to a specific user are automatically encrypted with OME you should just create a mail flow rule in Exchange admin center.
This can also be achieved with a DLP policy with only Exchange choosed as location.
upvoted 2 times

JCkD4Ni3L 11 months, 2 weeks ago
Selected Answer: C
Mail Flow rule will fit the bill.
upvoted 2 times

wooyourdaddy 1 year, 5 months ago
Selected Answer: C
I wrote the exam today, this question was on it, I choose C, scored 890!
upvoted 1 times

crista_ 1 year, 8 months ago
C is correct
upvoted 2 times

Pravda 1 year, 10 months ago
On exam 1/20/2022
upvoted 1 times

pixuefei 1 year, 11 months ago
correct, a mail flow rule is needed
upvoted 2 times

Question #22 *Topic 1*

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. Create a new sensitivity label scoped to Groups & sites.

C. Run the Execute-AzureAdLabelSync cmdlet.

D. Configure the EnableMIPLabels Azure Active Directory (Azure AD) setting.

Correct Answer: *B*
Reference:
https://docs.microsoft.com/en-us/microsoft-365/compliance/sensitivity-labels-teams-groups-sites?view=o365-worldwide

Community vote distribution

D (81%) C (19%)

Topaz007 Highly Voted 2 years, 1 month ago
It's C, but the cmdlet is different (Execute-AzureADLabelSync).

Since you need to enable this functionality first. Otherwise the option to scope a sensitivity label to Groups & Sites is greyed out.

See here: https://docs.microsoft.com/en-us/powershell/module/exchange/execute-azureadlabelsync?view=exchange-ps

It states: '...Use the Execute-AzureADLabelSync cmdlet to start the synchronization of sensitivity labels into Azure Active Directory. This allows the application of sensitivity labels to Microsoft Teams sites, Microsoft 365 Groups, and SharePoint sites....'
upvoted 20 times

zaqwsx 1 year, 11 months ago
Yes, but there is information that "This cmdlet is required if you were using sensitivity labels before September 2019." So I think it should be B
upvoted 6 times

MahmoudEldeep 2 years ago
Agree, You can not create a new sensitivity label for Groups & Sites unless you enable this option.
upvoted 4 times

sergioandreslq 1 year, 11 months ago
Agree, first step to remove the grayout for the sensitivity label is to run in powershell over the module IPPSSession (compliance center) the command: Execute-AzureADLabelSync.

See the steps:
Connect-ExchangeOnline -UserPrincipalName User@Domain.com
Connect-IPPSSession -UserPrincipalName User@Domain.com
Execute-AzureADLabelSync
https://docs.microsoft.com/en-us/microsoft-365/compliance/sensitivity-labels-teams-groups-sites?view=o365-worldwide#how-to-configure-groups-and-site-settings
upvoted 2 times

sergioandreslq 1 year, 11 months ago
However, this is a tricky question because you MUST have enable the parameter "EnableMIPLabels" to "True"
In theory, this is the first step which is to enable the capacity for Microsoft 365 group to use sensitivity label, then, You run the synchronization with the command "Execute-AzureADLabelSync", so, If we follow the steps, the correct answer is "D"
https://docs.microsoft.com/en-us/answers/questions/340223/how-enable-sensitivity-feature-for-sharepoint-site.html#:~:text=%20Here%20are%20the%20steps%20to%20enable%20sensitivity,scope%20for%20this%20label%20%22.%20Then...%20More%20

after some time thinking, I go with "D" assuming that I am begging from zero in the tenant I go with D
upvoted 10 times

Pravda Highly Voted 1 year, 10 months ago
Selected Answer: D
Defiantly D
Look at the links.
https://docs.microsoft.com/en-us/microsoft-365/compliance/sensitivity-labels-teams-groups-sites?view=o365-worldwide
Step 1 says - ollow the instructions from the Azure AD documentation to enable sensitivity label support
The link takes you to
https://docs.microsoft.com/en-us/azure/active-directory/enterprise-users/groups-assign-sensitivity-labels
Look at step 5 - Enable the feature "EnableMIPLabels"] = "True"

The AzureAdLabelSync cmdlet follows. See troubleshooting #3 and the sentence after #5, You will also need to synchronize your sensitivity labels to Azure AD
Select Groups, and then select New group is #2 in the next section AFTER EnableMIPLabels has been enabled.
D is the answer.
upvoted 10 times

JCkD4Ni3L 11 months, 2 weeks ago
You are right, I have done this countless times. The order is important if you are to be successfull. Best is to script this ... Answer is D.
upvoted 1 times

bhadolaa29 Most Recent 5 months, 1 week ago
D is the correct Answer. Tested
upvoted 2 times

dmoorthy 7 months, 1 week ago
Answers is D.
upvoted 1 times

luissaro 7 months, 2 weeks ago
Selected Answer: D
if you follow the guide you will understand the correct answer is D: "If you haven't yet enabled sensitivity labels for containers, do the following set of steps as a one-time procedure:
1. Because this feature uses Azure AD functionality, follow the instructions from the Azure AD documentation to enable sensitivity label support: Assign sensitivity labels to Microsoft 365 groups in Azure Active Directory.
2.You now need to synchronize your sensitivity labels to Azure AD. First, connect to Security & Compliance PowerShell. For example, in a PowerShell session that you run as administrator, sign in with a global administrator account.
3. Then run the following command to ensure your sensitivity labels can be used with Microsoft 365 groups: Execute-AzureAdLabelSync" in https://learn.microsoft.com/en-us/microsoft-365/compliance/sensitivity-labels-teams-groups-sites?view=o365-worldwide
upvoted 2 times

xswe 7 months, 3 weeks ago
To be able to apply and view sensitivty labels in Teams, Sharepoint, Outlook you need to enable it.
You do this with "$Setting["EnableMIPLabels"] = "True""
upvoted 3 times

wooyourdaddy 9 months, 1 week ago
Believe the answer is D as well. This link:

https://learn.microsoft.com/en-us/microsoft-365/compliance/migrate-aad-classification-sensitivity-labels?view=o365-worldwide#case-b-tenant-used-sensitivity-labels-for-documents-and-emails

States:

As soon as admin enables sensitivity label feature on the tenant by setting the tenant flag 'EnableMIPLabels' to true, the document and email sensitivity labels in group/site/team create and edit dialog boxes appear.
upvoted 1 times

Azurefox79 9 months, 1 week ago
Selected Answer: D
D. Labels need to first be configured to work with Azure AD (which is where MS365 groups live)
upvoted 2 times

Azurefox79 9 months, 1 week ago
D. Labels need to first be configured to work with Azure AD (which is where MS365 groups live)
upvoted 1 times

reastman66 9 months, 4 weeks ago
Selected Answer: C
https://learn.microsoft.com/en-us/microsoft-365/compliance/sensitivity-labels-teams-groups-sites?view=o365-worldwide#enable-this-preview-and-synchronize-labels

How to enable sensitivity labels for containers and synchronize labels
If you haven't yet enabled sensitivity labels for containers, do the following set of steps as a one-time procedure:

Because this feature uses Azure AD functionality, follow the instructions from the Azure AD documentation to enable sensitivity label support: Assign sensitivity labels to Microsoft 365 groups in Azure Active Directory.

You now need to synchronize your sensitivity labels to Azure AD. First, connect to Security & Compliance PowerShell.

For example, in a PowerShell session that you run as administrator, sign in with a global administrator account.

Then run the following command to ensure your sensitivity labels can be used with Microsoft 365 groups:

PowerShell

Copy
Execute-AzureAdLabelSync

upvoted 1 times

NinjaSchoolProfessor 11 months, 1 week ago

Answer = D.

[A] Set-SPOSite applies to SharePoint
[B] The action of creating a new sensitivity label scoped to Groups & sites will not be successful if
[C] Execute-AzureAdLabelSync cmdlet allows the application of sensitivity labels to Microsoft Teams sites, Microsoft 365 Groups, and SharePoint sites and is is required if you were using sensitivity labels before September 2019.
[D] EnableMIPLabels set to true is needed when assign sensitivity labels to Microsoft 365 groups in Azure Active Directory. Note that this can now be performed via the Azure Portal as referenced here: https://learn.microsoft.com/en-us/azure/active-directory/enterprise-users/groups-assign-sensitivity-labels

upvoted 2 times

JCkD4Ni3L 1 year ago

Selected Answer: D

You need to enable the use of Sensitivity labels within teams before you can do anything else.

upvoted 1 times

rexelek 1 year, 1 month ago

Selected Answer: D

https://learn.microsoft.com/en-us/azure/active-directory/enterprise-users/groups-assign-sensitivity-labels

upvoted 1 times

Thebald 1 year, 5 months ago

Selected Answer: C

https://docs.microsoft.com/en-us/microsoft-365/compliance/sensitivity-labels-teams-groups-sites?view=o365-worldwide#how-to-enable-sensitivity-labels-for-containers-and-synchronize-labels

upvoted 1 times

wooyourdaddy 1 year, 5 months ago

Selected Answer: D

I wrote the exam today, this question was on it, I choose D, scored 890!

upvoted 3 times

bliix 1 year, 6 months ago

Selected Answer: C

https://docs.microsoft.com/en-us/microsoft-365/compliance/sensitivity-labels-teams-groups-sites?view=o365-worldwide

Then run the following command to ensure your sensitivity labels can be used with Microsoft 365 groups:
PowerShell

Execute-AzureAdLabelSync

upvoted 2 times

JamesM9 1 year, 7 months ago

https://docs.microsoft.com/en-us/azure/active-directory/enterprise-users/groups-assign-sensitivity-labels

According to the link above, the answer is D - EnableMIPLabels

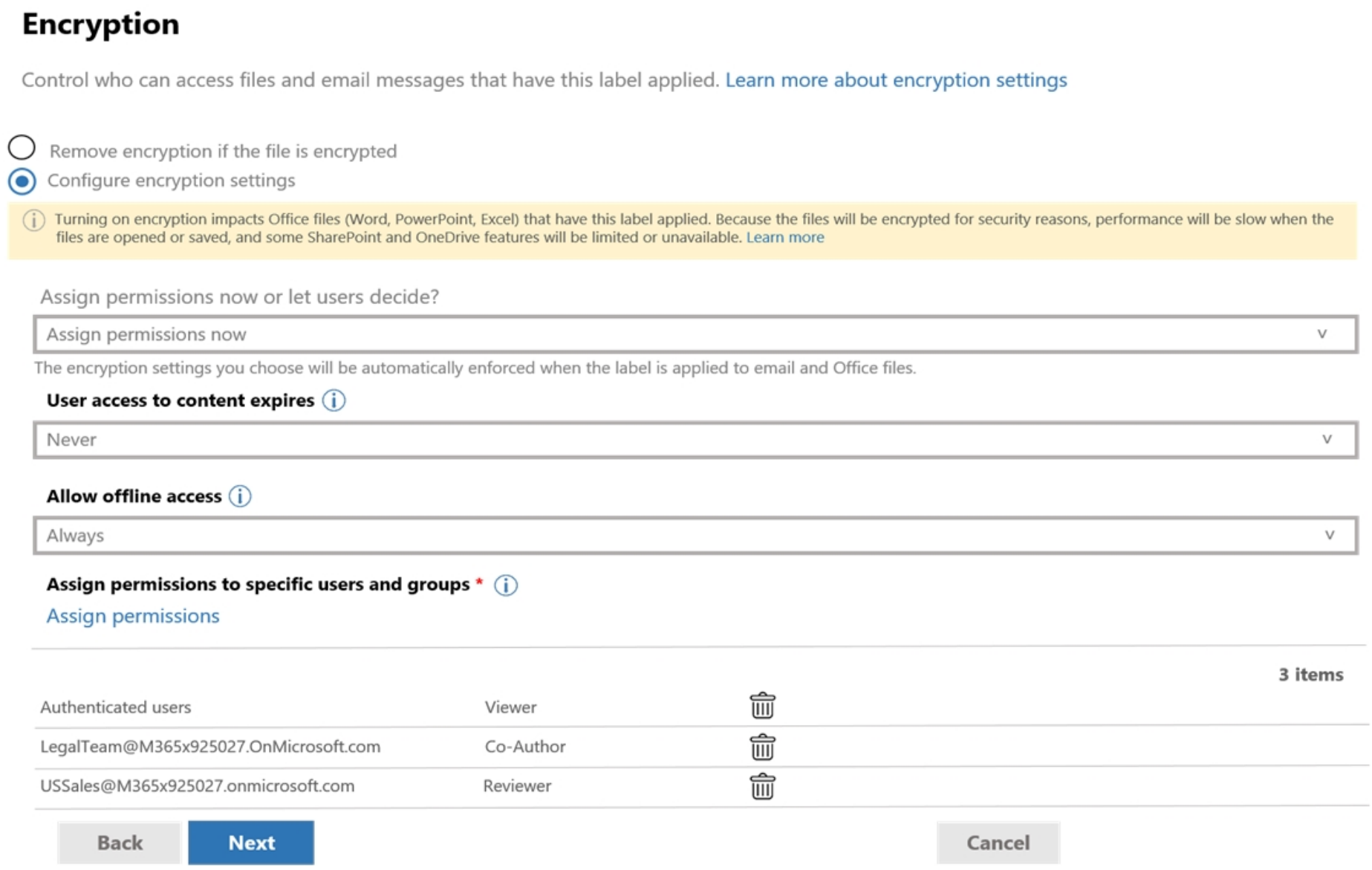
upvoted 1 times

HOTSPOT -

You have Microsoft 365 E5 tenant that has a domain name of M365x925027.onmicrosoft.com.

You have a published sensitivity label.

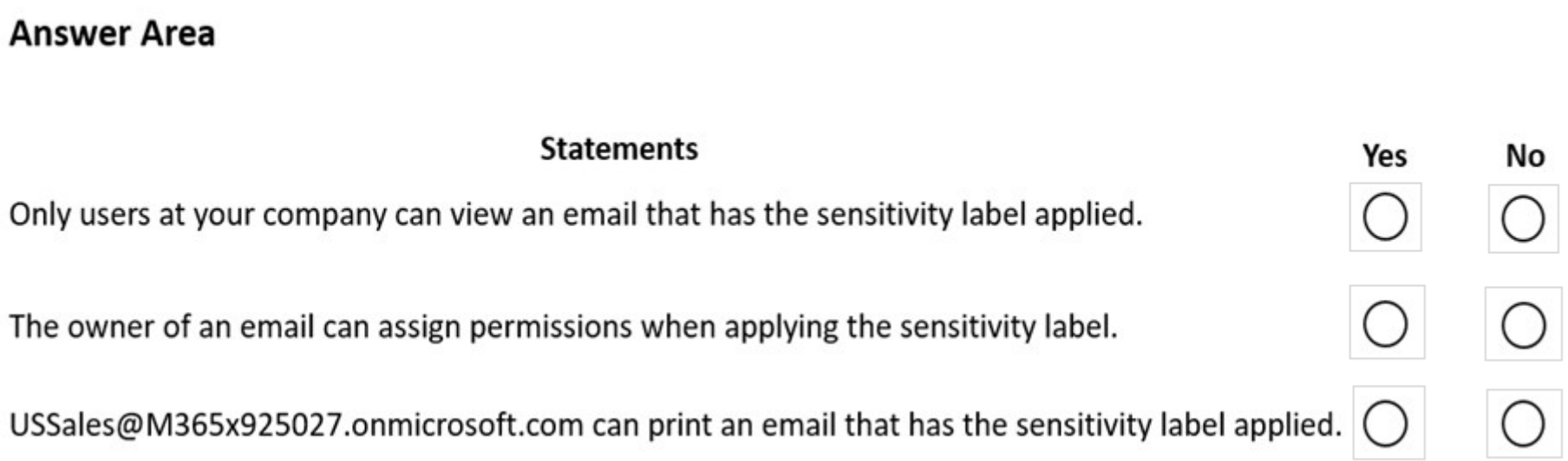
The Encryption settings for the sensitivity label are configured as shown in the exhibit.



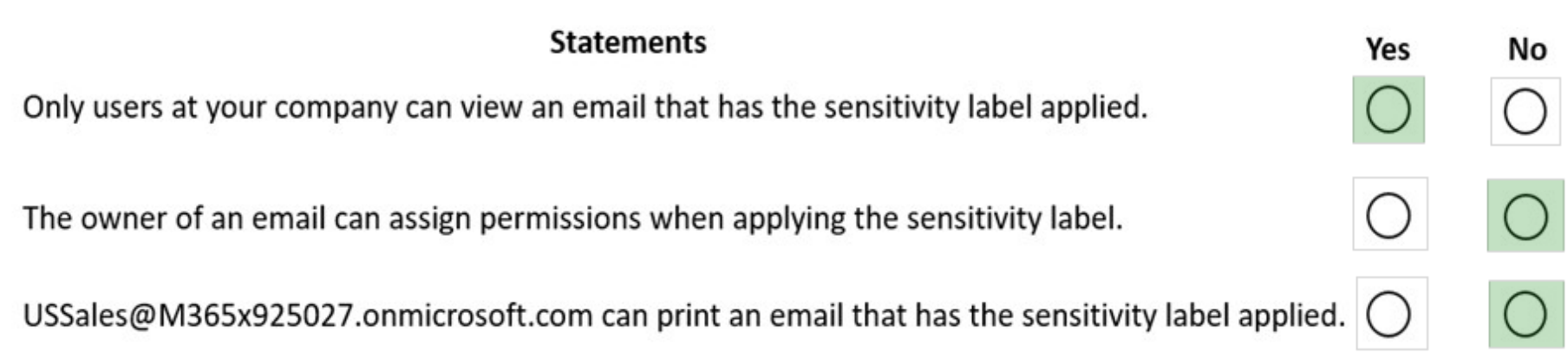
For each of the following statements, select Yes if statement is true. Otherwise, select No

NOTE: Each correct selection is worth one point.

Hot Area:



Correct Answer:

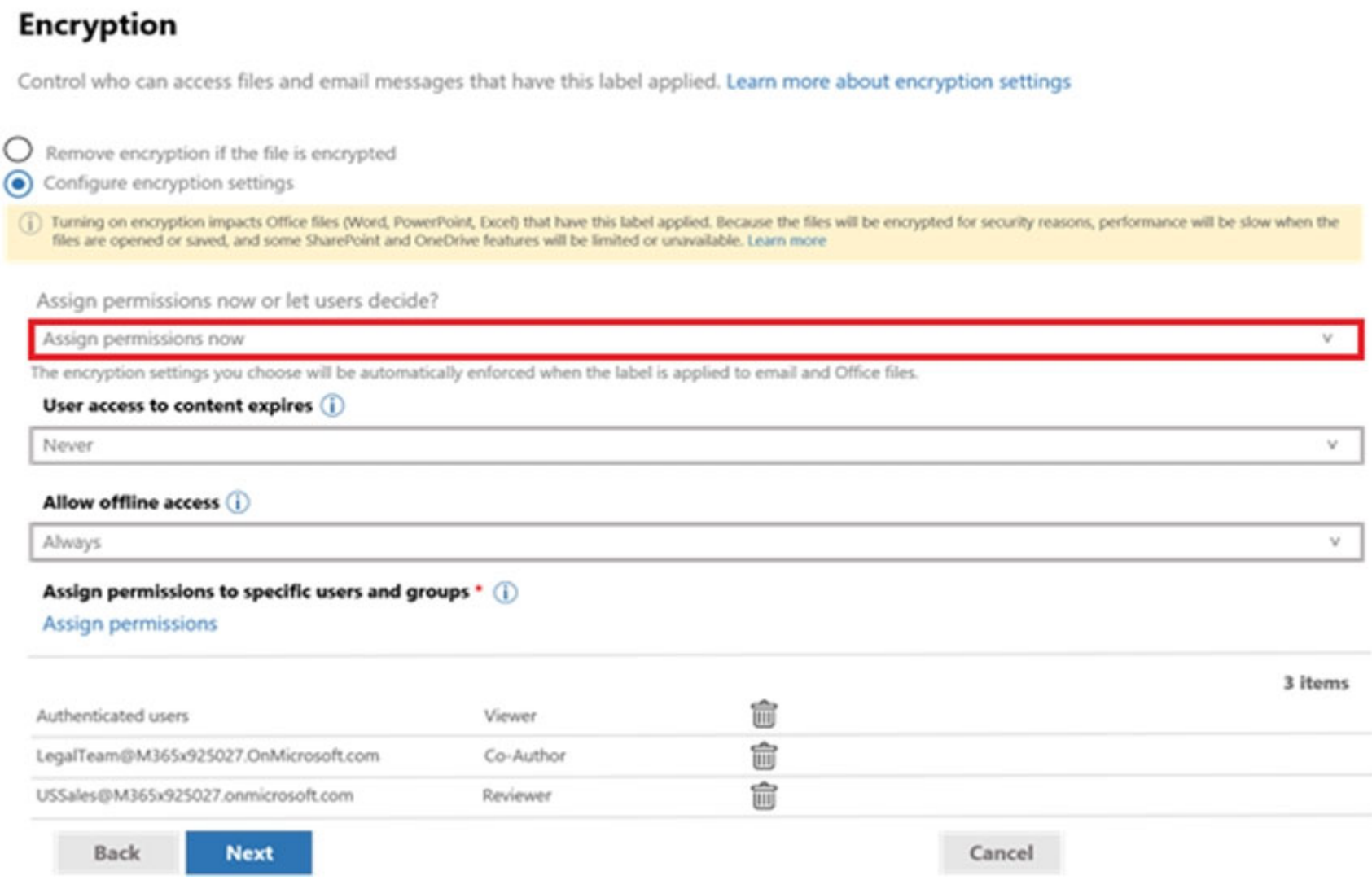


Box 1: Yes -

When you create a sensitivity label, you can restrict access to content that the label will be applied to. Only users within your organization can

open a confidential document or email.

Box 2: No -
Assign permissions now has been selected.



Box 3: No -
Only co-author and co-owner can print.
Reference:
https://docs.microsoft.com/en-us/microsoft-365/compliance/encryption-sensitivity-labels?view=o365-worldwide
https://docs.microsoft.com/en-us/azure/information-protection/configure-usage-rights

ExamReviewerIZ Highly Voted 2 years, 1 month ago
No, no, no.

If you choose to encrypt, you still need to specify who can view/read the documents, that includes your own organization.
upvoted 18 times

BTAB 1 year, 6 months ago
Yes, No, No. Authenticated Users has Viewer permissions, which will allow them to view emails based upon the policy settings
upvoted 3 times

BTAB 1 year, 6 months ago
Welp, I am wrong. I re-read the question, and as long as the authentication method is supported by external email sources like Gmail, etc... the email can be read by users outside of the organization -- "However, the application opening the encrypted content must be able to support the authentication being used. For this reason, federated social providers such as Google, and onetime passcode authentication work for email only"
https://docs.microsoft.com/en-us/microsoft-365/compliance/encryption-sensitivity-labels?view=o365-worldwide#requirements-and-limitations-for-add-any-authenticated-users
upvoted 2 times

McAlec 2 years ago
That's right. Answer is: No/No/No
"When a document or email is encrypted, access to the content is restricted, so that it:
Can be decrypted only by users authorized by the label's encryption settings...."
upvoted 9 times

Ras1364 Highly Voted 1 year, 12 months ago
I think Answer is No, no, no and for the first one, if you want all your users to view an email that has the sensitivity label applied, you should assign permissions for all users
and groups in your organization (M365x925027.onmicrosoft.com).
upvoted 11 times

Mdwro 1 year, 11 months ago
Hmm, but there is a viewer permission assigned to all authenticated users

upvoted 1 times

Ras1364 1 year, 12 months ago

Assign permissions:
Only the users or groups you choose will be assigned permissions to use the content that has this label applied.

upvoted 2 times

JCkD4Ni3L 11 months, 2 weeks ago

Exactly, otherwise how would you restrict access to sensitive content within your organisation ?

upvoted 1 times

heshmat2022 Most Recent 1 month, 1 week ago

IT WAS ON EXAM OCTOBER 18 2023

upvoted 1 times

Gesbie 3 months, 3 weeks ago

was on Exam August 9, 2023

upvoted 1 times

bhadolaa29 5 months, 1 week ago

Correct Answer No, No, Yes

Co Author permission includes print

upvoted 1 times

Sategi 4 months, 3 weeks ago

USSales us reviewer

upvoted 1 times

Jonclark 9 months ago

I went into Purview and experimented with this.. When you assign permissions for encryption within a sensitivity label, you can assign permissions to "any authenticated users" separately from "all users in your organization".

There's a tool-tip next to "any authenticated users". Here is what it says:

Includes any user who:
* Has an e-mail account that's authenticated by Azure AD or a federated social provider
* Is authenticated by a Microsoft Account
* Uses a one-time passcode for e-mail only

The tool-tip has a link to "learn more" which points to:
https://learn.microsoft.com/en-us/microsoft-365/compliance/encryption-sensitivity-labels?view=o365-worldwide

So... with "authenticated users" permissions to view, the content is encrypted, but not restricted to viewing by only members of the org.

upvoted 3 times

JCkD4Ni3L 1 year ago

No, No, No, for users to be able to view an encrypted email they MUST have explicit permission to do so. Also, for the 3rd answer Reviewer does NOT allow printing (see: https://learn.microsoft.com/en-us/azure/information-protection/configure-usage-rights#rights-included-in-permissions-levels)

upvoted 2 times

JamesM9 1 year, 7 months ago

Tricky, but at a push I am leaning towards N/N/N on the basis that it is not specified that all users can access.

The settings of the label specify that authenticated users have been assigned viewing permissions however this does not mean that it is restricted to users internally. If it was specified to all users within the domain only then this should be specified within the "add users or groups" setting.

So therefore, the answer for me is NNN.

upvoted 1 times

Pravda 1 year, 10 months ago

On exam 1/20/2022

upvoted 1 times

UWSFish 1 year, 10 months ago

I lean toward Y. N, N...yes only the users within the org that have been assigned permission will have access AND of course "A" could be more specific in that regard but is "A" true???Lean toward yes. Only users inside the org CAN view an email with the sensitivity label applied. Users outside the org can't And users inside the org CAN w/ the appropriate permissions. It's very close but Y/N/N for me. It really is an MS semantics question

upvoted 5 times

Pravda 1 year, 10 months ago

Answer is correct. Yes No No
Notice it says the setting doesn't restrict who can access the content when it comes to authenticated users.
https://docs.microsoft.com/en-us/microsoft-365/compliance/encryption-sensitivity-labels?view=o365-worldwide#requirements-and-limitations-for-add-any-authenticated-users
Requirements and limitations for "Add any authenticated users"

This setting doesn't restrict who can access the content that the label encrypts, while still encrypting the content and providing you with options to restrict how the content can be used (permissions), and accessed (expiry and offline access).

upvoted 5 times

AJ2021 1 year, 9 months ago

Read the first question again carefully and then read the link you provided. The correct answers are No, No, No

upvoted 3 times

nupagazi 1 year, 10 months ago

I think No/No/No. Authenticated users means any users from social provider or OTP can view, not users in orgnization

upvoted 7 times

HOTSPOT -

You plan to create a custom sensitive information type that will use Exact Data Match (EDM).

You need to identify what to upload to Microsoft 365, and which tool to use for the upload.

What 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

Upload:

- Data hashes
- Data in the XML format
- Digitally signed data

Use:

- Azure Storage Explorer
- EDM upload agent
- The Microsoft 365 compliance center
- The Set-DlpKeywordDictionary cmdlet

Correct Answer:

Answer Area

Upload:

- Data hashes
- Data in the XML format
- Digitally signed data

Use:

- Azure Storage Explorer
- EDM upload agent
- The Microsoft 365 compliance center
- The Set-DlpKeywordDictionary cmdlet

Reference:

https://docs.microsoft.com/en-us/microsoft-365/compliance/create-custom-sensitive-information-types-with-exact-data-match-based-classification?view=o365- worldwide

mmendozaf Highly Voted 2 years, 1 month ago

Based on - Authentication: https://docs.microsoft.com/en-us/microsoft-365/compliance/create-custom-sensitive-information-types-with-exact-data-match-based-classification?view=o365-worldwide#prerequisites I think that file to upload should be Data hashed.

upvoted 19 times

McAlec 2 years ago

You are right. Only the database schema shall be uploaded in XML format, the data should be in csv,tsv or pipe separated -> hashed data format.

The answer is: Data hashes and EDM upload agent

upvoted 15 times

sergioandreslq 1 year, 11 months ago

Correct Data hashes and EDM upload agent
Steps
1. Setup EDM-based classification
2. Hash and upload the sensitive data
3. Use EDM-based classification with your Microsoft cloud services

Hash and upload the sensitive information source table
1. set up a custom security group and user account
2. set up the EDM Upload Agent tool
3. Use the EDM Upload Agent tool to hash, with a salt value, the sensitive information source table, and upload it.
https://docs.microsoft.com/en-us/microsoft-365/compliance/sit-get-started-exact-data-match-hash-upload?view=o365-worldwide#hash-and-upload-the-sensitive-information-source-table

upvoted 6 times

ChaBum 1 year, 10 months ago
How do you hash the XML file containing the data?
I believe it's with the EDM agent...

upvoted 1 times

Holii 1 year, 6 months ago
You are going to upload both using the EDM Agent.
First upload isn't an 'upload', but is a function to return a hash value.

The question asks "What is uploaded to Microsoft 365"
In this case, it is Data hashes and EDM upload agent.

upvoted 2 times

Jonclark Highly Voted 9 months ago
This is confusing because there are two methods to uploading EDM data. a "Classic" and a "new" experience.
https://learn.microsoft.com/en-us/microsoft-365/compliance/sit-get-started-exact-data-match-based-sits-overview?view=o365-worldwide

For the CLASSIC experience: Both XML and data hashes are correct answers. This is because with the "Classic" experience, you first need to create and upload schema, which is XML format. After that you upload data hashes.

For the NEW experience, the correct answer would be "data hashes" because there is no longer a separate step to create the schema -- it's embedded into the data hashes when uploaded.

Both experiences are available today, so I have to agree with the folks in this discussion saying "both are correct" and hope I don't face this question on the exam....

upvoted 6 times

heshmat2022 Most Recent 1 month, 1 week ago
The default format for the sensitive data file is comma-separated values. You can specify a tab-separated file by indicating the "{Tab}" option with the /ColumnSeparator parameter, or you can specify a pipe-separated file by indicating the "|" option.

Example: EdmUploadAgent.exe /UploadData /DataStoreName PatientRecords /DataFile C:\Edm\Hash\PatientRecords.csv /HashLocation C:\Edm\Hash /Schema edm.xml /AllowedBadLinesPercentage 5

upvoted 1 times

NinjaSchoolProfessor 11 months, 1 week ago
Answer [Data hashes] and [EDM Upload Agent].

EDM Upload Agent creates hashes for your SITs and saves them in the .CSV format. However you can also upload .csv, .tsv or pipe (|) formatted files. It also saves schema in XML format.

upvoted 4 times

Harry008 1 year ago
Because the schema and primary and secondary data values are highly sensitive, you'll be encrypting them via a hash function that includes a randomly generated or self-supplied salt value. Only the hashed values are uploaded to the service, so your sensitive data is never in the open.
The schema is an xml file.
Answer hashed data format and EDM upload agent

upvoted 2 times

wooyourdaddy 1 year, 5 months ago
I wrote the exam today, this question was on it, I choose Box1: Date in the XML format, Box2: EDM upload agent, scored 890!

upvoted 1 times

Srd 8 months ago
This is a spam bot. Same answer under most questions.

upvoted 3 times

JCkD4Ni3L 11 months, 2 weeks ago
Blindly using answers here is not a good idea, you should research and leverage Microsoft documentations to actually learn something. :/

upvoted 3 times

dostras 1 year, 12 months ago
Both are correct:
https://docs.microsoft.com/en-us/microsoft-365/compliance/sit-get-started-exact-data-match-hash-upload?view=o365-worldwide

upvoted 2 times

Bongconnection 2 years, 1 month ago

Both are correct:
https://docs.microsoft.com/en-us/microsoft-365/compliance/create-custom-sensitive-information-types-with-exact-data-match-based-classification?view=o365-worldwide&viewFallbackFrom=o365-%20worldwide

upvoted 3 times

Juancho 2 years, 1 month ago

UPLOAD: Set up EDM-based classification require Database schema in XML format.
USE: EDM upload agent. To upload the sensitive data, the Local admin access to machine with EDM Upload Agent.

upvoted 2 times

JeromeE 1 year, 6 months ago

The sensitive data should be uploaded only in hashed values. The schema xml should not contain any of the sensitive data, only parameters for where the data is stored in the EDM DB.

upvoted 2 times

Question #25 *Topic 1*

DRAG DROP -

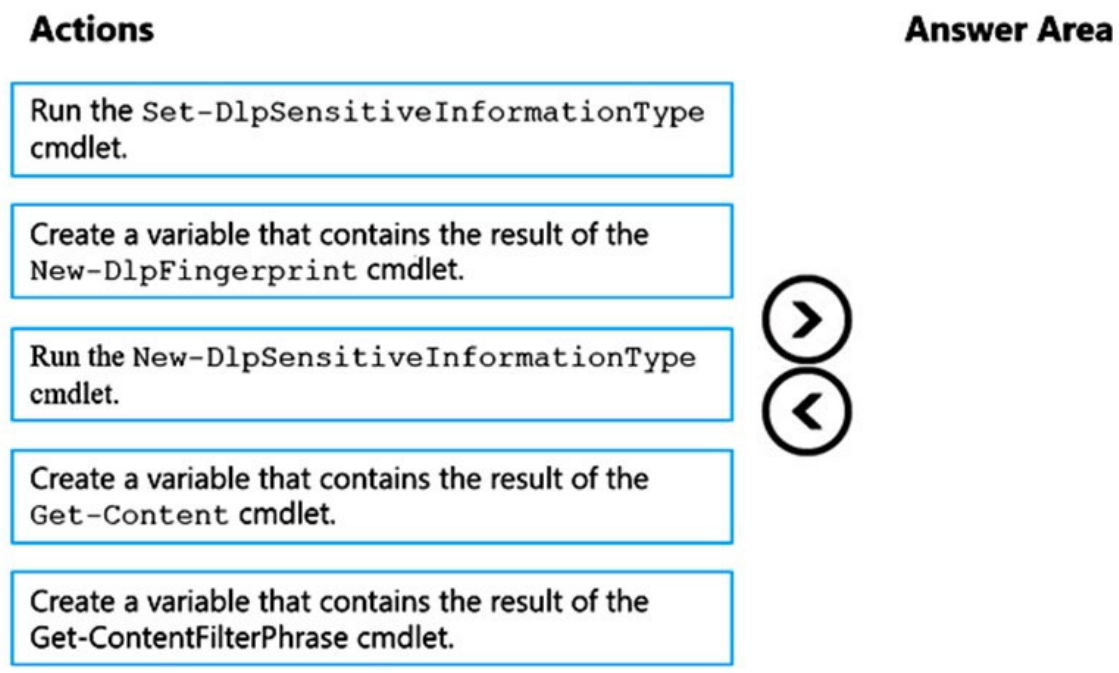
You have a Microsoft 365 tenant that uses data loss prevention (DLP).

You have a custom employee information form named Template1.docx.

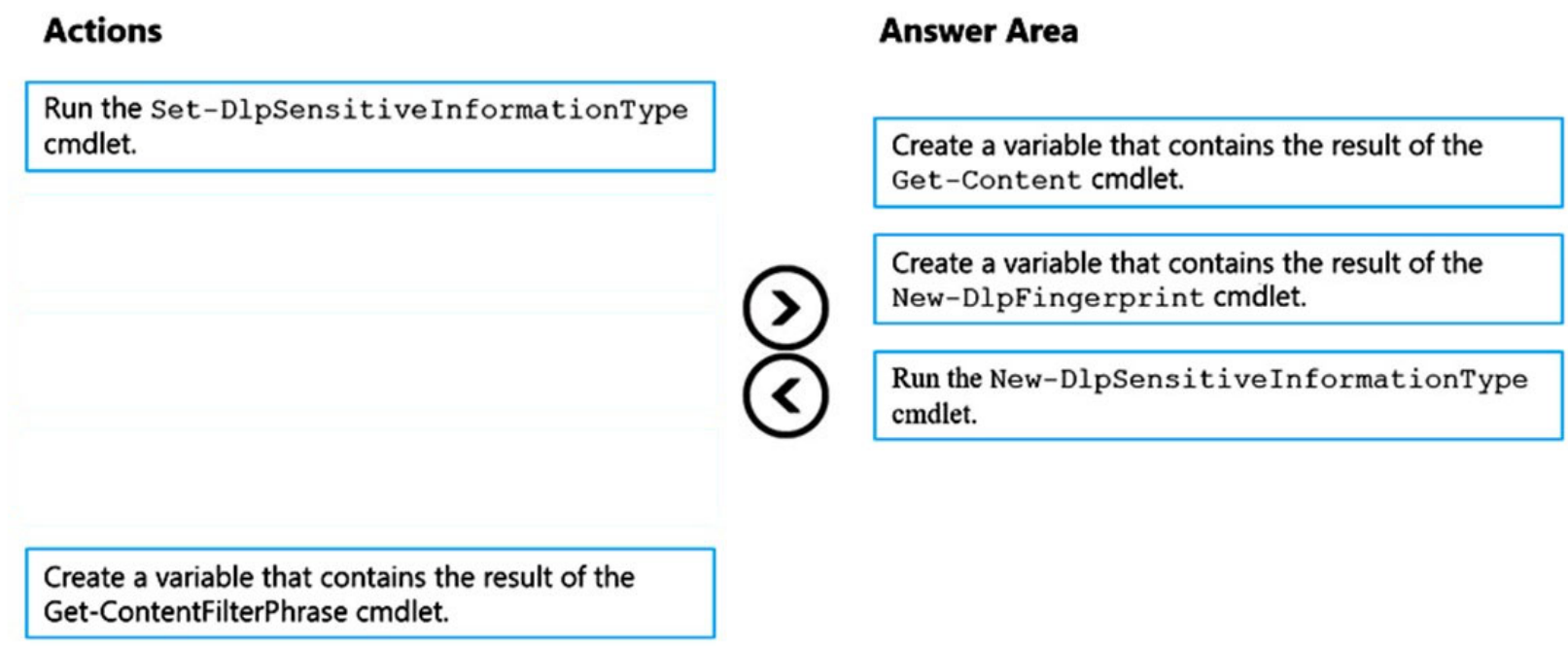
You need to create a classification rule package based on the document fingerprint of Template1.docx.

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.

Select and Place:



Correct Answer:



Reference:

https://docs.microsoft.com/en-us/microsoft-365/compliance/document-fingerprinting?view=o365-worldwide

kochunnee Highly Voted 2 years, 1 month ago

Answer is correct

$Customer_Form = Get-Content "C:\My Documents\Contoso Customer Information Form.docx" -Encoding byte -ReadCount 0
$Customer_Fingerprint = New-DlpFingerprint -FileData $Customer_Form -Description "Contoso Customer Information Form"
New-DlpSensitiveInformationType -Name "Contoso Customer Confidential" -Fingerprints $Customer_Fingerprint -Description "Message contains Contoso customer information."

upvoted 13 times

sergioandreslq 1 year, 11 months ago

Agreed, reviewed on the web site

upvoted 1 times

Jonclark Highly Voted 9 months ago

NOTE: Microsoft has changed the step-by-step instructions for setting this up since the older comments in this discussion. Follow the same link @PrettyFlyWifi posted below and you'll see that Microsoft has stopped using the Get-Content cmdlet.

Instead of:
$Customer_Form = Get-Content "C:\My Documents\Contoso Customer Information Form.docs" -Encoding Byte -ReadCount 0

Now it is:
$Customer_Form = ([System.IO.File]::ReadAllBytes('C:\My Documents\Contoso Customer Information Form.docx'))

Both of these commands do the same thing, but the latter is faster and more efficient. You should probably be ready for either version to be on the test.

upvoted 8 times

PrettyFlyWifi Most Recent 1 year, 11 months ago

Looks correct order, judging by the order of the PowerShell example in https://docs.microsoft.com/en-us/powershell/module/exchange/new-dlpsensitiveinformationtype?view=exchange-ps#examples

upvoted 3 times

Question #26 *Topic 1*

Your company has a Microsoft 365 tenant that uses a domain named contoso.com.
The company uses Microsoft Office 365 Message Encryption (OME) to encrypt email sent to users in fabrikam.com.
A user named User1 erroneously sends an email to user2@fabrikam.com.
You need to prevent user2@fabrikam.com from accessing the email.
What should you do?

A. Run the Get-MessageTrace cmdlet.

B. Run the Set-OMEMessageRevocation cmdlet.

C. Instruct User1 to delete the email from her Sent Items folder from Microsoft Outlook.

D. Run the New-ComplianceSearchAction cmdlet.

E. Instruct User1 to select Remove external access from Microsoft Outlook on the web.

Correct Answer: *A*

Community vote distribution

B (86%) 14%

researched_answer_boi Highly Voted 2 years ago
As this is a single choice question, based on
https://docs.microsoft.com/en-us/microsoft-365/compliance/revoke-ome-encrypted-mail?view=o365-worldwide#how-to-revoke-an-encrypted-message-as-an-administrator
A is the first step to perform.
upvoted 16 times

Pravda Highly Voted 1 year, 10 months ago
Terrible question.
B would be correct.
https://docs.microsoft.com/en-us/microsoft-365/compliance/revoke-ome-encrypted-mail?view=o365-worldwide#how-to-revoke-an-encrypted-message-as-an-administrator
Get the Message ID of the email.
Verify that you can revoke the message.
Revoke the mail.
It's not asking what to do first, but prevent user from accessing the email.
A is the first step, but doesn't prevent user from accessing.
B revokes the message.
C is what the user, not what you would do.
D is about compliance
E is user, not admin.
upvoted 11 times

heshmat2022 Most Recent 1 month, 1 week ago
IN EXAM OCTOBER 18TH 2023
upvoted 3 times

Mpho_S 5 months ago
The correct answer is B. Run the Set-OMEMessageRevocation cmdlet.

To prevent user2@fabrikam.com from accessing the email that was mistakenly sent by User1, you can use the Set-OMEMessageRevocation cmdlet. This cmdlet is used to revoke access to encrypted messages sent with Office 365 Message Encryption (OME).

By running the Set-OMEMessageRevocation cmdlet, you can specify the recipient's email address (user2@fabrikam.com) and revoke their access to the email. This will prevent them from being able to open or view the encrypted email.

Please note that this solution assumes you have administrative access to the Microsoft 365 tenant and the necessary permissions to run the cmdlet.
upvoted 5 times

xswe 7 months, 3 weeks ago
Verify first if the email is revocable with
Get-OMEMessageStatus -MessageId "<message id>" | ft -a Subject, IsRevocable
Then revoke the message with
Set-OMEMessageRevocation -Revoke $true -MessageId "<messageId>"
Check the revocation with Get-OMEMessageStatus again
Get-OMEMessageStatus -MessageId "<messageId>" | ft -a Subject, Revoked
upvoted 3 times

NinjaSchoolProfessor 11 months, 1 week ago

Answer is Set-OMEMessageRevocation - However you should note that you can revoke encrypted messages if the recipient received a link-based, branded encrypted email message. If the recipient received a native inline experience in a supported O365/M365/Outlook client, then you can't revoke encryption for the message. https://learn.microsoft.com/en-us/powershell/module/exchange/set-omemessagerevocation?view=exchange-ps

upvoted 4 times

GGFiogos 1 year, 2 months ago

Isnt B supposed to be for Advanced OME? First action should be A

upvoted 1 times

Lion007 1 year, 3 months ago

Selected Answer: A

A is the Correct answer. MessageTrace is required to get the Message ID, as explained in the first step:

Step 1. Obtain the Message ID of the email
identify the Message ID of the email you want to revoke by using "Message Trace".

Step 2. Verify that the mail is revocable
Get-OMEMessageStatus -MessageId "<message id>" | ft -a Subject, IsRevocable

Step 3. Revoke the mail
Set-OMEMessageRevocation -Revoke $true -MessageId "<messageId>"

To check whether the email was revoked, run the Get-OMEMessageStatus cmdlet as follows:
Get-OMEMessageStatus -MessageId "<messageId>" | ft -a Subject, Revoked

Ref: https://docs.microsoft.com/en-us/microsoft-365/compliance/revoke-ome-encrypted-mail?view=o365-worldwide#to-identify-the-message-id-of-the-email-you-want-to-revoke-by-using-message-trace-in-the-security--compliance-center

upvoted 1 times

wooyourdaddy 1 year, 5 months ago

Selected Answer: B

I wrote the exam today, this question was on it, I choose B, scored 890!

upvoted 1 times

sunilkms 1 year, 7 months ago

Selected Answer: B

Set-OMEMessageRevocation

upvoted 2 times

JamesM9 1 year, 7 months ago

Looking into this further, my instinct would be to run the get-messagetrace cmdlet first. However, doing this would not stop the user from accessing the email.

The question specfically states that YOU need to prevent user2 from accessing the email.

As a result of this, we are left with B or E as running the get-messagetrace cmdlet wouldnt actually prevent user2 from accessing the email.

E would work, however the question asks YOU to prevent user2 from accessing the email.

As a result of what is being asked for here the answer is to run the set-OMEMessageRevocation cmdlet.

"Use the Set-OMEMessageRevocation cmdlet to revoke Microsoft 365 Message Encryption (OME) for a message. Revoking encryption prevents the recipient from viewing the message in the Office 365 Message Encryption portal".

https://docs.microsoft.com/en-us/powershell/module/exchange/set-omemessagerevocation?view=exchange-ps

Therefore, the answer is B - run the Set-OMEMessageRevocation cmdlet.

upvoted 5 times

flashflo 1 year, 10 months ago

Selected Answer: B

The actual revocation is done with Set-OMEMessageRevocation cmdlet. If someone asks me, can I revokate a message, my answer would be yes, by Set-OMEMessageRevocation...

upvoted 3 times

Pravda 1 year, 10 months ago

On exam 1/20/2022

upvoted 1 times

Pravda 1 year, 10 months ago

Question reads YOU need to prevent user2@fabrikam.com from accessing the email.
E not correct, but would be IF you were telling the user how to do it.
A is the correct answer. You need to get information about the message before you can delete using PS command in B.

upvoted 2 times

ya12 1 year, 11 months ago

new-compliancesearchaction -Purge
The Purge switch specifies the action for the content search is to remove items that match the search criteria. You don't need to specify a value with this switch.
https://docs.microsoft.com/en-us/powershell/module/exchange/new-compliancesearchaction?view=exchange-ps
upvoted 1 times

Sam12 1 year, 10 months ago
this only works for content that exists inside your organizations. in this case, you want to revoke the email for just one external recipient.
upvoted 1 times

PrettyFlyWifi 1 year, 11 months ago
I would say this is E, because simply doing Get-MessageTrace does NOT prevent the recipient from accessing the email. This is one part answer, not asking you what you should do first, so it must be E. "If the mail is revocable, you'll see the "Remove external access" link at the top of the message." If you read https://docs.microsoft.com/en-us/microsoft-365/compliance/revoke-ome-encrypted-mail?view=o365-worldwide#how-to-revoke-an-encrypted-message-that-you-sent . This would prevent the email from being read in one move. E is correct in my eyes.
upvoted 5 times

IAGirl 1 year, 8 months ago
I agree
upvoted 2 times

sergioandreslq 1 year, 11 months ago
For me, correct is E:
Reason:
In Outlook on the web, in your Sent folder, browse to the message you want to revoke.
If the mail is revocable, you'll see the "Remove external access" link at the top of the message.
Click Remove external access to revoke the message.
The message shows that its status is revoked.
https://docs.microsoft.com/en-us/microsoft-365/compliance/revoke-ome-encrypted-mail?view=o365-worldwide#how-to-revoke-an-encrypted-message-that-you-sent
upvoted 3 times

sergioandreslq 1 year, 11 months ago
The others are more complicated as you need to get the messageID then, powershell to check if the message is revocable, and then, run the command:
Set-OMEMessageRevocation -Revoke $true -MessageId "<messageId>"
I believe option "E" is easier for admins and end-user
upvoted 2 times

Question #27 *Topic 1*

You have a Microsoft 365 tenant.
You discover that email does NOT use Microsoft Office 365 Message Encryption (OME).
You need to ensure that OME can be applied to email.
What should you do first?

A. Enable Microsoft Defender for Office 365.

B. Activate Azure Information Protection.

C. Activate Azure Rights Management (Azure RMS).

D. Create an Azure key vault.

Correct Answer: *C*
Reference:
https://docs.microsoft.com/en-us/microsoft-365/compliance/set-up-new-message-encryption-capabilities?view=o365-worldwide

Juancho Highly Voted 2 years ago
Good, The only prerequisite for using the new OME capabilities is that Azure Rights Management must be activated in your organization's tenant. If it is, Microsoft 365 activates the new OME capabilities automatically and you don't need to do anything.
upvoted 12 times

sergioandreslq 1 year, 11 months ago
Any Microsoft 365 tenant should be activated to use Azure RMS and IRM capabilities by default. To determine, if Azure RMS was deactivated for your tenant, run the following PowerShell cmdlets:
1. Run the following cmdlet to validate IRM configuration of a tenant:
Get-IRMConfiguration | fl AzureRMSLicensingEnabled
2. If the AzureRMSLicensingEnabled parameter is set to $False, activate OME for your tenant by using the following cmdlet:
Set-IRMConfiguration -AzureRMSLicensingEnabled:$True
upvoted 4 times

xswe Most Recent 7 months, 3 weeks ago
Azure RMS are needed for OME
upvoted 1 times

NinjaSchoolProfessor 11 months, 1 week ago
Correct but only if your subscription that includes Azure Rights Management or Azure Information Protection was obtained towards the end of February 2018 or later. All newer tenants have this enabled automatically.
upvoted 3 times

CEAUSESCU247 1 year, 4 months ago
Activate Azure Rights Management (Azure RMS).
upvoted 2 times

Pravda 1 year, 10 months ago
On exam 1/20/2022
upvoted 1 times

klosedotorg83 2 years, 1 month ago
Correct
upvoted 1 times

Question #28 *Topic 1*

HOTSPOT -

You plan to implement a sensitive information type based on a trainable classifier. The sensitive information type will identify employment contracts.

You need to copy the required files to Microsoft SharePoint Online folders to train the classifier.

What should you use to seed content and test the classifier? To answer, select the appropriate options in the answer area.

NOTE: Each correct selection is worth one point.

Hot Area:

Answer Area

Seed content:

- Only files that are poor examples of employment contracts
- Only files that are good examples of employment contracts
- Files that are a mix of good and poor examples of employment contracts
- A file that contains the metadata of the employment contracts in the CSV format
- A file that contains the metadata of the employment contracts in the JSON format

Testing the classifier:

- Only files that are poor examples of employment contracts
- Only files that are good examples of employment contracts
- Files that are a mix of good and poor examples of employment contracts
- A file that contains the metadata of the employment contracts in the CSV format
- A file that contains the metadata of the employment contracts in the JSON format

Correct Answer:

Answer Area

Seed content:

- Only files that are poor examples of employment contracts
- Only files that are good examples of employment contracts
- Files that are a mix of good and poor examples of employment contracts
- A file that contains the metadata of the employment contracts in the CSV format
- A file that contains the metadata of the employment contracts in the JSON format

Testing the classifier:

- Only files that are poor examples of employment contracts
- Only files that are good examples of employment contracts
- Files that are a mix of good and poor examples of employment contracts
- A file that contains the metadata of the employment contracts in the CSV format
- A file that contains the metadata of the employment contracts in the JSON format

Reference:

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

xswe Highly Voted 7 months, 3 weeks ago

You want to seed with only good documents to train your trainable classifier correctly so that it knows what to look for.
When you test it you want both good and bad examples to know if it can detect both false and true positives.

upvoted 6 times

kochunnee Highly Voted 2 years, 1 month ago

Correct Answer

Seeds

Make sure the items in your seed set are strong examples of the category. The trainable classifier initially builds its model based on what you seed it with. The classifier assumes all seed samples are strong positives and has no way of knowing if a sample is a weak or negative match to the category.

Testing content
Collect at least 200 test content items (10,000 max) for best results. These should be a mix of items that are strong positives, strong negatives and some that are a little less obvious in their nature. See, Default crawled file name extensions and parsed file types in SharePoint Server for the supported file types.
upvoted 5 times

Pravda Most Recent 1 year, 10 months ago
On exam 1/20/2022
upvoted 1 times

Ali_557 1 year, 11 months ago
In Seed content why its not the 3rd option?
upvoted 2 times

Dreamhaxx 1 year, 10 months ago
With Seed content you are helping the classifier with positive matches, atleast to my knowledge. Aswer is correct.
upvoted 2 times

Ali_557 1 year, 11 months ago
Collect at least 200 test content items (10,000 max) for best results. These should be a mix of items that are strong positives, strong negatives and some that are a little less obvious in their nature. See, Default crawled file name extensions and parsed file types in SharePoint Server for the supported file types.

From <https://docs.microsoft.com/en-us/microsoft-365/compliance/classifier-get-started-with?view=o365-worldwide>
upvoted 1 times

PrettyFlyWifi 1 year, 11 months ago
Looks correct as per https://docs.microsoft.com/en-us/microsoft-365/compliance/classifier-get-started-with?view=o365-worldwide
upvoted 1 times

HOTSPOT -

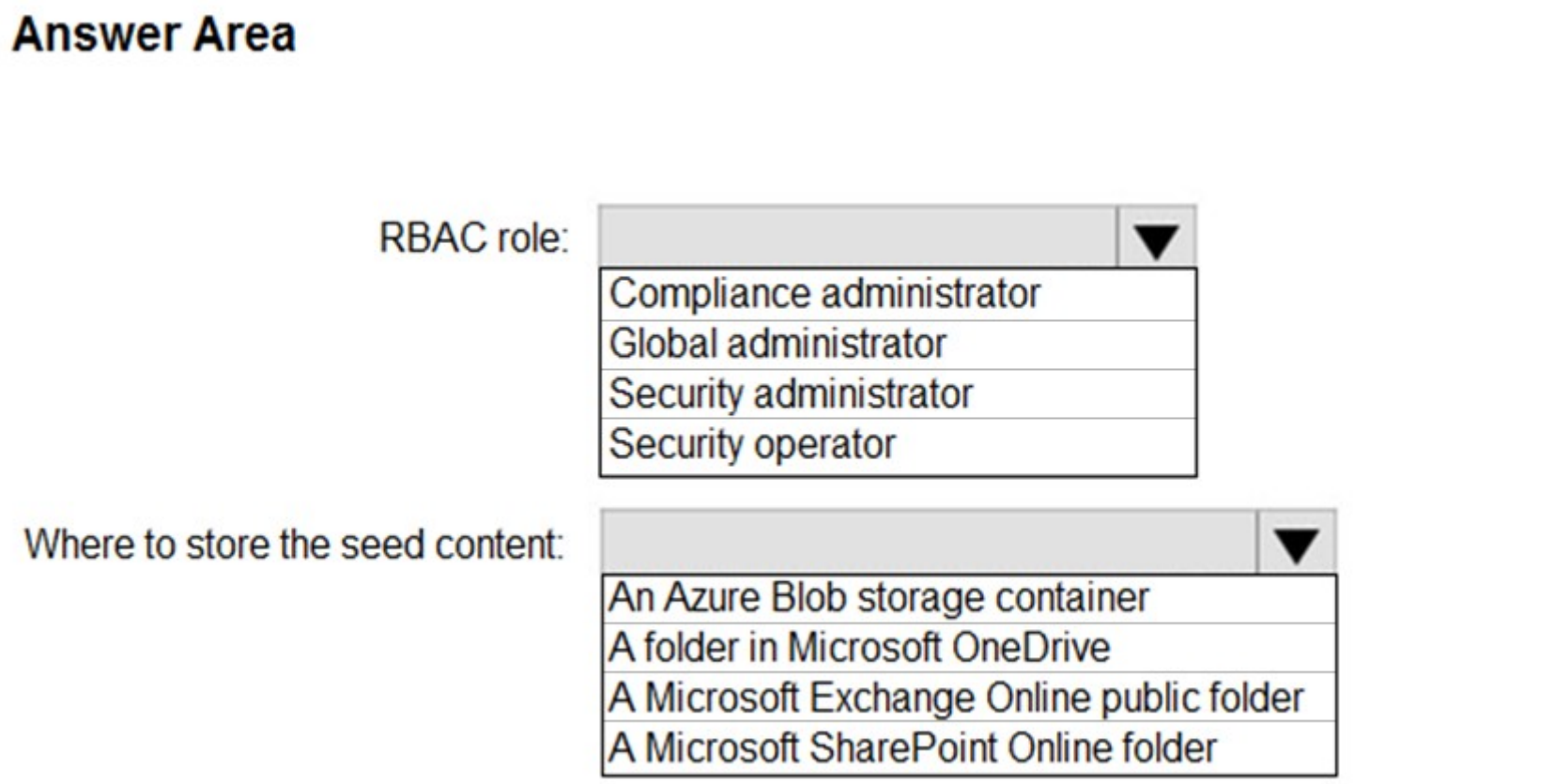
You plan to create a custom trainable classifier based on an organizational from template.

You need to identify which role-based access control (RBAC) role is required to create the trainable classifier and where to store the seed content for the trainable classifier. The solution must use the principle of least privilege.

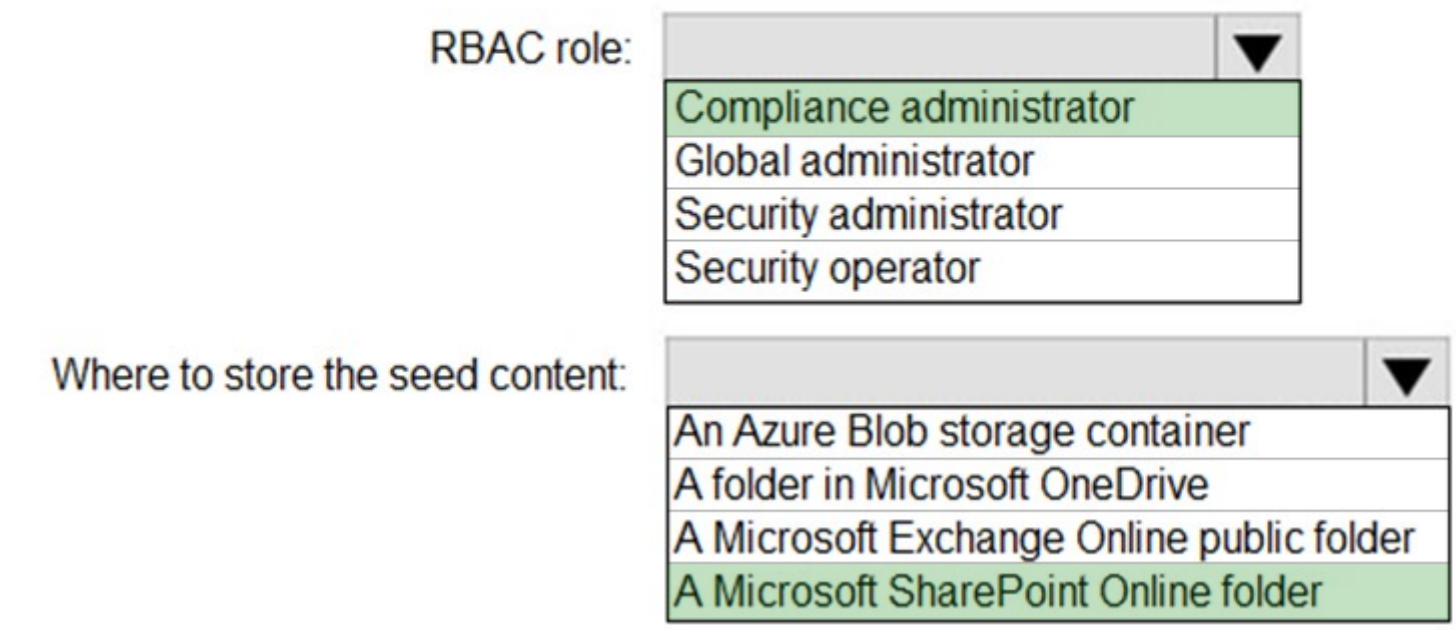
What should you identify? To answer, select the appropriate options in the answer area.

NOTE: Each correct selection is worth one point.

Hot Area:



Correct Answer:



Reference:

https://docs.microsoft.com/en-us/microsoft-365/compliance/classifier-get-started-with?view=o365-worldwide#prepare-for-a-custom-trainable-classifier

UWSFish Highly Voted 1 year, 10 months ago

I really think reading the question in it's entirety in this this question they are assuming that trainable classifiers have already been enabled. The context is much different from this "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?"
I go with A Compliance Admin

upvoted 10 times

NinjaSchoolProfessor Highly Voted 11 months, 1 week ago

o Global admin: required to enable trainable classifier capability in the tenant
o Compliance admin: required to use and train a trainable classifier

upvoted 7 times

ehommes Most Recent 5 days, 16 hours ago

Should it not be Security Admin?

Check this out: https://learn.microsoft.com/en-us/purview/classifier-get-started-with?view=o365-worldwide#prepare-for-a-custom-trainable-classifier

3. Sign in to the Microsoft Purview compliance portal with either Compliance admin or Security admin role access and navigate to Data classification > Classifiers.

4. Choose the Trainable classifiers tab.

5. Choose Create trainable classifier.

upvoted 1 times

xswe 7 months, 3 weeks ago

A bit tricky but as they ask for least privileges I'll go for Compliance administrator.
You have to store the seed content at SharePoint Online.

upvoted 3 times

Pravda 1 year, 10 months ago

On exam 1/20/2022

upvoted 4 times

Ali_557 1 year, 11 months ago

ermissions

To access classifiers in the UI:

the Global admin needs to opt in for the tenant to create custom classifiers.
Compliance Administrator role is required to train a classifier.

You'll need accounts with these permissions to use classifiers in these scenarios:

Retention label policy scenario: Record Management and Retention Management roles
Sensitivity label policy scenario: Security Administrator, Compliance Administrator, Compliance Data Administrator
Communication compliance policy scenario: Insider Risk Management Admin, Supervisory Review Administrator

upvoted 1 times

PrettyFlyWifi 1 year, 11 months ago

A global admin is needed to opt-in so trainable classifiers can be created and then a Compliance admin can train them. This one of those ambiguous questions, but as they are asking about least privilege, I'd say they want you to choose Compliance admin.
https://docs.microsoft.com/en-us/microsoft-365/compliance/classifier-get-started-with?view=o365-worldwide#permissions

upvoted 3 times

bingomutant 1 year, 11 months ago

the documentation refers to Sharepoint online folder there is no mention of public folder. Everybody note that for RBAC answer is always least privilege and Global Admin only required to opt-in for creation if first time doing trainable classifiers - as the question does not state this is the first time the tenant is creating a TC the compliance admin can create it.

upvoted 2 times

bingomutant 1 year, 11 months ago

compliance admin can definitely create a trainable classifier as can a security admin -says so in documentation - compliance admin is least privilege

upvoted 2 times

[Removed] 2 years ago

Wrong, only a global administrator van create a treinable classifier. Compliance admin can only train It.

upvoted 1 times

MahmoudEldeep 2 years ago

Tested, Compliance administrator can also create trainable classifier.

upvoted 7 times

Mdwro 1 year, 10 months ago

Global Admin is required to enable capability for trainable classifiers creation.
Compliance Admin can create the classifiers.
Here, Compliance admin is required, as question says about creation.

upvoted 1 times

Question #30 *Topic 1*

You have a Microsoft 365 tenant.
You create the following:
- A sensitivity label
- An auto-labeling policy

You need to ensure that the sensitivity label is applied to all the data discovered by the auto-labeling policy.
What should you do first?

A. Enable insider risk management.

B. Create a trainable classifier.

C. Run the Enable-TransportRule cmdlet.

D. Run the policy in simulation mode.

Correct Answer: *D*
Reference:
https://docs.microsoft.com/en-us/microsoft-365/compliance/apply-sensitivity-label-automatically?view=o365-worldwide

Community vote distribution

D (100%)

Pravda Highly Voted 1 year, 10 months ago
D - Here's why from the link given.
You can't automatically label documents and emails until your policy has run at least one simulation.
upvoted 10 times

oberte007 Highly Voted 2 years, 1 month ago
Yes! right! Simulation mode allows you to test the policy's efficiency and to make some adjustments as necessary
upvoted 5 times

sergioandreslq 1 year, 11 months ago
agreed, the question doesn't specify any other case for service-side auto-labeling, It is just, creates the label, Create the service-side auto-labeling policy, run in simulation, then, based on results you can tune-up the policy or turn on the policy to begin applying automatic label based on the rule.
upvoted 3 times

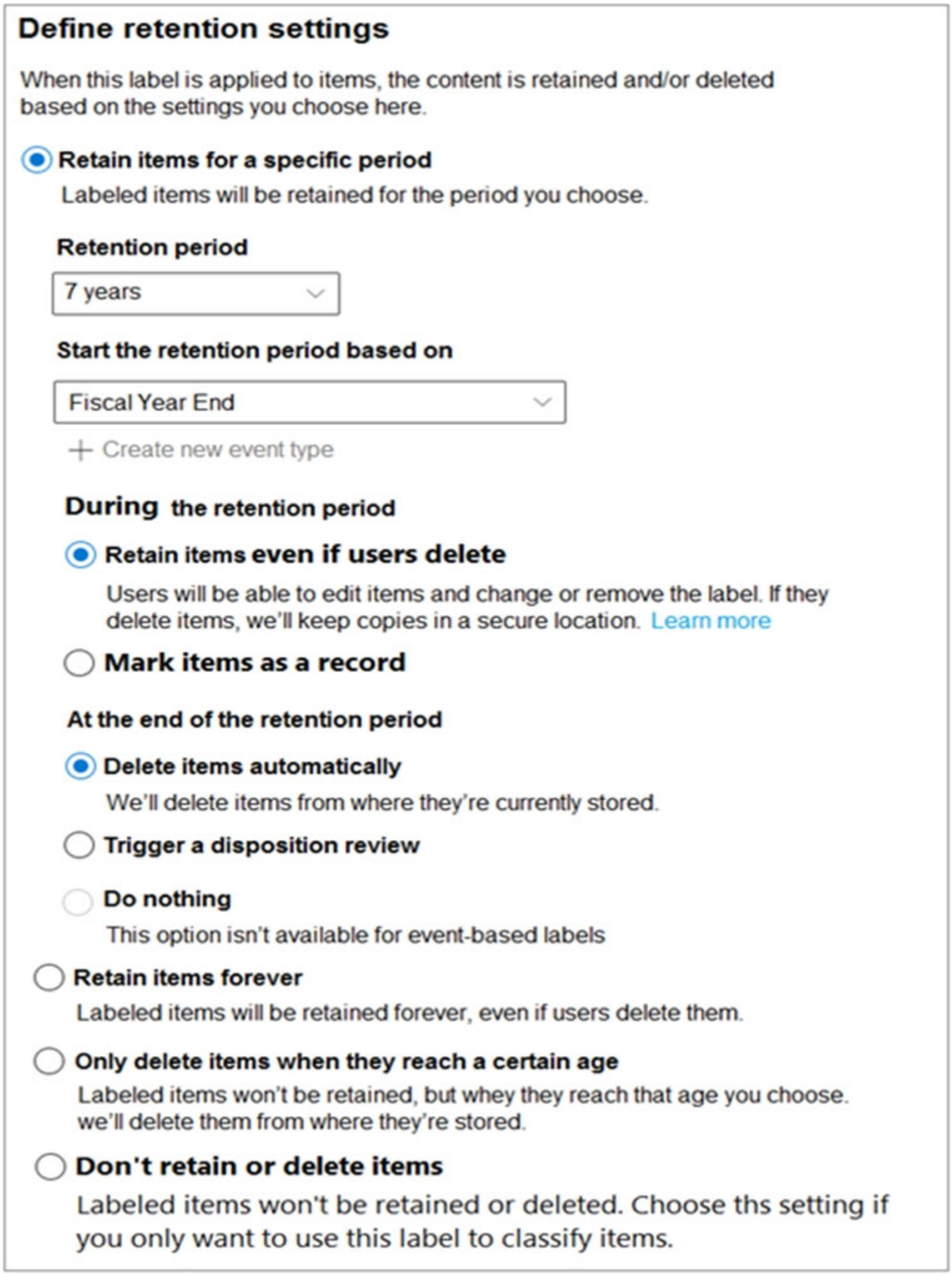
xswe Most Recent 7 months, 3 weeks ago
Best practice according to MS is the always test it out, trust me you dont want to deploy these and DLP policys in your enivornment without testing them out.
Correct answer "run policy in simulation mode"
upvoted 1 times

chrissempai 1 year, 2 months ago
Selected Answer: D
It needs to be an auto label
upvoted 2 times

Pravda 1 year, 10 months ago
On exam 1/20/2022
upvoted 1 times

HOTSPOT -

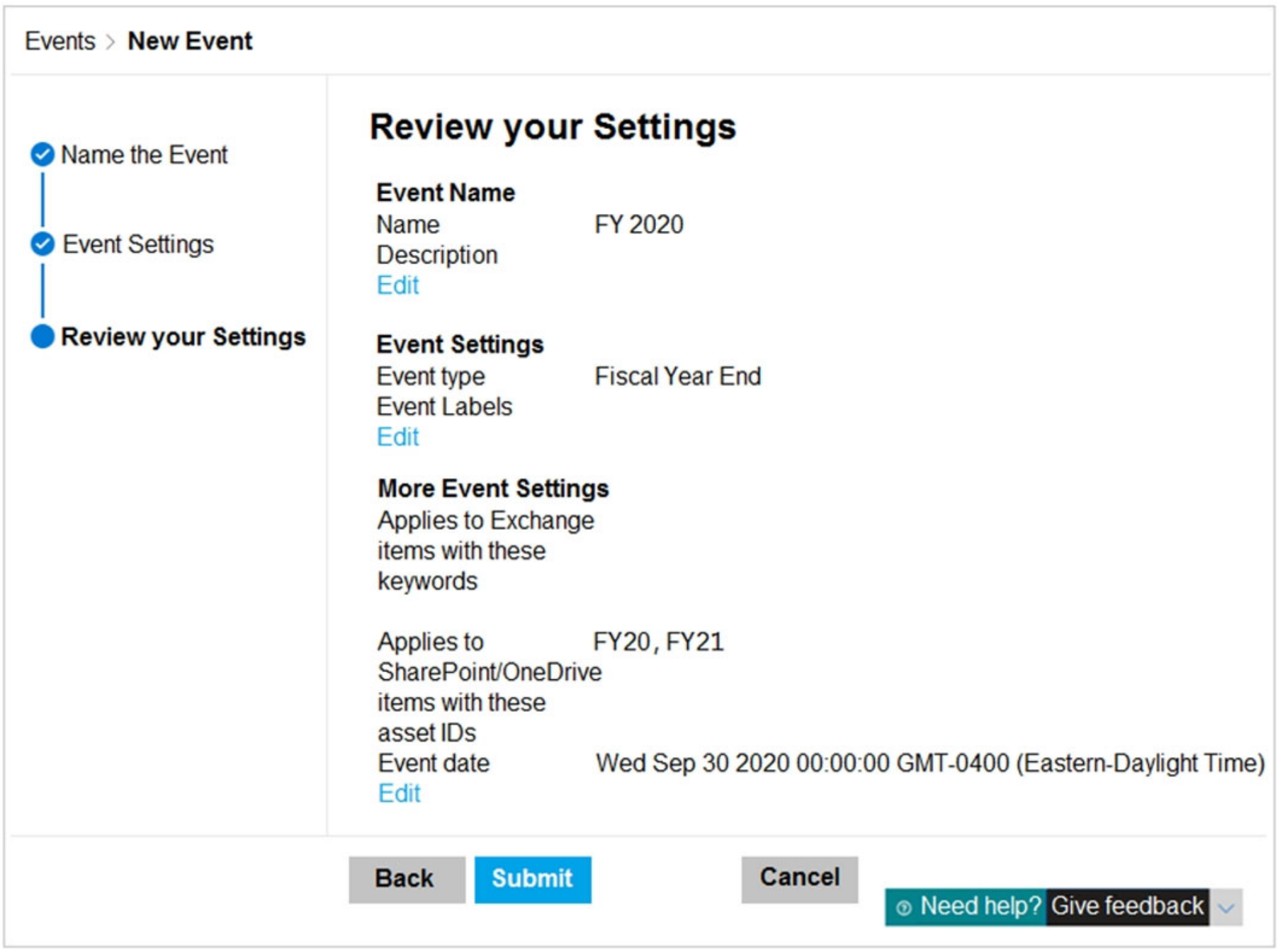
You have the retention label policy shown in the Policy exhibit. (Click the Policy tab.)



Users apply the retention label policy to files and set the asset ID as shown in the following table.

File name	Creation date	Asset ID
Doc1.docx	September 1, 2020	FY20
Doc2.docx	September 20, 2020	FY20
Doc3.docx	October 15, 2020	FY21

On December 1, 2020, you create the event shown in the Event exhibit. (Click the Event tab.)



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:

Answer Area

Statements	Yes	No
Doc1.docx will be retained until December 30, 2027.	○	○
Doc2.docx will be retained until September 30, 2027.	○	○
Doc3.docx will be retained until September 30, 2027.	○	○

Correct Answer:

Answer Area

Statements	Yes	No
Doc1.docx will be retained until December 30, 2027.	○	○
Doc2.docx will be retained until September 30, 2027.	○	○
Doc3.docx will be retained until September 30, 2027.	○	○

jimmyjose Highly Voted 1 year, 2 months ago

I am wondering why this question is not discussed though it is not answered correctly.
The correct answer is N, Y, Y. The 3rd one is also a Yes as both tags FY20 and FY21 apply to the policy in the screenshot.

upvoted 15 times

fimbulvetrk 1 year ago

I don't get the answer too, I agree with you.

upvoted 2 times

wooyourdaddy 9 months, 1 week ago

https://learn.microsoft.com/en-us/microsoft-365/compliance/event-driven-retention?view=o365-worldwide

Has the following sentence:

After creating an event, the retention settings take effect for the content that's already labeled and indexed. If the retention label is added to new content after the event is created, you must create a new event with the same details.

upvoted 1 times

Nickname 6 months ago

And the event was created over a month after the last file:
"On December 1, 2020, you create the event"

upvoted 1 times

[Removed] Highly Voted 9 months, 2 weeks ago

The answer is correct - N, Y, N
For Doc 1, 7 years after EOFY = Sept 30, 2027 (the option was Dec, so its N)
For Doc 2, 7 years after EOFY = Sept 30, 2027 (so its Y)
For Doc 3, 7 years after EOFY = Sept 30, 2028 (since it falls in the next FY of Sept 2021, so its N)

upvoted 6 times

heshmat2022 Most Recent 1 month, 1 week ago

IT WAS ON EXAM OCTOBER 18TH 2023

upvoted 2 times

Gesbie 3 months, 3 weeks ago

was on Exam August 9, 2023

upvoted 1 times

R3xx 5 months, 3 weeks ago

I believe it's n,y,n the the policy wouldn't start the count until September 30 of 2021. Since the doc was created in October after the count time for the policy, it's treated as September 30 of 2021. I think the hint here is the FY21

upvoted 1 times

xswe 7 months, 3 weeks ago

Since we are looking at a retention policy that will retain depending on the "fiscal year" we have to find out the fiscal years. It's every 3 months so the following months, 03 / 06 / 09 / 12.
No, it will be ratined until SEPT 30 2027.
Yes
No, this document is past 30th sept so it will be ratined until 30th dec 2027

upvoted 1 times

Nickname 6 months ago

Your assumption of the fiscal years is wrong since its based on baseless assumption. The only thing that matters is that the retention period starts from the point the event happened.

upvoted 2 times

Jonclark 9 months ago

N/Y/Y

What's important here is that doc1, doc2 and doc3 already existed with retention labels applied and asset IDs set to either FY20 or FY21 at the time the FY2020 retention event was created.

It kind of doesn't make sense to apply a 2020 year end policy to documents tagged as FY21, but they do include both FY20 and FY21 asset IDs in the example event -- don't let that trip you up.

The deletion date is based on the date set in the retention event, not the file creation dates. Don't let that trip you up either.

source: https://learn.microsoft.com/en-us/microsoft-365/compliance/event-driven-retention?view=o365-worldwide

upvoted 2 times

mcas 1 year, 1 month ago

N,Y,Y
the file creation date can be ignored because the time is based on the event that start on 30th Sept 2020

upvoted 6 times

fr54fr 1 year, 1 month ago

Label: Retention (7 years) is applied/starts on Event
Event date: 30 Sep 2020. This date is used as the start of the retention period.
doc1 & doc2 have been created before the event time so Retention label will be applied on 30 sep 2020 and documents retained for 7 years

doc3 was created october 15 . the Event does not trigger the start of retention period.
Y, Y, N

upvoted 2 times

fimbulvetrk 1 year ago

although doc1 was created before the event date, the answer says that it will be retained until 30 dec 2027, so the answer is NO in this case, because the retention starts in the date you set in the event, in this case, 30 september.

upvoted 2 times

Daanvanbeek 1 year, 2 months ago

N, Y, Y
Third is yes because the FY21 tag applies to the 2020 policy.

upvoted 4 times

avr 11 months ago

N, Y, N
Third is No because is retained until October 30, instead of September 30.

upvoted 4 times

Nickname 6 months ago

this is wrong. Retention period is based on event not the file.

upvoted 1 times

Question #32 *Topic 1*

You have a sensitive information type based on a trainable classifier.
You are unsatisfied with the result of the result of trainable classifier.
You need to retrain the classifier.
What should you use in the Microsoft 365 compliance center?

A. Labels from Information protection

B. Labels from Information governance

C. Content explorer from Data classification

D. Content search

Correct Answer: *C*
Reference:
https://docs.microsoft.com/en-us/microsoft-365/compliance/classifier-how-to-retrain-content-explorer?view=o365-worldwide

Community vote distribution

C (100%)

kochunnee Highly Voted 2 years, 1 month ago
Correct Answer

How to retrain a classifier in content explorer
Sign in to Microsoft 365 compliance center with compliance admin or security admin role access and open Microsoft 365 compliance center > Data classification > Content explorer.
Under the Filter on labels, info types, or categories list, expand Trainable classifiers.
upvoted 7 times

xswe Most Recent 7 months, 3 weeks ago
To retrain a trainable classifier you can easily do this through Content Explorer found under the same tab as you can find Trainable Classifier, under Data Classification.
upvoted 1 times

Jonclark 9 months ago
Selected Answer: C
It's a manual process. In Content Explorer, look at items which were considered a match for a trainable classifier and provide feedback by clicking "Not a Match" or "Match".

After 30 instances of feedback are submitted, the system will automatically retrain the classifier. Retraining takes 1-4 hours, and you can do it a maximum of two times per day.

https://learn.microsoft.com/en-us/microsoft-365/compliance/classifier-how-to-retrain-content-explorer?view=o365-worldwide

While not part of this question, I think it's fair game for MS to ask in another question what roles you need to do this activity: You need to be granted Content Explorer List Viewer and Content Explorer Content Viewer roles. These are roles that can be granted separately, but are also a part of these roles: Data Classification Content Viewer, Information Protection Investigator, Privacy Management Investigator.

https://learn.microsoft.com/en-us/microsoft-365/security/office-365-security/scc-permissions?view=o365-worldwide
upvoted 3 times

wooyourdaddy 1 year, 5 months ago
Selected Answer: C
I wrote the exam today, this question was on it, I choose C, scored 890!
upvoted 1 times

ayush0312 1 year, 8 months ago
GOOD please look in to the doc
upvoted 1 times

PrettyFlyWifi 1 year, 10 months ago
Selected Answer: C
Correct.... https://docs.microsoft.com/en-us/microsoft-365/compliance/classifier-how-to-retrain-content-explorer?view=o365-worldwide
upvoted 2 times

Question #33 *Topic 1*

You receive an email that contains a list of words that will be used for a sensitive information type.
You need to create a file that can be used as the source of a keyword dictionary.
In which format should you save the list?

A. a JSON file that has an element for each word

B. an ACCDB database file that contains a table named Dictionary

C. an XLSX file that contains one word in each cell of the first row

D. a text file that has one word on each line

Correct Answer: *D*
Keyword dictionaries can be created either from a text file or from csv file.
Note:
There are several versions of this question in the exam. The question has two possible correct answers:
1. a CSV file that contains words separated by commas
2. a text file that has one word on each line
Other incorrect answer options you may see on the exam include the following:
- a TSV file that contains words separated by tabs
- a DOCX file that has one word on each line
- an XML file that contains a keyword tag for each word

Reference:
https://docs.microsoft.com/en-us/microsoft-365/compliance/create-a-keyword-dictionary?view=o365-worldwide

Community vote distribution
D (100%)

xswe 7 months, 3 weeks ago
When creating keyword dictionaries for sensitive info types you can only use txt and csv documents.
upvoted 2 times

chrissempai 1 year, 2 months ago
Selected Answer: D
Basic steps to creating a keyword dictionary
The keywords for your dictionary could come from various sources, most commonly from a file (such as a .csv or .txt list) imported in the service or by PowerShell cmdlet, from a list you enter directly in the PowerShell cmdlet, or from an existing dictionary.
upvoted 4 times

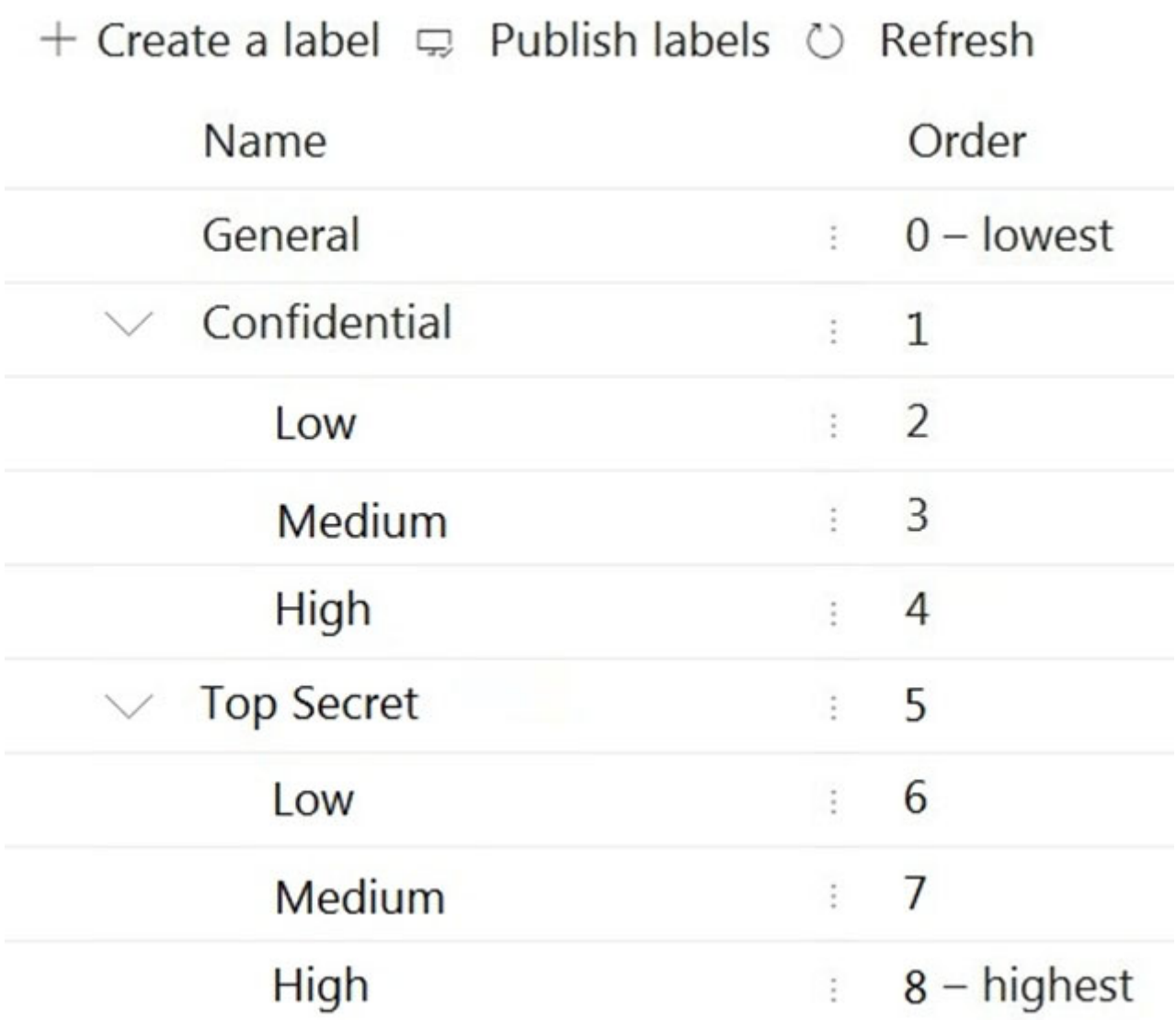
HOTSPOT -

You have a Microsoft 365 E5 tenant that contains three groups named Group1, Group2, and Group3.

You have the users shown in the following table.

Name	Member of
User1	Group1
User2	Group1, Group3
User3	Group2, Group3

You have the sensitivity labels shown in the following exhibit.



You have the label policies shown in the following table.

Name	Labels to publish	Group	Apply this default label to documents
Policy1	Confidential Confidential – Low Confidential – Medium Confidential – High	Group1	Confidential
Policy2	All labels	Group2	Confidential – Medium
Policy3	Confidential Confidential – Low Confidential – Medium Confidential – High Top Secret	Group3	Top Secret

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:

Answer Area

Statements	Yes	No
The Confidential label will be applied to all the documents created by User1.	○	○
User2 can apply the General label to all the documents created by User2.	○	○
User3 can change the label applied to a document created by User1.	○	○

Correct Answer:

Answer Area

Statements	Yes	No
The Confidential label will be applied to all the documents created by User1.	○	○
User2 can apply the General label to all the documents created by User2.	○	○
User3 can change the label applied to a document created by User1.	○	○

Reference:

https://docs.microsoft.com/en-us/microsoft-365/compliance/sensitivity-labels?view=o365-worldwide

wyindualizer Highly Voted 1 year, 3 months ago

The parent label Confidential is simply a text label with no protection settings, and because it has sublabels, it can't be applied to content. Instead, users must choose Confidential to view the sublabels, and then they can choose a sublabel to apply to content. So first will be NO.

upvoted 11 times

aashuboss 1 year, 1 month ago

Agree. "Don't choose a parent label as the default label, or configure a parent label to be automatically applied (or recommended). If you do, the parent label can't be applied."
No, No, Yes

upvoted 6 times

xswe Most Recent 7 months, 3 weeks ago

No, since the confidential label is a Parent label and cant be used.
No, since User2 are not a member of Group2 which has all the labels available (General is not available in either Confidential or Top Secret)
Yes, but only to labels available in Group2 and Group3 (All the labels)

upvoted 4 times

Jonclark 9 months ago

Answer 1: No.
Per MS documentation: "Don't choose a parent label as the default label, or configure a parent label to be automatically applied (or recommended). If you do, the parent label cannot be applied."
https://learn.microsoft.com/en-us/microsoft-365/compliance/sensitivity-labels?view=o365-worldwide

Answer 2: No.
User 2 will not see the General label because it has not been published to a group they belong to.

Answer 3: I don't like this question because it doesn't have enough information. User3 can see all of the sensitivity labels that user1 can see, but that doesn't mean that user3 automatically gets write permissions to every document that user1 creates. User3 will only be able to change a sensitivity label set by user1 if they have permissions to modify the item the label is applied to. For this question, let's assume user3 has permissions to modify the item, and then we can go with "Yes".

upvoted 3 times

iUser123 10 months, 3 weeks ago

Yes (https://m365admin.handsontek.net/updated-change-in-display-of-hierarchical-sensitivity-labels/)
No
Yes

upvoted 1 times

fr54fr 1 year, 1 month ago

Answer 3 = Yes
As member of Group 2, User 3 has access to labels with higher priorities (Top Secret - Low, Medium, Hight) than the labels that User 1 has, thus can replace any label set by User1

upvoted 2 times

kiketxu 1 year, 1 month ago

To be honest, I'm not sure but I will opt for YES for the third.
I have always thought you need to be owner/co-author of the label to change it, but in the question they does not mention any protection setting....so I would choose YES, because User3 probably can change to "Top Secret" any labels applied by User1. (I guess it is the only option User3 has and probably he can as there no protection on labels mentioned)
1 = YES
2 = NO (User2 is not member of Group2. He can't use General)
3= YES

upvoted 1 times

fr54fr 1 year, 1 month ago

Answer 2 = No,
Label General is not published for Group 1 & Group 3 of which User2 is member of

upvoted 1 times

HOTSPOT -

You have a Microsoft 365 E5 tenant that contains a sensitivity label named label1.

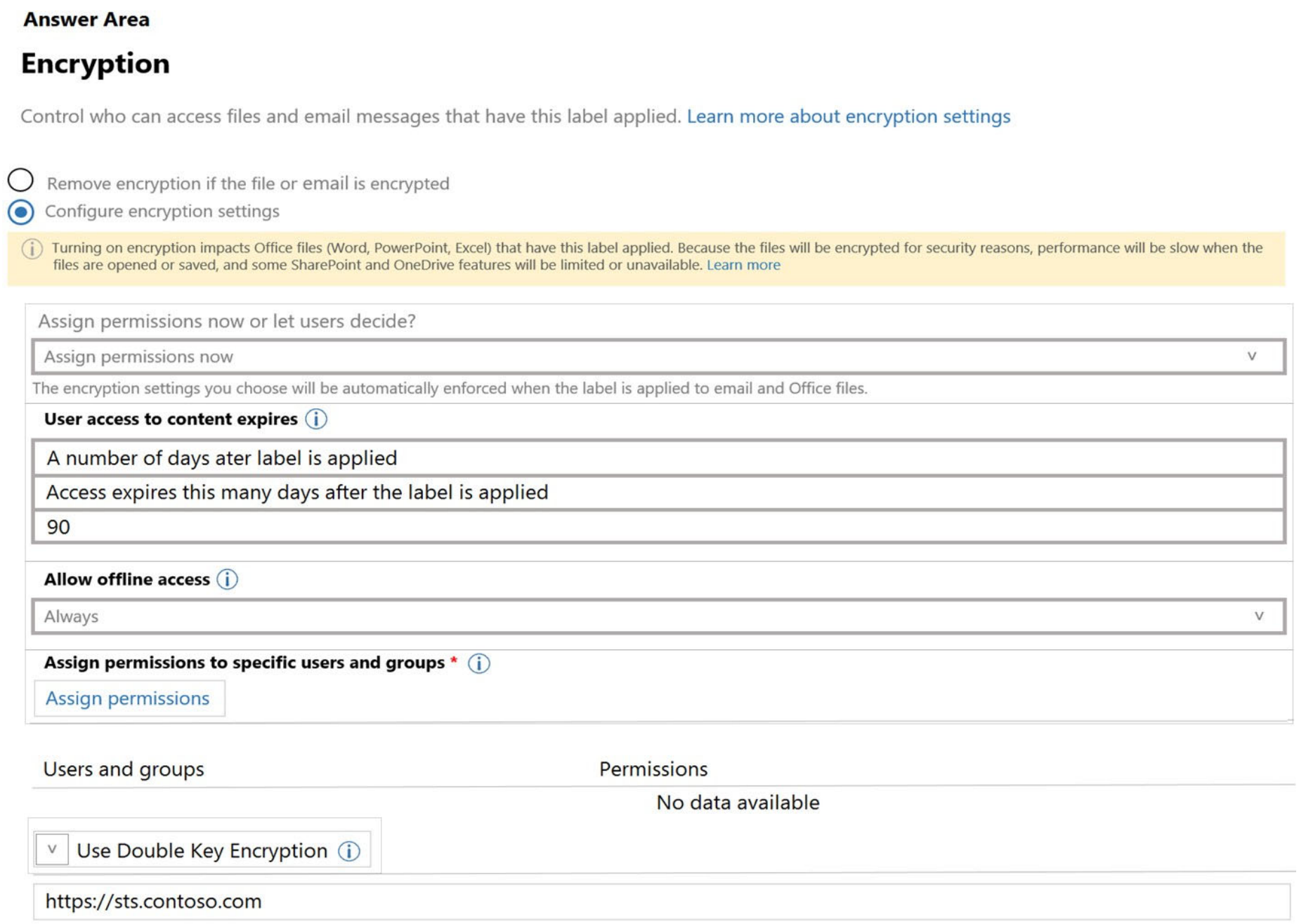
You plan to enable co-authoring for encrypted files.

You need to ensure that files that have label1 applied support co-authoring.

Which two settings should you modify? To answer, select the settings in the answer area.

NOTE: Each correct selection is worth one point.

Hot Area:



Correct Answer:

Answer Area

Encryption

Control who can access files and email messages that have this label applied. Learn more about encryption settings

○ Remove encryption if the file or email is encrypted
◉ Configure encryption settings

ⓘ Turning on encryption impacts Office files (Word, PowerPoint, Excel) that have this label applied. Because the files will be encrypted for security reasons, performance will be slow when the files are opened or saved, and some SharePoint and OneDrive features will be limited or unavailable. Learn more

Assign permissions now or let users decide?

Assign permissions now ∨

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

User access to content expires ⓘ

A number of days ater label is applied

Access expires this many days after the label is applied

90

Allow offline access ⓘ

Always ∨

Assign permissions to specific users and groups * ⓘ

Assign permissions

Users and groups	Permissions
	No data available

∨ Use Double Key Encryption ⓘ

https://sts.contoso.com

Co-authoring and AutoSave aren't supported and don't work for labeled and encrypted Office documents that use any of the following configurations for encryption:

☞ Let users assign permissions when they apply the label and the checkbox In Word, PowerPoint, and Excel, prompt users to specify permissions is selected.

This configuration is sometimes referred to as "user-defined permissions".

☞ User access to content expires is set to a value other than Never.

Double Key Encryption is selected.

▪

Reference:

https://docs.microsoft.com/en-us/microsoft-365/compliance/sensitivity-labels-coauthoring?view=o365-worldwide

https://techcommunity.microsoft.com/t5/security-compliance-and-identity/co-authoring-files-with-sensitivity-labels/ba-p/3029768

chrissempai Highly Voted 1 year, 2 months ago

The change you need to do is :
- disable the double encryption
- User access to content expires is set to a value other than Never.

upvoted 5 times

kiketxu 1 year, 1 month ago

You right, thanks.
https://techcommunity.microsoft.com/t5/security-compliance-and-identity/co-authoring-files-with-sensitivity-labels/ba-p/3029768
"documents cannot be co-authored if they're either protected with user-defined permissions or if they have User access to content expires set to a value other than Never"

"An Office version compatible with both Co-Authoring and DKE is not expected before 2023"

upvoted 1 times

phony Most Recent 1 month, 2 weeks ago

there is another option now, see:
https://learn.microsoft.com/en-us/purview/sensitivity-labels-coauthoring?view=o365-worldwide%20https%3A%2F%2Ftechcommunity.microsoft.com%2Ft5%2Fsecurity-compliance-and-identity%2Fco-authoring-files-with-sensitivity-labels%2Fba-p%2F3029768

upvoted 1 times

Jonclark 9 months ago

I agree with others in this discussion. Set expiration to never and turn off double encryption.

Note: The question starts with "You plan to enable co-authoring of encrypted files"....
If it's not enabled now, setting these configurations on a sensitivity label won't accomplish that. You need to make a bigger change that can affect your entire enterprise. Make sure you're familiar with this in prep for the test.
https://learn.microsoft.com/en-us/microsoft-365/compliance/sensitivity-labels-coauthoring?view=o365-worldwide

upvoted 2 times

Question #36 *Topic 1*

HOTSPOT
-

You have a Microsoft 365 E5 subscription.

You have a Microsoft Office 365 Advanced Message Encryption branding template named OME1.

You need to create a Microsoft Exchange Online mail flow rule to apply OME1 to email.

How should you configure the rule? To answer, select the appropriate options in the answer area.

NOTE: Each correct selection is worth one point.

Answer Area

Apply this rule if:

- A message header
- The message properties
- The recipient
- The sender

- Contains any of these sensitive info types
- Has specific properties including any of these words
- Includes the classification
- Includes the importance level
- Is external/internal

To apply custom branding to OME1 messages:

- Apply a disclaimer to the message.
- Modify the message properties.
- Modify the message security.
- Redirect the message.

Correct Answer:

Answer Area

Apply this rule if:

- A message header
- The message properties
- The recipient
- The sender

- Contains any of these sensitive info types
- Has specific properties including any of these words
- Includes the classification
- Includes the importance level
- Is external/internal

To apply custom branding to OME1 messages:

- Apply a disclaimer to the message.
- Modify the message properties.
- Modify the message security
- Redirect the message.

phony 1 month, 2 weeks ago

this question is nog complete, and a lot of settings are moved to OME is replaced by Microsoft Purview Message Encryption. May 2023.

https://go.microsoft.com/fwlink/?linkid=2213908

upvoted 1 times

217f3c9 6 months ago

"You need to create a Microsoft Exchange Online mail flow rule to apply OME1 to email." --> every mail will get OME1? Makes no sense

upvoted 2 times

spikep 7 months, 2 weeks ago

[Apply this rule if | The sender is located inside the organization | Modify the message security]
https://learn.microsoft.com/en-us/microsoft-365/compliance/add-your-organization-brand-to-encrypted-messages?view=o365-worldwide#create-an-exchange-mail-flow-rule-that-applies-your-custom-branding-to-encrypted-emails-sent-from-your-online-organization-to-external-recipients

upvoted 1 times

luissaro 7 months, 2 weeks ago

I guess something is missing in this question...

upvoted 1 times

See_Es 10 months, 1 week ago

I agree with the given answer. If sender is internal apply security would catch all sent messages from all internal users.

upvoted 4 times

Question #37 *Topic 1*

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

• Confidential:
o Internal
o 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.

What should you do?

A. Modify the scope of the Confidential label.

B. Modify the publishing settings of Policy1.

C. Enable sensitivity label support for Office files in Microsoft SharePoint Online and OneDrive.

D. Run the Execute-AzureAdLabelSync cmdlet.

Correct Answer: *C*

wooyourdaddy 9 months, 1 week ago

Very first sentence at this link:
https://learn.microsoft.com/en-us/microsoft-365/compliance/sensitivity-labels-sharepoint-onedrive-files?view=o365-worldwide

states:

Enable built-in labeling for supported Office files in SharePoint and OneDrive so that users can apply your sensitivity labels in Office for the web.

Answer C is correct.

upvoted 3 times

See_Es 10 months, 1 week ago

Correct. Web apps need to be enabled separately for sensitivity labels

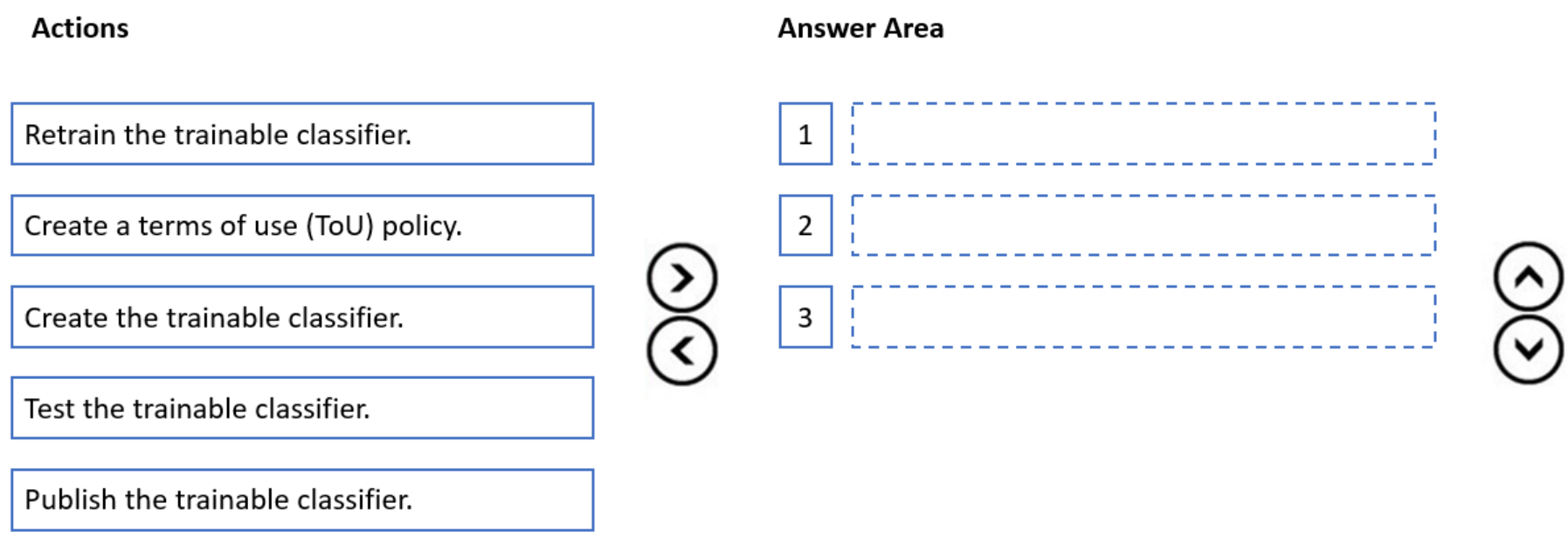
upvoted 3 times

DRAG DROP

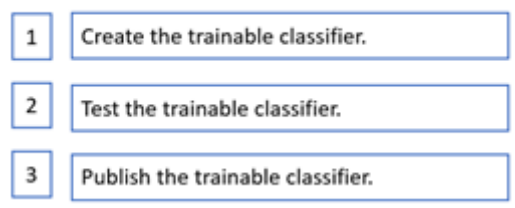
-

You need to create a trainable classifier that can be used as a condition in an auto-apply retention label policy.

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.



Correct Answer:



wooyourdaddy 9 months, 1 week ago

Answer is correct. Process flow for creating custom classifiers listed here:

https://learn.microsoft.com/en-us/microsoft-365/compliance/classifier-learn-about?view=o365-worldwide#process-flow-for-creating-custom-classifiers

Contains flow chart with 3 major steps: Create Classifier, Test Classifier and Publish Classifier.

upvoted 2 times

Chris7910 9 months, 3 weeks ago

Don't i need to train a classifier before testing it?

upvoted 1 times

[Removed] 9 months, 2 weeks ago

The option was to 'retrain' only, which would not be applicable in this case

upvoted 2 times

Jonclark 9 months ago

Training is included testing. When you test the classifier, you feed it positive and negative samples and provide feedback on whether you agree or disagree with the results. You can continue this process until you feel that the classifier is sufficiently trained and then publish it.

upvoted 3 times

Question #39 *Topic 1*

You have a Microsoft 365 E5 tenant.

You need to add a new keyword dictionary.

What should you create?

A. a trainable classifier

B. a sensitivity label

C. a sensitive info type

D. a retention policy

Correct Answer: *C*

Community vote distribution

C (100%)

jinxie Highly Voted 10 months, 2 weeks ago

Selected Answer: C

seems correct to me. https://learn.microsoft.com/en-us/microsoft-365/compliance/create-a-keyword-dictionary?view=o365-worldwide
Connect to the Microsoft Purview compliance portal.

Navigate to Classifications > Sensitive info types.

Select Create and enter a Name and Description for your sensitive info type, then select Next

upvoted 5 times

Domza Most Recent 3 weeks, 2 days ago

looks good~

upvoted 1 times

xswe 7 months, 3 weeks ago

Keyword dictionaries = Sensitive info type

upvoted 1 times

HOTSPOT
-

You have a Microsoft 365 E5 subscription that contains two users named User1 and User2 and a group named Group1. User1 is a member of Group1.

The subscription contains the sensitivity labels shown in the following table.

Name	Sublabel	Order
General	*None*	0
Confidential	*Not applicable*	1
	Confidential/Low	2
	Confidential/Medium	3
	Confidential/High	4
Secret	*Not applicable*	5
	Confidential/Low	6
	Confidential/Medium	7
	Confidential/High	8

You have a sensitivity label policy named Policy1 that is published to User1 and User2. The policy includes the following labels:

• General
• Confidential
• Confidential/Low
• Confidential/High
• Confidential/Medium

For Policy1, the default label for documents is Confidential/Low.

You have a sensitivity label policy named Policy2 that is published to Group1. The policy includes the following labels:

• Secret
• General
• Secret/Low
• Secret/High
• Secret/Medium

For Policy2, the default label for documents is Secret/Low.

You have a sensitivity label policy named Policy3 that is published to User1 and User2. The policy includes the following labels:

• Secret
• General
• Secret/Low
• Secret/High
• Secret/Medium

For Policy3, the default label for documents is Secret/Medium.

The order of the policies is shown in the following table.

Policy	Order
Policy1	0 – lowest
Policy2	1
Policy3	2 – highest

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	Yes	No
User2 can apply the General label to a document.	○	○
The default document label for User1 is Secret/Low.	○	○
User1 can apply the Confidential label to a document.	○	○

Correct Answer:

Answer Area

Statements	Yes	No
User2 can apply the General label to a document.	☒	○
The default document label for User1 is Secret/Low.	○	☒
User1 can apply the Confidential label to a document.	☒	○

See_Es Highly Voted 10 months, 1 week ago
Should be Y/N/N. The Confidential label is a parent label and cannot be selected as a document label
upvoted 11 times

Jonclark 9 months ago
I agree Y/N/N .

1. You can't select a parent label when applying a sensitivity label to an item.
2. You can include a user in multiple label policies, and the user will get all the sensitivity labels and settings from those policies. If there's a conflict in settings from multiple policies, the settings from the policy with the highest priority (highest order number) is applied. In other words, the highest priority wins for each setting.

https://learn.microsoft.com/en-us/microsoft-365/compliance/sensitivity-labels?view=o365-worldwide
upvoted 1 times

trojansrj Most Recent 2 months, 3 weeks ago
the 2d one is No, not even because of highest priority, but because default for policy 3 is secret Medium, not secret Low, as suggested in the question
upvoted 1 times

dmoorthy 7 months, 1 week ago
Answers is Y/N/N
upvoted 1 times

xswe 7 months, 3 weeks ago
Yes, since User2 are a member of Policy1 and the General label are not a parent label
No, if you have several labels as default label through different policys which we have here the policy with the higher priority is the one that will get used as default document label, in this is it is Confiddential/Low
No, since you cannot use parent labels they are there to give users a logical GUI/interface.
upvoted 2 times

Sategi 4 months, 2 weeks ago

agree, but for second answer, Policy 3 will be applied bacause policy has highest priority and default label will be Secret/Medium.
upvoted 1 times

Question #41 *Topic 1*

You plan to implement Microsoft Office 365 Advanced Message Encryption.

You need to ensure that encrypted email sent to external recipients expires after seven days.

What should you create first?

A. a custom branding template

B. a remote domain in Microsoft Exchange

C. a mail flow rule

D. an X.509 version 3 certificate

E. a connector in Microsoft Exchange

Correct Answer: *A*

Community vote distribution

A (100%)

heshmat2022 1 month, 1 week ago
IT WAS ON EXAM OCTOBER 18 2023
upvoted 1 times

Gesbie 3 months, 3 weeks ago
was on Exam August 9, 2023
upvoted 1 times

xswe 7 months, 3 weeks ago
Always custom branding templates for this, you can use the following cmdlet

New-OMEConfiguration -Identity "Expire in 7 days" -ExternalMailExpiryInDays 7
upvoted 2 times

jinxie 10 months, 1 week ago
answer seems correct to me https://learn.microsoft.com/en-us/microsoft-365/compliance/ome-advanced-expiration?view=o365-worldwide
upvoted 3 times

tetst 10 months, 1 week ago
Selected Answer: A
A
https://learn.microsoft.com/en-us/microsoft-365/compliance/ome-advanced-expiration?view=o365-worldwide#create-a-custom-branding-template-to-force-mail-expiration-by-using-powershell
upvoted 3 times

Jonclark 9 months ago
In case the test question asks you about the PowerShell cmdlet, it looks something like this:
Set-OMEconfiguration -Identity My_OME_Template -ExternalMailExpiryInDays 7
upvoted 1 times

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.

Answer 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.	○	○

Answer Area

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.	○	☒
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.	○	☒

See_Es Highly Voted 10 months, 1 week ago

NYN - Agreed.
First is not encrypted because of the exclusion.
Second is encrypted because this time the recipient is not excluded.
Third is not encrypted because policy 2 is the only policy for user 2 and policy 2 does not do the encryption

upvoted 6 times

heshmat2022 Most Recent 1 month, 1 week ago

IT WAS ON EXAM OCTOBER 18 2023

upvoted 1 times

luissaro 7 months, 2 weeks ago

to me is NYY because to User2 will be applied Policy2 that says restrict access or encrypt, it does not say block delivering email

upvoted 1 times

xswe 7 months, 3 weeks ago

No, sure user1 is a member of the Finance group but you have an exception here. The user4 are the exception so the policy wont get applied = message wont get encrypted as asked for.
Yes, since user is a memeber of the Finance group and the orders@adatum.com is not in the exceptions of the policy, in actions you can see "Encrypt mnessage" = Message will get encrypted
No, since user2 is NOT a member of the Finance group but the Sales group. The action in the other policy is "Restrict acces or encrypt content IN M365 LOCATION" = Message wont get encrypted

upvoted 3 times

Question #43 *Topic 1*

HOTSPOT
-

You have a Microsoft 365 E5 tenant that contains a trainable classifier named Classifier1.

You need to increase the accuracy of Classifier1. The solution must use the principle of least privilege.

Which feature should you use and to which role group should you be added? To answer, select the appropriate options in the answer area.

NOTE: Each correct selection is worth one point.

Answer Area

Feature:
- Activity explorer
- Content explorer
- Compliance Manager
- Microsoft Information Governance

Role group:
- Compliance Data Administrator
- Compliance Manager Contributors
- Compliance Manager Readers

Correct Answer:

Answer Area

Feature:
- Activity explorer
- Content explorer
- Compliance Manager
- Microsoft Information Governance

Role group:
- Compliance Data Administrator
- Compliance Manager Contributors
- Compliance Manager Readers

xswe Highly Voted 7 months, 3 weeks ago
To make trainable classifier better you can use Content explorer, found under data classification.
To retrain trainable classifiers you need to be Compliance Data Administrator or Compliance Administrator
upvoted 6 times

heshmat2022 Most Recent 1 month, 1 week ago
IT WAS ON EXAM OCTOBER 18 2023
upvoted 1 times

Gesbie 3 months, 3 weeks ago
was on Exam August 9, 2023
upvoted 1 times

shuffler 8 months ago
Good one: https://learn.microsoft.com/en-us/microsoft-365/compliance/classifier-how-to-retrain-content-explorer?source=recommendations&view=o365-worldwide
upvoted 1 times

Question #44 *Topic 1*

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 Purview compliance portal, start a data investigation.

B. From the Microsoft Defender for Cloud Apps portal, create a file policy.

C. From the Azure Active Directory admin center, configure an Identity Protection policy.

D. From the Exchange admin center, create a data loss prevention (DLP) policy.

Correct Answer: *B*

xswe Highly Voted 7 months, 3 weeks ago

This question is asking for a function that will detect when users SHARE sensitive information outside your company, which means with need to create a DLP policy.
The only logical answer here for creating a DLP policy is Cloud Apps - File Policy since we have a DLP category available here

upvoted 6 times

heshmat2022 Most Recent 1 month, 1 week ago

IT WAS ON EXAM OCTOBER 18 2023

upvoted 1 times

mstfcskn 4 months, 3 weeks ago

The correct action to be alerted when users share sensitive documents from Microsoft OneDrive to any users outside your company is to create a file policy in the Microsoft Defender for Cloud Apps portal, not from the Exchange admin center creating a DLP policy.

upvoted 2 times

Question #45 *Topic 1*

HOTSPOT
-

You have a Microsoft 365 E5 tenant.

You need to create a custom trainable classifier that will detect product order forms. The solution must use the principle of least privilege.

What should you do first? To answer, select the appropriate options in the answer area.

NOTE: Each correct selection is worth one point.

Answer Area

Action to perform:
- Create an Exact Data Match (EDM) schema
- Import a data loss prevention (DLP) rule package.
- Start the opt-in process

To perform the action, assign the role of:
- Compliance Administrator
- Global Administrator
- Security Administrator

Correct Answer:

Answer Area

Action to perform:
- Create an Exact Data Match (EDM) schema
- Import a data loss prevention (DLP) rule package.
- Start the opt-in process

To perform the action, assign the role of:
- Compliance Administrator
- Global Administrator
- Security Administrator

shuffler Highly Voted 8 months, 1 week ago
The opt-in can't be performed by the Compliance Administrator, the GA is required:
"To access classifiers in the UI:
the Global admin needs to opt in for the tenant to create custom classifiers.
Compliance Administrator role is required to train a classifier."

https://learn.microsoft.com/en-us/microsoft-365/compliance/classifier-get-started-with?view=o365-worldwide
upvoted 12 times

willowvine Most Recent 1 month, 1 week ago
It shows you can use Compliance Admin or Security Admin to create a trainable classifier https://learn.microsoft.com/en-us/purview/classifier-get-started-with
upvoted 1 times

heshmat2022 1 month, 1 week ago
IT WAS ON EXAM OCTOBER 18 2023
upvoted 1 times

ikidreamz 4 months, 2 weeks ago
looks like Opt-in and Global admin)(TO CREATE not train) my bad I thought least privilege earlier
upvoted 1 times

ikidreamz 4 months, 2 weeks ago
I think for least privilege question and i see it like this
Action = create a trainable classifier
To perform the action = Compliance admin

Compliance Administrator role is required to train a classifier.

upvoted 2 times

ikidreamz 4 months, 2 weeks ago

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

upvoted 1 times

ikidreamz 4 months, 2 weeks ago

so box 1 = create EDM schema and box 2 = Compliance admin

upvoted 1 times

GeoffLule 7 months ago

Correct in my view. The role of creating custom classifier is Compliance Admin

upvoted 1 times

dmoorthy 7 months, 1 week ago

Start the Opt-in process and Global Admin

upvoted 3 times

reastman66 7 months, 3 weeks ago

Start the Opt-in process and the role required to perform this action is Global Admin

upvoted 4 times

xswe 7 months, 3 weeks ago

To be able to create custom trainble classifiers you need to start with the "opt-in process" and the only one who can do this is the Global administrator

upvoted 4 times

Question #46 *Topic 1*

HOTSPOT
-

The subscription contains the users shown in the following table.

Name	Member of
User1	Group1
User2	Dist1
User3	*None*

You create the mail flow rules shown in the following table.

Name	Apply this rule if	Do the following
Rule1	The recipient is a member of group1@contoso.com	Apply Office 365 Message Encryption and rights protection
Rule2	The sender is dist1@contoso.com	Apply Office 365 Message Encryption and rights protection

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	Yes	No
If User2 sends an email message to User3, the message is encrypted automatically.	○	○
If User2 sends an email message to User1, the message is encrypted automatically.	○	○
If User3 sends an email message to Group1, the message delivered to User1 is encrypted automatically.	○	○

Correct Answer:

Answer Area

Statements	Yes	No
If User2 sends an email message to User3, the message is encrypted automatically.	○	☒
If User2 sends an email message to User1, the message is encrypted automatically.	☒	○
If User3 sends an email message to Group1, the message delivered to User1 is encrypted automatically.	○	☒

Franc_Coetzee 23 hours, 2 minutes ago

1 - N (Rule2 = "The sender is dist1@". User2 is part of Dist1, but here the sender is user2@)
2 - Y (User 1 is a member of Group 1)
3 - N (Rule1 is set to focus on the members and not the main email address)

upvoted 1 times

asdilhfnas 2 weeks, 2 days ago

1. Yes: User 2 is the sender and part of dist1 -> Email isautom. encrypted
2. Same as 1
3. User 1 is recipient and part of Group1 -> Mail is encrypted

upvoted 2 times

asdilhfnas 2 weeks, 2 days ago

3. Yes

upvoted 2 times

martutene 4 weeks ago

1-N user 2 IS NOT (rule 2 specifies USER IS)
2- Y since user 1 is MEMBER of (rule 1 applies to the RECIPIENT)
3- Y since user one is MEMBER and the email was sent to the recipient group

upvoted 3 times

Question #47 *Topic 1*

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

You need to ensure that you receive an alert when a user uploads a document to a third-party cloud storage service.

What should you use?

A. an insider risk policy

B. a file policy

C. a sensitivity label

D. an activity policy

Correct Answer: *B*

Community vote distribution

B (100%)

martutene 4 weeks ago

Selected Answer: B

Correct

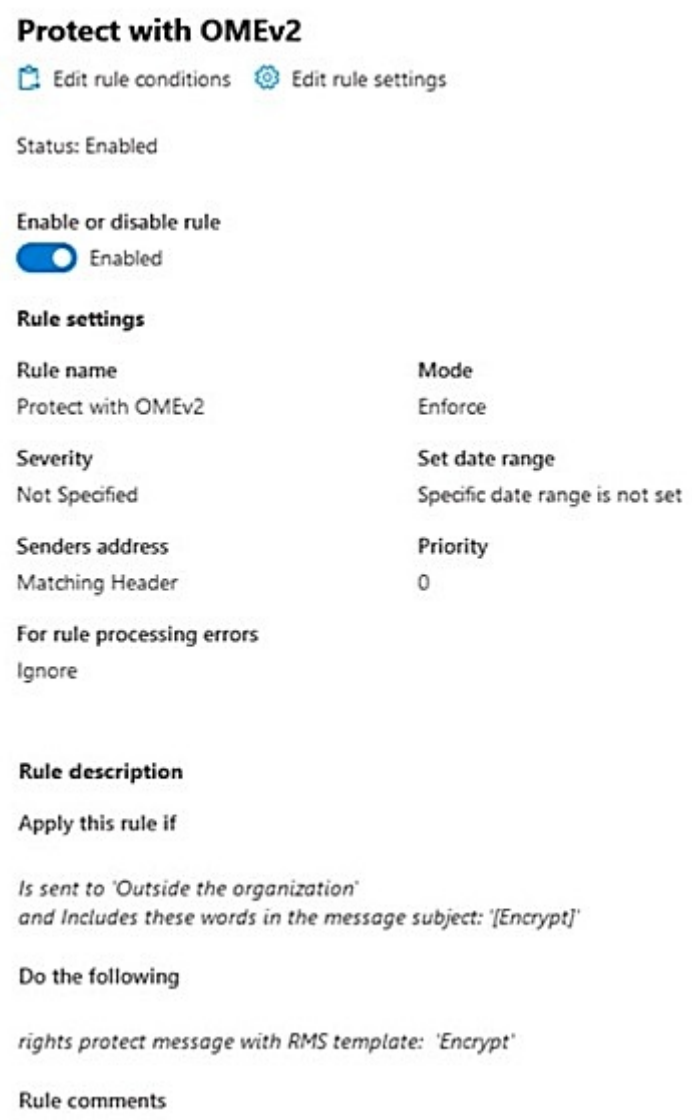
upvoted 2 times

Question #48 *Topic 1*

HOTSPOT
-

You have a Microsoft 365 subscription.

In Microsoft Exchange Online, you configure the mail flow rule shown in the following exhibit.



Use the drop-down menus to select the answer choice that completes each statement based on the information presented in the graphic.

NOTE: Each correct selection is worth one point.

Answer Area

Recipients, who use Gmail, **[answer choice]**.
- must sign in to the Office 365 Message Encryption (OME) portal to read messages
- will be unable to read messages
- will have messages decrypted automatically

Recipients from an external Microsoft 365 subscription **[answer choice]**.
- must sign in to the Office 365 Message Encryption (OME) portal to read messages
- will be unable to read messages
- will have messages decrypted automatically

Correct Answer:

Answer Area

Recipients, who use Gmail, **[answer choice]**.
- must sign in to the Office 365 Message Encryption (OME) portal to read messages
- will be unable to read messages
- will have messages decrypted automatically

Recipients from an external Microsoft 365 subscription **[answer choice]**.
- must sign in to the Office 365 Message Encryption (OME) portal to read messages
- will be unable to read messages
- will have messages decrypted automatically

JacoH 3 weeks ago

Answer is correct.
When someone sends an email message that matches an encryption mail flow rule, the message is encrypted before it's sent. All Microsoft 365 end users that use Outlook clients to read mail receive native, first-class reading experiences for encrypted and rights-protected mail even if they're not in the same organization as the sender. Supported Outlook clients include Outlook desktop, Outlook Mac, Outlook mobile on iOS and Android, and Outlook on the web (formerly known as Outlook Web App).

Recipients of encrypted messages who receive encrypted or rights-protected mail sent to their Gmail and Yahoo accounts receive a wrapper mail that directs them to the OME Portal where they can easily authenticate using a Microsoft account, Gmail, or Yahoo credentials.
https://learn.microsoft.com/en-us/purview/ome

upvoted 1 times

Question #49 *Topic 1*

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 E5 subscription.

You need to identify resumes that are stored in the subscription by using a built-in trainable classifier.

Solution: You create an auto-labeling policy for a retention label.

Does this meet the goal?

A. Yes

B. No

Correct Answer: *B*

JacoH 3 weeks ago
Answer is correct
https://learn.microsoft.com/en-us/purview/apply-sensitivity-label-automatically

upvoted 1 times

Question #50 *Topic 1*

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 E5 subscription.

You need to identify resumes that are stored in the subscription by using a built-in trainable classifier.

Solution: You create an auto-labeling policy for a sensitivity label.

Does this meet the goal?

A. Yes

B. No

Correct Answer: *A*

JacoH 3 weeks ago

Answer is correct
https://learn.microsoft.com/en-us/purview/apply-sensitivity-label-automatically

upvoted 1 times

Question #51 *Topic 1*

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 E5 subscription.

You need to identify resumes that are stored in the subscription by using a built-in trainable classifier.

Solution: You create a data loss prevention (DLP) policy.

Does this meet the goal?

A. Yes

B. No

Correct Answer: *B*

Domza 1 day, 1 hour ago

It says"identify resumes that are stored" - sensitivity labels do that

upvoted 1 times

JacoH 3 weeks ago

Answer is correct.
You can't use trainable classifiers in a (custom) DLP policy

upvoted 1 times

BJack 2 weeks ago

DLP does support trainable classifiers...
https://learn.microsoft.com/en-us/purview/classifier-learn-about

upvoted 1 times

Question #52 *Topic 1*

You have a Microsoft 365 E5 subscription.

You need to ensure that encrypted email messages sent to an external recipient can be revoked or will expire within seven days.

What should you configure first?

A. a custom branding template

B. a mail flow rule

C. a Conditional Access policy

D. a sensitivity label

Correct Answer: *A*

kingAzure 2 days ago

Answer is a custom branding template.

"With Microsoft Purview Advanced Message Encryption, anytime you apply custom branding, the Office 365 applies the wrapper to email that fits the mail flow rule to which you apply the template. In addition, you can only use expiration if you use custom branding."
https://learn.microsoft.com/en-us/purview/ome-advanced-expiration

upvoted 1 times

HOTSPOT
-

Your network contains an on-premises Active Directory domain named contoso.com. The domain contains the groups shown in the following table.

Name	Type	Email address
Group1	Security Group – Domain Local	Group1@contoso.com
Group2	Security Group - Universal	*None*
Group3	Distribution Group - Global	*None*
Group4	Distribution Group - Universal	Group4@contoso.com

The domain is synced to an Azure AD tenant that contains the groups shown in the following table.

Name	Type	Membership type
Group11	Security group	Assigned
Group12	Security group	Dynamic
Group13	Microsoft 365 group	Assigned
Group14	Mail-enabled security group	Assigned

You create a sensitivity label named Label1.

You need to publish Label1.

To which groups can you publish Label1? To answer, select the appropriate options in the answer area.

NOTE: Each correct selection is worth one point.

Answer Area

On-premises Active Directory groups:

- Group4 only
- Group1 and Group4 only
- Group3 and Group4 only
- Group1, Group3, and Group4 only
- Group1, Group2, Group3, and Group4

Azure AD groups:

- Group13 only
- Group13 and Group14 only
- Group11 and Group12 only
- Group11, Group13, and Group14 only
- Group11, Group12, Group13, and Group14

Correct Answer:

Answer Area

On-premises Active Directory groups:

- Group4 only
- Group1 and Group4 only
- Group3 and Group4 only
- Group1, Group3, and Group4 only
- Group1, Group2, Group3, and Group4

Azure AD groups:

- Group13 only
- Group13 and Group14 only
- Group11 and Group12 only
- Group11, Group13, and Group14 only
- Group11, Group12, Group13, and Group14

Question #1 *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 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 onboard the computers to Microsoft Defender for Endpoint.
Does this meet the goal?

A. Yes

B. No

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

Community vote distribution
A (69%) B (31%)

olsi Highly Voted 2 years, 6 months ago
Correct
upvoted 9 times

Gesbie Most Recent 3 months, 3 weeks ago
was on Exam August 9, 2023
upvoted 1 times

xswe 7 months, 3 weeks ago
To be able to deploy Endpoint DLP you need to ensure that you devices are onboarded.
upvoted 1 times

Abhishek1610 1 year ago
Selected Answer: A
Correct Answer A
upvoted 3 times

aclondon 1 year, 4 months ago
Selected Answer: A
Device onboarding is shared across Microsoft 365 and Microsoft Defender for Endpoint (MDE).
Answer is A.
upvoted 2 times

JamesM9 1 year, 7 months ago
The answer is A - Yes.
upvoted 1 times

JrGreen 1 year, 8 months ago
Selected Answer: A
A is right
upvoted 4 times

olsenOnS 1 year, 9 months ago
When you want to onboard devices that haven't been onboarded yet, you'll download the appropriate script and deploy it to those devices. Follow the device onboarding procedures below.

If you already have devices onboarded into Microsoft Defender for Endpoint, they will already appear in the managed devices list.

I think Ans: A i the right one.
upvoted 3 times

AJ2021 1 year, 9 months ago

Answer A is correct, read the first part of the question. Note: If Win10 devices are already registered in Defender for endpoint, then it is already ready to go, otherwise if not using Defender for endpoint the device needs to be either Azure AD joined or Hybrid Azure AD joined.

upvoted 2 times

srigowtham 1 year, 10 months ago

Selected Answer: B

MDE is not required for the DLP to manage.

upvoted 4 times

Jonclark 8 months, 4 weeks ago

Yes and no. I'm going with Answer A though.

Microsoft Defender for Endpoint and DLP for Endpoint are two separate features as more than one person pointed out in this discussion.

However;

"Device onboarding is shared across Microsoft 365 and Microsoft Defender for Endpoint (MDE). If you've already onboarded devices to MDE, they will appear in the managed devices list and no further steps are necessary to onboard those specific devices. Onboarding devices in Compliance center also onboards them into MDE."

https://learn.microsoft.com/en-us/microsoft-365/compliance/device-onboarding-overview?view=o365-worldwide

upvoted 1 times

nupagazi 1 year, 10 months ago

I think that Defender for endpoint focus on threats but not DLP. We need dlp for endpoint instead of Defender for endpoint

upvoted 3 times

Eltooth 2 years, 4 months ago

@JoeRoxy007 3 weeks, 2 days ago wrote:
https://docs.microsoft.com/en-us/microsoft-365/compliance/endpoint-dlp-getting-started?view=o365-worldwide
describes the conditions for this to work.
These conditions include that a device must be one of these :
• Azure Active Directory (Azure AD) joined
• Hybrid Azure AD joined
• AAD registered
AND enable device monitoring and onboard your endpoints before you can monitor and protect sensitive items on a device.

Both of these actions are done in the Microsoft 365 Compliance portal. However, device that have previously been onboarded into Microsoft Defender for Endpoint, will already appear in the managed devices list.

upvoted 4 times

Question #2 *Topic 2*

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

Community vote distribution
B (67%) A (33%)

ExamReviewerIZ Highly Voted 2 years, 1 month ago
Answer is C. To see the items (messages, emails, chat, files) that were blocked by DLP you see incidents. DLP incidents report allows to identify pieces of content, no matter how many DLP Policies applied to such item.

DLP Policies Repoet is used to identify how many policies were applied to one or many items. You could see a single email counted 100 times.
upvoted 7 times

ExamReviewerIZ 2 years, 1 month ago
Answer is B. Disregard my comment, indeed is DLP Policy Report, because we need to know how many emails were blocked by a specific policy.
upvoted 11 times

sergioandreslq 1 year, 11 months ago
The DLP policy matches report shows the count of DLP policy matches over time.
DLP Incidents: Like the policy matches report, the DLP incidents report shows policy matches over time, but in a different way - at the rule level. If an email matched three different rules, the DLP policy matches report shows three different line items. By contrast, the DLP incidents report shows matches at the item level: if an email matched three different rules, the incidents report shows a single line item for that item.

Summary:
Because the report counts are aggregated differently, the DLP policy matches report is better for identifying matches with specific rules and fine-tuning DLP policies. The DLP incidents report is better for identifying specific content causing issues with DLP policies.
upvoted 4 times

heshmat2022 Most Recent 1 month, 1 week ago
IT WAS ON EXAM OCTOBER 18 2023
upvoted 1 times

Gesbie 3 months, 3 weeks ago
was on Exam August 9, 2023
upvoted 1 times

heshmat2022 3 months, 2 weeks ago
YOU DID NOT MENTION WHAT WAS THE RIGHT ANSWER THOUGH.
upvoted 1 times

xswe 7 months, 3 weeks ago
The DLP Policy Matches in the DLP report in great when you want to see how many DLP policies that have been triggered. This part of the report will for example show you 3 policy triggers on one action if the action triggered 3 different DLP policies.
upvoted 2 times

wooyourdaddy 1 year, 5 months ago
Selected Answer: B
I wrote the exam today, this question was on it, I choose B, scored 890!
upvoted 4 times

LoNwUi2uprVHKCX9IlpE 1 year, 6 months ago
On exam 11/05/2022
upvoted 1 times

mT3 1 year, 7 months ago

Selected Answer: ^

Answer is C. https://docs.microsoft.com/en-us/microsoft-365/compliance/view-the-dlp-reports?view=o365-worldwide#view-the-reports-for-data-loss-prevention
"Because the report counts are aggregated differently, the policy matches report is better for identifying matches with specific rules and fine tuning DLP policies. The incidents report is better for identifying specific pieces of content that are problematic for your DLP policies."

upvoted 2 times

srchauhan 2 months, 1 week ago

ok, thank you

upvoted 1 times

Holii 1 year, 7 months ago

We aren't looking for specific pieces of content, we are looking for specific rules that are causing the violation.
We need "all messages on each DLP policy", keyword being "each DLP policy", I lean more towards B.

upvoted 2 times

AJ2021 1 year, 9 months ago

B is Correct: if an email matched three different rules, the policy matches report shows three different line items. By contrast, the incidents report shows matches at an item level; for example, if an email matched three different rules, the incidents report shows a single line item for that piece of content.

upvoted 2 times

Pravda 1 year, 10 months ago

On exam 1/20/2022

upvoted 2 times

Question #3 *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 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 Data Classification service inspection method and send alerts to Microsoft Power Automate.
Does this meet the goal?

A. Yes

B. No

Correct Answer: *B*
Reference:
https://docs.microsoft.com/en-us/cloud-app-security/dcs-inspection https://docs.microsoft.com/en-us/cloud-app-security/data-protection-policies

Community vote distribution

A (100%)

Anker Highly Voted 2 years, 5 months ago
Previous Answer should be No and this one should be Yes. You can't send messaged to the Teams channel with regular alerting method. You'd need to check the Power Automate box in the file policy. So I firmly believe this is Yes
upvoted 21 times

Eltooth Highly Voted 2 years, 6 months ago
You can use Power Automate to trigger an alert to send a message into a Teams channel.
upvoted 10 times

Eltooth 2 years, 5 months ago
Answer should be Yes
upvoted 8 times

mbhasker Most Recent 2 days, 20 hours ago
ans: No
upvoted 1 times

mbhasker 2 days, 20 hours ago
ans: B. No
upvoted 1 times

Gesbie 3 months, 3 weeks ago
was on Exam August 9, 2023
upvoted 1 times

xswe 7 months, 3 weeks ago
Microsoft Power Automate are needed to be able to get alerts sent to Microsoft Teams.
upvoted 3 times

NinjaSchoolProfessor 11 months, 1 week ago
Answer is Yes. The only option is to send an e-mail or send the alert to PowerAutomate. If using PowerAutomate you can then create a custom alert automation to notify users via Teams. https://learn.microsoft.com/en-us/defender-cloud-apps/flow-integration
upvoted 4 times

BTL_Happy 1 year ago
A should be the answer
upvoted 1 times

GGFiogos 1 year, 2 months ago
reference link is 404 for me
upvoted 1 times

NinjaSchoolProfessor 11 months, 1 week ago
There's a space between those two URLs, look again.

upvoted 1 times

Lion007 1 year, 3 months ago

Selected Answer: A

A (Yes) is the correct answer.

1- Select Data Classification Service, then from the Sensitive info type, select “Credit Card Number”

2- Select "Send alerts to Power Automate" and then select (or create a new) Microsoft Power Automate playbook that sends alerts to a specific Teams channel.

upvoted 4 times

wooyourdaddy 1 year, 5 months ago

Selected Answer: A

I wrote the exam today, this question was on it, I choose A, scored 890!

upvoted 3 times

JamesM9 1 year, 7 months ago

The answer here is A - Yes.

upvoted 1 times

ayush0312 1 year, 8 months ago

Yes is the correct ans

upvoted 1 times

crista_ 1 year, 8 months ago

Yes is correct answer

upvoted 2 times

PrettyFlyWifi 1 year, 10 months ago

I think this is "Yes". Check out point 7. and 8. here.... https://docs.microsoft.com/en-us/defender-cloud-apps/flow-integration#create-power-automate-playbooks-for-defender-for-cloud-apps

upvoted 5 times

Pravda 1 year, 10 months ago

On exam 1/20/2022

upvoted 1 times

Pravda 1 year, 10 months ago

Link is dead.

upvoted 1 times

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 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 Build-in DLP inspection method and send alerts to Microsoft Power Automate.
Does this meet the goal?

A. Yes

B. No

Correct Answer: *B*
Reference:
https://docs.microsoft.com/en-us/cloud-app-security/dcs-inspection https://docs.microsoft.com/en-us/cloud-app-security/data-protection-policies

Community vote distribution

B (85%) A (15%)

Val_0 Highly Voted 2 years, 5 months ago
I agree, this should be a "yes", because DLP inspection method can be applied to all files and can send results to P.A.
upvoted 21 times

luissaro Highly Voted 7 months, 2 weeks ago
Selected Answer: B
be careful lately it is B the answer: "Effective March 2023, we're retiring the built-in DLP content inspection engine. To ensure a smooth transition, we highly recommend that you begin transitioning your policies to the Data Classification Services (DCS) Content Inspection Engine. While the built-in DLP engine will continue to work, we strongly advise you to move your policies to the DCS engine to take advantage of its improved capabilities" in https://learn.microsoft.com/en-us/defender-cloud-apps/content-inspection-built-in
upvoted 11 times

mbhasker Most Recent 2 days, 20 hours ago
ans: NO
upvoted 1 times

heshmat2022 1 month, 1 week ago
IT WAS ON EXAM OCTOBER 18 2023
upvoted 1 times

dmoorthy 7 months, 1 week ago
Answer is B.
upvoted 1 times

xswe 7 months, 3 weeks ago
Microsoft Power Automate are needed to be able to get alerts sent to Microsoft Teams.
upvoted 1 times

wooyourdaddy 9 months, 1 week ago
The correct answer is true, however, this is likely an older question that will be replaced by question 3 in topic 2. As per this link:

https://learn.microsoft.com/en-us/defender-cloud-apps/content-inspection-built-in

which states:

Important

Effective March 2023, we're retiring the built-in DLP content inspection engine. To ensure a smooth transition, we highly recommend that you begin transitioning your policies to the Data Classification Services (DCS) Content Inspection Engine. While the built-in DLP engine will continue to work, we strongly advise you to move your policies to the DCS engine to take advantage of its improved capabilities.

Here's how to migrate:

Disable policies that include a content inspection condition with the built-in engine. This will ensure that all matched files remain unchanged until the specified transition date.

Create a new policy that includes the following two conditions:

A metadata condition with a "starting date" to avoid scanning all files from the start.
A content inspection condition using the DCS engine.

upvoted 2 times

Rockalm 11 months ago

Could somebody please shed some light? If it's A (Yes), but I don't get the point in the exam that doesn't really bring the effort.

upvoted 1 times

BTL_Happy 1 year ago

A (Yes) should be the answer.

upvoted 2 times

wooyourdaddy 1 year, 5 months ago

Selected Answer: A

I wrote the exam today, this question was on it, I choose A, scored 890!

upvoted 2 times

JamesM9 1 year, 7 months ago

The answer here is A - Yes.

upvoted 1 times

Pravda 1 year, 10 months ago

On exam 1/20/2022

upvoted 1 times

CalST 1 year, 11 months ago

File Policies in MCAS dont offer PowerAuotmate options which is needed to Teams Channel message. Session policies do so B is correct.

upvoted 1 times

CalST 1 year, 11 months ago

My bad - you can indeed.

upvoted 1 times

Zorolloo 1 year, 11 months ago

Question 4 and 26 are the same?

upvoted 1 times

Zorolloo 1 year, 11 months ago

Die Frage ist zwei mal drin. Einmal mit Yes und einmal mit No. Was ist denn nun richtig?

upvoted 1 times

CEAUSESCU247 1 year, 4 months ago

english bitte

upvoted 3 times

Eltooth 2 years, 5 months ago

Answer should be Yes

upvoted 7 times

Anker 2 years, 5 months ago

Why is this no? You can use built in DLP to look for Credit Card numbers and you would use Power Automate to get the alerts in the Teams channel.

upvoted 5 times

Question #5 *Topic 2*

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 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

Community vote distribution
CD (53%) CE (47%)

mcas Highly Voted 1 year, 1 month ago
Selected Answer: CE
with C, D alone users will not be prevented
the question says to "any cloud service" you can only achieve this if you put Contoso in the Allowed domain in DLP settings, so all other cloud services will be blocked
upvoted 7 times

Domza 3 weeks, 1 day ago
"any cloud service" it means - OneDrive, SharePoint that kind of services :)
upvoted 1 times

Azurefox79 9 months, 1 week ago
Incorrect. "from Firefox and Google Chrome to any cloud services." If those 2 are blocked then you just accomplished that. FROM the browsers is the key word. CD is correct. Devices must be onbaorded to EndPoint DLP or they will ignore anything you configure there.
upvoted 3 times

fimbulvetrk 1 year ago
agreed, I'd go with C and E
upvoted 2 times

Azurefox79 9 months, 1 week ago
C alone accomplishes the ask if the devices are onboarded. We don't have that information so we must assume we need to onboard them. EndPoint DLP does nothing if the EndPoint is not onboarded via local script, group policy, MdE or Intune/MEM.
upvoted 1 times

Azurefox79 Highly Voted 9 months, 1 week ago
Selected Answer: CD
CD is correct and clear. Spent a long time on this one. The question says prevent them from uploading to any cloud service VIA the Firefox and Chrome browsers. By blocking those browsers we achieve that. No additional actions needed there since the browsers are fully blocked for any sensitive files. Now, Edge is a managed browser and the only browser they can use with sensitivity labels. However, the devices wont honor Endpoint DLP on their own, they must be onbaorded. Therefore first you would onboard them and then you would block the 2 browsers. Dont believe all the comments here but do your own research and most importantly look at the wording.
upvoted 6 times

mbhasker Most Recent 2 days, 20 hours ago

ans: CD

upvoted 1 times

Domza 3 weeks, 1 day ago

It is in link provided below:
Once devices are onboarded into the Microsoft Purview solutions, the information about what users are doing with sensitive items is made visible in activity explorer. You can then enforce protective actions on those items via DLP policies.

CD - Enjoy !

upvoted 1 times

Tommytong 1 month, 2 weeks ago

Not a fan of the question since there should be three answers here technically.
C - block the browsers is given
E - allow only contoso because the wording says to block all other cloud services as someone else has mentioned
B- Can also be right because without creating a device location policy - I don't believe those settings get enforced without a policy created and targeted at the endpoint.

upvoted 1 times

ServerBrain 2 months ago

Selected Answer: CE

Users are already blocked from using Edge,
So block from using Firefox and Google Chrome
And to block from using any cloud services you have to allow only contoso.com

upvoted 1 times

Davidf 3 months, 3 weeks ago

Selected Answer: CD

another vote for CD, we need to onboard to endpoint DLP then we can block those browsers from accessing any files with labels applied to them and will be directed to edge to perform their actions. We are already blocking to the domain, so we don't need an allow to contoso.com

upvoted 1 times

cris_exam 5 months, 3 weeks ago

Selected Answer: CD

Clearly C is required to achieve the block but if devices are not onboarded it's not gonna work and even if it's mentioned if the devices are onboarded or no, since it gives the option within the answers, I say D.

Final answer: C and D.

upvoted 2 times

xswe 7 months, 3 weeks ago

To ensure that user cannot upload files from Firefox and Google Chrome and only use Microsoft Edge - Add Firefox and Chrome to the unallowed browser list in Endpoint DLP.

To ensure that this will get applied to all the users you are going to need to onboard all the devices, without the onboarding process the devices will not get the benefits from the configurations in the Endpoint DLP in Purview.

upvoted 2 times

UnDarisp 9 months, 2 weeks ago

The answer is A and C MS have this question on ESI and they say the answer is A and C

upvoted 1 times

Azurefox79 9 months, 1 week ago

No. A has nothing to do with the question at all. CD is correct.

upvoted 1 times

Harry008 1 year ago

When you select Devices as a location in a properly configured DLP policy and use the Microsoft Edge browser, the unallowed browsers that you've defined in these settings will be prevented from accessing the sensitive items that match your DLP policy controls
Answer B and C

upvoted 2 times

Azurefox79 9 months, 1 week ago

B has nothing to do with the question. This is EndPoint DLP settings in Purview. You don't need any policy, they are built in to allow you to block an unapproved browser.

upvoted 1 times

BTL_Happy 1 year ago

I will go with C & E

upvoted 2 times

HOTSPOT -

You have a Microsoft 365 tenant that uses Microsoft Teams.

You create a data loss prevention (DLP) policy to prevent Microsoft Teams users from sharing sensitive information.

You need to identify which locations must be selected to meet the following requirements:

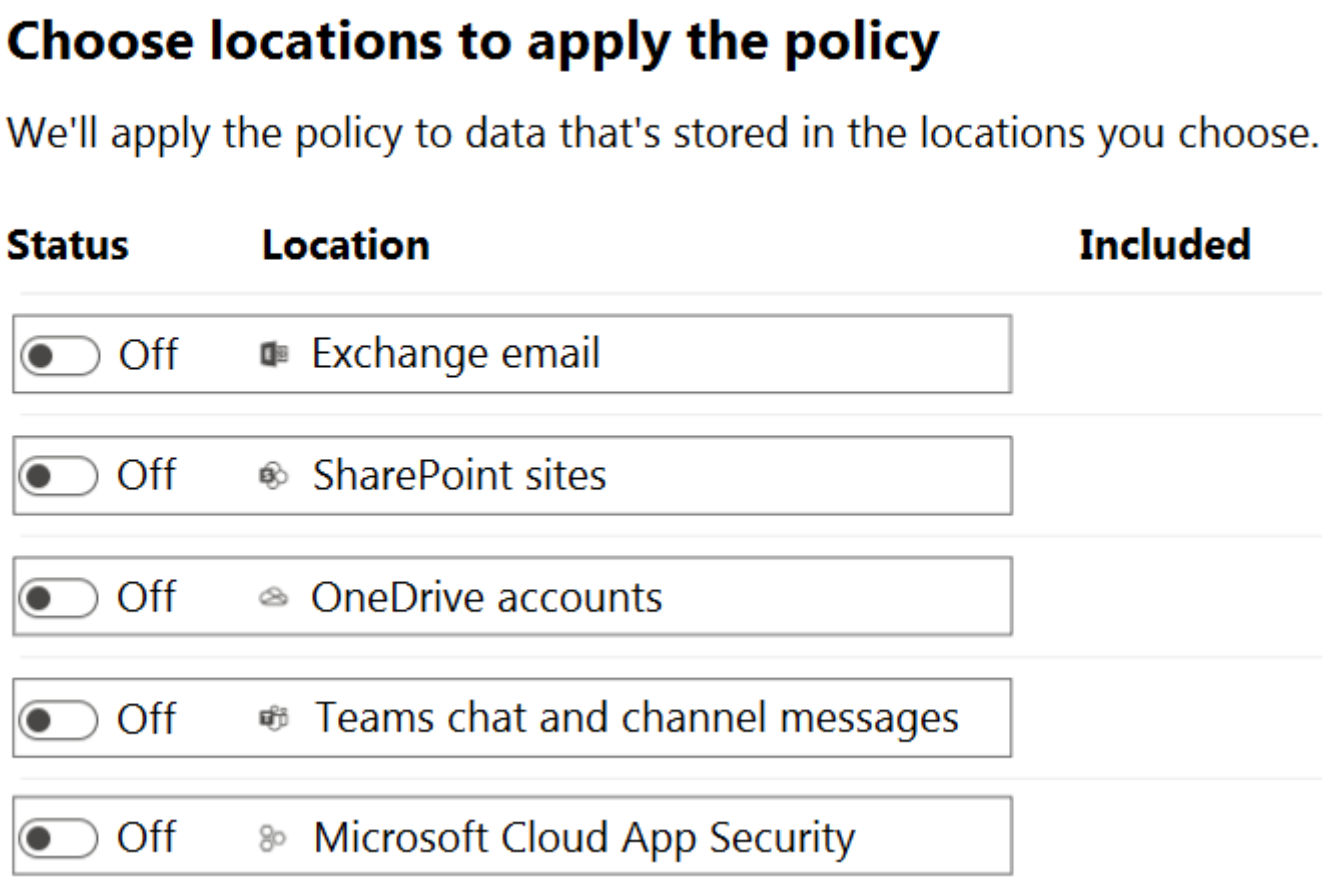
- Documents that contain sensitive information must not be shared inappropriately in Microsoft Teams.
- If a user attempts to share sensitive information during a Microsoft Teams chat session, the message must be deleted immediately.

Which three locations should you select? To answer, select the appropriate locations in the answer area. (Choose three.)

NOTE: Each correct selection is worth one point.

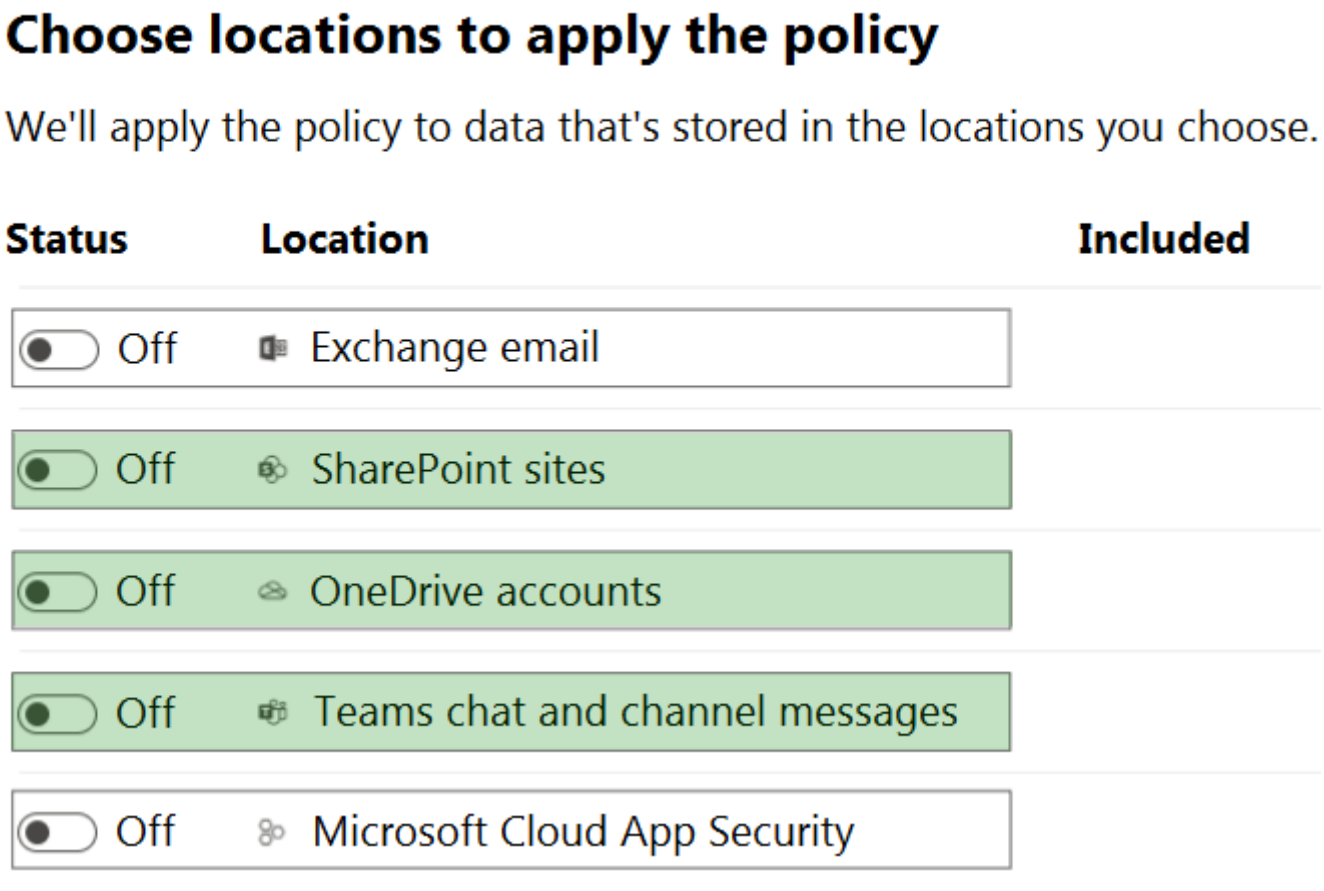
Hot Area:

Answer Area



Answer Area

Correct Answer:



Reference:

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

Eltooth Highly Voted 2 years, 5 months ago

Teams chat sharing 1-2-1 uses ODfB.
Teams channel uses Sharepoint

Teams channels and chat also needs policy applied
upvoted 16 times

JakubK64 Highly Voted 2 years, 5 months ago
Looks correct. Teams use SharePoint and OneDrive to store files
upvoted 7 times

heshmat2022 Most Recent 1 month, 1 week ago
IT WAS ON EXAM OCTOBER 18 2023
upvoted 1 times

xswe 7 months, 3 weeks ago
Since we want a DLP policy to prevent sharing of sensitive information in Teams and we are going to choose betweeen 3 location we should deploy the policy in the following locations:
Sharepoint (Channels)
Onedrive (Chats)
Teams chat and channel messages
upvoted 2 times

wooyourdaddy 1 year, 5 months ago
I wrote the exam today, this question was on it, I choose Box1: SharePoint sites, Box2: OneDrive accounts, Box3: Team chat and channel messages, scored 890!
upvoted 2 times

PrettyFlyWifi 1 year, 10 months ago
Correct. OneDrive also, "Private chat files are stored in the sender's OneDrive folder, and permissions are automatically granted to all participants as part of the file sharing process." See... https://docs.microsoft.com/en-us/microsoftteams/sharepoint-onedrive-interact
upvoted 1 times

Pravda 1 year, 10 months ago
On exam 1/20/2022
upvoted 1 times

HardcodedCloud 1 year, 11 months ago
If you want to make sure documents that contain sensitive information are not shared inappropriately in Teams, make sure SharePoint sites and OneDrive accounts are turned on, along with Teams chat and channel messages.
upvoted 2 times

NickTheo 2 years, 1 month ago
I think that we should include and MACS because only there is the option delete message available
upvoted 1 times

xofowi5140 2 years, 4 months ago
Why not Exchange email?
upvoted 1 times

HOTSPOT -

You have a data loss prevention (DLP) policy that has the advanced DLP rules shown in the following table.

Name	Priority	Actions
Rule1	0	• Notify users with email and policy tips • User overrides: Off
Rule2	1	• Notify users with email and policy tips • Restrict access to the content • User overrides: Off
Rule3	2	• Notify users with email and policy tips • Restrict access to the content • User overrides: On
Rule4	3	• Notify users with email and policy tips • Restrict access to the content • User overrides: Off

You need to identify which rules will apply when content matches multiple advanced DLP rules.

Which rules 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

If content matches Rule1, Rule2, and Rule3:

- Only Rule1 takes effect
- Only Rule2 takes effect
- Only Rule3 takes effect
- Rule1, Rule2, and Rule3 take effect

If content matches Rule2, Rule3, and Rule4:

- Only Rule2 takes effect
- Only Rule3 takes effect
- Only Rule4 takes effect
- Only Rule2 and Rule4 take effect
- Rule2, Rule3, and Rule4 take effect

Correct Answer:

Answer Area

If content matches Rule1, Rule2, and Rule3:

- Only Rule1 takes effect
- Only Rule2 takes effect
- Only Rule3 takes effect
- Rule1, Rule2, and Rule3 take effect

If content matches Rule2, Rule3, and Rule4:

- Only Rule2 takes effect
- Only Rule3 takes effect
- Only Rule4 takes effect
- Only Rule2 and Rule4 take effect
- Rule2, Rule3, and Rule4 take effect

Reference:

https://docs.microsoft.com/en-us/microsoft-365/compliance/data-loss-prevention-policies?view=o365-worldwide

JakubK64 Highly Voted 2 years, 5 months ago

Looks correct. DLP rules take effect in order of priority and beeing most restrictive. In first case rule 2 is most restrictive, in second case rule 2 is as restrictive as 4, but have lower priority number

upvoted 16 times

sergioandreslq 1 year, 11 months ago

DLP priority
When you have more than one DLP policy, it is important to prioritize policies with more restrictions above than less restrictive actions
To confiture DLP for policy precedence it is important that each one of those policies will have a numerical value which means the lower the value is, the higher priority.

1. The rules of DLP policy with the lowest order/priority number are processed first.
2. You need to set the priority number as “0” to set the highest priority

upvoted 3 times

sergioandreslq 1 year, 11 months ago

When content is evaluated against rules, the rules are processed in priority order. If content matches multiple rules, the first rule evaluated that has the most restrictive action is enforced. For example, if content matches all of the following rules, Rule 3 is enforced because it's the highest priority, most restrictive rule:

Rule 1: only notifies users
Rule 2: notifies users, restricts access, and allows user overrides
Rule 3: notifies users, restricts access, and does not allow user overrides
Rule 4: restricts access

Rules 1, 2, and 4 would be evaluated, but not applied. In this example, matches for all of the rules are recorded in the audit logs and shown in the DLP reports, even though only the most restrictive rule is applied.
Reference:
https://docs.microsoft.com/en-us/microsoft-365/compliance/dlp-policy-reference?view=o365-worldwide#hosted-service-workloads

upvoted 1 times

McAlec Highly Voted 2 years ago

Correct, but right reference is
https://docs.microsoft.com/en-us/microsoft-365/compliance/dlp-policy-reference?view=o365-worldwide

upvoted 5 times

xswe Most Recent 7 months, 3 weeks ago

When you have several DLP policies that applied when all of them matches the rules the most restrictive DLP policy with the highest priority will get applied, pretty understandeble.

Rule2 will take place since it has the higher restrictions out of all of them - User Overrides ON is less restrictive than having it OFF.
Rule2, both Rule2 and Rule4 have the same restrictivness so we have to look at the priority level here which means Rule2 gets applied.

upvoted 3 times

Pravda 1 year, 10 months ago

On exam 1/20/2022

upvoted 2 times

Question #8 *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 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 Endpoint DLP configuration package to the computers.
Does this meet the goal?

A. Yes

B. No

Correct Answer: *A*
Reference:
https://docs.microsoft.com/en-us/microsoft-365/compliance/endpoint-dlp-getting-started?view=o365-worldwide
https://docs.microsoft.com/en-us/microsoft-365/security/defender-endpoint/configure-endpoints?view=o365-worldwide

GY23 Highly Voted 2 years, 2 months ago
@Eltooth, to onboard the machine to Compliance center (as you mentioned in your comment), you need to install the Endpoint DLP package on the device. Only after that it will be onboarded to Compliance Center, you missed this part.
Defender for Endpoint has nothing to do with this question.
In normal scenarios, if and only if the Defender for Endpoint was ALREADY onboarded on the device, then it would be a plus and it would appear automatically in Endpoint DLP dashboard. So no package will be required on the device anymore.

Answer is Yes.
upvoted 13 times

sergioandreslq 1 year, 11 months ago
we need to assume that the Windows Defender for an endpoint is not present on the endpoint as the question doesn't mention it, meaning, we need to run the "Endpoint DLP configuration package" to begin receiving data from endpoints.
https://docs.microsoft.com/en-us/microsoft-365/compliance/device-onboarding-script?view=o365-worldwide
upvoted 3 times

Eltooth Highly Voted 2 years, 4 months ago
No - the machines need to be on boarded into either Compliance Centre or at a minimum have been on boarded withDefender for EndPoint and enabled through Compliance Centre Manager.

https://docs.microsoft.com/en-us/microsoft-365/compliance/endpoint-dlp-getting-started?view=o365-worldwide#onboarding-devices-into-device-management

https://docs.microsoft.com/en-us/microsoft-365/compliance/endpoint-dlp-learn-about?view=o365-worldwide
upvoted 6 times

bowlinbd 2 years, 3 months ago
Should be Yes. Deploying the package is what onboards the devices into the Compliance portal.
upvoted 13 times

kiketxu 1 year, 1 month ago
You right, thanks.
You must enable device monitoring first and second onboard your endpoints before you can monitor. Both of these actions are done in the Microsoft Purview compliance portal. With the package you have the second but you need to complete first too.
https://learn.microsoft.com/en-us/microsoft-365/compliance/device-onboarding-overview?view=o365-worldwide#onboarding-windows-10-or-windows-11-devices
upvoted 1 times

xswe Most Recent 7 months, 3 weeks ago
The DLP configuration packet will onboard the computers which is what we are looking for here to ensure that Endpoint DLP will protect the computers
upvoted 1 times

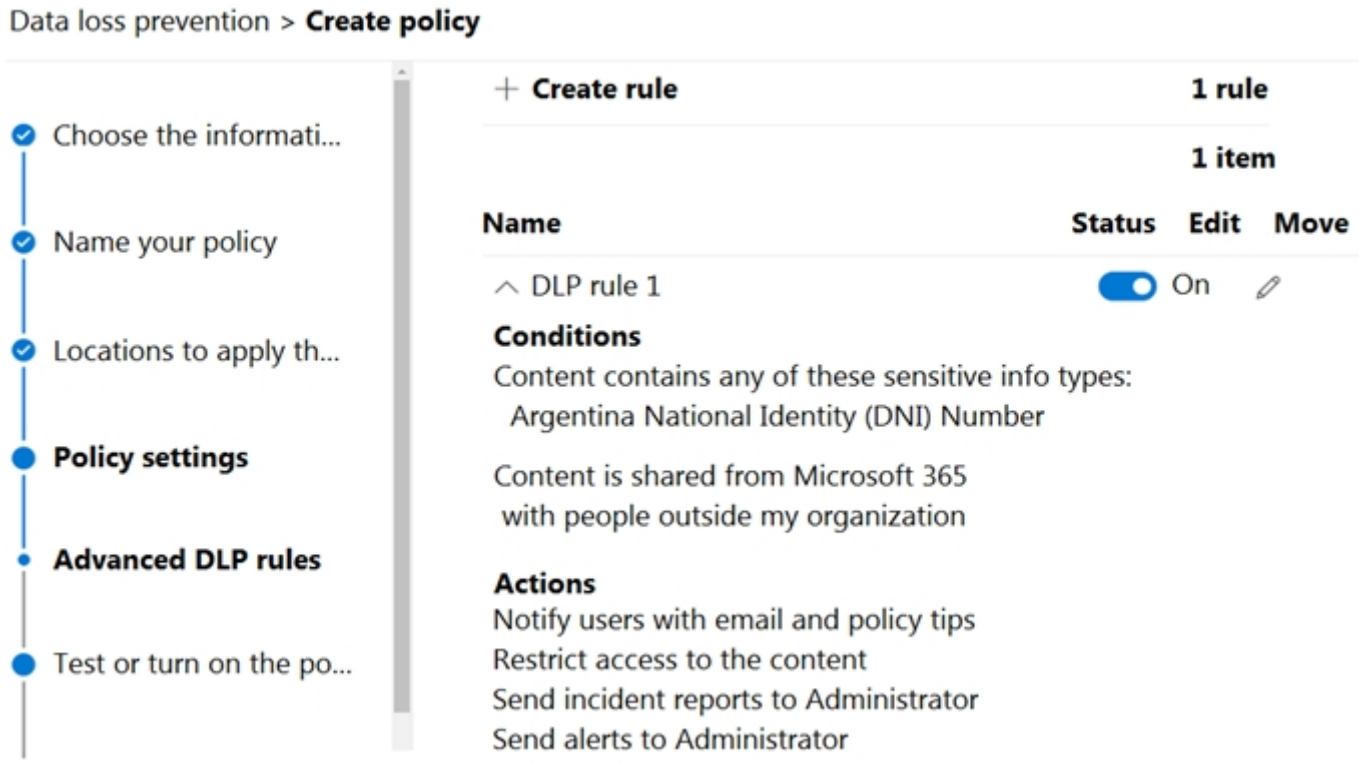
NinjaSchoolProfessor 11 months, 1 week ago
Answer [A] - The reference to deploying the Endpoint DLP configuration package implies that you're installing all required agents to communicate to M365 defender / Purview Compliance Center. https://learn.microsoft.com/en-us/microsoft-365/compliance/endpoint-dlp-getting-started?view=o365-worldwide#windows-10-and-windows-11-onboarding-procedures
upvoted 2 times

PrettyFlyWifi 1 year, 10 months ago

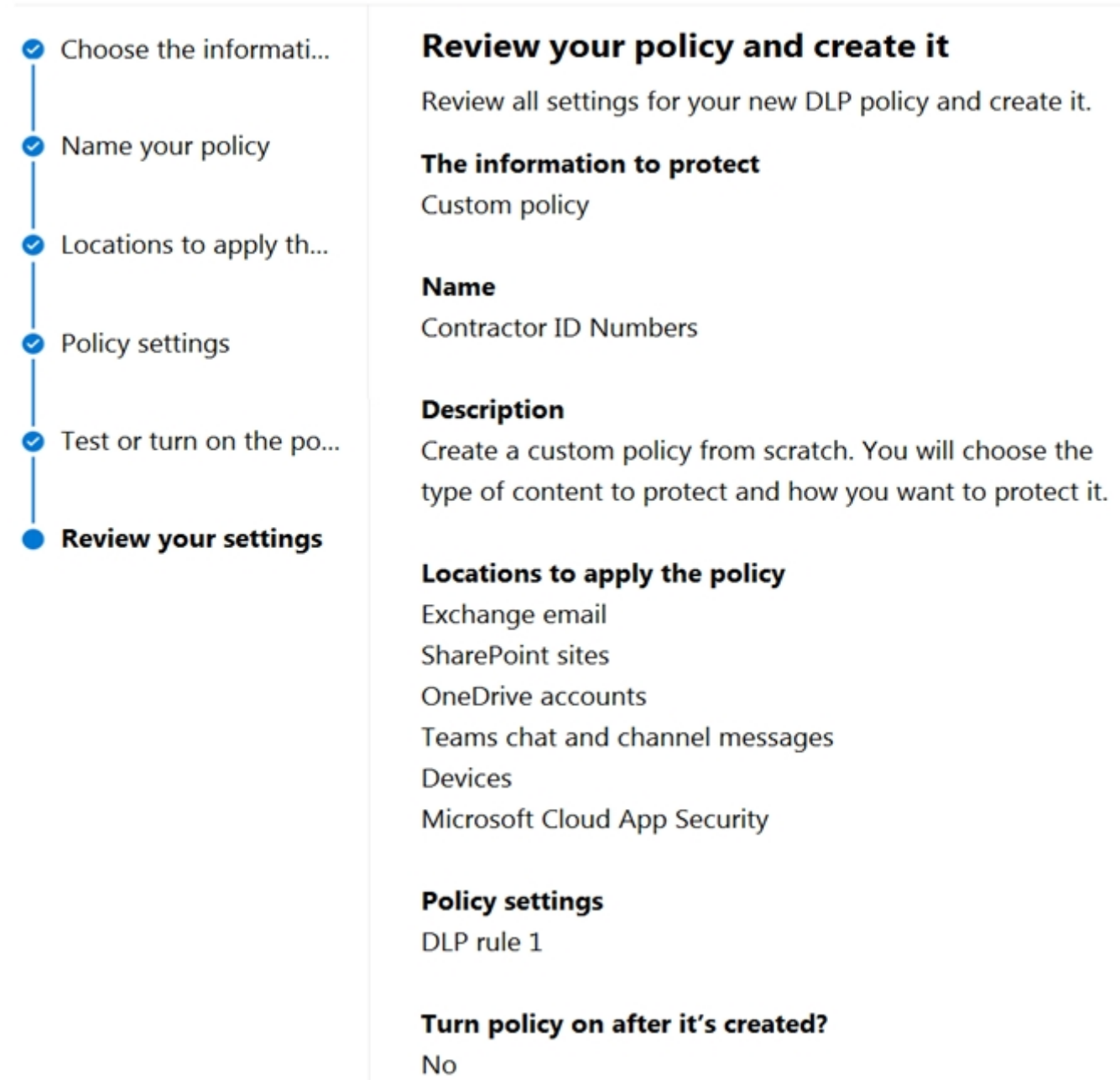
This seems like it should be Yes... https://docs.microsoft.com/en-us/microsoft-365/compliance/endpoint-dlp-getting-started?view=o365-worldwide#windows-10-and-windows-11-onboarding-procedures

upvoted 3 times

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 DLP 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. Edit 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.

Correct Answer: *D*

Reference:

https://docs.microsoft.com/en-us/microsoft-365/compliance/create-a-dlp-policy-from-a-template?view=o365-worldwide

Community vote distribution

D (100%)

fdifo Highly Voted 1 year, 10 months ago

Selected Answer: D

d is right

upvoted 7 times

Domza Most Recent 3 weeks, 1 day ago

Correct -D

upvoted 1 times

ServerBrain 2 months ago

Selected Answer: D

do is the only option that is closer to audit mode

upvoted 1 times

xswe 7 months, 3 weeks ago

Edit the policy and in the last step change it to "test it out" so that you can see the potential impact of the policy. This is the best practice when you are deploying new policies since they can encrypt everything in your network if you do it incorrectly.

upvoted 1 times

NinjaSchoolProfessor 11 months, 1 week ago

Answer [D] - https://learn.microsoft.com/en-us/microsoft-365/compliance/create-test-tune-dlp-policy

upvoted 1 times

Marzie 1 year ago

I liked the look of C too! Do that and then look at DLP policy matches and you've met the objective?

upvoted 1 times

Domza 3 weeks, 1 day ago

IF you remove the "Actions" nothing will happen lol

upvoted 1 times

wooyourdaddy 1 year, 5 months ago

Selected Answer: D

I wrote the exam today, this question was on it, I choose D, scored 890!

upvoted 1 times

Eltooth 2 years, 4 months ago

Correct answer is D

upvoted 4 times

sergioandreslq 1 year, 11 months ago

Agreed, test mode without any tips to end-users will just collect data from real live data and report it to the compliance admin center without any impact on the tenant. it is just to collect data

upvoted 1 times

JakubK64 2 years, 5 months ago

Looks correct

upvoted 1 times

Question #10 *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 keys in plain text to third parties.
You need to ensure that when Azure Storage keys are emailed, the emails are encrypted.
Solution: You configure a mail flow rule that matches a sensitive info type.
Does this meet the goal?

A. Yes

B. No

Correct Answer: *A*

Community vote distribution

A (100%)

PrettyFlyWifi Highly Voted 1 year, 9 months ago

Selected Answer: A

Within the mail flow options, you choose "the message..." , then choose 'contains any of theses sensitive info types', then you can add Azure storage account keys into it. "Yes" is the correct answer here.

upvoted 7 times

luissaro Most Recent 7 months, 2 weeks ago

shouldn't you first set the ome config?

upvoted 1 times

xswe 7 months, 3 weeks ago

To be able to enrypt messages sent through Exchange you should either create a mail flow rule in Exchange Admin center or DLP policy. The sensitive info type will be able to detect the Azure Storage keys which are binaries.

upvoted 3 times

Pravda 1 year, 10 months ago

On exam 1/20/2022

upvoted 1 times

digitallycan 2 years, 1 month ago

You can set up mail flow rules in Exchange Online or by using DLP in the MS365 Compliance Center to automatically encrypt messages.
https://docs.microsoft.com/en-us/microsoft-365/compliance/ome-faq?view=o365-worldwide#can-i-automatically-encrypt-messages-by-setting-up-policies-in-data-loss-prevention--dlp--through-the-microsoft-365-compliance-center-

upvoted 2 times

sergioandreslq 1 year, 11 months ago

the questions is tricky, there is not any reference that you can create EXO mail flow rule to encrypt a message using "Sensitive info Types" that comes from the M365 compliance center.
There is information to match "Sensitive Information Type" but I don't think this is the same object coming from "Sensitive info type". for me is a guess based on Sensitive info type== Sensitive Information Type from EXO.

upvoted 2 times

sergioandreslq 1 year, 11 months ago

After read more, I conclude that:
Sensitive info type== Sensitive Information Type from EXO.
So, the answer is YES

upvoted 3 times

Eltooth 2 years, 4 months ago

Correct.

https://docs.microsoft.com/en-us/exchange/security-and-compliance/data-loss-prevention/integrate-sensitive-information-rules#sensitive-information-rules-within-the-mail-flow-rule-framework

upvoted 2 times

Eltooth 2 years, 4 months ago

https://docs.microsoft.com/en-us/exchange/security-and-compliance/mail-flow-rules/mail-flow-rule-actions#actions-for-mail-flow-rules-in-exchange-online

upvoted 1 times

Question #11 *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 keys in plain text to third parties.
You need to ensure that when Azure Storage keys are emailed, the emails are encrypted.
Solution: You create a data loss prevention (DLP) policy that has all locations selected.
Does this meet the goal?

A. Yes

B. No

Correct Answer: *B*

Community vote distribution

B (71%) A (29%)

Eltooth Highly Voted 2 years, 4 months ago
Correct - no. Mail flow rules are needed.
upvoted 7 times

ExamReviewerIZ 2 years, 1 month ago
Incorrect. You can also create a DLP Policy choosing Exchange Online or all locations and the email will be encrypted if sensitive information is detected.

If you do it through Exchange Online - MailFlow Rules, it only applies to email.

Mailflow Rule is not a requirement.
upvoted 11 times

Sam12 1 year, 10 months ago
I just tested this, in compliance portal choose only exchange on the dlp policy an you will be able to ecrypt sensitive content
upvoted 5 times

BieLey 1 year, 8 months ago
But not if you have "all locations" selected.
upvoted 7 times

Lion007 1 year, 3 months ago
in DLP Policy, if you try to apply the message encryption, you will get this error: ("Validation failed Conditions/exceptions/actions on existing rules cannot apply on new locations. Please remove the unsupported conditions/exceptions/actions ' Encrypt email messages (applies only to content in Exchange)' on those rules and add the new locations."). So not to "all locations". But I tested it and it worked like a charm when selecting only "Exchange email" is the ONLY location.
upvoted 5 times

nupagazi Highly Voted 1 year, 10 months ago
No is correct, if you select all location (devices, on-premise), then the action of DLP rule does not have option encrypt content
upvoted 5 times

ServerBrain Most Recent 2 months ago
Selected Answer: B
selecting all locations will not suffice
upvoted 1 times

xswe 7 months, 3 weeks ago
If you deploy a DLP policy with all the location you wont be able to do much for the emails that are getting sent. You need to have only "Exchange" as the location to see all the options that are needed to achieve this.
upvoted 1 times

music_man 1 year, 2 months ago
Selected Answer: B
Answer is correct. If you select more than just Exchange as a location then the action to encrypt is removed. Must be Exchange only to see the encrypt action.
upvoted 2 times

Lion007 1 year, 3 months ago

Selected Answer: B

Given answer is Correct (B). In DLP Policy, if you try to apply the message encryption, you will get this error: ("Validation failed Conditions/exceptions/actions on existing rules cannot apply on new locations. Please remove the unsupported conditions/exceptions/actions ' Encrypt email messages (applies only to content in Exchange)' on those rules and add the new locations."). So not to "all locations". But I tested it and it worked like a charm when selecting only "Exchange email" is the ONLY location.

upvoted 2 times

PrettyFlyWifi 1 year, 10 months ago

No looks correct. Key part of the question.... "that has all locations selected". This question is specifically referring to Exchange Online and email only.

upvoted 5 times

Pravda 1 year, 10 months ago

On exam 1/20/2022

upvoted 2 times

Sam12 1 year, 10 months ago

you can use both portals to achieve this, but if "all locations selected." then there is no action to encrypt email. so, the answer is NO. Either you create it via transport rule, of if you use DLP portal you must choose to apply policy only to exchange.

upvoted 3 times

nupagazi 1 year, 10 months ago

I don't find the action encrypt message in DLP polic

upvoted 1 times

RAMmulator 1 year, 11 months ago

Selected Answer: A

I believe its A. See https://docs.microsoft.com/en-us/microsoft-365/compliance/ome-faq?view=o365-worldwide#can-i-automatically-encrypt-messages-by-setting-up-policies-in-data-loss-prevention--dlp--through-the-microsoft-365-compliance-center- "Yes! You can set up mail flow rules in Exchange Online or by using DLP in the Microsoft 365 compliance center."

upvoted 2 times

CalST 1 year, 11 months ago

DLP restricts the sending of the email as well as encrypting. The question just says the message must be encrypted (not blocked) so Mail Flow Rule

upvoted 2 times

digitallycan 2 years, 1 month ago

You can set up mail flow rules in Exchange Online or by using DLP in the MS365 Compliance Center to automatically encrypt messages. https://docs.microsoft.com/en-us/microsoft-365/compliance/ome-faq?view=o365-worldwide#can-i-automatically-encrypt-messages-by-setting-up-policies-in-data-loss-prevention--dlp--through-the-microsoft-365-compliance-center-

upvoted 1 times

Question #12 *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 keys in plain text to third parties.
You need to ensure that when Azure Storage 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

Correct Answer: *B*

Community vote distribution

A (75%) B (25%)

bgurny 2 months, 3 weeks ago

Selected Answer: A

https://learn.microsoft.com/en-us/purview/ome-faq?view=o365-worldwide#can-i-automatically-encrypt-messages-by-setting-up-policies-in-data-loss-prevention--dlp--through-the-microsoft-purview-compliance-portal-

upvoted 1 times

dmoorthy 7 months, 1 week ago

Answer is A- Yes.

upvoted 1 times

xswe 7 months, 3 weeks ago

Correct! With this solution you will be able to create a rule just like you can do in Exchange admin center

upvoted 1 times

formazionehs 9 months, 1 week ago

Selected Answer: A

Since Exchange is the only location selected, it is possible to meet the goal with a DLP policy.

upvoted 2 times

biff791 10 months, 1 week ago

Selected Answer: A

works if only exchange location is selected

upvoted 1 times

Harry008 1 year ago

Can I automatically encrypt messages by setting up policies in Data Loss Prevention (DLP) through the Microsoft Purview compliance portal?
Yes! You can set up mail flow rules in Exchange Online or by using DLP in the Microsoft Purview compliance portal.
Answer is A(Yes)

upvoted 3 times

BTL_Happy 1 year ago

A should be the answer, only on exchange location is selected.

upvoted 1 times

kiketxu 1 year, 1 month ago

If the question asks for meeting the goal, I see there is something missing. It is OK if you select only Exchange location. It will allow to encrypt messages mathing conditions, but what matches???
...to match Azure-Storage keys, you need to create regex to add in rule as sensitivity info. that is why I would opt to NO. The answer isnt' complete.

upvoted 1 times

Reinto 9 months, 3 weeks ago

You can create a custom DLP policy that matches a pattern in a document (or subject or body). So, I guess we agree that the answer is complete: A

upvoted 1 times

Reinto 9 months, 3 weeks ago

Never mind: Document does not equal attachment and this rule option is not relevant, I suspect.

upvoted 1 times

fimbulvetrk 1 year ago

you may have a sensitive info type based in a keyword list which may have contain all the storage keys

upvoted 1 times

chrissempai 1 year, 2 months ago

Selected Answer: A

The answer is A
you have only exchange selected

upvoted 1 times

Lion007 1 year, 3 months ago

Selected Answer: B

Given answer is Correct (B). In DLP Policy, if you try to apply the message encryption, you will get this error: ("Validation failed: Conditions/exceptions/actions on existing rules cannot apply on new locations. Please remove the unsupported conditions/exceptions/actions ' Encrypt email messages (applies only to content in Exchange)' on those rules and add the new locations."). So not to "all locations". But I tested it and it worked like a charm when selecting only "Exchange email" is the ONLY location.

upvoted 2 times

cwilson91 1 year, 2 months ago

This question IS asking when you select the Exchange email location only.. not All Locations (thats topic 4 question 11).. so answer should be A, Yes.

upvoted 4 times

Lion007 1 year, 3 months ago

So I'd go for A in real life, but hey this exam is in love with "mail flow rules"... so I'd stick with B for the exam.

upvoted 1 times

UWSFish 1 year, 9 months ago

Just set it up in DLP in my tenant. 100% yes

upvoted 4 times

PrettyFlyWifi 1 year, 9 months ago

Did the same, also tested in tenant and DLP also is a valid solution. So BOTH mail flow rule AND DLP policy can be used to meet this. Answer is YES.

upvoted 2 times

Pravda 1 year, 10 months ago

On exam 1/20/2022

upvoted 1 times

RAMmulator 1 year, 11 months ago

Selected Answer: A

See: https://docs.microsoft.com/en-us/microsoft-365/compliance/ome-faq?view=o365-worldwide#can-i-automatically-encrypt-messages-by-setting-up-policies-in-data-loss-prevention--dlp--through-the-microsoft-365-compliance-center-

upvoted 1 times

CalST 1 year, 11 months ago

DLP restricts the sending of the email as well as encrypting. The question just says the message must be encrypted (not blocked) so Mail Flow Rule

upvoted 2 times

ServerBrain 2 months ago

if you say so.
but Mail Flow Rule is more specific

upvoted 1 times

Holii 1 year, 7 months ago

DLP Policy provides an "Encrypt email messages (applies only to content in Exchange)" [not blocked]

upvoted 1 times

digitallycan 2 years, 1 month ago

You can set up mail flow rules in Exchange Online or by using DLP in the MS365 Compliance Center to automatically encrypt messages.
https://docs.microsoft.com/en-us/microsoft-365/compliance/ome-faq?view=o365-worldwide#can-i-automatically-encrypt-messages-by-setting-up-policies-in-data-loss-prevention--dlp--through-the-microsoft-365-compliance-center-

upvoted 1 times

klosedotorg83 2 years, 1 month ago

I think the answer is Correct (No) because creating a DLP policy that has only the Exchange email location selected could be part of the solution but it's not a complete solution. So creating a transport rule to encrypt those emails is a better/complete solution

upvoted 3 times

ExamReviewerIZ 2 years, 1 month ago

Answer is YES for all three questions. Mailflow Rules in Exchange Admin Center and DLP Policies in the Security Center, both can achieve the same, Encrypt emails based on sensitive information types detected in the message body.

upvoted 4 times

ExamReviewerIZ 2 years, 1 month ago

Also, MailFlow Rules in Exchange Admin Center BASED ON SENSITIVE TYPES are being deprecated, so in the near future the only option to Encrypt Emails based on Sensitive Types detected in a message will be through DLP Policies.

upvoted 2 times

rk4ai 2 years, 2 months ago

All three in the series should be Yes.

upvoted 2 times

Question #13 *Topic 2*

You are creating an advanced data loss prevention (DLP) rule in a DLP policy named Policy1 that will have all locations selected.
Which two conditions can you use in the rule? Each correct answer presents a complete solution. (Choose two.)
NOTE: Each correct selection is worth one point.

A. Content contains

B. Content is shared from Microsoft 365

C. Document size equals or is greater than

D. Attachment's file extension is

E. Document property is

Correct Answer: *AB*

Community vote distribution

AB (100%)

Val_0 Highly Voted 2 years, 4 months ago
This is only true if "Devices" and "On-premises repositories" are not selected as part of "Location". If they are, then only "Content Contains" is available.
upvoted 13 times

PrettyFlyWifi 1 year, 10 months ago
Almost correct here. You can select on-prem respositories and still get 2 options. Devices and Power BI selected mean you only get 1 option.
upvoted 1 times

nupagazi 1 year, 10 months ago
totally agree
upvoted 1 times

pheb 2 years, 3 months ago
this is wrong: you can select both, but you can not create a rule that includes "shared from M365" only. The questions is which two conditions you can choose, so the answer is correct.
upvoted 2 times

ServerBrain Most Recent 2 months ago
Selected Answer: AB
as these are your locations:

Microsoft 365 services such as Teams, Exchange, SharePoint, and OneDrive accounts
Office applications such as Word, Excel, and PowerPoint
Windows 10, Windows 11, and macOS (three latest released versions) endpoints
non-Microsoft cloud apps
on-premises file shares and on-premises SharePoint
Power BI
upvoted 1 times

xswe 7 months, 3 weeks ago
You have to try this out to remember this better imo, when you create a DLP policy with all the location choosed you can only choose the following conditions
- Content contains
- Content is shared from M365
upvoted 3 times

fimbulvetrk 1 year ago
Power BI option is currently in preview I guess, so it's no being considered in the available options. On-premises repositories can't be selected if you selected all other options, so, if you proceed this way (selecting everything but on-prem repo and PBI), the only available option is "Content Contains".
upvoted 2 times

chrissempai 1 year, 2 months ago
Selected Answer: AB
A and B
tested in test environnement
upvoted 3 times

wooyourdaddy 1 year, 5 months ago

Selected Answer: AB

I wrote the exam today, this question was on it, I choose AB, scored 890!

upvoted 1 times

PrettyFlyWifi 1 year, 10 months ago

Definitely A and B ... BUT ... you cannot have absolutely all locations selected as you only get "content contains". If you de-select "Devices" and "Power BI", then 2 options appear and these are as per the answer. IF you include all locations you only get 1 option. This must be an old question. Tested this in test tenant.

upvoted 4 times

sergioandreslq 1 year, 11 months ago

I got the condition option when I choose locations: EXO, SPO, ODfB and Teams.
If I choose all the locations, the only option to be used as the condition is "Sensitive Info Type".
The question is not correct, however, If I have to select an answer, I will go with AB

upvoted 3 times

pheb 2 years, 3 months ago

this is wrong: you can select both, but you can not create a rule that includes "shared from M365" only. The questions is which two conditions you can choose, so the answer is correct.

upvoted 1 times

JakubK64 2 years, 5 months ago

Correct

upvoted 2 times

Question #14 *Topic 2*

You need to provide a user with the ability to view data loss prevention (DLP) alerts in the Microsoft 365 compliance center. The solution must use the principle of least privilege.
Which role should you assign to the user?

A. Compliance data administrator

B. Security operator

C. Compliance administrator

D. Security reader

Correct Answer: *D*
Reference:
https://docs.microsoft.com/en-us/microsoft-365/compliance/dlp-configure-view-alerts-policies?view=o365-worldwide

Community vote distribution

D (100%)

Ali_557 Highly Voted 1 year, 11 months ago
Roles

If you want to view the DLP alert management dashboard or to edit the alert configuration options in a DLP policy, you must be a member of one of these role groups:

Compliance Administrator
Compliance Data Administrator
Security Administrator
Security Operator
Security Reader

To access the DLP alert management dashboard, you need the Manage alerts role and either of the following roles:

DLP Compliance Management
View-Only DLP Compliance Management
upvoted 6 times

JakubK64 Highly Voted 2 years, 5 months ago
Correct
upvoted 5 times

xswe Most Recent 7 months, 3 weeks ago
The least privileged role that can be used for reports in general are Security reader
upvoted 3 times

wooyourdaddy 1 year, 5 months ago
Selected Answer: D
I wrote the exam today, this question was on it, I choose D, scored 890!
upvoted 1 times

PrettyFlyWifi 1 year, 10 months ago
Correct, Security Reader is correct. https://docs.microsoft.com/en-us/microsoft-365/compliance/dlp-configure-view-alerts-policies?view=o365-worldwide#roles
upvoted 3 times

HardcodedCloud 1 year, 11 months ago
f you want to view the DLP alert management dashboard or to edit the alert configuration options in a DLP policy, you must be a member of one of these role groups:

Compliance Administrator
Compliance Data Administrator
Security Administrator
Security Operator
Security Reader
upvoted 2 times

Eltooth 2 years, 4 months ago

Correct - security reader is least privilege role that can read DLP reports.

upvoted 5 times

Question #15 *Topic 2*

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 Microsoft 365 compliance center, start a data investigation.

C. From the Microsoft 365 compliance center, create an insider risk policy.

D. From the Cloud App Security portal, create an activity policy.

Correct Answer: *A*

With a DLP policy, you can identify, monitor, and automatically protect sensitive items.

Note:

There are several versions of this question in the exam. The question has two possible correct answers:

1. From the Microsoft 365 compliance center, create a data loss prevention (DLP) policy.

2. From the Cloud App Security portal, create a file policy.

Other incorrect answer options you may see on the exam include the following:

☞ From the Exchange admin center, create a data loss prevention (DLP) policy.

☞ From the Microsoft 365 compliance center, create an insider risk policy.

☞ From the Azure portal, create an Azure Information Protection policy.

Reference:

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

Community vote distribution

A (100%)

chrissempai Highly Voted 1 year, 2 months ago

Selected Answer: A

On exam the 9/9/2022

correct answer :
1. From the Microsoft 365 compliance center, create a data loss prevention (DLP) policy.
2. From the Cloud App Security portal, create a file policy.

upvoted 9 times

heshmat2022 Most Recent 1 month, 1 week ago

IT WAS ON EXAM OCTOBER 18 2023

upvoted 1 times

xswe 7 months, 3 weeks ago

This question is asking about a feature that will detect when sensitive information is getting shared outisde the organization... DLP is the solution.
You can create a DLP policy either directly in Purview or Cloud apps with a file policy.
In this question DLP policy in compliance center is the correct answer.

upvoted 3 times

Jawad1462 1 year ago

Selected Answer: A

Correct

upvoted 1 times

Question #16 *Topic 2*

You need to protect documents that contain credit card numbers from being opened by users outside your company. The solution must ensure that users at your company can open the documents.
What should you use?

A. a sensitivity label policy

B. a sensitivity label

C. a retention policy

D. a data loss prevention (DLP) policy

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

Community vote distribution
D (60%) B (40%)

Browniez Highly Voted 2 years, 1 month ago
D is correct, as others are not solutions,
upvoted 15 times

Davidf Most Recent 3 months, 3 weeks ago
Selected Answer: B
A DLP policy will detect content, but a sensitivty label applies protection to the document
upvoted 1 times

T3st3r 6 months, 3 weeks ago
perhaps B ?

https://learn.microsoft.com/en-us/microsoft-365/compliance/encryption-sensitivity-labels?view=o365-worldwide
upvoted 1 times

xswe 7 months, 3 weeks ago
To protect documents from being opened by user outisde the organization you need a DLP policy.
upvoted 2 times

fimbulvetrk 1 year ago
why "sensitivity label" isn't an option in this case? if you configure your label to encrypt files and apply permissions to view only to members of your organization it would work, once the question is about to "prevent to be OPENED by people outside your org".
if the file is labeled this way it can't be opened.
upvoted 2 times

luissaro 7 months, 2 weeks ago
I guess the reason is that sensitivity label nee to be published by a policy otherwise they do not work
upvoted 2 times

Abhishek1610 1 year ago
Selected Answer: D
D is correct, as others are not solutions
upvoted 4 times

fimbulvetrk 1 year ago
but why sensitivity label isn't a valid option? you can configure your label to apply encryption and grant permission to view only to members of your organization. if you want to prevent people outside the org to OPEN the file, sensitivity label is valid, if you want to prevent people to SHARE outside the org (which may lead to prevent to be opened of course), DLP is valid.
this question is trickier than people are arguing.
upvoted 2 times

Abhishek1610 1 year ago
Selected Answer: D
I agree, D is correct, as others are not solutions,
upvoted 2 times

mcas 1 year, 1 month ago
Selected Answer: B

This question can be B and D
DLP is clear but you can achieve the same result with a sensitivity label. You apply encryption and assign permissions to all Authenticated users
upvoted 2 times

chrissempai 1 year, 1 month ago

Selected Answer: D

D is he only effective one in this case
upvoted 1 times

prabhjot 1 year, 2 months ago

D is Final
upvoted 1 times

JamesM9 1 year, 7 months ago

I have tested this today and within a DLP policy there is an option to add an action that can "restrict access or encrypt content in Microsoft 365 locations". We are given the option to specify those locations, Exchange being one of them.

Further to this, when configuring this action we are also given the option to "Block only people outside of your organisation". This will stop files with the specified sensitive information (in this case, credit card numbers) from being shared externally.

Therefore, the answer here is D - a data loss prevention (DLP) policy.
upvoted 4 times

Holii 1 year, 6 months ago

The issue here is with the question's wording. "From being opened by users outside your company" NOT "From being shared with users outside your company"

Depending on how you interpret it, the answer changes.
upvoted 2 times

SnottyPudding 1 year, 8 months ago

Selected Answer: D

Data loss prevention helps prevent unintentional sharing of sensitive items.
https://docs.microsoft.com/en-us/microsoft-365/compliance/information-protection?view=o365-worldwide
upvoted 2 times

Jahoor69 1 year, 8 months ago

Organizations have sensitive information under their control such as financial data, proprietary data, credit card numbers,
Also
item contains a specified kind of sensitive information that is being used in a certain context. For example, 95 social security numbers being emailed to recipient outside your org.

I put my money on D
upvoted 1 times

PrettyFlyWifi 1 year, 10 months ago

The specific settings within a sensitivity label for external sharing only refers to Sharepoint sites. Under "Define external sharing and conditional access settings" and then you see the text... "When this label is applied to a SharePoint site, these settings will replace existing external sharing settings configured for the site." You can set only people in your org, but the question doesn't state it's documents just from SharePoint sites. Makes more sense using DLP, as you can cover multiple document locations and still prevent external sharing. D is correct to me.
upvoted 2 times

Pravda 1 year, 10 months ago

On exam 1/20/2022
upvoted 1 times

Sam12 1 year, 10 months ago

DLP would be an option, but if the documents are already outside of the company, how would you prevent external users from access the documents?

You could create a sensitivity label for files and emails, enable the encryption option so that you can assign permissions (add all users and groups in your organization) and activate the auto labelling feature based on sensitive information types (as the credit card info is a built in sensitive info type).
upvoted 3 times

ReffG 1 year, 10 months ago

Answer B is correct. You choose encryption for the label and then select "Authenticated Users" for allowing only users from your tenant to open documents.
upvoted 2 times

217f3c9 6 months ago

This is wrong ... authenticated users means every user worldwide
upvoted 1 times

girikedar 1 year, 11 months ago

There is One answer Between B & E. not able to fix with these decision
upvoted 1 times

girikedar 1 year, 11 months ago

Sorry no E its D

upvoted 1 times

Question #17 *Topic 2*

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

You have the users shown in the following table.

Name	Group/role
User1	Site1 member group
User2	Site1 member group
User3	Site1 owner group
User4	Sharepoint administrator role

You create a data loss prevention (DLP) policy for Site1 that detects credit card number information. You configure the policy to use the following protection action:

☞ When content matches the policy conditions, show policy tips to users and send them an email notification.

You use the default notification settings.

To Site1, User1 uploads a file that contains a credit card number.

Which users receive an email notification?

A. User1 and User2 only

B. User1 and User4 only

C. User1, User2, User3, and User4

D. User1 only

E. User1 and User3 only

Correct Answer: *D*

Reference:

https://docs.microsoft.com/en-us/microsoft-365/compliance/get-started-with-the-default-dlp-policy?view=o365-worldwide

Community vote distribution

D (57%) E (43%)

DeeJayU Highly Voted 1 year, 11 months ago

Tested on a new tenant.
Default notifications settings are: The person who sent, shared, or modified the content / Owner of the SharePoint site or OneDrive account/ Owner of the SharePoint or OneDrive content.
Based on this the correct answer is E (User1 and User3 only)

upvoted 29 times

Mdwro 1 year, 11 months ago

You are right

upvoted 3 times

Mdwro 1 year, 10 months ago

Changed mind to User1 only. Tested it, and by default there is user only. You need to select owner additionally to get notification

upvoted 8 times

klosedotorg83 Highly Voted 2 years, 1 month ago

Correct - When you enable User notifications, the Default settings only notify the user who sent, shared, or last modified the content. So because User1 uploaded a file containing a credit card number to Site1, then only User1 receives the email notification.

upvoted 8 times

Domza Most Recent 3 weeks, 1 day ago

Its under "email notification" in DLP

D is correct

Enjoy

upvoted 1 times

heshmat2022 1 month, 1 week ago

IT WAS ON EXAM OCTOBER 18 2023

upvoted 1 times

ServerBrain 2 months ago

Selected Answer: D

notifications to other users are irrelevant
upvoted 1 times

dmoorthy 7 months, 1 week ago
E is the Answer
upvoted 1 times

xswe 7 months, 3 weeks ago
You can see here in the text that the user will recieve the policy tip with an email notification, and when you try to do this yourself you will see that no admin will get recieve an alert regarding this.
upvoted 2 times

NinjaSchoolProfessor 11 months, 1 week ago
Answer [D] User1 only Most Voted - As of Dec-2022, the default selection for notifications is "Notify the user who sent, shared, or last modified the content". https://learn.microsoft.com/en-us/microsoft-365/compliance/dlp-policy-reference?view=o365-worldwide#blocking-and-notifications-in-sharepoint-online-and-onedrive-for-business
upvoted 2 times

smiff 11 months, 3 weeks ago
Selected Answer: D
D is correct.
upvoted 1 times

RamenIsDelicious 1 year, 3 months ago
Selected Answer: E
Tested 8/11/22 its E with default notification settings on.
upvoted 2 times

Bear4 1 year, 6 months ago
There are Site owners but there is no site owner group. I am right?
upvoted 1 times

JamesM9 1 year, 7 months ago
I have created a DLP policy today to check this and the default notification setting is "notify the user who sent, shared or last modified the content".

In this circumstance, User1 was the person to upload the file and therefore this makes the answer D - User1 only.
upvoted 1 times

Fusion11 1 year, 7 months ago
Selected Answer: E
I believe E (User 1 and User 3) because the question says you create a policy for Site1 (We could understand only Sharepoint). Default notifications only for Sharepoint is: The person who sent, shared, or modified the content / Owner of the SharePoint site or OneDrive account/ Owner of the SharePoint or OneDrive content.
upvoted 2 times

Holii 1 year, 7 months ago
Default notification settings are only "The person who sent, shared, or modified the content"
Site owner / administrator are not enabled by default.
upvoted 1 times

[Removed] 1 year, 8 months ago
When I try this, in Define Policy Settings if I choose "review and customise default settings" then it later defaults to the person who sent, shared, or modified the content / Owner of the SharePoint site or OneDrive account/ Owner of the SharePoint or OneDrive content.

But if I choose "create or customise advanced DLP rules", it defaults to notify the user who sent, shared, or last modified the content.

To scan for credit card info I have to create my own (as the financial data template has other settings), so that makes me think that the answer is User1 only
upvoted 1 times

[Removed] 1 year, 8 months ago
just tried again and if I create a custom policy then it definitely defaults to user only
upvoted 1 times

PrettyFlyWifi 1 year, 9 months ago
Selected Answer: D
Just open a DLP policy and you'll see it defaults to just the person who sent shared or modified the content.
upvoted 3 times

Mdwro 1 year, 10 months ago
Selected Answer: D
D, as it is for defaults
upvoted 3 times

UWSFish 1 year, 9 months ago

Disregard my comment downthread. The user is the only one receiving an email notification

upvoted 1 times

nupagazi 1 year, 10 months ago

D is correct, User 1 only

upvoted 1 times

Question #18 *Topic 2*

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

B. File path exclusions

C. Unallowed apps

D. Service domains

Correct Answer: *D*
You can control whether sensitive files protected by your policies can be uploaded to specific service domains from Microsoft Edge.
☞ If the list mode is set to Block, then user will not be able to upload sensitive items to those domains. When an upload action is blocked because an item matches a DLP policy, DLP will either generate a warning or block the upload of the sensitive item.
☞ If the list mode is set to Allow, then users will be able to upload sensitive items only to those domains, and upload access to all other domains is not allowed.
Reference:
https://docs.microsoft.com/en-us/microsoft-365/compliance/endpoint-dlp-using?view=o365-worldwide

Community vote distribution
D (100%)

ExamReviewerIZ Highly Voted 2 years, 1 month ago
Correct, "Service Domain" (in Allow mode we add the website to the list, or if it's in Block mode we remove the website from the list)
upvoted 8 times

sergioandreslq 1 year, 11 months ago
referencei:
https://docs.microsoft.com/en-us/microsoft-365/compliance/endpoint-dlp-using?view=o365-worldwide#service-domains

You can control whether sensitive files protected by your policies can be uploaded to specific service domains from Microsoft Edge.

If the list mode is set to Block, then user will not be able to upload sensitive items to those domains. When an upload action is blocked because an item matches a DLP policy, DLP will either generate a warning or block the upload of the sensitive item.

If the list mode is set to Allow, then users will be able to upload sensitive items only to those domains, and upload access to all other domains is not allowed.
The Service domains setting only applies to files uploaded using Microsoft Edge or Google Chrome with the the Microsoft Compliance Extension installed.
upvoted 4 times

Domza Most Recent 3 weeks, 1 day ago
Correct~
upvoted 1 times

xswe 7 months, 3 weeks ago
Since they are asking for a configuration that will make it possible for users to upload the sensitive documents to a travel mgnt website you want to add this domain to the service domains, founder under Endpoint DLP in Purview and under Broswer and domain restricitons to sensitive data.
upvoted 2 times

wooyourdaddy 1 year, 5 months ago
Selected Answer: D
I wrote the exam today, this question was on it, I choose D, scored 890!
upvoted 4 times

Question #19 *Topic 2*

You have a Microsoft 365 tenant that has devices onboarded to Microsoft Defender for Endpoint as shown in the following table.

Name	Type
Device1	Windows 8.1
Device2	Windows 10
Device3	iOS
Device4	macOS
Device5	CentOS Linux

You plan to start using Microsoft 365 Endpoint data loss protection (Endpoint DLP).
Which devices support Endpoint DLP?

A. Device5 only

B. Device2 only

C. Device1, Device2, Device3, Device4, and Device5

D. Device3 and Device4 only

E. Device1 and Device2 only

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

Community vote distribution
B (100%)

sivis Highly Voted 2 years ago
Selected Answer: B
Endpoint data loss prevention (Endpoint DLP) extends the activity monitoring and protection capabilities of DLP to sensitive items that are physically stored on Windows 10, Windows 11, and macOS (Catalina 10.15 and higher) devices.

Correct answer is Device2 and Device4
upvoted 24 times

gursimran_s 1 year, 7 months ago
That is not an option here. Maybe the question is outdated!
upvoted 5 times

xswe Most Recent 7 months, 3 weeks ago
Outdated question, windows 10,11 and MacOS are supported for Endpoint DLP
upvoted 3 times

fimbulvetrk 12 months ago
this question is probably outdated once macOS is now supported:
https://learn.microsoft.com/en-us/microsoft-365/compliance/device-onboarding-macos-overview?view=o365-worldwide
upvoted 3 times

klosedotorg83 2 years, 1 month ago
Correct
https://docs.microsoft.com/en-us/microsoft-365/compliance/endpoint-dlp-getting-started?view=o365-worldwide
upvoted 3 times

Question #20 *Topic 2*

A compliance administrator recently created several data loss prevention (DLP) policies.
After the policies are created, you receive a higher than expected volume of DLP alerts.
You need to identify which rules are generating the alerts.
Which DLP report should you use?

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

Community vote distribution

B (100%)

xswe 7 months, 3 weeks ago
To be able to see what policy that have been matched and how many times you can use the DLP Policy matches
upvoted 2 times

wooyourdaddy 1 year, 5 months ago
Selected Answer: B
I wrote the exam today, this question was on it, I choose B, scored 890!
upvoted 4 times

BTAB 1 year, 6 months ago
"the policy matches report is better for identifying matches with specific rules and fine tuning DLP policies. The incidents report is better for identifying specific pieces of content that are problematic for your DLP policies."

https://docs.microsoft.com/en-us/microsoft-365/compliance/view-the-dlp-reports?view=o365-worldwide
upvoted 2 times

[Removed] 1 year, 9 months ago
Why is this policy matches when the incidents report shows matches at a rule level?
upvoted 1 times

[Removed] 1 year, 9 months ago
I was getting them the wrong way round: "the policy matches report shows matches at a rule level; for example, if an email matched three different rules, the policy matches report shows three different line items."
https://docs.microsoft.com/en-us/microsoft-365/compliance/view-the-dlp-reports?view=o365-worldwide#view-the-reports-for-data-loss-prevention
upvoted 2 times

Pravda 1 year, 10 months ago
On exam 1/20/2022
upvoted 1 times

Ras1364 2 years ago
https://docs.microsoft.com/en-us/microsoft-365/compliance/dlp-learn-about-dlp?view=o365-worldwide#dlp-alerts-dashboard
upvoted 2 times

klosedotorg83 2 years, 1 month ago
Correct
upvoted 4 times

HOTSPOT -

You have a Microsoft 365 tenant that uses data loss prevention (DLP) to protect sensitive information.

You create a new custom sensitive info type that has the matching element shown in the following exhibit.

Matching element

Detect content containing

Regular expression

^(\d{3}(-)){3}\d{3}|\d{12}$

The supporting elements are configured as shown in the following exhibit.

Supporting elements

Contains this keyword list

Keyword list

"Employee ID"

Minimum Count

1

The confidence level and character proximity are configured as shown in the following exhibit.

Confidence level

Default (60%) 75

Character proximity

Default (300 characters) 100

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

NOTE: Each correct selection is worth one point.

Hot Area:

Answer Area

Statements	Yes	No
A document that contains the following text will match the sensitive info type: James has an Employee ID of 555-343-111-065.	○	○
A document that contains the following text will match the sensitive info type: The Employee ID of the employee Ben Smith is 555343123444.	○	○
A document that contains the following text will match the sensitive info type: The id badge for 555-123 has expired.	○	○

Correct Answer:

Answer Area

Statements	Yes	No
A document that contains the following text will match the sensitive info type: James has an Employee ID of 555-343-111-065.	○	○
A document that contains the following text will match the sensitive info type: The Employee ID of the employee Ben Smith is 555343123444.	○	○
A document that contains the following text will match the sensitive info type: The id badge for 555-123 has expired.	○	○

Note: The regular expression has a starts with (^) and ends with ($) metacharacter and will not match any of the sentences. Without the starts with (^) metacharacter the first and second sentences would match and the supporting element (Employee ID) would be within 100 character proximity.

Reference:

https://docs.microsoft.com/en-us/microsoft-365/compliance/create-a-custom-sensitive-information-type?view=o365-worldwide

zaspamer Highly Voted 1 year, 11 months ago

The answer is no due to a } instead of a). The correct query would be ^(\d{3}(-)){3}\d{3}|\d{12}$. Then both A and B would have been corrected. Tested with https://regex101.com/

upvoted 14 times

Sam12 Most Recent 1 year, 10 months ago

regardless of the errors on the regex:

First regex (before the |) will never work because the options that contain digits and hyphens, the strings never starts with a digit (required by the regex because of the ^)

Second regex (after the |) (12 digits) must end on a digit ($), none of the options end on a digit.
NO for all the options.

upvoted 4 times

dmonton 1 year, 8 months ago

The dot is not part of the text. Microsoft allways ends the answers with a dot. So if in the case that the regular expresión is written correctly second is YES. If the regular expresion is written with the } instead of) all are NO

upvoted 4 times

nupagazi 1 year, 10 months ago

I tested with regex101; should be all No, the 12 digit number should start from begining (^); and yes,) instead of }. The correct regex should be: ^(\d{3}(-)){3}\d{3}|\d{12}$

upvoted 2 times

xlws 1 year, 12 months ago

that is 3 numbers - 3 numbers - 3 numbers - 3 numbers or 12 numbers, I vote for yes,no,no.

upvoted 2 times

sergioandreslq 1 year, 11 months ago

Nop, The issue is the "^" which for the maching at the beggining of the line.
I believe it is No, no, no.
I tested the regex on: https://regex101.com/
1st Capturing Group (\d{3}(-)){3}
{3} matches the previous token exactly 3 times
A repeated capturing group will only capture the last iteration. Put a capturing group around the repeated group to capture all iterations or use a non-capturing group instead if you're not interested in the data
\d matches a digit (equivalent to [0-9])
{3} matches the previous token exactly 3 times

2nd Capturing Group (-)
- matches the character - with index 4510 (2D16 or 558) literally (case sensitive)
\d matches a digit (equivalent to [0-9])
{3} matches the previous token exactly 3 times

2nd Alternative \d{12}
\d matches a digit (equivalent to [0-9])
{12} matches the previous token exactly 12 times

upvoted 4 times

klosedotorg83 2 years, 1 month ago

The regular expression ^ (\ d {3} (-)} {3} \ d {3} | \ d {12} $ shown in the exhibit is incorrect, so none statetement will match.

It should be like this ^ (\ d {3} (-)) {3} \ d {3} | \ d {12} $.
So, the second statement will match if the regular expression is fixed.
upvoted 4 times

Bongconnection 2 years, 1 month ago
option 2nd, 9 digit number matches regular expression... so is 2nd TRUE? not sure
upvoted 1 times

Sam12 1 year, 10 months ago
no because regex ends in $ which means that there can be nothing after the last digit, but you have the dot, so it does not match.
upvoted 2 times

dmonton 1 year, 8 months ago
The dot is not part of the text. Microsoft allways ends the answers with a dot
upvoted 1 times

Question #22 *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 10. The computers are onboarded to the Microsoft 365 compliance center.
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 the Cloud App Security portal, you create an app discovery policy.
Does this meet the goal?

A. Yes

B. No

Correct Answer: *B*
You can create app discovery policies to alert you when new apps are detected within your organization.
Use the unallowed apps list instead.
Reference:
https://docs.microsoft.com/en-us/cloud-app-security/cloud-discovery-policies https://docs.microsoft.com/en-us/microsoft-365/compliance/endpoint-dlp-using?view=o365-worldwide

Community vote distribution
B (100%)

NinjaSchoolProfessor 11 months, 1 week ago
Answer is No. - From within MDCA – If you're using MDE, once you mark an app as unsanctioned, it's automatically blocked. Within Purview - To block an unwanted app, Select DLP >> [Endpoint DLP settings] >> [Restricted apps and app groups] >> [Restricted apps] >> [Restricted app groups] OR [Add or edit restricted apps].
upvoted 2 times

wooyourdaddy 1 year, 5 months ago
Selected Answer: B
I wrote the exam today, this question was on it, I choose B, scored 890!
upvoted 1 times

McAlec 2 years ago
Correct.
Unallowed apps is a list of applications that you create which will not be allowed to access a DLP protected file.
upvoted 3 times

Question #23 *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 10. The computers are onboarded to the Microsoft 365 compliance center.
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 the Microsoft 365 Endpoint data loss prevention (Endpoint DLP) settings, you add a folder path to the file path exclusions.
Does this meet the goal?

A. Yes

B. No

Correct Answer: *B*
Folder path to the file path exclusions excludes certain paths and files from DLP monitoring.
Use the unallowed apps list instead.
Reference:
https://docs.microsoft.com/en-us/microsoft-365/compliance/endpoint-dlp-using?view=o365-worldwide

Community vote distribution

B (100%)

PhyMac 7 months, 3 weeks ago
A is the correct answer for this.
See below.

"You may want to exclude certain paths from DLP monitoring, DLP alerting, and DLP policy enforcement on your devices because they're too noisy or don't contain files you're interested in. Files in those locations won't be audited and any files that are created or modified in those locations won't be subject to DLP policy enforcement. You can configure path exclusions in DLP settings."
https://learn.microsoft.com/en-us/microsoft-365/compliance/dlp-configure-endpoint-settings?view=o365-worldwide#file-path-exclusions

This is how we exclude sensitive file files from DLP monitoring.
upvoted 1 times

Nickname 6 months, 2 weeks ago
Your explanation has nothing to do with the question.

The correct answer is "No". This setting does not prevent the local app from accessing certain data.
upvoted 2 times

hpl1908 10 months, 1 week ago
How come this solution meets the goal: From the Microsoft 365 Endpoint data loss prevention (Endpoint DLP) settings, you add a folder path to the file path exclusions ?
This solution meets the goal because by excluding the folder path that contains the sensitive documents, Endpoint DLP will ignore the files in that folder, and Tailspin will not be able to access them. By excluding the folder path, the sensitive documents will be protected while allowing Tailspin to access other files. This solution will block Tailspin from accessing sensitive documents on the computers without preventing the application from accessing other documents, which is the goal.

It is important to note that this solution relies on the assumption that the sensitive documents are stored in a specific folder and that Tailspin has access to that folder. Additionally, it is important to test the exclusion path before applying it to the production environment and to continuously monitor the folder path to ensure that no other sensitive information is stored in it.
So my conclusion is A - YES
upvoted 1 times

hpl1908 10 months, 1 week ago
From the Microsoft 365 Endpoint data loss prevention (Endpoint DLP) settings, you
add the application to the unallowed apps list.
This solution is NO.
upvoted 1 times

hpl1908 10 months, 1 week ago
Ho moderator please remove my above comments, as I am not sure about my comments as my assumption was wrong. Your original response remains correct.
upvoted 2 times

NinjaSchoolProfessor 11 months, 1 week ago

Answer is No. File path exclusions for Windows = Files in these Windows device locations won't be monitored by your policies. To block this from within MDCA – If you're using MDE, once you mark an app as unsanctioned, it's automatically blocked. Within Purview to block an unwanted app, Select DLP >> [Endpoint DLP settings] >> [Restricted apps and app groups] >> [Restricted apps] >> [Restricted app groups] OR [Add or edit restricted apps].

upvoted 2 times

wooyourdaddy 1 year, 5 months ago

Selected Answer: B

I wrote the exam today, this question was on it, I choose B, scored 890!

upvoted 3 times

Question #24 *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 10. The computers are onboarded to the Microsoft 365 compliance center.
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 the Microsoft 365 Endpoint data loss prevention (Endpoint DLP) settings, you add the application to the unallowed apps list.
Does this meet the goal?

A. Yes

B. No

Correct Answer: *A*

Unallowed apps is a list of applications that you create which will not be allowed to access a DLP protected file.
Reference:
https://docs.microsoft.com/en-us/microsoft-365/compliance/endpoint-dlp-using?view=o365-worldwide

Community vote distribution

A (100%)

PrettyFlyWifi Highly Voted 1 year, 9 months ago

Correct, Unallowed apps, see ... https://docs.microsoft.com/en-us/microsoft-365/compliance/endpoint-dlp-using?view=o365-worldwide#unallowed-apps

upvoted 5 times

xswe Most Recent 7 months, 3 weeks ago

Unallowed apps are now called Restrictied apps under Endpoint DLP, if you add the app here you will able to control the level of access for the app.

upvoted 1 times

NinjaSchoolProfessor 11 months, 1 week ago

Correct when referencing the legacy documentation as the GUI has changed. Reference the following: Within Purview to block an unwanted app, Select DLP >> [Endpoint DLP settings] >> [Restricted apps and app groups] >> [Restricted apps] >> [Restricted app groups] OR [Add or edit restricted apps]. Yyou can also add apps in the [Unallowed Bluetooth apps] section. - https://learn.microsoft.com/en-us/microsoft-365/compliance/dlp-configure-endpoint-settings?view=o365-worldwide // To block this from within MDCA – If you're using MDE, once you mark an app as unsanctioned, it's automatically blocked. - https://learn.microsoft.com/en-us/defender-cloud-apps/governance-discovery#blocking-apps-with-built-in-streams

upvoted 2 times

LamNV 1 year, 4 months ago

Correct answer A

upvoted 1 times

wooyourdaddy 1 year, 5 months ago

Selected Answer: A

I wrote the exam today, this question was on it, I choose A, scored 890!

upvoted 2 times

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 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 Data Classification service inspection method and send alerts as email.
Does this meet the goal?

A. Yes

B. No

Correct Answer: *B*
Alerts must be sent to the Microsoft Teams site of the affected department. A Microsoft Power Automate playbook should be used.
Reference:
https://docs.microsoft.com/en-us/cloud-app-security/dcs-inspection https://docs.microsoft.com/en-us/cloud-app-security/flow-integration

Topaz007 Highly Voted 2 years, 1 month ago

Answer is NO. For sure MCAS can send out alerts but only to preset e-mail address. BUT...

The question states '...alerts must be sent to the Microsoft Teams site of the affected department...'. As such the alerts are sent to different e-mail addresses.

In configs like this it's better to use Power Automate.

upvoted 7 times

ChaBum Highly Voted 1 year, 10 months ago

Answer should be YES, the alert email can be sent to the email associated to the Microsoft Teams site.
https://support.microsoft.com/en-us/office/send-an-email-to-a-channel-in-teams-d91db004-d9d7-4a47-82e6-fb1b16dfd51e

upvoted 6 times

mbhasker Most Recent 2 days, 20 hours ago

Ans: YES

upvoted 1 times

NinjaSchoolProfessor 11 months, 1 week ago

Answer = [A]. During the creation of a policy within Defender for Cloud apps, the Data Classification Services integration capability allows you to select the [Inspection method] and choose either [Built-in DLP] or select the [Data Classification Services]. If choosing the latter, you will then be given the choice to select a Purview SIT, EDM, Fingerprint, or Trainable Classifier. The next section below that allows you to send alerts via Email. While the answer in the example is vague, it's still correct.

upvoted 2 times

Cybersecgirl 11 months, 3 weeks ago

Alert to a team's channel can only be sent via Powerautomate
https://techcommunity.microsoft.com/t5/microsoft-teams-community-blog/integrating-microsoft-teams-with-microsoft-cloud-app-security/ba-p/2986865#:~:text=When%20we%20integrate%20the%20MCAS,alert%20triggered%20in%20the%20MCAS.

upvoted 1 times

Pravda 1 year, 10 months ago

On exam 1/20/2022

upvoted 1 times

klosedotorg83 2 years, 1 month ago

It seems to be Correct.

Microsoft Data Classification Services integration:
Leveraging file policies, you can also set alerts and governance actions for the policy. For more information, see file policies and governance actions. Leveraging session policies, you can also monitor and control actions in real-time when a file matches a DCS type. For more information, see session policy.
https://docs.microsoft.com/en-us/cloud-app-security/dcs-inspection

File governance actions:
Alerts – Alerts can be triggered in the system and propagated via email and text message, based on severity level.
https://docs.microsoft.com/en-us/cloud-app-security/governance-actions

upvoted 3 times

Question #26 *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 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

Community vote distribution

A (57%) B (43%)

Domza 3 weeks, 6 days ago
Quest 4 and Quest 26 the same
upvoted 1 times

Artgum 3 months ago
Should be "B" - MDCA does not allow use of Built-In Inspection anymore. The default and only choice is Data Classification Service.
upvoted 3 times

Gesbie 3 months, 3 weeks ago
was on Exam August 9, 2023
upvoted 1 times

dmoorthy 7 months, 1 week ago
Answer is B
upvoted 2 times

RamenIsDelicious 1 year, 3 months ago
Selected Answer: A
Tested 8/15/22 should be a=YES
upvoted 4 times

IAGirl 1 year, 9 months ago
Sorry, my mistake, I think the answer is Yes, we need power automate and we can scan all files with Built-in DLP
upvoted 2 times

IAGirl 1 year, 9 months ago
I think the answer is No, because we need to scan all files and Built-in DLP cannot inspect protected files
upvoted 1 times

PrettyFlyWifi 1 year, 9 months ago
Selected Answer: B
Like DeeJayU says, you can use both methods to cover credit cards, but I think the Power Automate option is the one that makes this answer incorrect. Why do you need Power Automate to alert a Teams site? You just email that teams site directly and all members will see it, so PA is unnecessary for this. Best answer for a "Yes" is to use the Data Classification Service as the inspection method.
upvoted 3 times

PrettyFlyWifi 1 year, 9 months ago
Hmmm, I'm changing my mind again.... Maybe the Built-in DLP and Power Automate is correct. How would every file owner and the affected department be able to be noitified. The email alert would be for a specific admin, but if a credit card number is found in a document then that is dynamic and you'd probably need a Flow with an IF/ELSE setup to pull out the owner property of the document so it could send the alert out.
upvoted 3 times

Pravda 1 year, 10 months ago
On exam 1/20/2022

upvoted 1 times

DeeJayU 1 year, 11 months ago

As per https://docs.microsoft.com/en-us/defender-cloud-apps/tutorial-dlp Data Classification Services is the preferred content inspection method, not Built-in DLP.
Both inspection methods cover credit card numbers.

upvoted 2 times

Zorolloo 1 year, 11 months ago

Question 4 and 26 are the same? Why?

upvoted 2 times

casti 2 years, 1 month ago

this should be a "yes", because DLP inspection method can be applied to all files and can send results to P.A.

upvoted 4 times

Question #27 *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 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 as email.
Does this meet the goal?

A. Yes

B. No

Correct Answer: *B*
Alerts must be sent to the Microsoft Teams site of the affected department. A Microsoft Power Automate playbook should be used.
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

Community vote distribution

B (78%) A (22%)

IAGirl Highly Voted 1 year, 9 months ago

Selected Answer: B

To send messages to teams we need power automate

upvoted 7 times

ChaBum Highly Voted 1 year, 10 months ago

Answer should be YES, the alert email can be sent to the email associated to the Microsoft Teams site.
https://support.microsoft.com/en-us/office/send-an-email-to-a-channel-in-teams-d91db004-d9d7-4a47-82e6-fb1b16dfd51e

upvoted 5 times

ranc1d Most Recent 1 year, 8 months ago

Selected Answer: A

Voting for A:
"must be sent to the Microsoft Teams site of the affected department"
sent to the teams SITE -> email
if it would be "sent to teams channel" -> power automate

upvoted 2 times

Holii 1 year, 6 months ago

This is being applied to all files- and must send an alert to the specific Teams Site that triggered the alert.
How are you going to dynamically process what Site/email address is needed without an automation tool?

upvoted 3 times

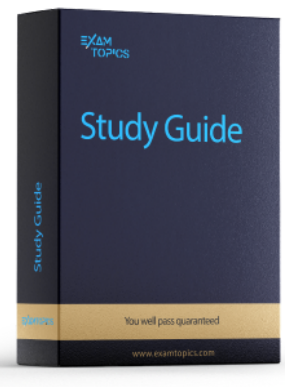
Pravda 1 year, 10 months ago

On exam 1/20/2022

upvoted 2 times

EXAMTOPICS
- Expert Verified, Online, **Free**.

Prepare for your SC-400 exam with additional products



Study Guide

427 PDF Pages

$19.99

Buy Now

Video Course

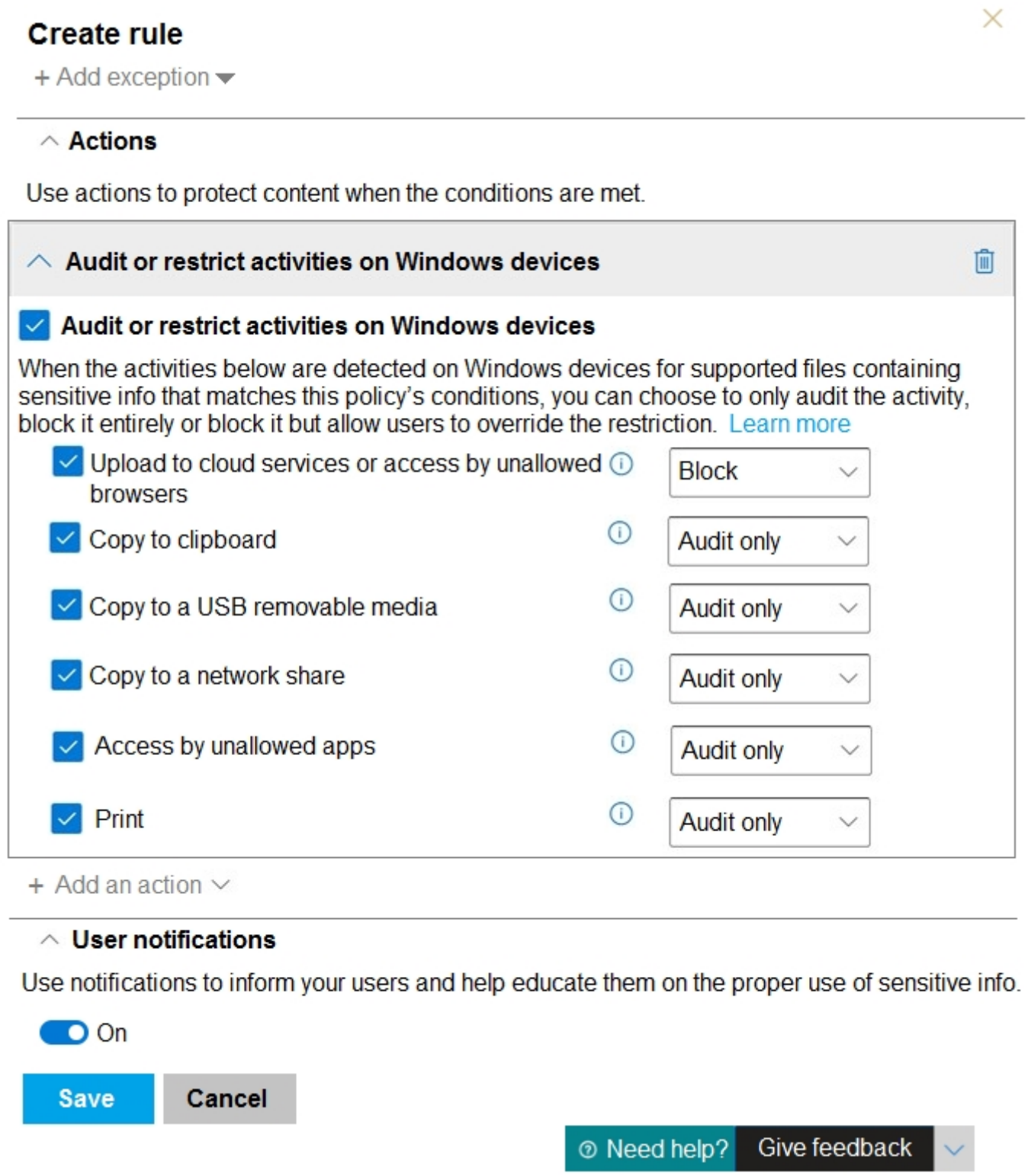
58 Lectures

$19.99

Buy Now

Custom View Settings

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



From a computer named Computer1, a 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 computers are NOT onboarded to the Microsoft 365 compliance center.

B. The Copy to clipboard action is set to Audit only.

C. There are file path exclusions in the Microsoft 365 Endpoint data loss prevention (Endpoint DLP) settings.

D. The Access by unallowed apps action is set to Audit only.

E. The unallowed browsers in the Microsoft 365 Endpoint data loss prevention (Endpoint DLP) settings are NOT configured.

Correct Answer: *CD*

Community vote distribution

CE (67%) AE (21%) 13%

IAGirl Highly Voted 1 year, 9 months ago

Selected Answer: CE

The computers are already onboarded, that's why sometimes can upload files and sometines cannot, the answer is C and E

upvoted 8 times

heshmat2022 Most Recent 1 month, 1 week ago

IT WAS ON EXAM OCTOBER 18 2023

upvoted 1 times

Tommytong 1 month, 2 weeks ago

Originally thought it was A,E however after looking at it again along with the comments I'm switching to C,E.

E - if you don't have the browser configured in the global DLP settings - putting it to block state won't prevent it.
A - Does not work like I originally thought because the issue happens sporadically. If it wasn't onboarded, there would be zero policies and nothing to enforce.
C - while it seems odd because it's file path exclusion and you're connecting to cloud services, you can absolutely have private cloud network shares or even OneDrive type WebDAV locations

upvoted 1 times

Gesbie 3 months, 3 weeks ago

was on Exam August 9, 2023

upvoted 1 times

xswe 7 months, 3 weeks ago

This is a tricky one but I would exclude E since we can see in the picture that the unallowed browsers is set to "Block" so it should be configured already.
The copy to clicpboard should not cover the uploading of files since you dont copy files when you upload them to a cloud solution.
Unallwed apps should not be the correct solution since they are problably uploading the files to the cloud service with a browser.

I would choose "device not onboarded" and "file path exclusion in endpoint DLP".

upvoted 1 times

Nickname 6 months, 2 weeks ago

It can't be A since the user reports he is sometimes blocked from his computer1. If computer1 is not onboarded he wouldn't be blocked at all.

upvoted 3 times

Reinto 9 months, 3 weeks ago

Selected Answer: CE

The only logical choices

upvoted 1 times

Rockalm 11 months ago

"D:The Access by unallowed apps action is set to Audit only." Audit only doesn't block the upload.

upvoted 1 times

chrissempai 1 year, 1 month ago

Selected Answer: AC

AC is the correct answer.
If you pay attention the unallowed browser is set to block so E is not a valid answer

upvoted 3 times

JamesM9 1 year, 7 months ago

The answer here is C & E.

upvoted 4 times

PrettyFlyWifi 1 year, 9 months ago

E looks a certain answer, as if you go into a DLP policy and choose 'Actions', you can hover over the i for a description. It states "When this action is set to Block, other browsers (defined in the unallowed browsers list in Endpoint DLP settings) are blocked from accessing the file." This would make sense, because if you don't define the browsers you want to block, it will still let you upload files.

The other answer seems like it should be A, because you only get these options if you select the "devices" location in the DLP policy. This means you'd need to onboard the device to be able to use these policy settings properly.

A and E for me.

upvoted 4 times

UWSFish 1 year, 10 months ago

I have AC....If you read carefully on choice E...Unallowed browser is NOT configured...as has been pointed out by bing

upvoted 1 times

UWSFish 1 year, 9 months ago

I was wrong...is CE:

Detects when a user attempts to upload an item to a restricted service domain or access an item through a browser. If they are using a browser that is listed in DLP as an unallowed browser, the upload activity will be blocked and the user is redirected to use Microsoft Edge . Microsoft Edge will then either allow or block the upload or access based on the DLP policy configuration

....so if unallowed browser is NOT configured you can use chrome/etc with impugnity anc won't be kicked over to edge which observes the DLP policy, in other words, sometimes can upload (chrome), sometimes can not (edge).

upvoted 5 times

Pravda 1 year, 10 months ago

On exam 1/20/2022

upvoted 1 times

Sam12 1 year, 10 months ago

Selected Answer: CE

CE for me!

upvoted 4 times

ChaBum 1 year, 10 months ago

Selected Answer: CE

C: depending if the source path is part of the exception or not, the upload is allowed or not
E relates to users behavior, using different browsers with some being allowed and other blocked

upvoted 3 times

doori88 5 months, 2 weeks ago

totally agree

upvoted 1 times

Pereiraman 1 year, 10 months ago

agree, the only ones that can cause unstable and related with DLP.

upvoted 1 times

solfis737 1 year, 11 months ago

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

"You may want to exclude certain paths from DLP monitoring, DLP alerting, and DLP policy enforcement on your devices because they are too noisy or don't contain files you are interested in. Files in those locations will not be audited and any files that are created or modified in those locations will not be subject to DLP policy enforcement."

upvoted 2 times

Ali_557 1 year, 11 months ago

AE looks more valid.

upvoted 1 times

CalST 1 year, 11 months ago

The users can 'sometimes' upload so it has to be C and D. B is not relevant, A cant be it as they sometimes cannot upload, and the unallowed browser is blocked which wouldn't allow 'sometimes'

upvoted 2 times

Question #29 *Topic 2*

You are planning a data loss prevention (DLP) solution that will apply to computers that run Windows 10.
You need to ensure that when users attempt to copy a file that contains sensitive information to a USB storage device, the following requirements are met:
- If the users are members of a group named Group1, the users must be allowed to copy the file, and an event must be recorded in the audit log.
- All other users must be blocked from copying the file.

What should you create?

A. two DLP policies that each contains one DLP rule

B. one DLP policy that contains one DLP rule

C. one DLP policy that contains two DLP rules

Correct Answer: *A*

Community vote distribution

A (56%) B (44%)

ExamReviewerIZ Highly Voted 2 years, 1 month ago

Obviously refers to 2 DLP Policies, as you can only have the policy in Audit Mode or On.
Audit Mode for Group 1.
On for everyone else.

upvoted 13 times

xswe Most Recent 7 months, 3 weeks ago

You should go for two DLP policies and one DLP rule to achieve this

upvoted 1 times

Azurefox79 9 months, 2 weeks ago

Selected Answer: A

The real question is whether a group excluded from a policy setting still generates an audit record of the exclusion. If yes, then 1 for each is good. If no, we need 2 policies. I believe its the Latter

upvoted 2 times

JCkD4Ni3L 11 months, 3 weeks ago

Selected Answer: B

Hmmmm, the audit question is irrelevant here because as soon as an event takes place, an Audit log is created (this is implied). Also creating an exclusion in a simple rule is perfectly possible, therefore 1 policy 1 rule.

upvoted 2 times

mcas 1 year, 1 month ago

Selected Answer: A

With 1 policy you cannot choose both Audit and Block.
You need 1 policy for all users with block rule, and exclude group1
and 1 policy that includes group1 only and the rule set to Audit only

upvoted 2 times

chrissempai 1 year, 2 months ago

Selected Answer: A

A is the only way

upvoted 1 times

Lion007 1 year, 3 months ago

Selected Answer: B

Correct answer is (B). 1 policy and 1 rule. From the DLP Policy, under "Choose locations to apply the policy", when you select "Devices", you are provided with "Included" and "Excluded" to allow you to "Exclude user or group" which you add Group1 to for exclusion from this one policy scope, all other users will be included.

So you only need one DLP policy, with the scope excluding Group1. Then you create 1 rule that has an action (from Actions > selecy "Apply restrictions to specific activity" > and select only "Copy to a USB removable media" > and make the action "Block") which will block copying files to USB for the scope you chose.

upvoted 2 times

wyindualizer 1 year, 3 months ago

And what about audit?

upvoted 5 times

Pravda 1 year, 10 months ago

On exam 1/20/2022

upvoted 1 times

nupagazi 1 year, 10 months ago

I think 1 policy, 1 rule using exlusion group or user

upvoted 3 times

PrettyFlyWifi 1 year, 9 months ago

You cannot have a single policy handling multiple actions for multiple scopes, i.e. actions for 1 for all users and then more actions just for a group of users. You need the 2nd policy to differentiate the actions.

upvoted 4 times

Question #30 *Topic 2*

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 Exchange admin 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 Cloud App Security portal, create a file policy.

Correct Answer: *D*
File Policies allow you to enforce a wide range of automated processes using the cloud provider's APIs. Policies can be set to provide continuous compliance scans, legal eDiscovery tasks, DLP for sensitive content shared publicly, and many more use cases.
Note:
There are several versions of this question in the exam. The question has two possible correct answers:
1. From the Microsoft 365 compliance center, create a data loss prevention (DLP) policy.
2. From the Cloud App Security portal, create a file policy.
Other incorrect answer options you may see on the exam include the following:
☞ From the Microsoft 365 compliance center, start a data investigation.
☞ From the Azure portal, create an Azure Information Protection policy.
Reference:
https://docs.microsoft.com/en-us/defender-cloud-apps/data-protection-policies

Community vote distribution
D (83%) Other

sivis Highly Voted 2 years ago
Selected Answer: D
Answer is D.
We can configure an alert in MCAS by creating a file policy
upvoted 14 times

sergioandreslq 1 year, 11 months ago
In Microsoft 365, you can create a data loss prevention (DLP) policy in two different admin centers:
In the Microsoft 365 Compliance Center, you can create a single DLP policy to help protect content in SharePoint, OneDrive, Exchange, Teams, and now Endpoint Devices. We recommend that you create a DLP policy here. For more information
In the past, we were able to create DLP in the Exchange admin center, you were able to create a DLP policy to help protect content only in Exchange, however, this functionality was migrated to M365 Compliance admin center DLP. The policy was created to use Exchange mail flow rules (also known as transport rules), so it has more options specific to handling email. Remember that this one was deprecated.
In the options, there is not M365 compliance center DLP, so, the only option available is D which creates the policy using the MCAS (now Defender for Cloud Apps) to create the DLP policy and warning the owner of the file.
upvoted 6 times

digitallycan Highly Voted 2 years, 1 month ago
Answer is A. DLP in Exchange admin center is being deprecated. Newer question/answer to create DLP using MS Compliance Center was asked earlier on pg12 Q15 in this set.
https://docs.microsoft.com/en-us/exchange/security-and-compliance/data-loss-prevention/data-loss-prevention
upvoted 8 times

heshmat2022 Most Recent 1 month, 1 week ago
IT WAS ON EXAM OCTOBER 18 2023
upvoted 2 times

xswe 7 months, 3 weeks ago
DLP Policy in Purview or File Policy should be used to achieve this
upvoted 1 times

xswe 7 months, 3 weeks ago
File policy in MCA and DLP policy in Purview should be used to achieve this.
upvoted 1 times

mcas 1 year, 1 month ago
Selected Answer: C
this is also possible with insider risk policy

upvoted 1 times

chrissempai 1 year, 2 months ago

Selected Answer: A

Answer A is correct.
For the exam SC-400 you need to focus on what you are studying so A is the answer

upvoted 2 times

luissaro 7 months, 2 weeks ago

you do not create in EAC a DLP policy related to onedrive, either the topic is exchange or onedrive

upvoted 1 times

MahmoudEldeep 1 year, 7 months ago

Selected Answer: D

Answer is D

upvoted 1 times

JamesM9 1 year, 7 months ago

I have tested this in my tenancy today and the easier option is to create a file policy - it meets all the requirements specified within the question.

Therefore, the answer is D - Create a file policy.

upvoted 1 times

daavidsc400 1 year, 9 months ago

I actually think this can be done with an insider risk policy

upvoted 2 times

daavidsc400 1 year, 9 months ago

How could the answer be A when the question doesn't mention Exchange or Emails? It only mentions OneDrive and sharing. Sharing does not necessarily mean email.

upvoted 2 times

PrettyFlyWifi 1 year, 9 months ago

Depending on the question options, this could be either A or D. If it is this question, then D looks a good choice. If it stated Compliance admin center instead of Exchange, I'd go for A and a DLP policy. However, you can use a file policy "Sharing with external domains - Receive an alert about any file shared with accounts owned by specific external domains. For example, files shared with a competitor's domain. Select the external domain with which you want to limit sharing." You can use the Access Level setting and select public and external so any files shared with those people not internal, it would flag and use the alert option in the same policy. D looks like a solid option either way.

upvoted 2 times

PrettyFlyWifi 1 year, 9 months ago

A DLP policy is much less convoluted than a file policy though.
Create DLP policy
Location > OneDrive
Conditions > content is shared from M365 > outside organisation AND is sensitive type/label
Alert > send to admin or persons

upvoted 2 times

PrettyFlyWifi 1 year, 9 months ago

Maybe they are trying to catch you out as you shouldn't be trying to use Exchange admin center for DLP policies any more anyway

upvoted 1 times

UWSFish 1 year, 10 months ago

I think a current exam would be updated to state that DLP is in compliance center...making A closest to correct

upvoted 2 times

cwilson91 1 year, 2 months ago

It's intentionally misleading.. Yes you can accomplish the same goal by creating a DLP policy within the compliance center, but they try to trick you by saying Exchange. The same can be said with topic 2 question 15. (Where they give compliance center DLP policy but try to trick you with MCAS 'activity policy')

Correct answer for this question is D.

upvoted 1 times

Pravda 1 year, 10 months ago

On exam 1/20/2022

upvoted 1 times

Sam12 1 year, 10 months ago

The answer is in fact exchange. I just tested, when you try to open the DLP page it will send you to the new compliance portal.

upvoted 1 times

CalST 1 year, 11 months ago

Shared isnt performed just via email so D

upvoted 1 times

klosedotorg83 2 years, 1 month ago

It should be D. - From the Cloud App Security portal, create a file policy

upvoted 4 times

Question #31 *Topic 2*

Your company has a Microsoft 365 tenant.
The company performs annual employee assessments. The assessment results are recorded in a document named AssessmentTemplate.docx that is created by using a Microsoft Word template. Copies of the employee assessments are sent to employees and their managers. The assessment copies are stored in mailboxes, Microsoft SharePoint Online sites, and OneDrive for Business folders. A copy of each assessment is also stored in a SharePoint Online folder named
Assessments.
You need to create a data loss prevention (DLP) policy that prevents the employee assessments from being emailed to external users. You will use a document fingerprint to identify the assessment documents. The solution must minimize effort.
What should you include in the solution?

A. Create a fingerprint of 100 sample documents in the Assessments folder.

B. Create a sensitive info type that uses Exact Data Match (EDM).

C. Import 100 sample documents from the Assessments folder to a seed folder.

D. Create a fingerprint of AssessmentTemplate.docx.

Correct Answer: *D*
Reference:
https://docs.microsoft.com/en-us/microsoft-365/compliance/document-fingerprinting?view=o365-worldwide

Community vote distribution
D (83%) C (17%)

sergioandreslq Highly Voted 1 year, 11 months ago
I going with D,
It is just created document fingerprint using the template, this will be used as "Sensitive Info Type" to discover any employee assessment and apply the control over this file as required.
upvoted 8 times

yoshizutakahiro Most Recent 5 months, 1 week ago
Selected Answer: D
Dが正解です。
upvoted 2 times

xswe 7 months, 3 weeks ago
Since we want to go for the solution with the most minimized effort we should create a fingerprint of the AssessmentTemplate, when they are getting filled by the users we can still detect them thanks to the fingerprint of the docx file we have created.
upvoted 4 times

nicekoda 10 months, 2 weeks ago
D is wrong. Neither mail flow rules nor Document Fingerprinting supports the .dotx file type, even if this is a common file type for Word documents. https://learn.microsoft.com/en-us/training/modules/create-manage-sensitive-information-types/5-implement-document-fingerprint
upvoted 2 times

nicekoda 10 months, 2 weeks ago
pls disregard. Confused dotx with docx
upvoted 2 times

chrissempai 1 year, 2 months ago
Selected Answer: D
Was on exam the 9/9/22
upvoted 1 times

music_man 1 year, 3 months ago
Selected Answer: D
For document fingerprinting all we need is single template document to create a fingerprint using New-DlpFingerprint command. Then an SIT is created from the fingerprint.
upvoted 1 times

Azuz 1 year, 9 months ago
Selected Answer: D
Because the question states "The solution must minimize effort."
upvoted 1 times

Pravda 1 year, 10 months ago

On exam 1/20/2022

upvoted 1 times

Pravda 1 year, 10 months ago

Answer D
Key in the question are Word Template. For a template document you would create a fingerprint of the template. For a template I would think it would be .dotx and not a docx. But then that would give the answer away.

upvoted 3 times

Sam12 1 year, 10 months ago

A and E are missleading, seeds are used for trainable classifiers which is not the case for this question.

Fingerprinting uses file in your local drive and you do it via powershell:

$Employee_Template = Get-Content "C:\My Documents\Contoso Employee Template.docx" -Encoding byte -ReadCount 0
$Employee_Fingerprint = New-DlpFingerprint -FileData $Employee_Template -Description "Contoso Employee Template"

upvoted 1 times

MischaR 1 year, 10 months ago

Selected Answer: C

Documents are already in the assessment folder.. So you just need to choose this folder as a seed. Seems to be the fastest and easiest way to do it.

upvoted 1 times

bingomutant 1 year, 11 months ago

on second thoughts I will stick with A as must be administratively simpler

upvoted 3 times

bingomutant 1 year, 11 months ago

I would go for C here - it seems to satisfy the requirements especially sharepoint online - only doubt I have is the administrative ease.

upvoted 1 times

Domza 3 weeks, 1 day ago

Really!! Import 100 sample documents - is what you call minimize effort?? OMG

upvoted 1 times

Question #32 *Topic 2*

You have a Microsoft 365 subscription that uses Microsoft Exchange Online.
You need to receive an alert if a user emails sensitive documents to specific external domains.
What should you create?

A. a data loss prevention (DLP) policy that uses the Privacy category

B. a Microsoft Cloud App Security activity policy

C. a Microsoft Cloud App Security file policy

D. a data loss prevention (DLP) alert filter

Correct Answer: *A*
Reference:
https://docs.microsoft.com/en-us/microsoft-365/compliance/dlp-policy-reference?view=o365-worldwide

Community vote distribution
D (51%) C (27%) A (19%)

xlws Highly Voted 1 year, 12 months ago
The answer is C, https://docs.microsoft.com/en-us/defender-cloud-apps/data-protection-policies, sharing with external domain.
upvoted 14 times

sivis Highly Voted 2 years ago
Selected Answer: D
Correct answer is D
Alert can be configured in alert filter. Privacy category is used to choose templates and not alerts
upvoted 10 times

samrith Most Recent 1 month, 1 week ago
Community vote D(50%). A(19%) why sugguest answer A
upvoted 1 times

TomasValtor 2 months ago
Correct answer is A
To receive an alert if a user emails sensitive documents to specific external domains in a Microsoft 365 subscription that uses Microsoft Exchange Online, you should create a data loss prevention (DLP) policy that uses the Privacy category.
upvoted 2 times

TomasValtor 2 months ago
Option B, a Microsoft Cloud App Security activity policy, is not the correct answer because it is used to monitor and analyze user and admin activity across cloud apps, but it does not specifically monitor email attachments.

Option C, a Microsoft Cloud App Security file policy, is not the correct answer because it is used to scan files in cloud storage locations such as OneDrive and SharePoint, but it does not specifically monitor email attachments.

Option D, a DLP alert filter, is not the correct answer because it is used to filter the alerts generated by a DLP policy based on specific criteria, but it does not create the initial DLP policy.
upvoted 1 times

TomasValtor 2 months ago
To configure the DLP policy to send an alert when a user emails sensitive documents to specific external domains, you can follow these steps:

Open the Microsoft 365 compliance center and go to the Data loss prevention page.

Click Create a policy to create a new DLP policy.

In the Policy settings page, select the Privacy category and choose the sensitive information types that you want to protect.

In the Locations section, select the email option to apply the policy to emails.

In the Policy tips section, configure the action that you want to take when a sensitive document is detected. For example, you can send an alert to the user, manager, or administrator.

In the Policy settings section, select the external domains that you want to monitor.

Save the policy and test it to ensure that it is working as expected.
upvoted 2 times

Davidf 3 months, 3 weeks ago

Selected Answer: A

Only a DLP policy can create an alert. An alert filter just filters existing alerts. File and activity policies don't make sense in this context

upvoted 1 times

cris_exam 5 months, 2 weeks ago

Selected Answer: C

It says specific external domains so I'll go with C.

https://learn.microsoft.com/en-us/defender-cloud-apps/data-protection-policies#policies

Sharing with external domains - Receive an alert about any file shared with accounts owned by specific external domains. For example, files shared with a competitor's domain. Select the external domain with which you want to limit sharing.

upvoted 2 times

doori88 6 months ago

its A correct, when you create a DLP policy you can use custom category or the privacy category implied, from there you do not need to set an action rather than sending alert to admin about it

upvoted 2 times

AIPL200 6 months, 3 weeks ago

Why not C?

upvoted 1 times

joshuactz 7 months, 1 week ago

Selected Answer: A

I go for option A too:
You should create a DLP policy that detects sensitive information being sent to specific external domains. Once the policy is in place, it will trigger alerts when sensitive documents are emailed to those domains.

DLP alert filter (Option D) is a mechanism for narrowing down and monitoring specific DLP policy violations or incidents. However, it doesn't directly prevent or alert you when sensitive documents are emailed to specific external domains. It is used in conjunction with a DLP policy to refine the alerts generated by the policy. So, the primary action should be creating a DLP policy, and the alert filter can be used to fine-tune the notifications.

upvoted 2 times

wooyourdaddy 9 months, 1 week ago

I believe the answer is C as per this link:

https://learn.microsoft.com/en-us/defender-cloud-apps/data-protection-policies#policies

Which states:

The following are examples of file policies that can be created:

Sharing with external domains - Receive an alert about any file shared with accounts owned by specific external domains. For example, files shared with a competitor's domain. Select the external domain with which you want to limit sharing.

upvoted 2 times

Rockalm 10 months, 4 weeks ago

Tried answer A in my test tenant. There is the option to "Customize advanced DLP rules". With "Create Rule" you can define "Recipient domain is". As action you can send an email to the admin. So, also A can be right.

upvoted 3 times

NinjaSchoolProfessor 11 months, 1 week ago

Answer is [C]. Search for "External" file policy: https://learn.microsoft.com/en-us/defender-cloud-apps/data-protection-policies . If the question had stated "alert policy" instead of "alert filter" in [D], then both [C] and [D] would have been correct. Alert Policy URL for reference: https://learn.microsoft.com/en-us/microsoft-365/compliance/alert-policies

upvoted 1 times

lkeinater 1 year ago

Question asks " if a user emails" I don't think MCAS applies to emails only cloud applications?
Either A or D for me. I can't confirm either one though. Very tough question.

upvoted 5 times

chrissempai 1 year, 2 months ago

Selected Answer: C

the good answer should be B.
A : not possible
B : it report on activity
C : see : https://docs.microsoft.com/en-us/defender-cloud-apps/data-protection-policies
D: Alert filter is a reporting not an alerting possibility

upvoted 1 times

chrissempai 1 year, 2 months ago

C not B, sorry

upvoted 1 times

music_man 1 year, 3 months ago

Selected Answer: D

I'm going with D because the question only mentions an M365 subscription with Exchange Online. MCAS would likely not be included. The alert filter for DLP works with E1 and E3 skus. https://docs.microsoft.com/en-us/microsoft-365/compliance/dlp-configure-view-alerts-policies?view=o365-worldwide#alert-configuration-experience

upvoted 3 times

MahmoudEldeep 1 year, 7 months ago

Selected Answer: D

Correct answer is D

upvoted 2 times

JamesM9 1 year, 7 months ago

I have tested this in my tenancy today and can see that the MCAS file policy has a specific template for this named "File shared with an unauthorised domain". This gives you the option to configure alert notifications and specify which domains this alert applies to.

Very confusing, as I could also create something similar when creating a DLP policy, but the MCAS file policy appears to be more specific (and easier to create). Within the MCAS file policy I could also specify sensitive information types, so that covers another part of the question.

A very tricky question that as with many of these, there is a good case for more than one answer to be correct.

For me, the answer is C - MCAS file policy.

upvoted 4 times

HOTSPOT -

You create a data loss prevention (DLP) policy that meets the following requirements:

- Prevents guest users from accessing a sensitive document shared during a Microsoft Teams chat
- Prevents guest users from accessing a sensitive document stored in a Microsoft Teams channel

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

NOTE: Each correct selection is worth one point.

Hot Area:

Answer Area

Prevents guest users from accessing a sensitive document shared during a Microsoft Teams chat: [ ]
- Exchange email
- OneDrive accounts
- SharePoint sites
- Teams chat and channel messages

Prevents guest users from accessing a sensitive document stored in a Microsoft Teams channel: [ ]
- Exchange email
- OneDrive accounts
- SharePoint sites
- Teams chat and channel messages

Correct Answer:

Answer Area

Prevents guest users from accessing a sensitive document shared during a Microsoft Teams chat: [ ]
- Exchange email
- OneDrive accounts
- SharePoint sites
- Teams chat and channel messages

Prevents guest users from accessing a sensitive document stored in a Microsoft Teams channel: [ ]
- Exchange email
- OneDrive accounts
- SharePoint sites
- Teams chat and channel messages

Reference:

https://docs.microsoft.com/en-us/microsoft-365/compliance/dlp-microsoft-teams?view=o365-worldwide https://docs.microsoft.com/en-us/microsoftteams/sharepoint-onedrive-interact

Eltooth Highly Voted 2 years, 6 months ago

Team chat implies a 1-2-1 conversation therefore any docs are shared from users ODfB.
Teams channel used SPO to store and share docs. Answer looks correct.

upvoted 20 times

xswe Most Recent 7 months, 3 weeks ago

DLP policy that will protect documents shared in Teams chat = Onedrive
Teams channels = Sharepoint

upvoted 1 times

wooyourdaddy 1 year, 5 months ago

I wrote the exam today, this question was on it, I choose Box1: OneDrive accounts, Box2: SharePoint sites, scored 890!

upvoted 2 times

Jahoor69 1 year, 8 months ago

its correct.
https://docs.microsoft.com/en-us/microsoft-365/compliance/dlp-microsoft-teams?view=o365-worldwide#:~:text=Example%202%3A%20Protecting,365%20Advanced%20Compliance.)

upvoted 2 times

Pravda 1 year, 10 months ago

On exam 1/20/2022

upvoted 1 times

Cmora 1 year, 11 months ago

This should be:
1. One Drive and Teams Chat... OneDrive is where Teams Chat files are stored.
2.Sharepoint and Teams Channel... Sharepoint is where Teams Channel files are stored.

For both, you need to have the Teams Location and the respective storage location selected.

upvoted 1 times

[Removed] 2 years ago

The answer is correct, in the documentation has an example of this scenario:

"Example 2: Protecting sensitive information in documents. Suppose that someone attempts to share a document with guests in a Microsoft Teams channel or chat, and the document contains sensitive information. If you have a DLP policy defined to prevent this, the document won't open for those users. Your DLP policy must include SharePoint and OneDrive in order for protection to be in place. This is an example of DLP for SharePoint that shows up in Microsoft Teams, and therefore requires that users are licensed for Office 365 DLP (included in Office 365 E3), but does not require users to be licensed for Office 365 Advanced Compliance.)"

https://docs.microsoft.com/en-us/microsoft-365/compliance/dlp-microsoft-teams?view=o365-worldwide&viewFallbackFrom=o365-worldwide%20https%3A%2F%2Fdocs.microsoft.com%2Fen-us%2Fmicrosoftteams%2Fsharepoint-onedrive-interact

upvoted 2 times

Goseu 2 years, 5 months ago

As stated at the given article :
Protecting sensitive information in documents. Suppose that someone attempts to share a document with guests in a Microsoft Teams channel or chat, and the document contains sensitive information. If you have a DLP policy defined to prevent this, the document won't open for those users. Your DLP policy must include SharePoint and OneDrive in order for protection to be in place

upvoted 1 times

Anker 2 years, 5 months ago

Based on the docs statement of"If you want to make sure documents that contain sensitive information are not shared inappropriately in Teams, make sure SharePoint sites and OneDrive accounts are turned on, along with Teams chat and channel messages" I would think 1) ODfB + Teams locations and then 2) SPO + Teams locations

upvoted 2 times

dasha_an 2 years, 6 months ago

It must be sharePoint + Onedrive + Teams chat and channel messages

upvoted 1 times

dasha_an 2 years, 6 months ago

"If you want to make sure documents that contain sensitive information are not shared inappropriately in Teams, make sure SharePoint sites and OneDrive accounts are turned on, along with Teams chat and channel messages"
The first answer will be : sharePoint + Onedrive
The second is correct

upvoted 1 times

Question #34 *Topic 2*

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

Correct Answer: *D*
Reference:
https://docs.microsoft.com/en-us/microsoft-365/compliance/endpoint-dlp-using?view=o365-worldwide

Community vote distribution

liozuf Highly Voted 2 years, 6 months ago
B. an action is a better answer
upvoted 32 times

Eltooth Highly Voted 2 years, 6 months ago
B. An action would prevent a data copy function.
upvoted 14 times

mbhasker Most Recent 2 days, 20 hours ago
D. user overrides
upvoted 1 times

TomasValtor 2 months ago
To configure 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), and then use the information from the policy to restrict the ability to copy the sensitive data to the clipboard, you need to configure an "Action" in the policy rule.
upvoted 1 times

TomasValtor 2 months ago
The "Action" is a response that occurs when a data loss prevention (DLP) policy is triggered. In this case, when the policy rule detects credit card data on a Windows 10 device joined to Azure AD, it will trigger the "Action" you have configured.
To restrict the ability to copy the sensitive data to the clipboard, you need to choose an appropriate "Action." One of the available actions is to "Block Access" to the sensitive data. You can also customize the action by choosing to "Notify User" with a custom message that explains why the access has been blocked. This will help prevent users from unknowingly violating the policy by providing them with clear information about what actions are permitted and what are not.
Therefore, the correct answer is B - an Action. The incident report is used to notify the appropriate personnel when a policy rule is triggered. User notifications and user overrides are not directly related to configuring an action to restrict the ability to copy sensitive data to the clipboard.
upvoted 1 times

dmoorthy 7 months, 1 week ago
B is the right Answer.
upvoted 1 times

GeoffLule 7 months, 1 week ago
Scenario 3: Modify the existing policy, block the action with allow override
upvoted 1 times

xswe 7 months, 3 weeks ago
An action, test it out in purview to find this out by yourself!
upvoted 2 times

Katea 8 months, 3 weeks ago
Selected Answer: B
B. an action is a better answer
upvoted 1 times

Katea 8 months, 3 weeks ago

it's confusing because we can block the action by allow override : https://docs.microsoft.com/en-us/microsoft-365/compliance/endpoint-dlp-using?view=o365-worldwide

upvoted 1 times

chrissempai 1 year, 2 months ago

Selected Answer: B

The good answer is B, it's an action.

If you choose D, you can only do :
User overrides
-Allow overrides from M365 services
-Business justifications
When users override an activity, you can require them to provide a business justification when overriding an activity.

upvoted 1 times

Lotanna_ 1 year, 4 months ago

B for me

upvoted 1 times

wooyourdaddy 1 year, 5 months ago

Selected Answer: B

I wrote the exam today, this question was on it, I choose B, scored 890!

upvoted 2 times

MahmoudEldeep 1 year, 7 months ago

Selected Answer: B

Correct answer is B

upvoted 1 times

Solozero 1 year, 9 months ago

Selected Answer: B

B. an action

upvoted 2 times

Pravda 1 year, 10 months ago

On exam 1/20/2022

upvoted 1 times

Mdwro 1 year, 10 months ago

Selected Answer: A

I read it multiple times and have doubts. Initially thought about B. But then, questions says:
"You PLAN TO USE information from the policy to restrict the ability to copy the sensitive data to the clipboard.".
If we plan to use information, shouldn't it trigger an indcident report, which later we can re-use?

upvoted 5 times

Zorolloo 1 year, 11 months ago

Selected Answer: B

B. is the correct answer

upvoted 3 times

Ras1364 2 years ago

The given answer seems correct due to the question that says: Configure a DLP policy to "report" when credit card data is found on a Windows 10 device joined to Azure Active Directory.

upvoted 1 times

Ras1364 1 year, 11 months ago

I changed my mind to "B" because it makes more sense

upvoted 1 times

Question #35 *Topic 2*

HOTSPOT -

You have a Microsoft 365 E5 tenant.

Data loss prevention (DLP) policies are applied to Exchange email, SharePoint sites, and OneDrive accounts locations.

You need to use PowerShell to retrieve a summary of the DLP rule matches from the last seven days.

Which PowerShell module and cmdlet should you use? To answer, select the appropriate options in the answer area.

NOTE: Each correct selection is worth one point.

Hot Area:

Answer Area

Module:
- Azure Active Directory (Azure AD)
- Exchange Online
- SharePoint Online

Cmdlet:
- Get-DlpDetailReport
- Get-DlpDetectionsReport
- Get-DlpPolicy
- Get-DlpSiDetectionsReport

Correct Answer:

Answer Area

Module:
- Azure Active Directory (Azure AD)
- Exchange Online
- SharePoint Online

Cmdlet:
- Get-DlpDetailReport
- Get-DlpDetectionsReport
- Get-DlpPolicy
- Get-DlpSiDetectionsReport

Reference:

https://docs.microsoft.com/en-us/powershell/module/exchange/get-dlpdetectionsreport?view=exchange-ps

Eltooth Highly Voted 2 years, 5 months ago

Exchange Online and Get-DlpDetectionsReport.
" Use the Get-DlpDetectionsReport cmdlet to list a summary of Data Loss Prevention (DLP) rule matches for Exchange Online, SharePoint Online and OneDrive for Business in your cloud-based organization for the last 30 days."

upvoted 12 times

Gesbie Most Recent 3 months, 3 weeks ago

was on Exam August 9, 2023

upvoted 1 times

xswe 7 months, 3 weeks ago

Exchange Online
Get-DLPDetectionsReport cmdlet will show a summary of the DLP rule matches in Exchange, Sharepoint and Onedrive

upvoted 2 times

wooyourdaddy 1 year, 5 months ago

I wrote the exam today, this question was on it, I choose Box1: Exchange Online, Box2: Get-DlpDectioinsReport, scored 890!

upvoted 4 times

PrettyFlyWifi 1 year, 9 months ago

Correct answer here. Key word being "summary" as the Get-DlpDetailReport is near identical, as it "lists details" about DLP rule matches, whereas Get-DlpDetections is focused on the summary of the DLP rule matches.

upvoted 1 times

Pravda 1 year, 10 months ago

On exam 1/20/2022

upvoted 2 times

shanti0091 2 years, 4 months ago

correct Answer

upvoted 4 times

HOTSPOT -

You plan to implement Microsoft 365 Endpoint data loss prevention (Endpoint DLP).

You need to identify which end user activities can be audited on the endpoints, and which activities can be restricted on the endpoints.

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

NOTE: Each correct selection is worth one point.

Hot Area:

Answer Area

Print a protected document: [ ]
- Can be audited only
- Can be restricted only
- Can be audited and restricted

Create a document in a monitored location: [ ]
- Can be audited only
- Can be restricted only
- Can be audited and restricted

Copy a protected document to USB removable media: [ ]
- Can be audited only
- Can be restricted only
- Can be audited and restricted

Answer Area

Print a protected document: [ ]
- Can be audited only
- Can be restricted only
- Can be audited and restricted

Create a document in a monitored location: [ ]
- Can be audited only
- Can be restricted only
- Can be audited and restricted

Copy a protected document to USB removable media: [ ]
- Can be audited only
- Can be restricted only
- Can be audited and restricted

Correct Answer:

Reference:

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

Banzaaai Highly Voted 2 years, 6 months ago

Print: audited and restricted
Creation: audited only

USB: audited and restricted

checked, all are corrected
upvoted 22 times

xswe Highly Voted 7 months, 3 weeks ago
Its important to know that the ONLY actions the Endpoint DLP cant restrict is
- Creation an item
- Rename an item

So.. the correct answer is:
Audited + Restricted
Audited
Audited + Restricted
upvoted 5 times

Pravda Most Recent 1 year, 10 months ago
On exam 1/20/2022
upvoted 2 times

Eltooth 2 years, 5 months ago
Looks correct.
upvoted 4 times

Che1 2 years, 5 months ago
All correct
upvoted 4 times

k4d4v4r 2 years, 6 months ago
https://docs.microsoft.com/en-us/microsoft-365/compliance/endpoint-dlp-learn-about?view=o365-worldwide#endpoint-activities-you-can-monitor-and-take-action-on
upvoted 4 times

Question #37 *Topic 2*

You have a Microsoft 365 E5 tenant and the Windows 10 devices shown in the following table.

Name	Azure Active Directory (Azure AD)-joined	Configuration
Device1	Yes	Onboarded to the Microsoft 365 compliance center
Device2	Yes	Onboarded to Microsoft Defender for Endpoint
Device3	Yes	Enrolled in Microsoft Intune
Device4	No	Enrolled in Microsoft Intune

To which devices can you apply Microsoft 365 Endpoint data loss prevention (Endpoint DLP) settings?

A. Device1, Device3, and Device4 only

B. Device1, Device2, Device3, and Device4

C. Device1 and Device2 only

D. Device1 and Device3 only

E. Device1 only

Correct Answer: *C*

Reference:

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

Community vote distribution

C (100%)

Che1 Highly Voted 2 years, 5 months ago

Correct answer. If you already have device on boarded to Microsoft Defender for endpoint then device will appear in the list.

upvoted 11 times

Gesbie Most Recent 3 months, 3 weeks ago

was on Exam August 9, 2023

upvoted 2 times

xswe 7 months, 3 weeks ago

If you want to use endpoint DLP you have to onboard the devices

upvoted 1 times

prabhjot 1 year, 2 months ago

seems correct

upvoted 1 times

wooyourdaddy 1 year, 5 months ago

Selected Answer: C

I wrote the exam today, this question was on it, I choose C, scored 890!

upvoted 2 times

Pravda 1 year, 10 months ago

On exam 1/20/2022

upvoted 1 times

HardcodedCloud 1 year, 11 months ago

Device onboarding is shared across Microsoft 365 and Microsoft Defender for Endpoint (MDE). If you've already onboarded devices to MDE, they will appear in the managed devices list and no further steps are necessary to onboard those specific devices. Onboarding devices in Compliance center also onboards them into MDE.

upvoted 4 times

Eltooth 2 years, 5 months ago

Correct.

upvoted 4 times

HOTSPOT -

You have a Microsoft SharePoint Online site that contains the following files.

Name	Modified by	Data loss prevention (DLP) status
File1.docx	Manager1	None
File2.docx	Manager1	Matched by DLP
File3.docx	Manager1	Blocked by DLP

Users are assigned roles for the site as shown in the following table.

Name	Role
User1	Site owner
User2	Site member

Which files can User1 and User2 view? To answer, select the appropriate options in the answer area.

NOTE: Each correct selection is worth one point.

Hot Area:

Answer Area

User1:
- File1.docx only
- File1.docx and File2.docx only
- File1.docx, File2.docx, and File3.docx

User2:
- File1.docx only
- File1.docx and File2.docx only
- File1.docx, File2.docx, and File3.docx

Correct Answer:

Answer Area

User1:
- File1.docx only
- File1.docx and File2.docx only
- File1.docx, File2.docx, and File3.docx

User2:
- File1.docx only
- File1.docx and File2.docx only
- File1.docx, File2.docx, and File3.docx

Reference:

https://social.technet.microsoft.com/wiki/contents/articles/36527.implement-data-loss-prevention-dlp-in-sharepoint-online.aspx

HardcodedCloud Highly Voted 1 year, 11 months ago

Tested & verified

upvoted 8 times

Discuss4certi Highly Voted 2 years, 3 months ago

according to the link in the answer: Until the sensitive information has been removed from the user, the document access will be restricted to its owner, last modified and the Site owner

upvoted 6 times

TAN 1 year, 10 months ago

except owner, last modifier and site owner.. "For use only by"

upvoted 1 times

izgi43 Most Recent 2 weeks, 4 days ago

on exam thu nov 9
upvoted 1 times

daavidsc400 1 year, 9 months ago
What does "matched by dlp" actually mean in terms of access?
upvoted 3 times

Rockalm 10 months, 4 weeks ago
Matched by another DLP rulethat doesn't block.
upvoted 1 times

Pravda 1 year, 10 months ago
On exam 1/20/2022
upvoted 1 times

Eltooth 2 years, 4 months ago
Correct.
upvoted 1 times

shanti0091 2 years, 4 months ago
correct
upvoted 1 times

Goseu 2 years, 5 months ago
looks good .
upvoted 1 times

Question #39 *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 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 enroll the computers in Microsoft Intune.
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

Community vote distribution

B (100%)

Gesbie 3 months, 3 weeks ago

was on Exam August 9, 2023

upvoted 1 times

Gesbie 3 months, 3 weeks ago

was on Exam August 9, 2023

upvoted 1 times

IAGirl 1 year, 9 months ago

Selected Answer: B

Intune can be used to install package to enroll on Microsoft 365 compliance center or Microsoft Defender for Endpoint. The answer is No

upvoted 2 times

remy75 1 year, 11 months ago

According to this document, Intune can be used for onboarding:
https://docs.microsoft.com/en-us/microsoft-365/security/defender-endpoint/configure-endpoints-mdm?view=o365-worldwide
so the answer seems to be YES

upvoted 1 times

girikedar 1 year, 11 months ago

I think Enrolling the Device into intune & onboarding the device might work

upvoted 4 times

Dreamhaxx 1 year, 10 months ago

Correct, but you don't see onboarding of Defender for Endpoint here. This is why no is the correct answer.
b - Correct

upvoted 4 times

bingomutant 1 year, 11 months ago

I dont know why Intune does not satisfy this

upvoted 3 times

sergioandreslq 1 year, 11 months ago

The documentation says that you need to have defender for endpoint or deploy the Endpoint DLP configuration package.
The documentation doesn't mention onboarding with Intune, So, based on the documentation, we should assume that intune is not enough as pre-requirement for endpoint DLP.

upvoted 5 times

Eltooth 2 years, 4 months ago

Correct - No.

upvoted 1 times

olsi 2 years, 6 months ago

Correct

upvoted 4 times

Question #40 *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 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

Gesbie 3 months, 3 weeks ago
was on Exam August 9, 2023
upvoted 1 times

Gesbie 3 months, 3 weeks ago
was on Exam August 9, 2023
upvoted 1 times

NinjaSchoolProfessor 11 months, 1 week ago
Correct since there is no mention to the use of MPIP (formerly AIP) being deployed. If MPIP was deployed and communicating with that endpoint, then installing the unified labeling client would be correct.
upvoted 1 times

Eltooth 2 years, 4 months ago
Correct - no.
upvoted 2 times

JoeRoxy007 2 years, 5 months ago
https://docs.microsoft.com/en-us/microsoft-365/compliance/endpoint-dlp-getting-started?view=o365-worldwide describes the conditions for this to work. These conditions include that a device must be one of these : • Azure Active Directory (Azure AD) joined
• Hybrid Azure AD joined
• AAD registered
AND enable device monitoring and onboard your endpoints before you can monitor and protect sensitive items on a device. Both of these actions are done in the Microsoft 365 Compliance portal. However, device that have previously been onboarded into Microsoft Defender for Endpoint, will already appear in the managed devices list.
upvoted 4 times

olsi 2 years, 6 months ago
Correct. Devices have to be onboarded in DLP Endpoint mgmt
upvoted 2 times

Question #41 *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 10. The computers are onboarded to the Microsoft 365 compliance center.
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 the Cloud App Security portal, you mark the application as Unsanctioned.
Does this meet the goal?

A. Yes

B. No

Correct Answer: *B*
Reference:
https://docs.microsoft.com/en-us/microsoft-365/compliance/endpoint-dlp-using?view=o365-worldwide

FronsterRoo 1 year, 6 months ago
Sanctioning/unsanctioning an app

You can unsanction a specific risky app by clicking the three dots at the end of the row. Then select Unsanction. Unsanctioning an app doesn't block use, but enables you to more easily monitor its use with the Cloud Discovery filters. You can then notify users of the unsanctioned app and suggest an alternative safe app for their use.
upvoted 3 times

arlia 1 year, 9 months ago
talking about dlp not about blocking the app, B
upvoted 3 times

Question #42 *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 keys in plain text to third parties.
You need to ensure that when Azure Storage keys are emailed, the emails are encrypted.
Solution: You configure a mail flow rule that matches the text patterns.
Does this meet the goal?

A. Yes

B. No

Correct Answer: *B*
Reference:
https://docs.microsoft.com/en-us/exchange/policy-and-compliance/mail-flow-rules/conditions-and-exceptions?view=exchserver-2019

Community vote distribution

B (100%)

nupagazi Highly Voted 1 year, 10 months ago
Answer is correct, you can use mail flow rule to match text pattern but storage account key is binary value
upvoted 7 times

[Removed] Highly Voted 2 years ago
Selected Answer: B
The answer is right, using the "text patterns" condition in the Exchange transport rule would not work.

The condition to be used in the Exchange transport rule would be "The message contains any of this sensitive information..." and select the Sensitive Info Type "Azure Account Storage Key".
upvoted 6 times

kiketxu 1 year, 1 month ago
Agreed. Regex can be used to match text paterns in subject or body.
https://learn.microsoft.com/en-us/exchange/policy-and-compliance/mail-flow-rules/conditions-and-exceptions?view=exchserver-2019#message-subject-or-body
upvoted 1 times

Pravda Most Recent 1 year, 10 months ago
On exam 1/20/2022
upvoted 1 times

ExamReviewerIZ 2 years, 1 month ago
I believe this could be achieved using Mailflow Rules, as you can use regex for Azure Storage Keys.

Someone could confirm if is possible to represent an Azure Storage Key using regular expressions.
upvoted 2 times

Question #43 *Topic 2*

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.

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
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
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

See_Es Highly Voted 10 months, 1 week ago

I would say the answer is wrong. The Win11 device is not enrolled in Intune so the Endpoint Manager is not an option. The macos device is enrolled in intune so this devices can be enrolled with endpoint manager
https://learn.microsoft.com/en-us/microsoft-365/compliance/device-onboarding-macos-overview?view=o365-worldwide
upvoted 5 times

See_Es 10 months, 1 week ago
I would say Win11 would be local script and GPO (however we don't even know the device is AD-Joined so GPO might not even be an option. And for the mac it is endpoint management only.
upvoted 9 times

Sango Most Recent 3 months, 1 week ago
macOS is now both Local Script and Intune.
upvoted 3 times

cris_exam 5 months, 2 weeks ago
Based on the below documentation my answer is:

Device1: Local Script, GPO and Ms Endpoint Config Manager
Device2: Microsoft Endpoint Config Manager only

For Win:
https://learn.microsoft.com/en-us/microsoft-365/compliance/device-onboarding-overview?view=o365-worldwide#onboarding-windows-10-or-windows-11-devices

In this deployment scenario, you'll onboard Windows 10 or Windows 11 devices that have not been onboarded yet.

5. Choose the appropriate procedure to follow from the table below:
- Intune
- Config Manager
- Group Policy
- Local Script
- VDI

For macOS:
https://learn.microsoft.com/en-us/microsoft-365/compliance/device-onboarding-macos-overview?view=o365-worldwide

MacOS devices can be onboarded into Microsoft Purview solutions using either Intune or JAMF Pro.
upvoted 1 times

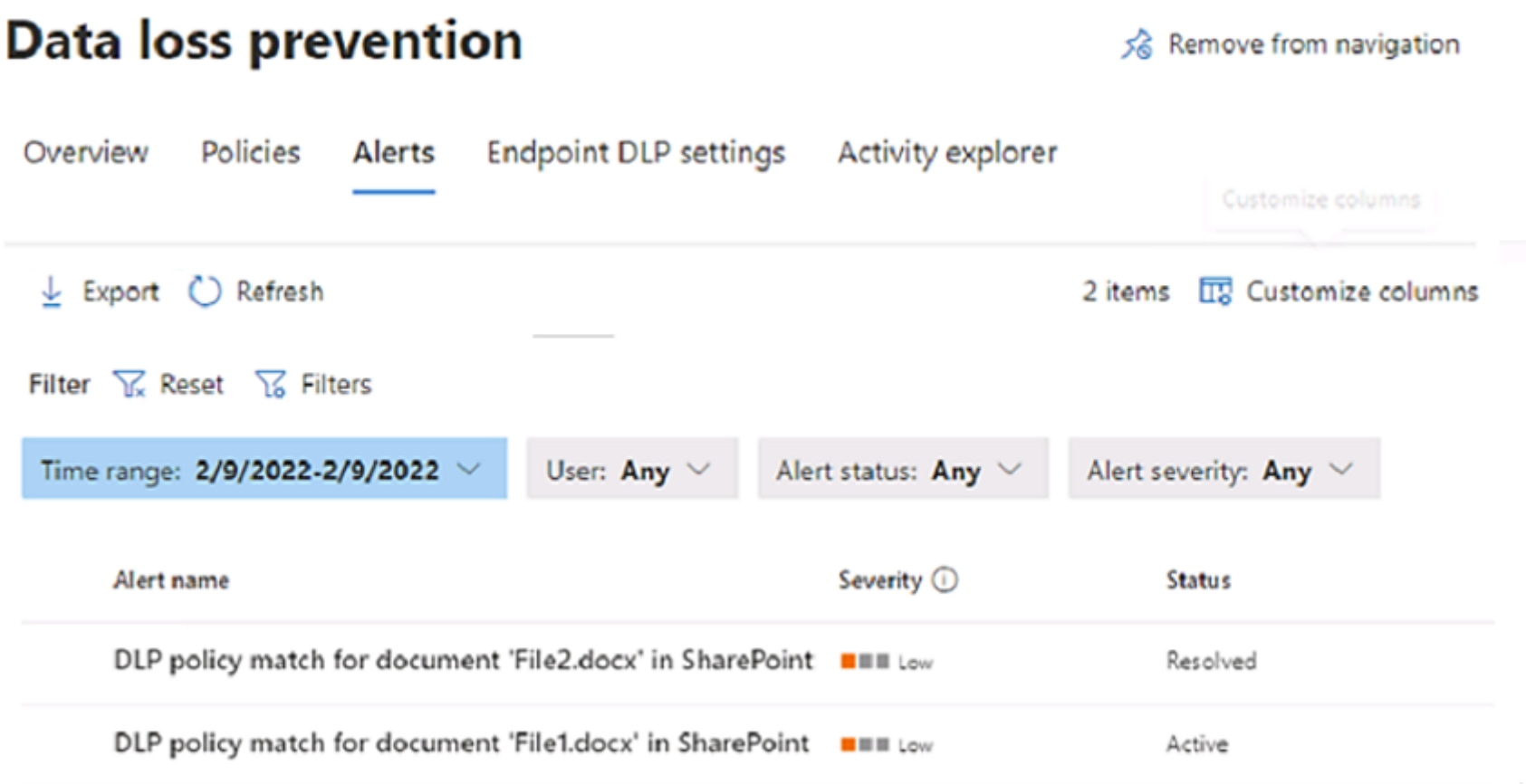
js124 8 months ago
Mac OS is enrolled by Endpoint management(Intune).
"MacOS devices can be onboarded into Microsoft Purview solutions using either Intune or JAMF Pro."
https://learn.microsoft.com/en-us/microsoft-365/compliance/device-onboarding-macos-overview?view=o365-worldwide
upvoted 1 times

formazionehs 9 months ago
The Win 11 device is not enrolled in Intune so can be onboarded using a Local Script or GPO.
The Mac OS device is enrolled in Intune and can be onboarded using a Local Script or MEM / Intune.
upvoted 3 times

HOTSPOT
-

You have a Microsoft 365 E5 subscription.

You have the alerts shown in the following exhibit.



Use the drop-down menus to select the answer choice that completes each statement based on the information presented in the graphic.

NOTE: Each correct selection is worth one point.

Answer Area

The alert status for File1.docx can be changed to **[answer choice]**.

- Dismissed only
- Investigating only
- Resolved only
- Investigating and Dismissed only
- Investigating, Dismissed, and Resolved

The alert status for File2.docx can be changed to **[answer choice]**.

- Active only
- Investigating only
- Investigation and Dismissed
- Active, Investigation, and Dismissed

Correct Answer:

Answer Area

The alert status for File1.docx can be changed to **[answer choice]**.

- Dismissed only
- Investigating only
- Resolved only
- Investigating and Dismissed only
- Investigating, Dismissed, and Resolved

The alert status for File2.docx can be changed to **[answer choice]**.

- Active only
- Investigating only
- Investigation and Dismissed
- Active, Investigation, and Dismissed

CharlieGolf Highly Voted 8 months, 2 weeks ago

Correct. See discussion of this in MS-500 exam question: https://www.examtopics.com/discussions/microsoft/view/82178-exam-ms-500-topic-3-question-27-discussion/

upvoted 5 times

ServerBrain Most Recent 2 months ago

Box 1 = Investigation and Dismissed
Box 2 = Investigation, Dismissed and Resolved
Why would you want to change it to the same status in each box

upvoted 2 times

Question #45 *Topic 2*

You are creating a data loss prevention (DLP) policy that will apply to all available locations.

You configure an advanced DLP rule in the policy.

Which type of condition can you use in the rule?

A. Keywords

B. Content search query

C. Sensitive info type

D. Sensitive label

Correct Answer: *C*

Community vote distribution

C (100%)

See_Es Highly Voted 10 months, 1 week ago

Selected Answer: C

Correct. Tested in my tenant. With all locations selected the sensitive info type is the only option left.

upvoted 7 times

Domza 3 weeks, 1 day ago

Thank you

upvoted 1 times

Question #46 *Topic 2*

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*

Community vote distribution

B (57%) D (43%)

Vashill 1 month, 2 weeks ago

Selected Answer: B

It should be B

upvoted 1 times

jamspurple 1 month, 3 weeks ago

Selected Answer: B

There is already a Sensitive Info Type for source code. So it should not be trainable classifier

upvoted 2 times

Davidf 3 months, 3 weeks ago

Selected Answer: D

There is a source code trainable classifier

upvoted 2 times

217f3c9 6 months, 2 weeks ago

Selected Answer: D

I owuld say D. a source code trainable classifier is pretrained in PurView. Less effort than monitor source code dictionary

upvoted 1 times

mclean 6 months, 3 weeks ago

Selected Answer: B

Sensitive info types in SharePoint Online help you identify and protect sensitive content such as credit card numbers, social security numbers, and source code. In this case, you want to prevent the sharing of files that contain source code.

A sensitive info type that uses a keyword dictionary allows you to define a list of specific keywords or phrases associated with source code. SharePoint Online will scan the content and metadata of files for matches against the keyword dictionary, and if a match is found, it can trigger appropriate actions such as blocking or alerting.

This approach minimizes administrative effort because you can maintain and update the keyword dictionary as needed without requiring extensive manual configuration or training.

Therefore, option B is the correct choice for creating a DLP policy to prevent the sharing of files containing source code in Microsoft SharePoint Online.

upvoted 1 times

xswe 7 months, 3 weeks ago

Just use the trainable classifier that have been configured and trained already to look for source code

upvoted 1 times

Chris7910 9 months, 3 weeks ago

Isn't it an administrative effort creating a trainable classifier here?

upvoted 1 times

wooyourdaddy 9 months, 1 week ago

There is a pre-trained classifiers for source code documented at:

https://learn.microsoft.com/en-us/microsoft-365/compliance/classifier-tc-definitions?view=o365-worldwide#source-code

Microsoft has also announced a new update version that is in public preview:

https://techcommunity.microsoft.com/t5/security-compliance-and-identity/public-preview-of-new-source-code-classifier-and-general/ba-p/3732696

upvoted 5 times

Question #47 *Topic 2*

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*

Community vote distribution

C (100%)

Domza 3 weeks, 1 day ago

Correct ~

upvoted 1 times

Gesbie 3 months, 3 weeks ago

was on Exam August 9, 2023

upvoted 1 times

xswe 7 months, 3 weeks ago

Changing the alert threshold will create less alerts but not effect the policy

upvoted 4 times

See_Es 10 months, 1 week ago

Selected Answer: C

Correct. Tested in my tenant

upvoted 4 times

wooyourdaddy 9 months, 1 week ago

Also documented here:

https://learn.microsoft.com/en-us/microsoft-365/compliance/dlp-configure-view-alerts-policies?view=o365-worldwide#alert-configuration-experience

upvoted 2 times

Question #48 *Topic 2*

HOTSPOT
-

Your company has offices in 30 countries.

The company has a Microsoft 365 E5 subscription that uses Microsoft SharePoint Online.

You create SharePoint sites for each department and country. The sites are named by using a naming convention of [Department]-[Country], for example, Sales-France.

You need to prevent files stored on the sites of the sales department from being deleted permanently for five years. The solution must meet the following requirements:

• Only affect the files on the sales department sites.
• Minimize administrative effort.

What should you include in the solution? To answer, select the appropriate options in the answer area.

NOTE: Each correct selection is worth one point.

Answer Area

To prevent the file deletion, use:

An auto-labeling retention policy
A records management file plan
A retention policy
An auto-labeling retention policy

Restrict the solution to the sales department sites by using:

A sensitive info type
A static scope
An adaptive scope

Correct Answer:

Answer Area

To prevent the file deletion, use:

An auto-labeling retention policy
A records management file plan
A retention policy
An auto-labeling retention policy

Restrict the solution to the sales department sites by using:

A sensitive info type
A static scope
An adaptive scope

CharlieGolf Highly Voted 8 months, 2 weeks ago

Retention policy + Adaptive scope. See justification (minimal effort/policies) for adaptive scopes here: https://learn.microsoft.com/en-us/microsoft-365/compliance/purview-adaptive-scopes?view=o365-worldwide

upvoted 5 times

xswe Highly Voted 7 months, 3 weeks ago

A retention policy will ensure that content stored in one location in SharePoint will get retained for 5 years, no label needed here if we want to retain a whole site.
An adaptive scope can be used to ensure that only the correct users will get this retention policy applied to them

upvoted 5 times

217f3c9 Most Recent 6 months ago

Would say retention policy and adaptive scope - for the future additional offices can be included without touching the policy >> minimize effort

upvoted 2 times

See_Es 10 months, 1 week ago

Incorrect. Should be a retention policy and adaptive scope.
It should adapt to the naming convention of [Department]-[Country]. Department being Sales.

upvoted 5 times

ARYMBS 7 months ago

You forgot "Minimize administrative effort.". Retention policy with static scope (required SharePoint site) will be enough.

upvoted 1 times

ImparaLeon 1 month ago

In the question they speak of "department siteS" so I would say multiple.. In the situation of multiple sites for the Sales department, I would go with Retention policy + Adaptive scope.

upvoted 1 times

Question #49 *Topic 2*

You have a Microsoft 365 E5 tenant.

You create a data loss prevention (DLP) policy.

You need to ensure that the policy protects documents in Microsoft Teams chat sessions.

Which location should you enable in the policy?

A. OneDrive accounts

B. Exchange email

C. Teams chat and channel messages

D. SharePoint sites

Correct Answer: *C*

Community vote distribution

A (100%)

tarroka Highly Voted 10 months, 1 week ago

Correct Answer is A OneDrive as it refers to document in the question

upvoted 13 times

See_Es 10 months, 1 week ago

Agreed. Documents that are shared in a chat are uploaded to onedrive. The question does not regard the chat messages but the documents shared in the chat. So A; OneDrive.

upvoted 5 times

xswe Most Recent 7 months, 3 weeks ago

You have to create a DLP policy that protects files in Onedrive if you want to protect documents being shared in Teams Chat sessions

upvoted 1 times

FireOzzie 8 months, 4 weeks ago

Selected Answer: A

Answer must be A - OneDrive.
Documents shared in Team Chats are stored in OneDrive and shared in Channel Chats are stored in SharePoint Sites

upvoted 2 times

FireOzzie 8 months, 4 weeks ago

Answer must be A - OneDrive.
Documents shared in Team Chats are stored in OneDrive and shared in Channel Chats are stored in SharePoint Sites

upvoted 1 times

Paruns 9 months ago

yes agreed

upvoted 1 times

formazionehs 9 months, 1 week ago

Selected Answer: A

Documents shared via Teams chat are uploaded to OneDrive.

upvoted 4 times

Question #50 *Topic 2*

You have a Microsoft SharePoint Online site named Site1 that contains the following files:

• File1.docx
• File2.xlsx
• File3.pdf

You have a retention label named Retention1.

You plan to use an auto-labeling policy to apply Retention1 to any content on Site1 that matches the Targeted Harassment trainable classifier.

To which files will Retention1 be applied?

A. File1.docx only

B. File1.docx and File2.xlsx

C. File1.docx and File3.pdf only

D. File1.docx, File2.xlsx, and File3.pdf

Correct Answer: *D*

Community vote distribution

C (100%)

CharlieGolf Highly Voted 8 months, 2 weeks ago

Selected Answer: C

Incorrect. Answer is C. "Harrassment" trainable classifier does not apply to .xlsx file types. https://learn.microsoft.com/en-us/microsoft-365/compliance/classifier-tc-definitions?view=o365-worldwide#harassment

upvoted 8 times

naren49 Most Recent 2 days, 16 hours ago

Answer D is correct
Below are file types supported
Detects content in docx, .docm, .doc, .dotx, .dotm, .dot, .pdf, .rtf, .txt, .one, .pptx, .pptm, .ppt, .potx, .potm, .pot, .ppsx, .ppsm, .pps, .ppam, .ppa, .txt files.

upvoted 1 times

hsinchang 3 months, 1 week ago

Selected Answer: C

Auto-labeling policies for retention labels can only apply to files that are supported by the trainable classifiers, which are:

Word documents (.docx)
PowerPoint presentations (.pptx)
PDF documents (.pdf)
Text files (.txt)
Email messages (.eml)1
Excel workbooks (.xlsx) are not supported by the trainable classifiers, so they will not be labeled by the auto-labeling policy.

upvoted 1 times

xswe 7 months, 3 weeks ago

The trainable classifier Targeted Harassment only covers docx and pdf files in this case.
This classifier only detects: .docx, .pdf, .txt, .rtf, .jpeg, .jpg, .png, .gif, .bmp, .svg files.

upvoted 2 times

xswe 7 months, 3 weeks ago

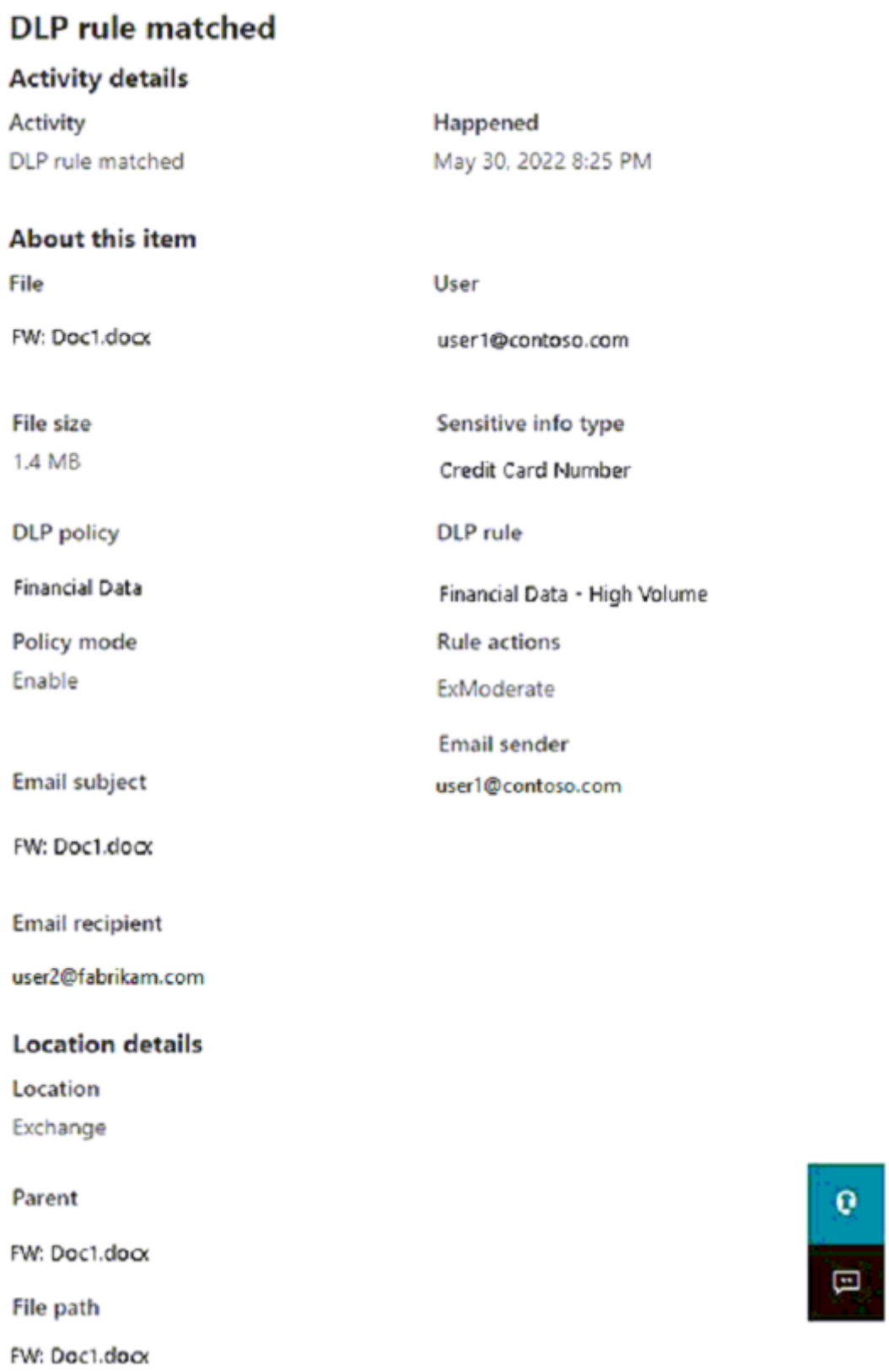
The trainable classifier Targeted Harassment only covers docx and pdf files in this case.
This classifier only detects: .docx, .pdf, .txt, .rtf, .jpeg, .jpg, .png, .gif, .bmp, .svg files.

upvoted 1 times

HOTSPOT
-

You have a Microsoft 365 E5 subscription.

You have the data loss prevention (DLP) rule match shown in the following exhibit.



Use the drop-down menus to select the answer choice that completes each statement based on the information presented in the graphic.

NOTE: Each correct selection is worth one point.

Answer Area

The email [ ]
- generated a policy tip when the email was being written
- generated an incident report
- was forwarded to another user for approval

The Financial Data policy is configured to [ ]
- enforce DLP rules
- test the policy by using notifications
- test the policy without using notifications

Answer Area

Correct Answer:

The email
- generated a policy tip when the email was being written
- generated an incident report
- [x] was forwarded to another user for approval

The Financial Data policy is configured to
- [x] enforce DLP rules
- test the policy by using notifications
- test the policy without using notifications

xswe Highly Voted 7 months, 3 weeks ago
The email... was forwarded to another user for approval, user2
Enforce DLP rules, since "Policy mode: Enable"
upvoted 5 times

luissaro 7 months, 2 weeks ago
how can approver be of another domain?
upvoted 1 times

217f3c9 6 months, 2 weeks ago
afaik the approver is not listed here.
upvoted 1 times

hsinchang Most Recent 3 months, 1 week ago
Moderate -> Forward the message for approval
Policy mode: Enable -> Enforce DLP rules
upvoted 1 times

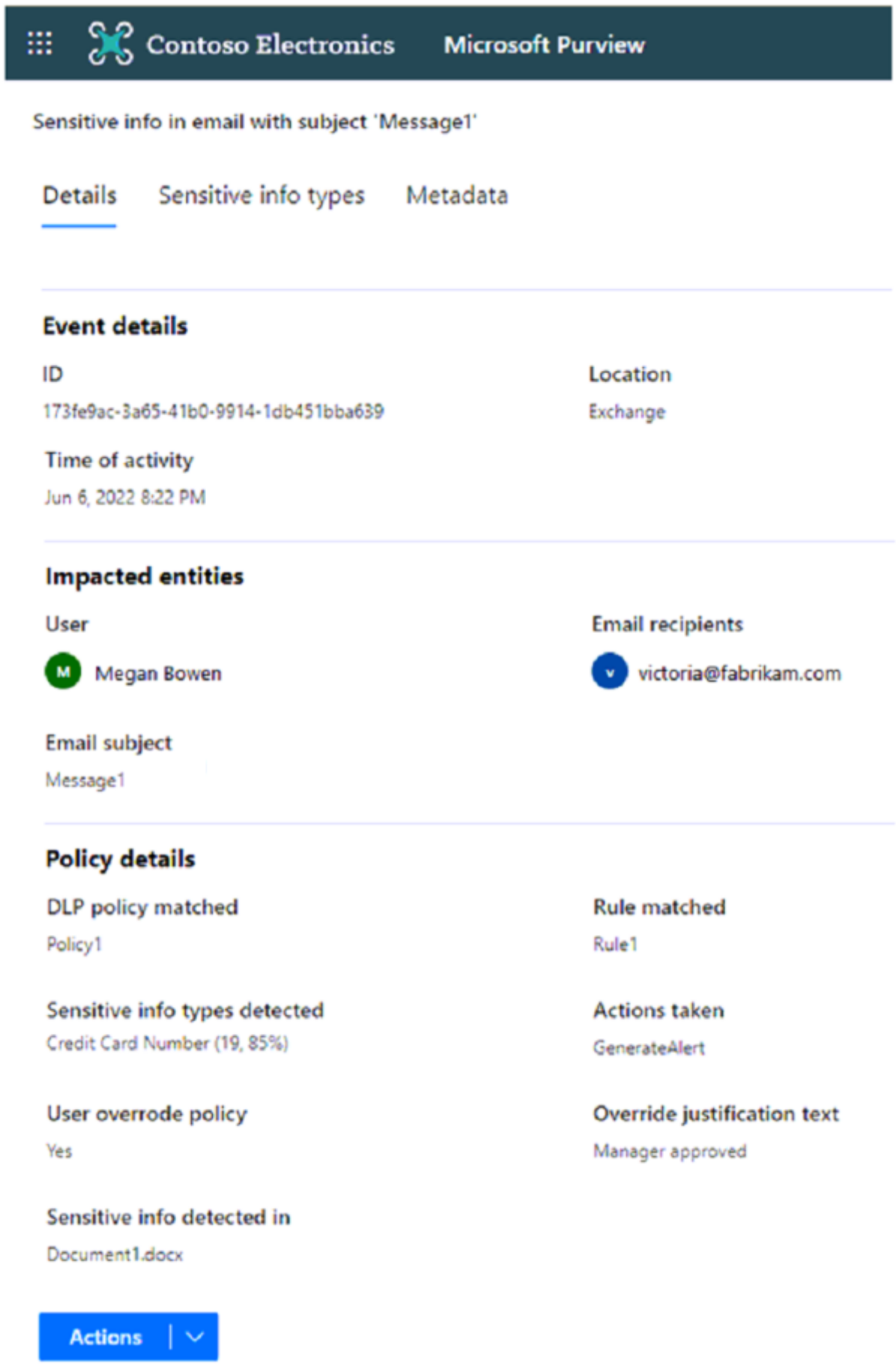
cris_exam 5 months, 2 weeks ago
Given answers appear to be correct.
Check this below to understand the action and the Policy mode Enable is what makes the rule to be enforced.

https://learn.microsoft.com/en-us/microsoft-365/compliance/dlp-conditions-and-exceptions?view=o365-worldwide#actions-for-dlp-policies
upvoted 1 times

HOTSPOT
-

You have a Microsoft 365 E5 subscription.

You receive the data loss prevention (DLP) alert shown in the following exhibit.



Use the drop-down menus to select the answer choice that completes each statement based on the information presented in the graphic.

NOTE: Each correct selection is worth one point.

Answer Area

The email was
- delivered immediately
- quarantined and undelivered
- sent to a manager for approval

The sender's manager
- approved the email by using a workflow
- overrode Rule1
- was uninvolved in the override process

Correct Answer:

Answer Area

The email was
- delivered immediately
- quarantined and undelivered
- sent to a manager for approval

The sender's manager
- approved the email by using a workflow
- overrode Rule1
- was uninvolved in the override process

GeoffLule Highly Voted 7 months, 1 week ago

I believe this email was delivered immediately. The sender overode rule 1 by providing justification that it was a manager approved transaction. The manager was not involved here.

upvoted 7 times

cris_exam Most Recent 5 months, 2 weeks ago

I have spent a bit too much time on this one, lol.

After more then 30 min of reading and digging, I agree with what other said here that the User overruled with the mentioned text: "Manager approved" and the email was sent immediately, also because there is no block mentioned in the Actions Taken category and just generate alert.

1. delivered immediately
2. overrode rule one

upvoted 3 times

xswe 7 months, 3 weeks ago

Sent to manager for approval, since "Manager approved"
Overrode Rule1 since "User overrode policy = Yes"

upvoted 3 times

217f3c9 6 months ago

Its only the text the user put in while overriding the policy.

upvoted 2 times

CharlieGolf 8 months, 2 weeks ago

I don't think the second part is correct. The user's manager was not involved in the override process. User override was allowed and the text was simply selected from the admin-configured toaster options. It did not go through a workflow to the manager.
https://microsoft.github.io/ComplianceCxE/enduser/dlpenduser/

upvoted 4 times

bsongwk 7 months, 3 weeks ago

If manager is not involved since user override is allowed, the email would have be delivered immediately? If so, the answer to first part is wrong as well. It should be "delivered immediately".

upvoted 3 times

pokus00132 7 months, 3 weeks ago

I agree that the first part is also wrong, it should be "delivered immediately"

upvoted 3 times

Question #53 *Topic 2*

You have a Microsoft 365 E5 subscription.

You need to create a Microsoft Defender for Cloud Apps policy that will detect data loss prevention (DLP) violations.

What should you create?

A. a Cloud Discovery anomaly detection policy

B. an activity policy

C. a session policy

D. a file policy

Correct Answer: *D*

Domza 3 weeks ago

Looks good~

upvoted 1 times

heshmat2022 1 month ago

Once enabled, the policy continuously scans your cloud environment and identifies files that match the content and context filters, and apply the requested automated actions. These policies detect and remediate any violations for at-rest information or when new content is created. Policies can be monitored using real-time alerts or using console-generated reports.

upvoted 1 times

Gesbie 3 months, 3 weeks ago

was on Exam August 9, 2023

upvoted 1 times

xswe 7 months, 3 weeks ago

File policy in MCA is used for DLP policies

upvoted 1 times

CharlieGolf 8 months, 2 weeks ago

Agreed. https://learn.microsoft.com/en-us/defender-cloud-apps/data-protection-policies

upvoted 4 times

Question #54 *Topic 2*

You have a Microsoft 365 E5 tenant that uses Microsoft Teams and contains two users named User1 and User2.

You create a data loss prevention (DLP) policy that is applied to the Teams chat and channel messages location for User1 and User2.

Which Teams entities will have DLP protection?

A. 1:1/n chats and private channels only

B. 1:1/n chats and general channels only

C. 1:1/n chats, general channels, and private channels

Correct Answer: *A*

Community vote distribution

A (100%)

CharlieGolf Highly Voted 8 months, 2 weeks ago

Selected Answer: A

Correct. Scoped to individual users ("for User1 and User2"). https://learn.microsoft.com/en-us/microsoft-365/compliance/dlp-microsoft-teams?view=o365-worldwide#scope-of-dlp-protection

upvoted 5 times

Domza 3 weeks ago

Thank you for the link

upvoted 1 times

xswe Most Recent 7 months, 3 weeks ago

Tested out, its correct

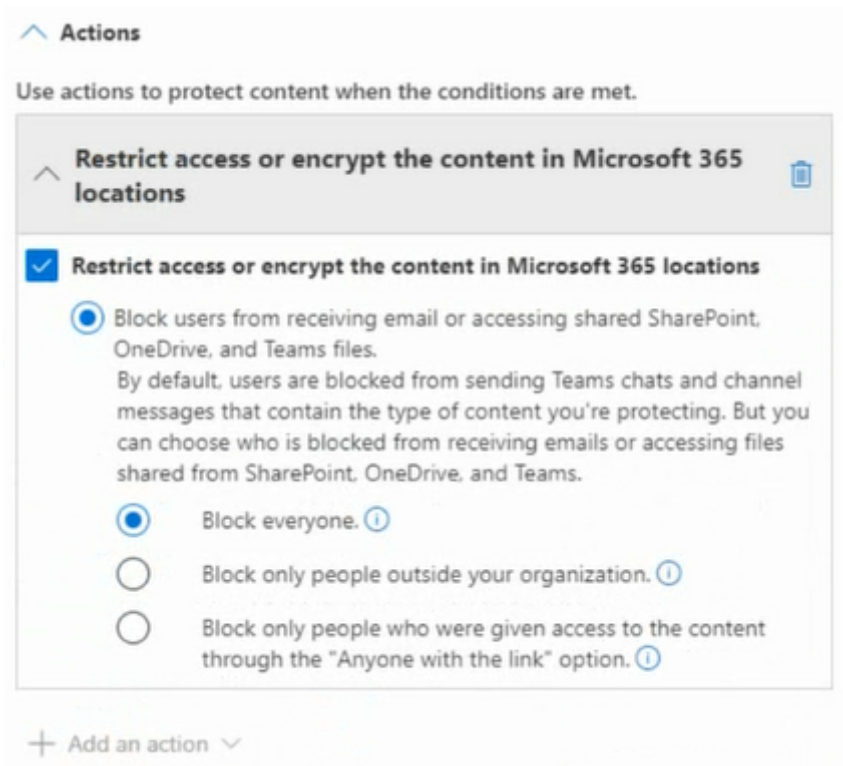
upvoted 1 times

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	Member of
User1	Members group of Site1
User2	Owner group of Site1
Admin1	SharePoint Administrator role

You have a data loss prevention (DLP) policy named DLP1 as shown in the following exhibit.



You apply DLP1 to Site1.

User1 uploads a file named File1 to Site1. File1 does NOT match any of the DLP1 rules. User2 updates File1 to contain data that matches the DLP1 rules.

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	Yes	No
User1 can access File1 on Site1.	○	○
User2 can access File1 on Site1.	○	○
Admin1 can access File1 on Site1.	○	○

Answer Area

	Statements	Yes	No
Correct Answer:	User1 can access File1 on Site1.	○	○
	User2 can access File1 on Site1.	○	○
	Admin1 can access File1 on Site1.	○	○

cris_exam 5 months, 2 weeks ago

User1 = he is just a guy that uploaded the file, no confirmation that he is the content owner/author => access denied
User2 = he's the last modifier => has access
Admin1 = site admin => has access

As per doc:
https://learn.microsoft.com/en-us/microsoft-365/compliance/dlp-policy-reference?view=o365-worldwide#actions

Block users from accessing shared SharePoint, OneDrive, and Teams content:
- Block everyone. Only the content owner, last modifier, and site admin will continue to have access

upvoted 2 times

cris_exam 5 months, 2 weeks ago

Hence answer is: N / Y / Y

upvoted 2 times

xswe 7 months, 3 weeks ago

As mentioned earlier, "Block everyone" option dont block the content owner, last modifier and site admin

Yes, Owners of the file are not blocked by the DLP policies
Yes, last modifiers are not blocked by the DLP policies
Yes, site admins are not blocked by the DLP policies

upvoted 1 times

pokus00132 7 months, 1 week ago

It is question if there exists permission "owner" on Sharepoint file, User1 is rather Author
User2 is content owner (member of owner group of site) and last modifier.
So it should be: NO, YES, YES

upvoted 3 times

cris_exam 5 months, 2 weeks ago

I agree with NO, YES, YES - no mention that user1 is the content owner.

upvoted 1 times

luissaro 7 months, 2 weeks ago

there is no evidence user1 is owner of the file, he just uploaded it

upvoted 3 times

CharlieGolf 8 months, 2 weeks ago

Incorrect. Should be Yes/Yes/Yes, because "Block everyone" excludes the content owner, last modifier, and site admin, per
https://learn.microsoft.com/en-us/microsoft-365/compliance/dlp-policy-reference?view=o365-worldwide#actions

upvoted 3 times

Question #56 *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 10. The computers are onboarded to the Microsoft 365 compliance center.

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 the Microsoft Defender for Cloud Apps portal, you create an app discovery policy.

Does this meet the goal?

A. Yes

B. No

Correct Answer: *B*

Community vote distribution

B (100%)

Davidf 3 months, 2 weeks ago

Selected Answer: B

Cloud app discovery monitors network traffic to discover apps in the cloud, not local executable

upvoted 1 times

pokus00132 7 months, 3 weeks ago

B is right. Cloud discovery policy is used to generate alert when new apps are detected and not for blocking access.

upvoted 2 times

xswe 7 months, 3 weeks ago

Nope, app discovery wont succeed with what they are asking for

upvoted 1 times

Question #57 *Topic 2*

HOTSPOT
-

You have a Microsoft 365 E5 subscription that uses data loss prevention (DLP) to protect sensitive information.

You need to create scheduled reports that generate:

• DLP policy matches reported over the shortest frequency of time
• DLP incidents reported over the longest frequency of time

Which frequency should you configure for each report? To answer, select the appropriate options in the answer area.

NOTE: Each correct selection is worth one point.

Answer Area

DLP policy matches:
- Daily
- Every two days
- Weekly
- Every two weeks
- Monthly

DLP incidents:
- Weekly
- Every two weeks
- Monthly
- Every three months
- Every six months

Correct Answer:

Answer Area

DLP policy matches:
- Daily
- Every two days
- Weekly
- Every two weeks
- Monthly

DLP incidents:
- Weekly
- Every two weeks
- Monthly
- Every three months
- Every six months

You have a Microsoft SharePoint Online site named Site1 that contains the files shown in the following table.

Name	Number of IP addresses in the file
File1	2
File2	3

You have a data loss prevention (DLP) policy named DLP1 that has the advanced DLP rules shown in the following table.

Name	Content contains	Policy tip	If match, stop processing	Priority
Rule1	1 or more IP addresses	Tip1	No	0
Rule2	3 or more IP addresses	Tip2	Yes	1
Rule3	2 or more IP addresses	Tip3	No	2

You apply DLP1 to Site1.

Which policy tips will appear for File2?

A. Tip1 only

B. Tip2 only

C. Tip3 only

D. Tip1 and Tip2 only

Correct Answer: *D*

Community vote distribution

B (100%)

Romeokton 5 days, 17 hours ago

Selected Answer: B

I agree with ae88d96

upvoted 1 times

ae88d96 2 weeks, 1 day ago

Since Rule2 has a higher priority (1) than Rule1 (0) and Rule3 (2), and File2 contains 3 IP addresses, which matches the condition "3 or more IP addresses" in Rule2, the policy tip associated with Rule2 (Tip2) will appear for File2. Additionally, because "If match, stop processing" is set to "Yes" for Rule2, no further rules will be evaluated, and only Tip2 will be displayed.

upvoted 2 times

Pablosanchez 3 weeks, 6 days ago

Flaco no entiendo

upvoted 1 times

Question #59 *Topic 2*

You have a Microsoft 365 E5 tenant that has devices onboarded to Microsoft Defender for Endpoint as shown in the following table.

Name	Type
Device1	Windows 11
Device2	Windows 10
Device3	iOS
Device4	macOS

You plan to start using Microsoft 365 Endpoint data loss protection (Endpoint DLP).

Which devices support Endpoint DLP?

A. Device1 only

B. Device1 and Device2 only

C. Device1 and Device4 only

D. Device1, Device2, and Device4 only

E. Device1, Device2, Device3, and Device4

Correct Answer: *D*

Community vote distribution

D (100%)

Romeokton 5 days, 17 hours ago

Selected Answer: D

Definitely D

upvoted 1 times

Domza 3 weeks ago

Win10/11 and macOs

upvoted 2 times

izgi43 3 weeks ago

on the exam thu nov 9

upvoted 2 times

Pablosanchez 3 weeks, 6 days ago

Agreed. This is correct because it explains it in this link https://learn.microsoft.com/es-es/purview/endpoint-dlp-getting-started

upvoted 1 times

Question #60 *Topic 2*

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 #61 *Topic 2*

You have a Microsoft 365 E5 subscription.

You need to prevent users from uploading data loss prevention (DLP)-protected documents to the following third-party websites:

• web1.contoso.com
• web2.contoso.com

The solution must minimize administrative effort.

To what should you set the Service domains setting for Endpoint DLP?

A. contoso.com

B. web*.contoso.com

C. *.contoso.com

D. web1.contoso.com and web2.contoso.com

Correct Answer: *D*

Question #62 *Topic 2*

You plan to create a new data loss prevention (DLP) policy named DIP1.

DLP1 will be applied to the Exchange email location.

You need to exclude two users named User1 and User2 from DLP1.

What should you do first?

A. Create an organization sharing policy in Microsoft Exchange.

B. Create a mail flow rule in Microsoft Exchange.

C. Create a distribution list that contains User1 and User2.

D. Create an advanced DLP rule.

Correct Answer: *C*

Romeokton 5 days, 16 hours ago

Selected Answer: C

After reviewing carefully I agree with C.

https://learn.microsoft.com/en-us/purview/dlp-policy-reference#policy-scoping

upvoted 1 times

Romeokton 5 days, 17 hours ago

Selected Answer: D

I disagree with the proposed answer "C". When creating a DLP policy it is optional that you exclude people or groups, so I would go with D

upvoted 1 times

HOTSPOT
-

You have a Microsoft 365 subscription that uses an Azure AD tenant named contoso.com.

OneDrive stores files that are shared with external users. The files are configured as shown in the following table.

Name	Applied label
File1	Label1
File2	Label1, Label2
File3	Label2

You create a data loss prevention (DLP) policy that applies to the content stored in OneDrive accounts. The policy contains the following three rules:

Rule1
-
• Conditions: Label1, Detect content that's shared with people outside my organization
• Actions: Restrict access to the content for external users
• User notifications: Notify the user who last modified the content
• User overrides: On
• Priority: 0

Rule2:
• Conditions: Label1 or Label2
• Actions: Restrict access to the content
• Priority: 1

Rule3:
• Conditions: Label2, Detect content that's shared with people outside my organization
• Actions: Restrict access to the content for external users
• User notifications: Notify the user who last modified the content
• User overrides: On
• Priority: 2

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	Yes	No
External users can access File1.	○	○
The users in contoso.com can access File2.	○	○
External users can access File3.	○	○

Answer Area

Correct Answer:

Statements	Yes	No
External users can access File1.	○	○
The users in contoso.com can access File2.	○	○
External users can access File3.	○	○

Romeokton 5 days, 16 hours ago

Agree with the answer - N, N, N.

upvoted 1 times

Question #64 *Topic 2*

You have a Microsoft 365 E5 subscription.

Users access their mailbox by using the following apps:

- Outlook Win32
- Outlook on the web
- Outlook for iOS and Android

You create a data loss prevention (DLP) policy named DLP1 that has the following settings:

- Location: Exchange email
- Status: On
- User notifications: On
- Notify users in Office 365 service with a policy tip: Enabled

Which apps display a policy tip when content is matched by using DLP1?

A. Outlook Win32 only

B. Outlook on the web only

C. Outlook Win32 and Outlook on the web only

D. Outlook Win32 and Outlook for iOS and Android only

E. Outlook Win32, Outlook on the web, and Outlook for iOS and Android

Correct Answer: *C*

Romeokton 5 days, 16 hours ago

Selected Answer: C

I spent a lot of tine on this. Found the correct answer here https://learn.microsoft.com/en-us/purview/dlp-policy-tips-reference#support-matrix-for-dlp-policy-tips-across-microsoft-apps

upvoted 1 times

Question #65 *Topic 2*

You have a Microsoft 365 E5 subscription that contains a device named Device1.

You need to enable Endpoint data loss prevention (Endpoint DLP) for Device1.

What should you do first in the Microsoft Purview compliance portal?

A. Turn on device onboarding.

B. Add a Microsoft Purview Information Protection scanner cluster.

C. Onboard Device1 to Microsoft Purview.

D. Create a Microsoft Purview Information Barriers (IBs) segment.

E. Enable Microsoft Priva Privacy Risk Management.

Correct Answer: *A*

Question #66 *Topic 2*

You have Microsoft 365 E5 subscription that uses data loss prevention (DLP) to protect sensitive information.

You have a document named Form.docx.

You plan to use PowerShell to create a document fingerprint based on Form.docx.

You need to first connect to the subscription.

Which cmdlet should you run?

A. Connect-SPOService

B. Connect-IPPSSession

C. Connect-AzureAD

D. Connect-ExchangeOnline

Correct Answer: *B*

Romeokton 5 days, 16 hours ago

Selected Answer: B

Agreed with B

upvoted 1 times

Question #1 *Topic 3*

You have a Microsoft 365 E5 tenant that contains the policies shown in the following table.

Name	Type	Retention period	Start the retention period based on	At the end of the retention period
Label1	Label	5 years	When items were created	Delete items automatically
Label2	Retention	7 years	When items were created	Delete items automatically
Label3	Retention	10 years	When items were created	Do nothing

A file named File1 has all the policies applied.

How long will File1 be retained?

A. File1 will be deleted automatically after seven years.

B. File1 will be deleted automatically after five years.

C. File1 will be retained until the file is deleted manually.

D. File1 will be deleted automatically after 10 years.

Correct Answer: *D*

Retention always takes precedence over permanent deletion, with the longest retention period taking preference.

The delete action from a retention label always takes precedence over the delete action from a retention policy.

Reference:

https://docs.microsoft.com/en-us/microsoft-365/compliance/retention?view=o365-worldwide#the-principles-of-retention-or-what-takes-precedence

jimmyjose Highly Voted 1 year, 2 months ago

'Retention' wins over 'deletion'. The longest configured retention period is 10 years and its corresponding action is 'Do nothing', which means the file needs to be deleted manually.

Hence, the answer is C.

upvoted 13 times

Schuiram Highly Voted 6 months, 3 weeks ago

Selected Answer: D

https://learn.microsoft.com/en-us/microsoft-365/compliance/retention-flowchart?view=o365-worldwide <- follow this decision tree and you will end up deleting it after 10 years as another policy/label was defined with a deletion request.

upvoted 7 times

Romeokton Most Recent 5 days, 16 hours ago

Selected Answer: D

This question was on exam November 2023. The correct answer is D, as explained here: An item has the following retention settings applied to it:

An org-wide retention policy that deletes-only after ten years
A retention policy scoped with specific instances that retains for five years and then deletes
A retention label that retains for three years and then deletes

Outcome: The item is retained for five years because that's the longest retention period for the item. At the end of that retention period, the item is permanently deleted because of the delete action of three years from the retention label. Deletion from retention labels takes precedence over deletion from all retention policies. In this example, all conflicts are resolved by the third level.

upvoted 2 times

Domza 3 weeks ago

Hello all, please read the question)) it says how long File1 will be retained? - not deleted

Retain for 1o yrs~ + manual deletion :)

upvoted 1 times

ikidreamz 4 months, 1 week ago

what does it mean Do nothing ? I think it will not automatically deleted the file so It should be C

upvoted 1 times

xswe 7 months, 3 weeks ago

File will be RETAINED for 10 YEARS then it will get deleted.
In other words C is NOT correct since the file wont be able to get deleted until 10 years has passed.

Check this if you dont understand how retention policies works,
https://learn.microsoft.com/en-us/microsoft-365/compliance/retention-flowchart?view=o365-worldwide

upvoted 2 times

FireOzzie 8 months, 4 weeks ago

Selected Answer: C

Must be C.

upvoted 2 times

boxerwalrus 9 months ago

Selected Answer: C

C is the least wrong

upvoted 1 times

wooyourdaddy 9 months, 1 week ago

As other have stated, retention over deletion so the file is kept for 10 years.

The following link discusses order of precedence when mixing delete and retain actions:

https://learn.microsoft.com/en-us/microsoft-365/compliance/retention?view=o365-worldwide#principles-of-retention-examples-that-combine-retain-and-delete-actions

Which confirms that the delete would happen at the end of the longest retention period.

upvoted 1 times

wooyourdaddy 9 months, 1 week ago

Specifically, it states:

"Deletion from retention labels takes precedence over deletion from all retention policies."

So the deletion action in Label1 (which is a retention label) would override anything set in Label2 or Label3 which are retention policies.

upvoted 2 times

See_Es 10 months, 1 week ago

Correct. This clears it all up:
https://learn.microsoft.com/en-us/microsoft-365/compliance/retention?view=o365-worldwide#the-principles-of-retention-or-what-takes-precedence

Example for this first principle: An email message is subject to a retention policy for Exchange that is configured to delete items three years after they are created, and it also has a retention label applied that is configured to retain items five years after they are created.

The email message is retained for five years because this retention action takes precedence over deletion. The email message is permanently deleted at the end of the five years because of the delete action that was suspended while the retention action was in effect.

upvoted 3 times

vasskliss 11 months, 4 weeks ago

D is correct. Deletion will be suspended until 10 years have passed.

upvoted 3 times

bollag 1 year ago

C is also not correct as "File1 will be retained until the file is deleted manually" means also that it could be deleted after 1 or so years which is not true...

upvoted 3 times

BTL_Happy 1 year ago

C should be the answer

upvoted 2 times

mcas 1 year, 1 month ago

Selected Answer: C

Agree with jimmyjose

upvoted 2 times

chrissempai 1 year, 2 months ago

Selected Answer: D

In case of multi match, Microsoft keep the minimum of risk so it will not be deleted and keep the longest time of the policy.
In this case it will be 10 years and not deleted
https://docs.microsoft.com/en-us/microsoft-365/compliance/retention?view=o365-worldwide

upvoted 3 times

chrissempai 1 year, 2 months ago

C not D, sorry

upvoted 2 times

cwilson91 1 year, 2 months ago

Am I going crazy or shouldn't the answer be B, 5 years?

upvoted 4 times

lkazimirs 1 year, 2 months ago

i would agree as well - does it not state that the most restrictive rule wins?

upvoted 1 times

Question #2 *Topic 3*

You have a Microsoft 365 tenant that uses Microsoft Teams.
You need to ensure that all internal communication is stored for a minimum of seven years.
What should you create first?

A. a retention label

B. a Microsoft SharePoint Online site

C. a Microsoft Exchange Online shared mailbox

D. a retention label policy

Correct Answer: *A*
Reference:
https://docs.microsoft.com/en-us/microsoft-365/compliance/retention?view=o365-worldwide

chrissempai Highly Voted 1 year, 2 months ago
Selected Answer: A
A is correct
in temas you have all documents share, a policy can't mark them, you need a label.
see : https://docs.microsoft.com/en-us/microsoft-365/compliance/retention?view=o365-worldwide
upvoted 7 times

ikidreamz 4 months, 3 weeks ago
A is correct

By default they say 3 yrs retention policy for SP sites, but if you need 7 years you need EXCEPTION which is Label

https://learn.microsoft.com/en-us/microsoft-365/compliance/create-retention-labels-data-lifecycle-management?view=o365-worldwide
upvoted 1 times

Quester Highly Voted 1 year, 1 month ago
Selected Answer: D
I think it should be D - Retension Policy.
They are saying that all communication should be saved. Which would be a policy.
Not anything regarding documents, which then would be OneDrive/Sharepoint based.
upvoted 6 times

mcas 1 year, 1 month ago
agree all communication means you have to target containers (e.g. mailboxes) which requires a policy. label is only used for exceptions, or specific files/content
upvoted 1 times

vasskliss 11 months, 4 weeks ago
It says "retention label policy", not the same with "retention policy". A is correct.
upvoted 6 times

Romeokton Most Recent 5 days, 15 hours ago
The question was on exam in November 2023. My opinion is it is not put in the best possible wording. Microsoft says:
Use a retention policy to assign the same retention settings for content at a site or mailbox level, and use a retention label to assign retention settings at an item level (folder, document, email).

However, here the answer is "retention label policy". That's why it seems A as first you need to create the label.
upvoted 1 times

Sango 3 months, 1 week ago
The Retention Policy, Retention Label and Retention Label Policy are the exact key words. You can't create a "Retention Label Policy" (User or Auto) without a "Retention Label" to Use. That said, you can create a "Retention Policy" but that isn't on an option for the multi-choice question.
upvoted 2 times

doori88 5 months, 4 weeks ago
answer is D, you dont need a label but you need to apply it on Teams & Yammer --> therefore policy
upvoted 2 times

dmoorthy 7 months, 1 week ago
Exchange public folders, Skype, Teams and Yammer messages don't support retention labels. To retain and delete content from these locations, use retention policies instead.

https://learn.microsoft.com/en-us/microsoft-365/compliance/retention?view=o365-worldwide

upvoted 1 times

bsongwk 7 months, 3 weeks ago

A is correct. U need to create a label first before u can create a policy.

upvoted 1 times

bsongwk 7 months, 3 weeks ago

Ignore my previous comment.

The answer should be D. Policy can be created without first creating a label: https://learn.microsoft.com/en-us/microsoft-365/compliance/create-retention-policies?view=o365-worldwide&tabs=teams-retention

upvoted 1 times

CharlieGolf 8 months, 1 week ago

Selected Answer: D

Per the following link, it should be "Retention Policy", but the poorly worded "Retention Label Policy" answer still seems a better answer than "Retention Label" for "communications" (vs files). https://learn.microsoft.com/en-us/microsoft-365/compliance/create-retention-policies?view=o365-worldwide&tabs=teams-retention

upvoted 3 times

Question #3 *Topic 3*

In Microsoft Exchange Online, you have a retention policy named Policy1 that applies a retention tag named Tag1.
You plan to remove Tag1 from Policy1.
What will occur when you remove the tag from Policy1?

A. The content will remain tagged and the Managed Folder Assistant will process Tag1.

B. Tag1 will be removed if Policy1 applied the tag to the content.

C. The content will remain tagged, but the Managed Folder Assistant will ignore Tag1.

Correct Answer: *A*
Reference:
https://docs.microsoft.com/en-us/exchange/security-and-compliance/messaging-records-management/retention-tags-and-policies#removing-or-deleting-a- retention-tag-from-a-retention-policy

ExamReviewerIZ Highly Voted 2 years, 1 month ago
Tricky question. You can DELETE and you can REMOVE a tag from a retention policy in Exchange. Two different things.

If you REMOVE the tag only, everything (retention) stays the same in Exchange Mailbox, but the used won't be able to apply the tag to other mails of folders.

If you DELETE the tag, then that also removes the retention policies from the emails of folders where it was originally applied.

Answer is A.
upvoted 6 times

NinjaSchoolProfessor Highly Voted 11 months, 1 week ago
Answer is [A]. When a retention tag is removed from the retention policy applied to a mailbox, the tag is no longer available to the user and can't be applied to items in the mailbox. Existing items that have been stamped with that tag continue to be processed by the Managed Folder Assistant based on those settings and any retention action specified in the tag is applied to those messages. However, if you delete the tag, the tag definition stored in Active Directory is removed. This causes the Managed Folder Assistant to process all items in a mailbox and restamp the ones that have the removed tag applied. Depending on the number of mailboxes and messages, this process may significantly consume resources on all Mailbox servers that contain mailboxes with retention policies that include the removed tag.

https://learn.microsoft.com/en-us/exchange/security-and-compliance/messaging-records-management/retention-tags-and-policies#removing-or-deleting-a-retention-tag-from-a-retention-policy
upvoted 5 times

ServerBrain Most Recent 1 month, 4 weeks ago
Selected Answer: A
It's not about the policy, it's about Tag1 which has not been removed from the content
upvoted 1 times

wooyourdaddy 1 year, 5 months ago
Selected Answer: A
I wrote the exam today, this question was on it, I choose A, scored 890!
upvoted 1 times

PrettyFlyWifi 1 year, 9 months ago
When a retention tag is removed from the retention policy applied to a mailbox, the tag is no longer available to the user and can't be applied to items in the mailbox.

Existing items that have been stamped with that tag continue to be processed by the Managed Folder Assistant based on those settings and any retention action specified in the tag is applied to those messages.

However, if you delete the tag, the tag definition stored in Active Directory is removed. This causes the Managed Folder Assistant to process all items in a mailbox and restamp the ones that have the removed tag applied. Depending on the number of mailboxes and messages, this process may significantly consume resources on all Mailbox servers that contain mailboxes with retention policies that include the removed tag.

https://docs.microsoft.com/en-us/exchange/security-and-compliance/messaging-records-management/retention-tags-and-policies#removing-or-deleting-a-retention-tag-from-a-retention-policy
upvoted 3 times

Pravda 1 year, 10 months ago
On exam 1/20/2022
upvoted 1 times

test123123 2 years, 5 months ago

Removing or deleting a retention tag from a retention policy
When a retention tag is removed from the retention policy applied to a mailbox, the tag is no longer available to the user and can't be applied to items in the mailbox.

Existing items that have been stamped with that tag continue to be processed by the Managed Folder Assistant based on those settings and any retention action specified in the tag is applied to those messages.

upvoted 3 times

Question #4 *Topic 3*

You have a Microsoft 365 E5 tenant that contains a user named User1.

You need to identify the type and number of holds placed on the mailbox of User1.

What should you do first?

A. From the Microsoft 365 compliance center, create an eDiscovery case.

B. From Exchange Online PowerShell, run the Get-Mailbox cmdlet.

C. From the Microsoft 365 compliance center, run a content search.

D. From Exchange Online PowerShell, run the Get-HoldCompliancePolicy cmdlet.

Correct Answer: *B*
Reference:
https://docs.microsoft.com/en-us/microsoft-365/compliance/identify-a-hold-on-an-exchange-online-mailbox?view=o365-worldwide

Gesbie 3 months, 3 weeks ago
was on Exam August 9, 2023
upvoted 1 times

xswe 7 months, 3 weeks ago
Get-Mailbox cmdlet can be used to find out retention policies for a specific mailbox and also find out holds placed in the mailbox.
upvoted 1 times

JCkD4Ni3L 11 months, 2 weeks ago
Selected Answer: B
Correct, B.
upvoted 1 times

wyindualizer 1 year, 3 months ago
Correct
upvoted 1 times

Question #5 *Topic 3*

You have a Microsoft 365 tenant that uses Microsoft Exchange Online.
You need to recover deleted email messages from a user's mailbox.
Which two PowerShell cmdlets should you use? Each correct answer presents part of the solution.
NOTE: Each correct selection is worth one point.

A. Restore-RecoverableItems

B. Get-MailboxRestoreRequest

C. Restore-Mailbox

D. Get-RecoverableItems

E. Set-MailboxRestoreRequest

Correct Answer: *AD*
Reference:
https://docs.microsoft.com/en-us/exchange/recipients-in-exchange-online/manage-user-mailboxes/recover-deleted-messages

xswe 7 months, 3 weeks ago
Since deleted messages in exchange gets placed in Recoverable Item folder this is pretty logical.
Get-RecoverableItems = Find the item you are looking for
Recover-RecoverableItems = Recover the items you wish to restore
upvoted 3 times

JCkD4Ni3L 11 months, 3 weeks ago
Selected Answer: AD
Correct
upvoted 1 times

wyindualizer 1 year, 3 months ago
Correct
https://docs.microsoft.com/en-us/exchange/recipients-in-exchange-online/manage-user-mailboxes/recover-deleted-messages
upvoted 2 times

Question #6 *Topic 3*

HOTSPOT -

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

Name	Role
User1	Global Administrator
User2	Compliance admin

You have a retention policy that has the following configurations:

- Name: Policy1
- Retain items for a specific period: 5 years
- Locations to apply the policy: Exchange email, SharePoint sites

You place a Preservation Lock on Policy1.

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:

Answer Area

Statements	Yes	No
User1 can remove Exchange email from the locations	○	○
User2 can increase the retention period to seven years	○	○
User1 can decrease the retention period to three years	○	○

Correct Answer:

Answer Area

Statements	Yes	No
User1 can remove Exchange email from the locations	○	○
User2 can increase the retention period to seven years	○	○
User1 can decrease the retention period to three years	○	○

When a retention policy is locked:

- No one, including the global admin, can disable the policy or delete it
- Locations can be added but not removed

You can extend the retention period but not decrease it

▪

Reference:

https://docs.microsoft.com/en-us/microsoft-365/compliance/retention-preservation-lock?view=o365-worldwide

gurpreet79in Highly Voted 1 year, 1 month ago

Correct

Preservation Lock locks a retention policy or retention label policy so that no one—including a global admin—can turn off the policy, delete the policy, or make it less restrictive. This configuration might be needed for regulatory requirements and can help safeguard against rogue administrators.

When a retention policy is locked:

No one can disable the policy or delete it

Locations can be added but not removed
You can extend the retention period but not decrease it
When a retention label policy is locked:

No one can disable the policy or delete it
Locations can be added but not removed
Labels can be added but not removed
In summary, a locked policy can be increased or extended, but it can't be reduced or turned off.
upvoted 10 times

JCkD4Ni3L 11 months, 2 weeks ago
Correct.
upvoted 1 times

Davidf Most Recent 3 months, 2 weeks ago
Disagree, answer should be Y/Y/N
Retention policies don't stop you deleting from an exchange location, they are just moved to a hidden folder and retained there. Locking the policy doesn't change the policy behaviour, just how you can interact with the policy itself.
Yes we can increase the retention period
No we can't reduce it
upvoted 1 times

GeoffLule 7 months, 1 week ago
Correct
upvoted 1 times

xswe 7 months, 3 weeks ago
Since we have a preservation lock on this policy the GA wont be able to remove email from the location.
But we can extend the retention period, but NOT make it less restrictive. Which means that we cannot decrease the retention period.
upvoted 2 times

Question #7 *Topic 3*

HOTSPOT -

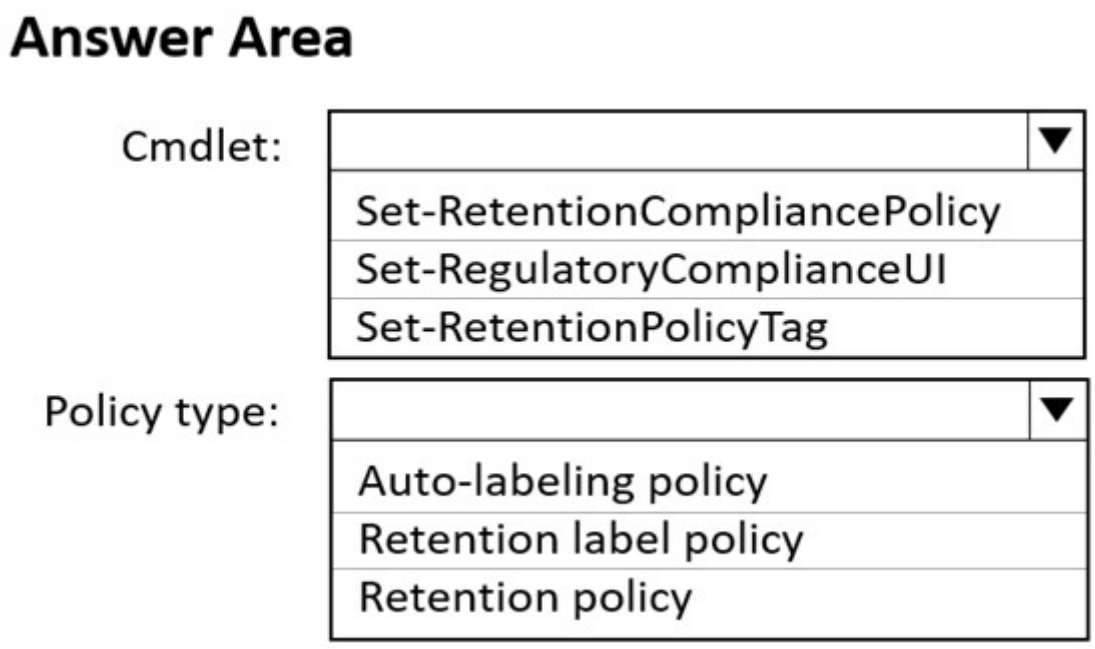
You have a Microsoft E5 365 tenant.

You need to ensure that you can use sensitivity labels to declare regulatory records.

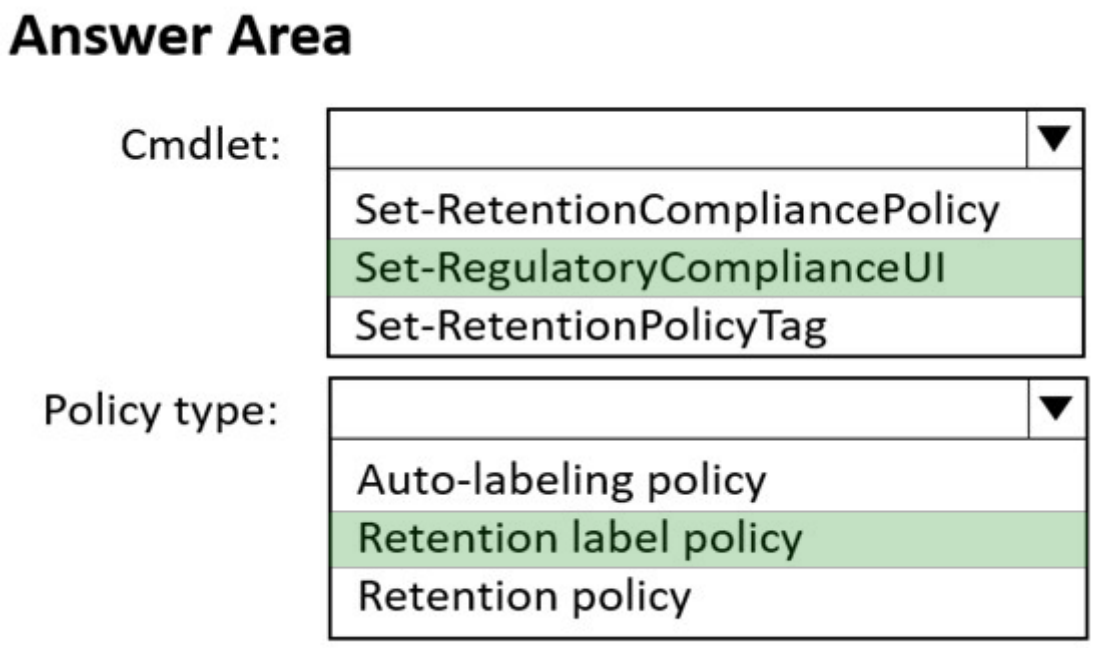
Which PowerShell cmdlet should you run, and which type of policy should you use? To answer, select the appropriate options in the answer area.

NOTE: Each correct selection is worth one point.

Hot Area:



Correct Answer:



Reference:

https://docs.microsoft.com/en-us/microsoft-365/compliance/declare-records?view=o365-worldwide https://docs.microsoft.com/en-us/microsoft-365/compliance/get-started-with-sensitivity-labels?view=o365-worldwide

mcas Highly Voted 1 year, 1 month ago

To declare documents and emails as records, you use retention labels that mark the content as a record or a regulatory record.

You can then either publish those labels in a retention label policy so that users and administrators can apply them to content, or for labels that mark items as records (but not regulatory records), auto-apply those labels to content that you want to declare a record.

https://learn.microsoft.com/en-us/microsoft-365/compliance/declare-records?view=o365-worldwide

upvoted 7 times

Romeokton Most Recent 5 days, 15 hours ago

Here is the answer regarding the PowerShell https://learn.microsoft.com/en-us/powershell/module/exchange/set-regulatorycomplianceui?view=exchange-ps

upvoted 1 times

izgi43 3 weeks ago

on the exam thu nov 9

upvoted 1 times

Question #8 *Topic 3*

DRAG DROP -

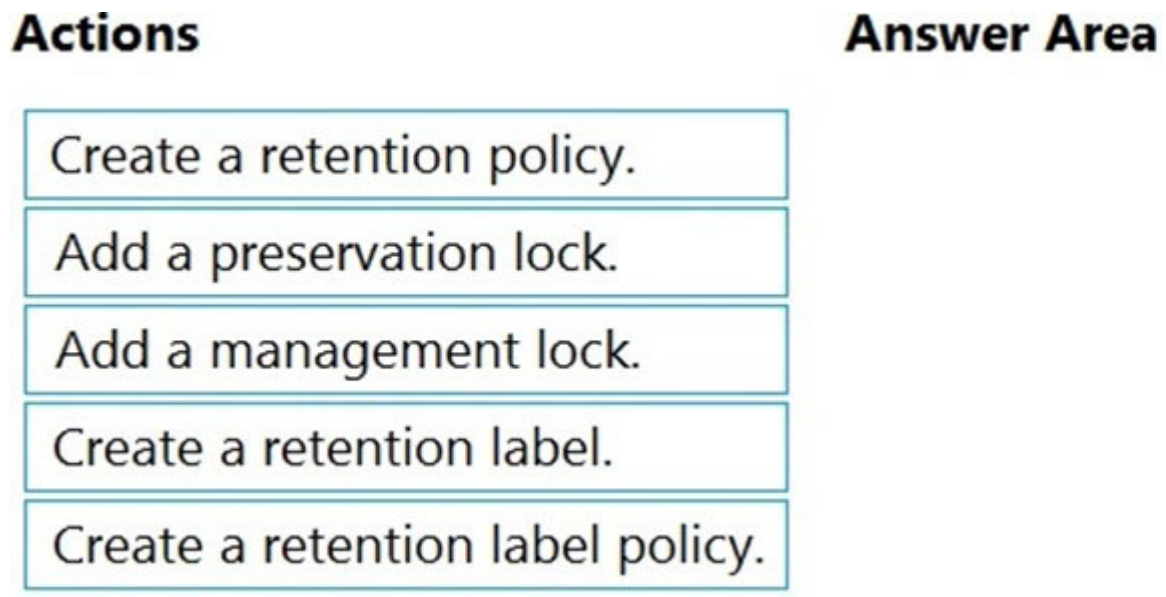
You have a Microsoft 365 tenant.

A new regulatory requirement states that all documents containing a patent ID be labeled, retained for 10 years, and then deleted. The policy used to apply the retention settings must never be disabled or deleted by anyone.

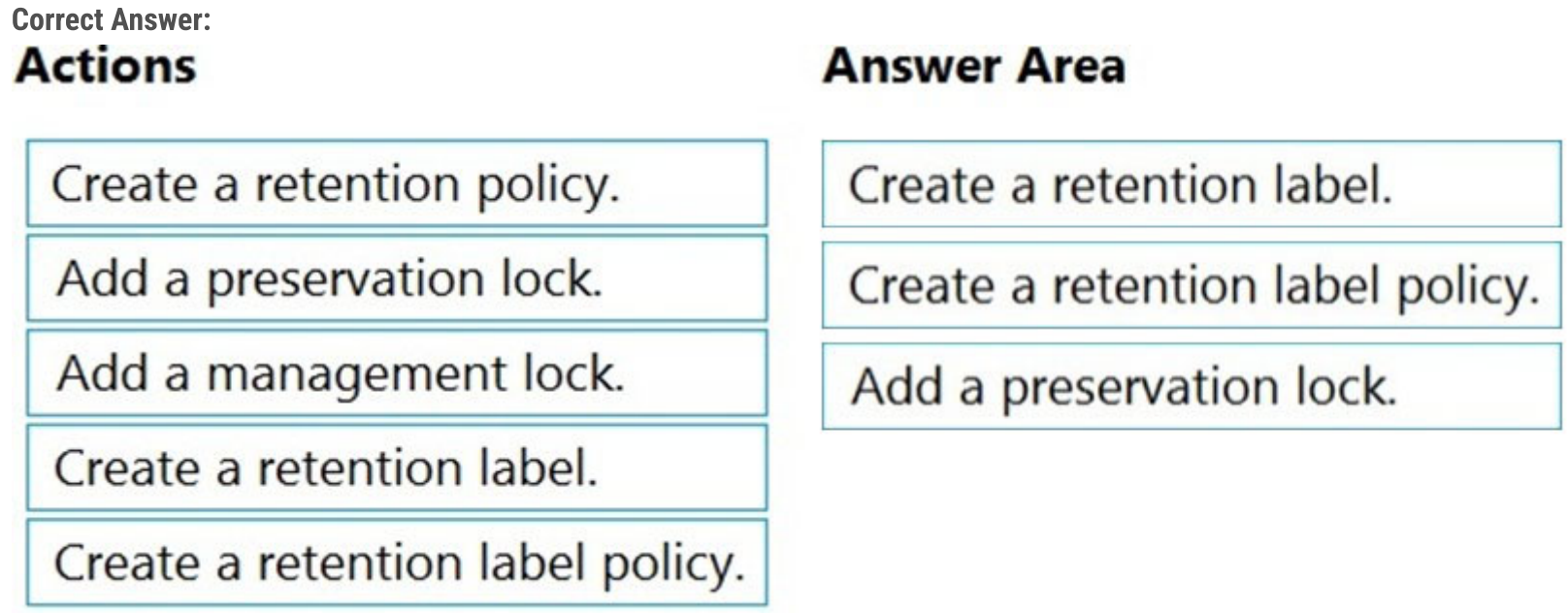
You need to implement the regulatory requirement.

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. (Choose three.)

Select and Place:



Correct Answer:



Reference:

https://docs.microsoft.com/en-us/microsoft-365/compliance/retention?view=o365-worldwide https://docs.microsoft.com/en-us/microsoft-365/compliance/retention-preservation-lock?view=o365-worldwide

jcgonzalez1978 Highly Voted 2 years, 3 months ago

I think the answer provided is correct, particularly the Preservation lock part:
Preservation Lock locks a retention policy or retention label policy so that no one—including a global admin—can turn off the policy, delete the policy, or make it less restrictive. This configuration might be needed for regulatory requirements and can help safeguard against rogue administrators.

When a retention policy is locked:

No one can disable the policy or delete it
Locations can be added but not removed
You can extend the retention period but not decrease it
When a retention label policy is locked:

No one can disable the policy or delete it
Locations can be added but not removed
Labels can be added but not removed

upvoted 9 times

xswe Most Recent 7 months, 3 weeks ago

To achieve this we need to create a retention label and retention label policy with a preservation lock to ensure that on one can disable the policy or change the settings of it.

upvoted 3 times

JCkD4Ni3L 11 months, 3 weeks ago

Answer is correct
upvoted 3 times

wooyourdaddy 1 year, 5 months ago
I wrote the exam today, this question was on it, I choose Box1: Create a retention policy, Box2: Create a retention label policy, Box3: Add a preservation lock., scored 890!
upvoted 3 times

wooyourdaddy 1 year, 5 months ago
Same as question #18, Topic 3:

Box1: Create a retention policy
Box2: Create a retention label policy
Box3: Add a preservation lock.
upvoted 1 times

nupagazi 1 year, 10 months ago
Agree. Use retention label policy at folder, document or email
upvoted 2 times

nupagazi 1 year, 10 months ago
But why create retention label policy instead of retention policy ?
upvoted 1 times

ARYMBS 7 months ago
Label applied per items, Policies per locations.
Question asks you to do something with specific items in some locations not all items on some locations (if you catch my drift..).
upvoted 1 times

PrettyFlyWifi 1 year, 9 months ago
Because a retention policy just looks at a Location to retain EXO, SPO, Teams data etc. But a retention label policy depends on the retention label applied to doc to apply the retention settings. Its more granular in the retention controls.
upvoted 3 times

ExamReviewerIZ 2 years, 1 month ago
Indeed, by the questions and answers provided, this is correct.

Otherwise, you could only create a Retention Policy with a Preservation Lock and that's ok too. 2 answers. (But it's asking for 3 answers)
upvoted 2 times

Question #9 *Topic 3*

You have a Microsoft SharePoint Online site that contains employee contracts in a document library named Contracts.
The contracts must be treated as records in accordance with your company's records management policy.
You need to implement a solution to automatically mark all the contracts as records when they are uploaded to Contracts.
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. Create a sensitivity label.

B. Create a retention label.

C. Configure a default label on the Contracts document library.

D. Create a retention policy.

E. Create a file plan.

F. Create a retention lock.

Correct Answer: *BC*
Reference:
https://docs.microsoft.com/en-us/microsoft-365/compliance/create-apply-retention-labels?view=o365-worldwide

Sam12 Highly Voted 1 year, 10 months ago

Selected Answer: CE

You cannot create mark a document as a record through regular retention label (information government), the only way is to create a file plan in records management (which will be a retention label but with extra options such as "Mark items as record").
And the second options is to make this label as a default on that specific sharepoint folder, as publishing the label will not automatically apply it o files.

upvoted 9 times

Harold_Finch 1 year, 4 months ago

Really? https://docs.microsoft.com/en-us/microsoft-365/compliance/retention#:~:text=default%20retention%20label.-,Mark%20items%20as%20a%20record,-as%20part%20of

upvoted 3 times

wooyourdaddy 9 months, 1 week ago

Incorrect on the label as a record comment. Question 12, Topic 3 further down this page asks:

You have a Microsoft 365 tenant that uses records management.
You use a retention label to mark legal files stored in a Microsoft SharePoint Online document library as regulatory records.

Which confirms that a label can mark a document as a regulatory record.

upvoted 2 times

ExamReviewerIZ Highly Voted 2 years, 1 month ago

Answer is B & C (just because is asking for two answers/two steps to achieve this)

A. Sensitivity Labels is used for different purposes.
D. Create a retention policy can achieve this, but this would only be one step.
E. Create a File Plan is an extra step in any process for retention policies. So this would be the third and first answer it the question would ask for 3 answers.
F. Create a retention Lock this is not a thing.

upvoted 9 times

TomasValtor Most Recent 1 month, 3 weeks ago

Answer AC
To automatically mark all the contracts in the SharePoint Online site as records when they are uploaded to the Contracts document library, you need to perform the following two actions:

upvoted 1 times

TomasValtor 1 month, 3 weeks ago

Based on the information provided in the question, the two actions that you should perform are A and B. Create a sensitivity label that marks the contracts as "Records" and create a retention label that is associated with the "Records" sensitivity label. Configuring a default label on the Contracts document library may also be required to ensure that all the contracts uploaded to the Contracts document library are automatically labeled as "Records."

upvoted 1 times

TomasValtor 1 month, 3 weeks ago

A. Create a Sensitivity Label: Sensitivity labels help you classify and protect your sensitive content. Sensitivity labels can be used to automatically classify and protect documents and emails in Microsoft 365 services. In this case, you can create a sensitivity label that marks the contracts as "Records" when they are uploaded to the Contracts document library. To create a sensitivity label, you need to have the appropriate permissions and access to the Microsoft 365 Compliance center.

upvoted 1 times

TomasValtor 1 month, 3 weeks ago

C. Configure a default label on the Contracts document library: To ensure that all the contracts uploaded to the Contracts document library are automatically labeled as "Records," you need to configure a default label on the Contracts document library. This will ensure that when a user uploads a contract to the Contracts document library, it is automatically labeled as "Records" using the created sensitivity and retention labels.

upvoted 1 times

xswe 7 months, 3 weeks ago

To be able to treat the contracts as records with need retention labels.
To mark automatically mark the contracts with can place the retention label as default label in the a document library

upvoted 1 times

CharlieGolf 8 months, 1 week ago

Selected Answer: BC

Seems like B&C based on this as well: https://learn.microsoft.com/en-us/microsoft-365/compliance/declare-records?view=o365-worldwide

upvoted 2 times

JamesM9 1 year, 7 months ago

The correct answer is B&C.

upvoted 4 times

Jahoor69 1 year, 8 months ago

Answer is B & C

Configure a Retention Label, then apply it as a default to all uploads in the document library named contracts.

upvoted 4 times

Topaz007 2 years, 1 month ago

This is a tricky question. A Retention POLICY is used for LOCATIONS, like a site, a library or mailboxes (and much more!). A Retention LABEL is used at ITEM level, like documents.

In this case I would initially say a Retention POLICY will do the job. BUT since a Retention POLICY is tied to a specific container, the content will loose the settings when moved to another location where the Retention POLICY isn't present. The question however isn't clear on this, so that's open for debate.

Therefore B & C are the most viable options here. Also because you CAN'T combine a Retention LABEL with a Retention POLICY, only with a Retention LABEL POLICY.

In real life though I would opt for a Retention POLICY, and apply it to the Contracts document library and be done with it.

upvoted 6 times

Topaz007 2 years, 1 month ago

See here: https://docs.microsoft.com/en-us/microsoft-365/compliance/retention?view=o365-worldwide#:~:text=Unlike%20retention%20policies%2C%20retention%20settings,retention%20policies%20don't%20support%3A&text=Apply%20a%20default%20label%20for%20SharePoint%20documents.

upvoted 1 times

jcgonzalez1978 2 years, 3 months ago

Tricky one in my opinion...I would say you need the three actions:
1. Create a retention label
2. Create a retention policy
3. Configure a default label on the Contracts document library

upvoted 4 times

Eltooth 2 years, 4 months ago

B & D would make more sense.

upvoted 3 times

pheb 2 years, 3 months ago

No, a retention label can be used in a retention "label" policy, but not in a retention policy. The answer is correct: B & C.

upvoted 9 times

xofowi5140 2 years, 4 months ago

Why not "Configure a default label on the Contracts document library"?

upvoted 2 times

Question #10 *Topic 3*

You need to create a retention policy to delete content after seven years from the following locations:
- Exchange Online email
- SharePoint Online sites
- OneDrive accounts

Microsoft 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

Correct Answer: *A*
Reference:
https://docs.microsoft.com/en-us/microsoft-365/compliance/retention?view=o365-worldwide

Romeokton 5 days, 15 hours ago
Selected Answer: B
As the other people explained already. I have tested it also.
upvoted 1 times

NoOne24 3 months, 2 weeks ago
Selected Answer: B
B - you need 2
upvoted 2 times

doori88 5 months, 3 weeks ago
Answer is B
for each of the following you can have a retention policy

1.EXO, SPO, ODfB, M365 groups
2.Teams channel messages, teams chat
3.Teams private channel messages
upvoted 1 times

xswe 7 months, 3 weeks ago
If you want to create a policy for all of these location you are going to need to create 2 since you cant choose Teams chat with the other location.

Try it out!
upvoted 3 times

JCkD4Ni3L 11 months, 3 weeks ago
Selected Answer: B
Correct, the Teams portion forces the use of 2 policies
upvoted 1 times

mcas 1 year, 1 month ago
Selected Answer: B
B, 2 policies
upvoted 1 times

chrissempai 1 year, 2 months ago
Selected Answer: B
B is correct, you need 2 policy
upvoted 1 times

lkazimirs 1 year, 2 months ago

Selected Answer: B

Agree- Teams chat and channels need separate policy.

upvoted 1 times

wyindualizer 1 year, 3 months ago

Selected Answer: B

Although a retention policy can support multiple services that are identified as "locations" in the retention policy, you can't create a single retention policy that includes all the supported locations:

Exchange email
SharePoint site
OneDrive accounts
Microsoft 365 groups
Skype for Business
Exchange public folders
Teams channel messages
Teams chats
Teams private channel messages
Yammer community messages
Yammer user messages
If you select the Teams or Yammer locations when you create a retention policy, the other locations are automatically excluded.

upvoted 2 times

music_man 1 year, 3 months ago

Selected Answer: B

Answer should be B: Teams Chat and channel messages require a separate policy.

upvoted 4 times

HOTSPOT -

You create a retention policy as shown in the following exhibit.

Retention Policy 1

Status
Enabled (Pending)

Policy name
Retention Policy 1

Description
Retention Policy for SharePoint Site1 and Exchange

Applies to content in these locations
Exchange email
SharePoint sites

Settings
Retention period
Keep content, and delete it if it's older than 10 years

Preservation lock
No data available

A user named User1 deletes a file named File1.docx from a Microsoft SharePoint Online site named Site1.

A user named User2 deletes an email and empties the Deleted Items folder in Microsoft Outlook.

Where is the content retained one year after deletion? To answer, select the appropriate options in the answer area.

NOTE: Each correct selection is worth one point.

Hot Area:

Answer Area

File1.docx: [ ]
- Preservation Hold
- Recoverable Items
- SubstrateHolds
- The first-stage Recycle Bin

Email: [ ]
- Preservation Hold
- Recoverable Items
- SubstrateHolds
- The first-stage Recycle Bin

Correct Answer:

Answer Area

File1.docx:

- Preservation Hold
- Recoverable Items
- SubstrateHolds
- The first-stage Recycle Bin

Email:

- Preservation Hold
- Recoverable Items
- SubstrateHolds
- The first-stage Recycle Bin

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

k4d4v4r Highly Voted 2 years, 6 months ago
For SharePoint and OneDrive sites: The copy is retained in the Preservation Hold library.

For Exchange mailboxes: The copy is retained in the Recoverable Items folder.

https://docs.microsoft.com/en-us/microsoft-365/compliance/retention?view=o365-worldwide
upvoted 18 times

lkazimirs 1 year, 2 months ago
but the retention policy is still pending - it has not applied....
upvoted 4 times

ruscomike 11 months, 3 weeks ago
agree, the policy is not applied. so it's:
SPO --> recycle bin
EXO--> recoverable items
upvoted 5 times

wooyourdaddy 9 months, 1 week ago
Correct, there is a chart at the following link:

https://learn.microsoft.com/en-us/training/modules/m365-compliance-information-govern-information/configure-retention-policies

Under Step 4: Review your settings section which shows all states. Under the chart it states:

The image below shows the retention policy Teams Chats Retention Policy with a status of On (Pending). The (On Pending) status means the policy is still being deployed and not being enforced on content yet.
upvoted 1 times

Gesbie Most Recent 3 months, 3 weeks ago
was on Exam August 9, 2023, but the status was not in pending, but applied successfully
upvoted 2 times

xswe 7 months, 3 weeks ago
Retained data that gets deleted in the following location gets retained...
Sharepoint = Preservation Hold
Outlook = Recoverable Items
upvoted 1 times

Pravda 1 year, 10 months ago

On exam 1/20/2022
upvoted 1 times

Ali_557 1 year, 11 months ago
When content has retention settings assigned to it, that content remains in its original location. Most of the time, people continue to work with their documents or mail as if nothing's changed. But if they edit or delete content that's included in the retention policy, a copy of the content is automatically retained.

For SharePoint and OneDrive sites: The copy is retained in the Preservation Hold library.

For Exchange mailboxes: The copy is retained in the Recoverable Items folder.

For Teams and Yammer messages: The copy is retained in a hidden folder named SubstrateHolds as a subfolder in the Exchange Recoverable Items folder.
upvoted 4 times

girikedar 1 year, 11 months ago
For the Sharepoint and OneDrive sites the copy is retain in Preservation hold & for Exchange mailboxes the copy is is stored in Recoverable items folder even you delete it from the Deleted items folder.
Tested the the answer is correct.
https://docs.microsoft.com/en-us/microsoft-365/compliance/retention?view=o365-worldwide#how-retention-settings-work-with-content-in-place
upvoted 1 times

skalolaz 2 years, 4 months ago
I would say file deleted from SPO library would be moved to first stage recycle bin.
upvoted 1 times

jcgonzalez1978 2 years, 3 months ago
Yes initally, but after one year nothing is there
upvoted 4 times

pheb 2 years, 3 months ago
No, if a file in SPO is deleted or modified before the retention time is over, it is moved to the 2nd stage recycle bin.

https://docs.microsoft.com/en-us/microsoft-365/compliance/retention-policies-sharepoint?view=o365-worldwide#how-retention-works-for-sharepoint-and-onedrive
upvoted 1 times

Senior 1 year, 10 months ago
The correct answer is preservation hold for Sharepoint as explained in the link you share. In the link you can see when the item is deleted it is moved to the preservation hold library (see 1)

"1. If the content is modified or deleted during the retention period, a copy of the original content as it existed when the retention settings were assigned is created in the Preservation Hold library. "

The other answer is Recoverable items folder as you can see in the link https://docs.microsoft.com/en-us/microsoft-365/compliance/retention-policies-exchange?view=o365-worldwide
upvoted 1 times

shanti0091 2 years, 4 months ago
correct
upvoted 3 times

MNC 1 year, 11 months ago
Which one you are referring is correct?
upvoted 1 times

Question #12 *Topic 3*

You have a Microsoft 365 tenant that uses records management.
You use a retention label to mark legal files stored in a Microsoft SharePoint Online document library as regulatory records.
What can you do to the legal files?

A. Remove the retention label of the files.

B. Edit the properties of the files.

C. Move the files to a different folder within the document library.

D. Delete the content from the files.

Correct Answer: *C*
When content is declared a regulatory record, restrictions are placed on the items in terms of what actions are allowed or blocked. Most actions are blocked except:
- Copy
- Open/Read
- Move within container

Note: Containers include SharePoint document libraries, OneDrive accounts, and Exchange mailboxes.
Note:
There are several versions of this question in the exam. The question has two possible correct answers:
1. Move the files to a different folder within the document library.
2. Copy the content of the files.
Other incorrect answer options you may see on the exam include the following:
1. Change the retention label of the files.
2. Rename the files.
Reference:
https://docs.microsoft.com/en-us/microsoft-365/compliance/records-management?view=o365-worldwide

Eltooth Highly Voted 2 years, 4 months ago
Answer is correct. Regulatory roles are highest level of retention and cannot be removed - even by global admin. Only enabled on tenant by power shell script. Link in answer is really helpful.
C. Move the files to a different folder within the document library.
upvoted 6 times

Gesbie Most Recent 3 months, 3 weeks ago
was on Exam August 9, 2023
upvoted 1 times

xswe 7 months, 3 weeks ago
Regulatory records are the most restrictive type which means that you cannot do much to the files, they are well protected.
In this case you will only be able to move the file WIHTHIN the container
upvoted 1 times

wooyourdaddy 1 year, 5 months ago
Selected Answer: C
I wrote the exam today, this question was on it, I choose C., scored 890!
upvoted 2 times

Pravda 1 year, 10 months ago
On exam 1/20/2022
upvoted 1 times

dasha_an 2 years, 6 months ago

Answer is correct.
https://docs.microsoft.com/en-us/microsoft-365/compliance/create-apply-retention-labels?view=o365-worldwide

"For SharePoint and OneDrive sites: The copy is retained in the Preservation Hold library.

For Exchange mailboxes: The copy is retained in the Recoverable Items folder.

For Teams and Yammer messages: The copy is retained in a hidden folder named SubstrateHolds as a subfolder in the Exchange Recoverable Items folder."

upvoted 2 times

Question #13 *Topic 3*

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

Name	Role
User1	Global administrator
User2	Security administrator
User3	Compliance administrator
User4	Search administrator

You configure a retention label to trigger a disposition review at the end of the retention period.

Which users can access the Disposition tab in the Microsoft 365 compliance center to review the content?

A. User1 only

B. User2 only

C. User3 only

D. User1 and User3

E. User3 and User4

Correct Answer: *C*

Reference:

https://docs.microsoft.com/en-us/microsoft-365/security/office-365-security/permissions-in-the-security-and-compliance-center?view=o365-worldwide

Alpha25 6 months ago

the Compliance Administrator, can access the Disposition tab in the Microsoft 365 compliance center to review the content. The Disposition Management role is included in the Records Management default role group, which is assigned to Compliance Administrators by default. Global Administrators, Security Administrators, and Search Administrators do not have the Disposition Management role by default.

upvoted 1 times

xswe 7 months, 3 weeks ago

Disposition review can only performed members of Disposition Management Role, by default both Compliance Administrator och Compliance Data Administrator have access to this but NOT GA.

upvoted 2 times

prahalski 11 months, 2 weeks ago

While C is technically correct (a compliance admin would see a list of dispositions), they can't actually see the contents unless they are a member of the records management security group that you designate in records management...

upvoted 2 times

IAGirl 1 year, 9 months ago

The disposition management role is assigned by default to compliance administrator and compliance data administrator

upvoted 4 times

Pravda 1 year, 10 months ago

On exam 1/20/2022

upvoted 1 times

Eltooth 2 years, 4 months ago

Answer is correct - User 3 only as GA role does not inherit all compliance roles. Compliance Admin role has this disposition management role be default.

upvoted 3 times

Lineup 2 years, 6 months ago

Shouldnt the global administrator also have access?

upvoted 3 times

Piper 2 years, 6 months ago

I dont think so, for some Security and Compliance stuff, even a GA doesnt have everything and needs adding to some of the roles.

upvoted 7 times

Anker 2 years, 5 months ago

Correct,

Permissions for disposition
To successfully access the Disposition tab in the Microsoft 365 compliance center, users must have the Disposition Management role.

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

Dispisition management role is included in the Compliance Administrator role so this looks correct
upvoted 9 times

HOTSPOT -

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

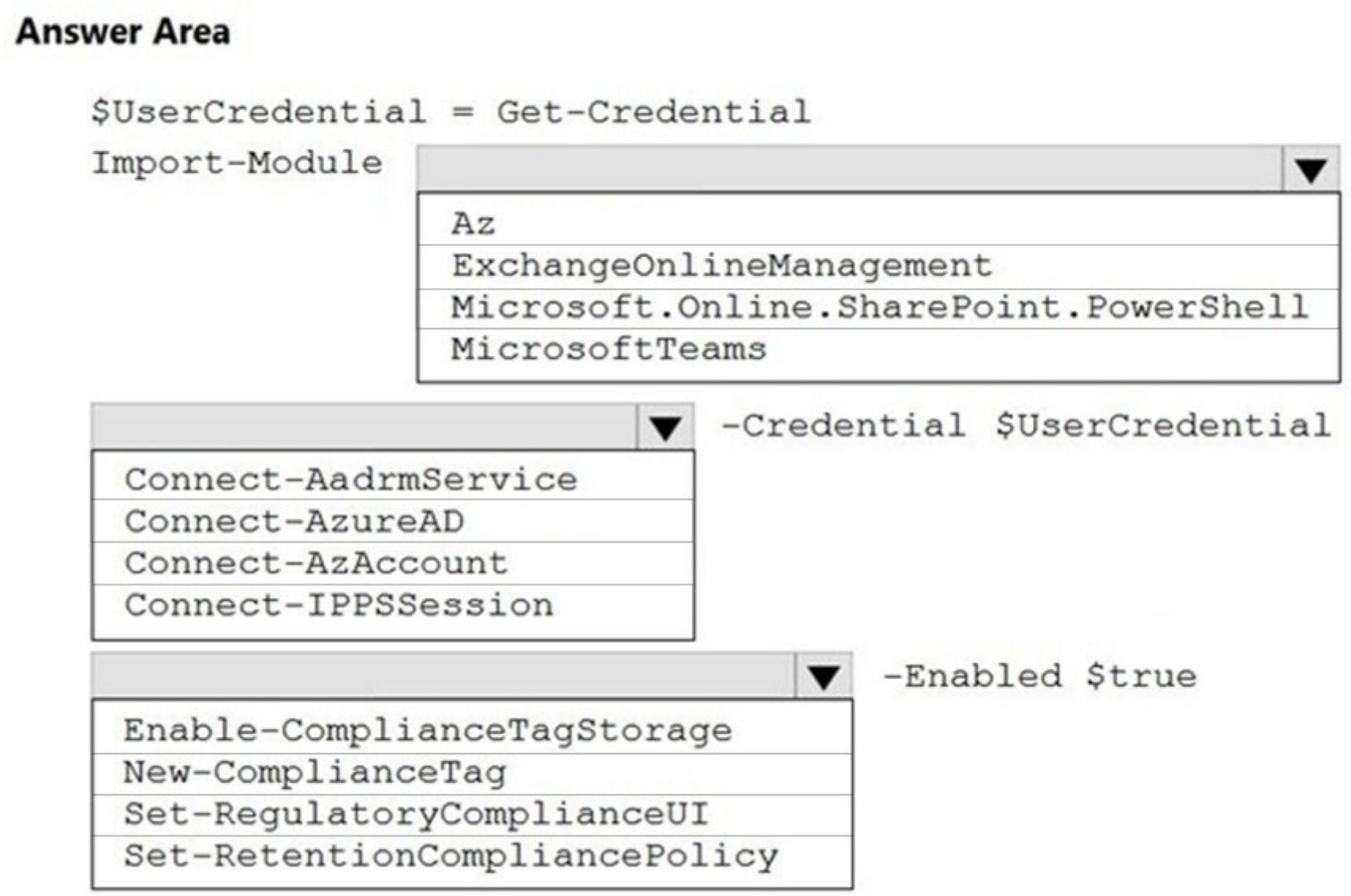
- Mark items as a record
- Mark items as a regulatory record

You need to ensure that the options are available when you create retention labels 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.

Hot Area:



Correct Answer:

Answer Area

```
$UserCredential = Get-Credential
Import-Module [ ▼ ]
```

- Az
- ExchangeOnlineManagement
- Microsoft.Online.SharePoint.PowerShell
- MicrosoftTeams

```
[ ▼ ] -Credential $UserCredential
```

- Connect-AadrmService
- Connect-AzureAD
- Connect-AzAccount
- Connect-IPPSSession

```
[ ▼ ] -Enabled $true
```

- Enable-ComplianceTagStorage
- New-ComplianceTag
- Set-RegulatoryComplianceUI
- Set-RetentionCompliancePolicy

Reference:
https://docs.microsoft.com/en-us/microsoft-365/compliance/declare-records?view=o365-worldwide https://docs.microsoft.com/en-us/powershell/exchange/connect-to-scc-powershell?view=exchange-ps

wooyourdaddy 9 months, 1 week ago

Answer can be confirmed in these links:

https://learn.microsoft.com/en-us/powershell/module/exchange/connect-ippssession?view=exchange-ps

Where the Prerequisites for the Exchange Online PowerShell module hyperlink mentions the ExchangeOnlineManagement module being needed for the Connect-IPPSSession command.

And this link:

https://learn.microsoft.com/en-us/powershell/module/exchange/set-regulatorycomplianceui?view=exchange-ps

Which states:

Use the Set-RegulatoryComplianceUI cmdlet to display the UI option in retention label settings to mark content as a regulatory record.

upvoted 3 times

JCkD4Ni3L 11 months, 2 weeks ago

Correct !

upvoted 2 times

chrissempai 1 year, 2 months ago

the answer is correct

upvoted 3 times

Question #15 *Topic 3*

You need to ensure that documents in a Microsoft SharePoint Online site that contain a reference to Project Alpha are retained for two years, and then deleted.
Which two objects should you create? Each correct answer presents part of the solution. (Choose two.)
NOTE: Each correct selection is worth one point.

A. a retention policy

B. an auto-apply label policy

C. a sensitive info type

D. a retention label

E. a sensitivity label

F. a publish labels policy

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

k4d4v4r Highly Voted 2 years, 6 months ago
Should be BD as seem here in the link. In the note above the explanation it says that we can ALSO create retention policies for that... so I assume that the more correct answer should be BD.
https://docs.microsoft.com/en-us/microsoft-365/compliance/apply-retention-labels-automatically?view=o365-worldwide#how-to-auto-apply-a-retention-label
upvoted 14 times

xswe Most Recent 7 months, 3 weeks ago
Since we want to retain the documents for 2 years and then delete them we want to have a retention label that will get applied to these documents that contains the reference.
To apply the retention label correctly we can use an auto-apply label policy and when configuring it we can add the reference Project Alpha to the auto-labeling policy
upvoted 1 times

Valavan 11 months, 3 weeks ago
Answer is correct
upvoted 2 times

chrissempai 1 year, 2 months ago
Selected Answer: BD
on exam 9/9/2022
upvoted 1 times

RamenIsDelicious 1 year, 3 months ago
Selected Answer: BD
B D tested 8/11/22.
upvoted 1 times

PrettyFlyWifi 1 year, 9 months ago
Selected Answer: BD
B and D looks correct
Retention label is needed to define the 2 years and then delete setting
An auto-label policy lets you choose an option on what to look for and you can tell it look for 'Project Alpha', then at the end of the policy you apply the label you just created and it'll use those two elements to meet the answer.
upvoted 1 times

Pravda 1 year, 10 months ago
On exam 1/20/2022
upvoted 1 times

Elyamany 1 year, 10 months ago
I think the answer is right, because you have to create the retention label first to define the action, then you create the auto apply retention policy, then choose the Info Sensitivity type and choose the created retention label.
We assume that the sensitivity info type is already created.
upvoted 1 times

Pravda 1 year, 10 months ago

B D correct.
Step 1 and Step 2 in the link.
upvoted 1 times

hydrillo 2 years, 3 months ago
I cannot wrap my head around this. First you need a sensivity info type for the Project Alpha references, then you need a retention label for the retention settings and an auto-apply label policy to publish it to the site. So it is C, B and D in that order. You need all three. What am I missing here?
upvoted 4 times

pheb 2 years, 3 months ago
it should be C and D then.
upvoted 1 times

hydrillo 2 years, 3 months ago
I got around this. You can define a content query for the project Alpha references in the auto-label policy. Therefore it is B & D for sure
upvoted 4 times

hydrillo 2 years, 3 months ago
I finally got this question. Sorry for the confusion. With a retention policy you can apply a sensitivity info type directly to a SP site. Tested in lab. Answer A+C
upvoted 2 times

sergioandreslq 1 year, 11 months ago
I believe it is BC.
You create the custom Sensitive info type with keyword "Project Alpha".
Then, You create an "auto-labeling policy" that use the custom Sensitive info type above and choose the location SPO.
Incorrect A: I didn't find how to use Sensitive information type using Retention, Policies. The retention policy apply to the whole SPO not to specific items, if you use retention policies, It will retain all the files inside the SPO, not only the files with "Project Alpha"
upvoted 4 times

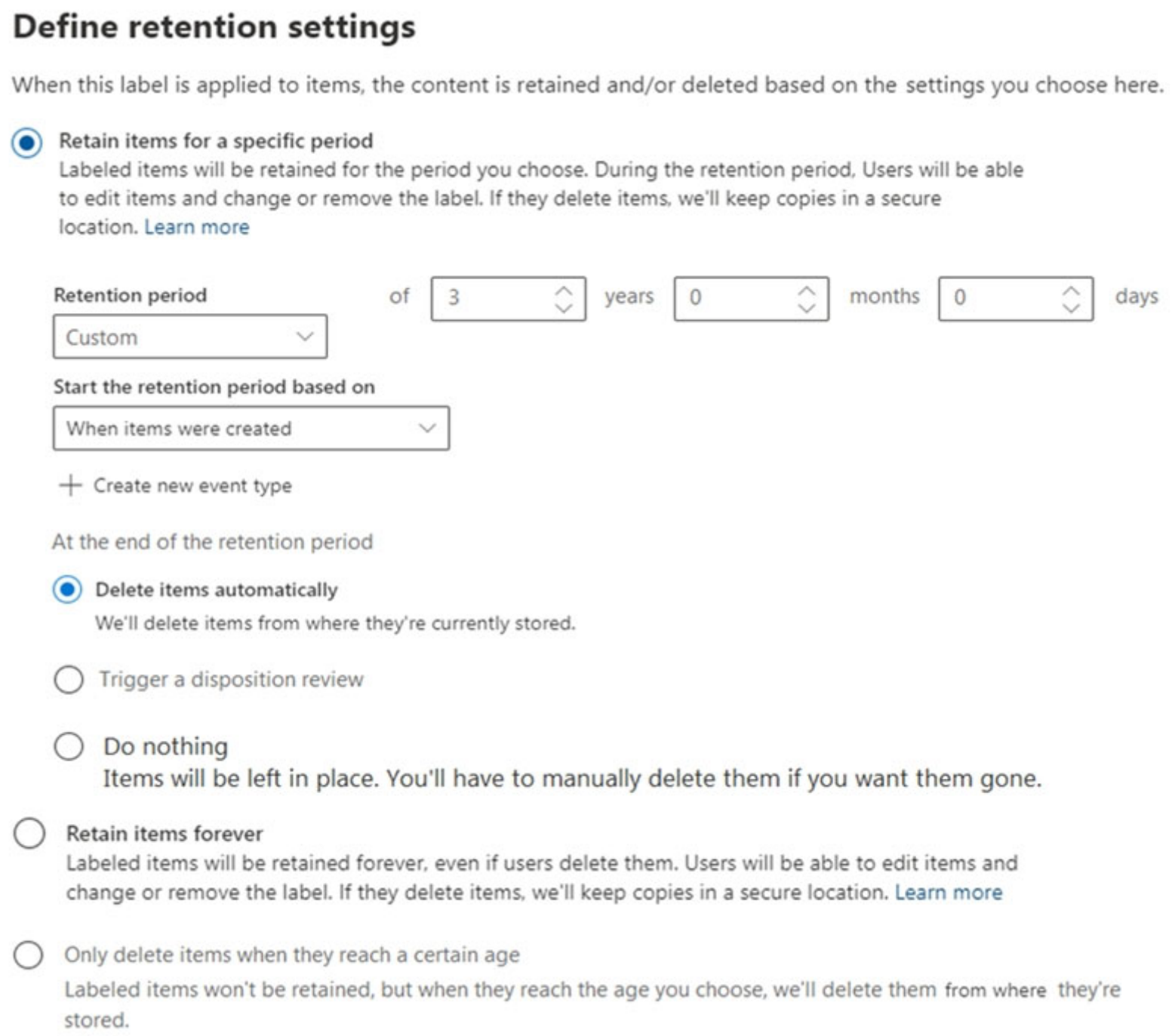
k4d4v4r 2 years, 6 months ago
Keep in mind that "Retention Policy" is for being the default retention schema for the new itens... the auto-apply is also for what is already inside SP without a label.
upvoted 3 times

olsi 2 years, 6 months ago
not agree with the proposed answer. It should be A, D.
Retention label policy applies to single document (item level).
Whereas Retention Policy to a whole container, like SP Site content, Mailbox
See: https://docs.microsoft.com/en-us/microsoft-365/compliance/retention?view=o365-worldwide#retention-policies-and-retention-labels
upvoted 3 times

Val_0 2 years, 4 months ago
I think the key here is "reference to...", which means there are other documents in the SP site that do not reference the Alpha Project and therefor do not need to be retained/labeled. If this is the case, then BD is the answer, otherwise you'll end up retaining all the documents in the site and not just those with the reference to the project.
upvoted 6 times

Anker 2 years, 5 months ago
I'd tend to agree with you on this one. Since the question asks you to label multiple documents within a SP site this would likely be done at the site level not the document level so I'd probably use a retention policy. Unless I'm missing something in the question
upvoted 1 times

You are configuring a retention label named Label1 as shown in the following exhibit.



You need to ensure that documents that have Label1 applied are deleted three years after the end of your company's fiscal year. What should you do?

A. Create a new event type.

B. Select Only delete items when they reach a certain age.

C. Modify the Retention period setting.

D. Set At the ends of the retention period to Trigger a disposition review.

Correct Answer: *A*

Reference:

https://docs.microsoft.com/en-us/microsoft-365/compliance/event-driven-retention?view=o365-worldwide

Nvdp Highly Voted 2 years, 5 months ago

Should be C, "retention should start based on Fiscal year"

upvoted 5 times

Nvdp 2 years, 5 months ago

A is correct - new event type

upvoted 12 times

xswe Most Recent 7 months, 3 weeks ago

A new event type will make sure that the retention period will use fiscal year instead of when items were created

upvoted 1 times

chrissempai 1 year, 2 months ago

Selected Answer: A

A is correct

on exam the 9/9/22

upvoted 3 times

wooyourdaddy 1 year, 5 months ago

Selected Answer: A

I wrote the exam today, this question was on it, I choose A, scored 890!

upvoted 3 times

Azuz 1 year, 9 months ago

Selected Answer: A

A is correct, You can create a new event type and specify a date.

upvoted 2 times

Pravda 1 year, 10 months ago

On exam 1/20/2022

upvoted 1 times

olsi 2 years, 6 months ago

correct, agree

upvoted 4 times

HOTSPOT -

You enable archive mailboxes for all the users at your company.

The Default MRM Policy is shown in the MRM exhibit.

Default MRM Policy

This policy contains the following retention tags

1 Month Delete
1 Week Delete
1 Year Delete
5 Year Delete
6 Month Delete
Default 2 year move to archive
Junk Email
Never Delete
Personal 1 year move to archive
Personal 5 year move to archive
Personal never move to archive
Recoverable items 14 days move to archive

A Microsoft 365 retention label policy is shown in the Label Policy exhibit.

Exchange Label Policy

Status
Enabled (Pending)

Policy name
Exchange Label Policy

Description
Label policy for Exchange

Applies to content in these locations
Exchange email

Settings
Publish labels for your users
- 10 Year – Do not Delete
- 2 Year Delete

Preservation lock
No

You need to identify the following:

☞ How many years until an email is archived?

☞ What should you modify to change the retention period for archiving?

What 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

By default, email is:

- Deleted after two years
- Deleted after one month
- Retained in the mailbox for 10 years
- Moved to the archive mailbox after two years

To change the retention period for archiving, modify:

- The Default MRM Policy
- The Exchange Label Policy
- The properties of the archive mailbox

Correct Answer:

Answer Area

By default, email is:

- Deleted after two years
- Deleted after one month
- Retained in the mailbox for 10 years
- Moved to the archive mailbox after two years

To change the retention period for archiving, modify:

- The Default MRM Policy
- The Exchange Label Policy
- The properties of the archive mailbox

Reference:
https://docs.microsoft.com/en-us/microsoft-365/compliance/retention?view=o365-worldwide#the-principles-of-retention-or-what-takes-precedence

olsi Highly Voted 2 years, 6 months ago

first box: 10 yeas
second box: Exchange label policy
reason:
- explicit over implicit --> thus exchange label policy over default
- retention wins over deletion --> thus 10 years
- longest retention wins --> another argument for 10 years instead of moving to archive (explicit)

upvoted 13 times

ExamReviewerIZ 2 years, 1 month ago

This is so wrong. I'm sorry. But labels must be applied manually by the users.

upvoted 5 times

DeeJayU 1 year, 11 months ago

After 2y emails are moved to archive and retain for 8y+ (assuming the label was applied).

upvoted 3 times

Discuss4certi 2 years, 3 months ago

I disagree, first one stays 2 years to the archive folder. as it is the default we are looking for, not one of the labels you provide for your users in the screenshot. Unless it is mentioned that one of them is applied the default remains 2 years to archival folder.

upvoted 5 times

LHADUK Highly Voted 11 months, 2 weeks ago

guys, I have been working with exchange labels for years.
Setup is - if u enable arhcive mailbox for user, the Default MRM policy is applied.
Default MRM policy has default action - automatic move mail to online archive after reaches 2 years.

If u want to change that, you need to create new retention tag, edit default MRM policy, delete default retention tag and select new one or just create new Exchange label policy choose your default retention tag and apply policy to users.
upvoted 7 times

NinjaSchoolProfessor Most Recent 11 months, 1 week ago
Outdated question. Microsoft recommends to retain and delete emails, we recommend you use Microsoft 365 retention policies and retention labels rather than the older messaging records management (MRM) from Exchange Online.

https://learn.microsoft.com/en-us/microsoft-365/compliance/set-up-an-archive-and-deletion-policy-for-mailboxes?view=o365-worldwide
upvoted 3 times

Jahoor69 1 year, 8 months ago
correct.

https://docs.microsoft.com/en-us/exchange/security-and-compliance/messaging-records-management/default-retention-policy#:~:text=Managed%20Folder%20Assistant-,Retention%20tags%20linked%20to%20the%20Default%20MRM%20Policy,-The%20following%20table
upvoted 1 times

IAGirl 1 year, 9 months ago
-> Moved to the archive mailbox after two years, because is the default policy
-> The default MRM: " you should continue using messaging records management to move messages to archive mailboxes."
https://docs.microsoft.com/en-us/exchange/security-and-compliance/messaging-records-management/messaging-records-management
upvoted 4 times

IAGirl 1 year, 9 months ago
For archive policies use MRM
https://docs.microsoft.com/en-us/microsoft-365/compliance/set-up-an-archive-and-deletion-policy-for-mailboxes?view=o365-worldwide on Exchange Admin Center
upvoted 2 times

Pravda 1 year, 10 months ago
I think default answer are correct.
There is only one move policy. After 2 years it will be moved,
Second is defiantly MRM.
Microsoft recommends using retention policies and labels over MRM. However, mailbox archiving is only available in MRM.
upvoted 2 times

girikedar 1 year, 11 months ago
the status is in pending so Default Move to archive after 2 years will be the first box answer
& to change default archiving-- box 2 - answer is Exchange Label policy
answer is Default Move to archive after 2 years & Exchange Label policy
upvoted 1 times

ExamReviewerIZ 2 years, 1 month ago
Only the Default MRM policy applies in this scenario. The second part of the question says you PUBLISH the labels, but none is applied unless the users apply it to folders or individual emails.

Answers are: Move to the archive after two years, Default MRM Policy.

Just ingnore the labels, unless the scenario says "the user applied X label".
upvoted 5 times

wooyourdaddy 9 months, 1 week ago
Adding to this, the label is in an Enabled (Pending) state which means the policy is still being deployed and not being enforced on content yet.

Answers are Moved to the archive box after two years and
upvoted 1 times

wooyourdaddy 9 months, 1 week ago
Default MRM Policy
upvoted 1 times

xofowi5140 2 years, 4 months ago
So is 2 years or 10 years?
upvoted 1 times

kingsmiill00 2 years, 4 months ago
1) Move to the archive mailbox after 2 years
2) Exchange label policy
upvoted 6 times

Brox 2 years, 5 months ago

default is that user doesn't apply a special label to a mail(del2years or ret10 years). So default is move to archive 2 years.
upvoted 2 times

dasha_an 2 years, 6 months ago
Agree with olsi.
first box: 10 yeas
second box: Exchange label policy

"When you have retention policies only: If a retention policy for a location is scoped to use an include configuration (such as specific users for Exchange email) that retention policy takes precedence over unscoped retention policies for the same location."
upvoted 3 times

Question #18 *Topic 3*

You have a Microsoft 365 tenant.
You have a Microsoft SharePoint Online site that contains employment contracts in a folder named EmploymentContracts. All the files in EmploymentContracts are marked as records.
You need to recommend a process to ensure that when a record is updated, the previous version of the record is kept as a version of the updated record.
What should you recommend?

A. Upload an updated file plan that contains the record definition.

B. Unlock the record, modify the record, and then lock the record.

C. Create a copy of the record and enter a version in the file metadata.

D. Create a new label policy associated to an event that will apply to the record.

Correct Answer: *B*
Reference:
https://docs.microsoft.com/en-us/microsoft-365/compliance/record-versioning?view=o365-worldwide

Discuss4certi Highly Voted 2 years, 3 months ago
Correct - B. Each time a user unlocks a record, the latest version is copied to the Preservation Hold library, and that version contains the value of Record in the Comments field of the version history.
upvoted 8 times

Pravda Most Recent 1 year, 10 months ago
On exam 1/20/2022
upvoted 3 times

Eltooth 2 years, 4 months ago
Correct - Answer B.
upvoted 2 times

Question #19 *Topic 3*

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 User1 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. the Restore-SPODeletedSite PowerShell cmdlet

B. the OneDrive recycle bin

C. the Restore-ADObject PowerShell cmdlet

D. Deleted users in the Microsoft 365 admin center

Correct Answer: *B*
Reference:
https://docs.microsoft.com/en-us/onedrive/set-retention
https://docs.microsoft.com/en-us/onedrive/retention-and-deletion

Krille Highly Voted 1 year, 11 months ago

Selected Answer: A

According to https://docs.microsoft.com/en-us/onedrive/restore-deleted-onedrive the Powershell command "Restore-SPODeletedSite -Identity <URL>" should be used to "Restore a deleted OneDrive when the deleted user no longer appears in the Microsoft 365 admin center"

upvoted 10 times

Domza Most Recent 3 weeks ago

A is correct~ Restore from SharePoint with PS after 30 days

upvoted 1 times

chrissempai 1 year, 2 months ago

Selected Answer: A

By default you can restore by the OneDrive bon only for 93 days after that you need to do the Powershell command

upvoted 4 times

odbjegli 1 year, 7 months ago

Selected Answer: A

https://support.microsoft.com/en-us/office/restoring-a-deleted-onedrive-for-business-site-c5595183-a1ef-4931-8201-48a62134f5af

upvoted 2 times

Melwin86 1 year, 9 months ago

Selected Answer: A

https://docs.microsoft.com/en-us/onedrive/restore-deleted-onedrive

If the user was deleted within 30 days, you can restore the user and all their data from the Microsoft 365 admin center. To learn how, see Restore a user in Microsoft 365. If you deleted the user more than 30 days ago, the user will no longer appear in the Microsoft 365 admin center, and you'll need to use PowerShell to restore the OneDrive.

upvoted 3 times

nupagazi 1 year, 10 months ago

B is correct. You can use both Recycle bin and cmdlet to resotre data from recycle bin. Cmdlet is sued when you want to restore whole site. Using recyle bin you can pick up file by file. The question is about restore an important file, not whole site
https://support.microsoft.com/en-us/office/restore-deleted-files-or-folders-in-onedrive-949ada80-0026-4db3-a953-c99083e6a84f?ui=en-us&rs=en-us&ad=us

upvoted 3 times

Abiy006 1 year, 5 months ago

I think the Recycle bin is for deleted files, hear the user is deleted, you can't recover the file before restoring the AD user first

upvoted 2 times

Pravda 1 year, 10 months ago

On exam 1/20/2022

upvoted 1 times

tunstila 1 year, 10 months ago

Selected Answer: A

If you deleted the user more than 30 days ago, the user will no longer appear in the Microsoft 365 admin center, and you'll need to use PowerShell to restore the OneDrive.

To restore the OneDrive to an active state, run;

Restore-SPODeletedSite cmdlet

Answer is A..

Reference:
https://docs.microsoft.com/en-us/onedrive/restore-deleted-onedrive

upvoted 2 times

tunstila 1 year, 10 months ago

If you deleted the user more than 30 days ago, the user will no longer appear in the Microsoft 365 admin center, and you'll need to use PowerShell to restore the OneDrive.

To restore the OneDrive to an active state, run;

Restore-SPODeletedSite cmdlet

Answer is A..

upvoted 1 times

Eltooth 2 years, 4 months ago

OneDrive data retention is at to retain data for 5 years (10 years maximum) so data can be restored by an admin from OneDrive recycle bin.

upvoted 2 times

HOTSPOT -

You have the files shown in the following table.

Name	Location	Date modified	Date created
File1	Microsoft SharePoint Online site	June 01, 2018	December 28, 2011
File2	Microsoft OneDrive account	February 02, 2017	January 02, 2011
File3	Microsoft Exchange Online public folder	May 01, 2006	May 01, 2006

You configure a retention policy as shown in the exhibit.

RetentionPolicy 1

Status
Enabled (Pending)

Policy name
RetentionPolicy1

Description
RetentionPolicy1

Applies to content in these locations
SharePoint sites

Settings
Retention period
Keep content, and delete it if it's older than 7 years

Preservation lock
No data available

The start of the retention period is based on when items are created. The current date is January 01, 2021.

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:

Answer Area

Statements	Yes	No
File1 will be deleted after you turn on the policy.	○	○
File2 will be deleted after you turn on the policy.	○	○
File3 will be deleted after you turn on the policy.	○	○

Answer Area

	Statements	Yes	No
Correct Answer:	File1 will be deleted after you turn on the policy.	○	○
	File2 will be deleted after you turn on the policy.	○	○
	File3 will be deleted after you turn on the policy.	○	○

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

Deepak9826 Highly Voted 2 years, 4 months ago
Answers are correct. Label is applied only for Sharepoint ..based on which only File 1 will be deleted as the date creation exceeds 7yrs retention
upvoted 15 times

daavidsc400 1 year, 8 months ago
agreed that file 1 is the only 1 that would apply in this scenario. However, the status says "enabled pending" and I would think that means the policy might not have been applied to the file yet. Doesn't that mean that the file is not going to be deleted yet?
upvoted 2 times

wooyourdaddy 9 months, 1 week ago
Good observation @daavidsc400. The question asks what will happen when you turn on the policy, which would then trigger the conditions. The key to the answer for this question is the locations, which is only SharePoint Sites as @Deepak9826 stated.
upvoted 2 times

PhyMac 8 months ago
I always show your comments.
So I understand that the policy is not currently in effect because it says "enabled pending".
So the answer to box 1 is NO correct?
upvoted 1 times

HDEIWDEOW Most Recent 3 months, 2 weeks ago
Got this question on exam on 17th August
upvoted 1 times

cris_exam 5 months, 2 weeks ago
Ahh, tricky one!

So, if the policy would have been just "Enabled" the correct answer is indeed Y/N/N.

But since it shows "Enabled (Pending)" it means that it has not yet fully applied to the location/s and hence even though the way is configured should delete File1, since it's pending it's not 100% guaranteed that this will happen, however, the pending state theoretically should only take a "not so long" amount of time - maybe few hours - 1 day at most and then the Retention policy is good successful.

So what should we pick??? :))
Very tricky...

It could be that for this question when they create the lab for it, the policy was still pending and the intended answer is Y / N / N, or it may not and in fact should be N / N / N. Too ambiguous tbh.
upvoted 1 times

PhyMac 7 months, 3 weeks ago
Since the status of the retention policy says Pending, I think BOX 1 is NO.
upvoted 1 times

xswe 7 months, 3 weeks ago
Remember to check "Applies to content in these location", only File1 will get applied to the policy since its located in SharePoint.
Yes, 7 has passed
No, wrong location
No, wrong location
upvoted 2 times

daavidsc400 1 year, 8 months ago
The status of the policy says enabled pending. Doesn't that mean that the policy hasn't completely sync'd to all locations and been applied? If that's the case, no files are going to be deleted right away when the policy is turned on.
upvoted 1 times

Pravda 1 year, 10 months ago
On exam 1/20/2022
upvoted 1 times

Zorolloo 1 year, 11 months ago
This is Correct
upvoted 2 times

ExamReviewerIZ 2 years, 1 month ago
Every file is older than 7 years, so everything would be deleted, except it only applies to SharePoint sites (and this does NOT include OneDrive sites)

Answer: Y, N, N
upvoted 2 times

oberte007 2 years, 2 months ago
Right answer. the retention policy is scoped to sharepoint sites only not to ondrive accounts and Exchange online. Further the duration between modification date and creation date of files should be 7 years in order files be deleted referencing to policy settings.
upvoted 1 times

xofowi5140 2 years, 4 months ago
Why file 3 is not deleted?
upvoted 1 times

xofowi5140 2 years, 4 months ago
The current date is January 01, 2021. File3 date may 2006
upvoted 1 times

xofowi5140 2 years, 4 months ago
Admin please delete the previous comment.
upvoted 1 times

xofowi5140 2 years, 4 months ago
I understand is not Microsoft SharePoint Online site file.
upvoted 3 times

xofowi5140 2 years, 4 months ago
Date created
June 01,2018 - January 01, 2021 = 9 years
January 02, 2011 - January 01, 2021 = 9 years
May, 01, 2006 - January 01, 2021 = 14 years

Date modified:

June 01,2018 - January 01, 2021 = 2 years
February 02,2017 - January 01, 2021 = 3 years
May, 01, 2006 - January 01, 2021 = 14 years
upvoted 1 times

xofowi5140 2 years, 4 months ago
Admin. Please delete the previous comment.
upvoted 2 times

jaycn67 2 years, 4 months ago
Answer is N/N/N
is 6 years, 5 months, 4 days excluding the end date
upvoted 1 times

Eltooth 2 years, 4 months ago
Correct - Y / N / N.
upvoted 2 times

Eniola 2 years, 4 months ago
It is not correct, from the calculation...that is not 7 years yet!
upvoted 2 times

JakubK64 2 years, 5 months ago
Correct. It based on creation date and apply only to SharePoint sites
upvoted 4 times

Question #21 *Topic 3*

At the end of a project, you upload project documents to a Microsoft SharePoint Online library that contains many files. The following is a sample of the project document file names:

- aei_AA989.docx
- bci_WS098.docx
- cei_DF112.docx
- ebc_QQ454.docx
- ecc_BB565.docx

All documents that use this naming format must be labeled as Project Documents:

You need to create an auto-apply retention label policy.

What should you use to identify the files?

A. A sensitive info type

B. A retention label

C. A trainable classifier

Correct Answer: *C*

Reference:

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

test123123 Highly Voted 2 years, 5 months ago

I think this should be A.
A sensitive info type, a regular expression kan detect filename (a-z + d{3}) easy and fast.

upvoted 16 times

IAGirl Highly Voted 1 year, 9 months ago

I tested and a sensitive info type is not able to verify the file name.

upvoted 5 times

IAGirl 1 year, 9 months ago

All methods checks for content. In this case we don't know the content, so the best thing to do is use trainable classifiers to check the content and find a pattern to identify the files. In my opinion, the question includes files names just for confuse us!

upvoted 2 times

Romeokton Most Recent 5 days, 13 hours ago

Wow, what a tricky question. Really a hard one. From all I've read, I found out that DLP policy applied to Exchange online has the option to check if file name matches a pattern. https://learn.microsoft.com/en-us/purview/dlp-policy-reference

SIT definitely does not identify file names. Hence, I would also opt for trainable classifier.

upvoted 1 times

cris_exam 5 months, 2 weeks ago

Selected Answer: A

Because the question says: All documents that use this naming format must be labeled as Project Documents

I chose SIT - A

upvoted 1 times

ivzdf 5 months, 2 weeks ago

the question says that the documents are uploaded to a Microsoft SharePoint Online library
One of the requirements for trainable classifiers is: Place the seed content in a SharePoint Online folder that is dedicated to holding the seed content only. Make note of the site, library, and folder URL.
https://learn.microsoft.com/en-us/microsoft-365/compliance/classifier-get-started-with?view=o365-worldwide

Since the upload can easily be used to train the classifier since many examples are in it. I agree with C.

upvoted 1 times

xswe 7 months, 3 weeks ago

Since we have a bunch of documnents with content that we are going to look for we can create an auto-apply label policy that will use a trainable classifier that will use documents as seed documents to find them in the future.

upvoted 1 times

kvdvliert 8 months ago

Selected Answer: C

Trainable classifiers work with .docx files.

https://learn.microsoft.com/en-us/microsoft-365/compliance/classifier-learn-about?view=o365-worldwide&viewFallbackFrom=o365-worldwid
upvoted 1 times

JamesM9 1 year, 7 months ago
The answer is C - trainable classifier.
upvoted 2 times

ex_panonija 1 year, 8 months ago
Selected Answer: A
Question #4 actually contains the answer ;)

Question #4Topic 1
HOTSPOT -
You use project codes that have a format of three alphabetical characters that represent the project type, followed by three digits, for example Abc123.
You need to create a new sensitive info type for the project codes.
How should you configure the regular expression to detect the content?
upvoted 3 times

omnomsnom 1 month ago
"How should you configure the regular expression to detect the content?" - Content, not file name.
upvoted 1 times

PrettyFlyWifi 1 year, 9 months ago
Selected Answer: A
Sensitivity info type makes more sense to me, as it's focused on just the project documents in a site with "many files". If you do a trainable classifier you'd need a large set of "good" examples and this could take a while. But if you were to create a custom sensitive info type and use regex expressions then it should be simpler to implement.
upvoted 2 times

olsenOnS 1 year, 8 months ago
SIT verify file names or only content of that files ?
upvoted 1 times

Elyamany 1 year, 10 months ago
I think he has chosen the trainable classifier as it is mentioned in the question:
"you upload project documents to a Microsoft SharePoint Online library that contains many files." So the requested files are existing only in SharePoint Library. So I believe the answer is right
upvoted 1 times

Pravda 1 year, 10 months ago
C is the correct answer. Everyone if focusing on the ###_ll### and not the simple .docx.
Trainable classifiers work with .docx files. (It's that simple.)
https://docs.microsoft.com/en-us/microsoft-365/compliance/classifier-learn-about?view=o365-worldwide
upvoted 1 times

jkklim 2 years, 2 months ago
Answer = A

what they want is a NAMING format, NOT the inside of the file contents as classifer is looking at contents
upvoted 3 times

[Removed] 2 years ago
Agree, I did a test and the filenames are also detected by a sensitive info type.
upvoted 4 times

rlama 2 years, 2 months ago
a senstive info type might do but project is organisation specific thus a trainable classifier is correct anwser
upvoted 1 times

MahmoudEldeep 2 years, 3 months ago
Sensitive info type does not classify based on file name
upvoted 4 times

Discuss4certi 2 years, 3 months ago
My first thought was what, that's not true, but indeed it only checks the content not the file name.
upvoted 1 times

JakubK64 2 years, 5 months ago
I don't think so. For me A is better answer, even C should also work. Name of file have easy pattern, so sensitivi info type based on RegEx will be best choice for me
upvoted 1 times

xofowi5140 2 years, 4 months ago

Why A?
Sensitive info type is for sensitive content.

upvoted 1 times

Question #22 *Topic 3*

You need to create a retention policy to retain all the files from Microsoft Teams channel conversations and private chats.
Which two locations should you select in the retention policy? Each correct answer presents part of the solution. (Choose two.)
NOTE: Each correct selection is worth one point.

A. OneDrive accounts

B. Office 365 groups

C. Team channel messages

D. SharePoint sites

E. Team chats

F. Exchange email

Correct Answer: *AD*
Reference:
https://support.microsoft.com/en-us/office/file-storage-in-teams-df5cc0a5-d1bb-414c-8870-46c6eb76686a

xswe 7 months, 3 weeks ago
Retention policies for Teams has to choose Onedrive and Sharepoint to make sure that you retain all the files that gets shared in private chats and teams channels
upvoted 1 times

JCkD4Ni3L 11 months, 2 weeks ago
Selected Answer: AD
Correct, A & D. The question states about files, not the conversations, so the backend is built upon OneDrive and Sharepoint Online.
upvoted 2 times

IAGirl 1 year, 9 months ago
Selected Answer: AD
Teams channel conversations: documents shared -> Sharepoint
Teams private chat: documents shared -> OneDrive for Bussiness
upvoted 3 times

PrettyFlyWifi 1 year, 9 months ago
Key bit i think is "retain all the files", so I'd say ODfB and SPO. Selecting Teams locations are retention on actual chat messages, not files.
upvoted 1 times

examdoer 1 year, 9 months ago
Selected Answer: AD
question is about retaining files. Files in private chats are stored in the personal OD and files in channel messages are stored in SPO.
upvoted 1 times

yitbos 1 year, 10 months ago
It asks about documents and not messages, so AD. CE would be chat messages and not documents.
upvoted 1 times

Pravda 1 year, 10 months ago
A and D are correct. The question was asked slightly different previously.
upvoted 3 times

Robert__Susin 1 year, 10 months ago
Selected Answer: CE
Sorry, it's not about private channel messages, but still it's not possible to mark both OneDrive/SharePoint and Teams chats/channel messages, I would go with C/E
upvoted 1 times

examdoer 1 year, 9 months ago
question is about retaining files. Files in private chats are stored in the personal OD and files in channel messages are stored in SPO. so CE is not the answer.
upvoted 1 times

Robert__Susin 1 year, 10 months ago
This is wrong, it should be Teams private channel messages which is not presented as part of the answer. You only select + those when you are dealing with DLP

It's not allowed to select both Teams and OneDrive/SharePoint when creating retention policy!
upvoted 1 times

Eltooth 2 years, 4 months ago
Correct - ODfB stores files from 1-2-1 and private group chats. SPO stores files from Teams channels.
upvoted 3 times

JakubK64 2 years, 5 months ago
Looks correct. Files from private chats are stored on OneDrive, files from channels are stored on SP
upvoted 4 times

Question #23 *Topic 3*

You have a Microsoft 365 tenant that uses records management.
You use a retention label to mark legal files stored in a Microsoft SharePoint Online document library as regulatory records.
What can you do to the legal files?

A. Rename the files.

B. Edit the properties of the files.

C. Change the retention label of the files.

D. Copy the content of the files.

Correct Answer: *D*
When content is declared a regulatory record, restrictions are placed on the items in terms of what actions are allowed or blocked. Most actions are blocked except:
☞ Copy
☞ Open/Read
☞ Move within container
Note: Containers include SharePoint document libraries, OneDrive accounts, and Exchange mailboxes.
Note:
There are several versions of this question in the exam. The question has two possible correct answers:
1. Move the files to a different folder within the document library.
2. Copy the content of the files.
Other incorrect answer options you may see on the exam include the following:
☞ Delete the content from the files.
☞ Remove the retention label of the files.
Reference:
https://docs.microsoft.com/en-us/microsoft-365/compliance/records-management?view=o365-worldwide

Eltooth Highly Voted 2 years, 4 months ago
Correct - D.
upvoted 6 times

xswe Most Recent 7 months, 3 weeks ago
Regulatory records are the most restrictive record, in this case you can only copy the content of the files.
No changes can be made when you have this record retention label applied.
upvoted 1 times

wooyourdaddy 9 months, 1 week ago
https://learn.microsoft.com/en-us/microsoft-365/compliance/records-management?view=o365-worldwide#compare-restrictions-for-what-actions-are-allowed-or-blocked
upvoted 2 times

Pravda 1 year, 10 months ago
On exam 1/20/2022
upvoted 2 times

Question #24 *Topic 3*

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:

- Status: Off (Error)
- It's taking longer than expected to deploy the policy

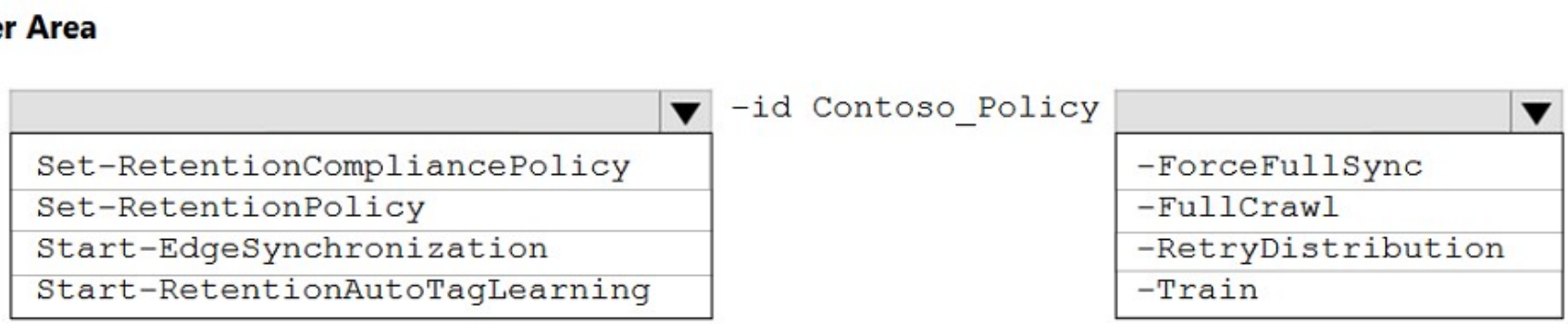
You need to reinitiate the policy.

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

NOTE: Each correct selection is worth one point.

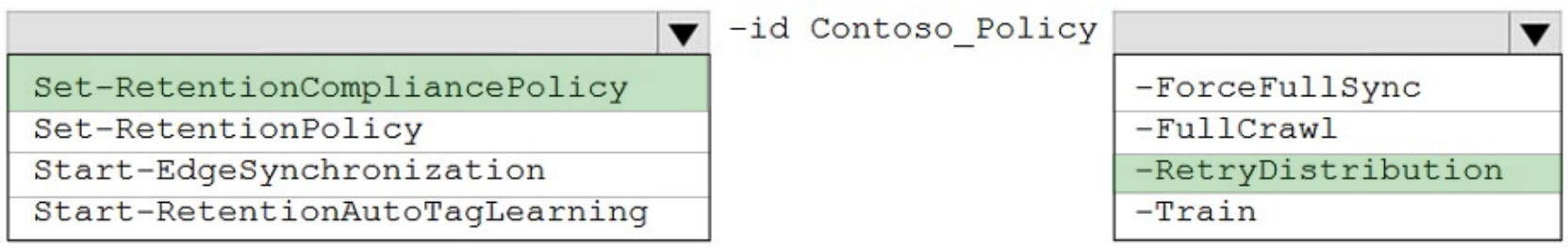
Hot Area:

Answer Area



Correct Answer:

Answer Area



Reference:

https://docs.microsoft.com/en-us/powershell/module/exchange/set-retentioncompliancepolicy?view=exchange-ps

jaycn67 Highly Voted 2 years, 4 months ago

Answer is correct, https://docs.microsoft.com/en-us/microsoft-365/compliance/ediscovery-troubleshooting-common-issues?view=o365-worldwide#resolution-8

upvoted 6 times

wooyourdaddy Most Recent 9 months, 1 week ago

Set-RetentionCompliancePolicy and -RetryDistribution are correct. This use case, with the command to fix it are defined here:

https://learn.microsoft.com/en-us/microsoft-365/compliance/apply-retention-labels-automatically?view=o365-worldwide#how-long-it-takes-for-retention-labels-to-take-effect

upvoted 2 times

Pravda 1 year, 10 months ago

On exam 1/20/2022

upvoted 2 times

Eltooth 2 years, 4 months ago

Answer is correct.

upvoted 2 times

Question #25 *Topic 3*

HOTSPOT -

You have a Microsoft 365 tenant.

A retention hold is applied to all the mailboxes in Microsoft Exchange Online.

A user named User1 leaves your company, and the account of User1 is deleted from Azure Active Directory (Azure AD).

You need to create a new user named User2 and provide User2 with access to the mailbox of User1.

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:

Answer Area

```
$InactiveMailbox = Get-Mailbox -InactiveMailboxOnly -Identity <distinguished name>
```

[ ]	[ ]	
New-Mailbox	-InactiveMailbox	$InactiveMailbox.DistinguishedName
New-MailboxRestoreRequest	-LitigationHoldEnabled	
Restore-RecoverableItems	-RetentionHoldEnabled	
Set-Mailbox	-SourceMailbox	

```
-Name User2 -DisplayName User2 -MicrosoftOnlineServicesID user2@contoso.com
-Password (ConvertTo-SecureString -String 'RdFGFfhjjhgff$^^7' -AsPlainText -Force)
-ResetPasswordOnNextLogon $true
```

Correct Answer:

Answer Area

```
$InactiveMailbox = Get-Mailbox -InactiveMailboxOnly -Identity <distinguished name>
```

[ ]	[ ]	
New-Mailbox	-InactiveMailbox	$InactiveMailbox.DistinguishedName
New-MailboxRestoreRequest	-LitigationHoldEnabled	
Restore-RecoverableItems	-RetentionHoldEnabled	
Set-Mailbox	-SourceMailbox	

```
-Name User2 -DisplayName User2 -MicrosoftOnlineServicesID user2@contoso.com
-Password (ConvertTo-SecureString -String 'RdFGFfhjjhgff$^^7' -AsPlainText -Force)
-ResetPasswordOnNextLogon $true
```

Reference:

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

klosedotorg83 Highly Voted 2 years, 1 month ago

Correct

upvoted 6 times

Pravda Most Recent 1 year, 10 months ago

On exam 1/20/2022

upvoted 2 times

Eltooth 2 years, 4 months ago

Answer is correct.
https://docs.microsoft.com/en-us/microsoft-365/compliance/recover-an-inactive-mailbox?view=o365-worldwide#recover-inactive-mailboxes

upvoted 3 times

Question #26 *Topic 3*

Your company manufactures parts that are each assigned a unique 12-character alphanumeric serial number. Emails between the company and its customers reference the serial number.
You need to ensure that only Microsoft Exchange Online emails containing the serial numbers are retained for five years.
Which three objects should you create? Each correct answer presents part of the solution.
NOTE: Each correct selection is worth one point.

A. a sensitivity label

B. a retention policy

C. an auto-labeling policy

D. a trainable classifier

E. a sensitive info type

F. a retention label

G. a data loss prevention (DLP) policy

Correct Answer: *CEF*
C: One of the most powerful features of retention labels is the ability to apply them automatically to content that matches specified conditions.
F: You can apply retention labels to content automatically when that content contains:
- Specific types of sensitive information
- Specific keywords or searchable properties that match a query you create
- A match for trainable classifiers

E: Sensitive information types are pattern-based classifiers. They detect sensitive information like social security, credit card, or bank account numbers to identify sensitive items. Custom sensitive information types use regular expressions, keywords, and keyword dictionaries.
Reference:
https://docs.microsoft.com/en-us/microsoft-365/compliance/sensitive-information-type-learn-about?view=o365-worldwide
https://docs.microsoft.com/en-us/microsoft-365/compliance/apply-sensitivity-label-automatically?view=o365-worldwide
https://docs.microsoft.com/en-us/microsoft-365/compliance/retention?view=o365-worldwide

batabata Highly Voted 1 year, 11 months ago
Answer is correct
upvoted 5 times

xswe Most Recent 7 months, 3 weeks ago
Detect the unique 12-character serial number = Sensitive info type
Retain for 5 years = Retention label
Automatically retain = Auto labeling policy
upvoted 3 times

Rockalm 10 months, 4 weeks ago
Correct. Tried with a DLP rule, but you're not able to apply a label to the email. Aoto-apply rule works.
upvoted 4 times

Question #27 *Topic 3*

You plan to import a file plan to the Microsoft 365 compliance center.
Which object type can you create by importing a records management file plan?

A. retention label policies

B. sensitive info types

C. sensitivity labels

D. retention labels

Correct Answer: *D*
File plan in Records management allows you to bulk-create retention labels by importing the relevant information from a spreadsheet.
Reference:
https://docs.microsoft.com/en-us/microsoft-365/compliance/file-plan-manager?view=o365-worldwide

xswe 7 months, 3 weeks ago
Record management file plan is helpful when you want to import already created or planned retention labels, you can easily import it via the CSV file available in Purview
upvoted 2 times

Pravda 1 year, 10 months ago
On exam 1/20/2022
upvoted 2 times

ankilo2011 1 year, 11 months ago
Correct Answer: D
upvoted 2 times

Duncan 2 years ago
D; retention labels
See https://docs.microsoft.com/en-us/microsoft-365/compliance/file-plan-manager?view=o365-worldwide#import-retention-labels-into-your-file-plan
upvoted 4 times

HOTSPOT -

You have a Microsoft 365 tenant that uses a domain named contoso.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

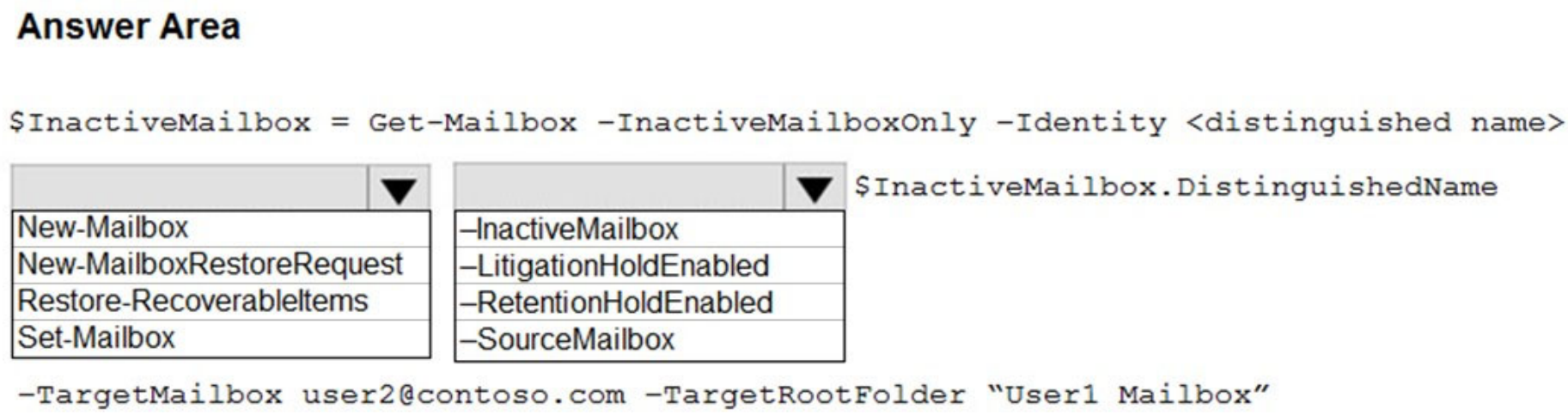
Directory (Azure AD).

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

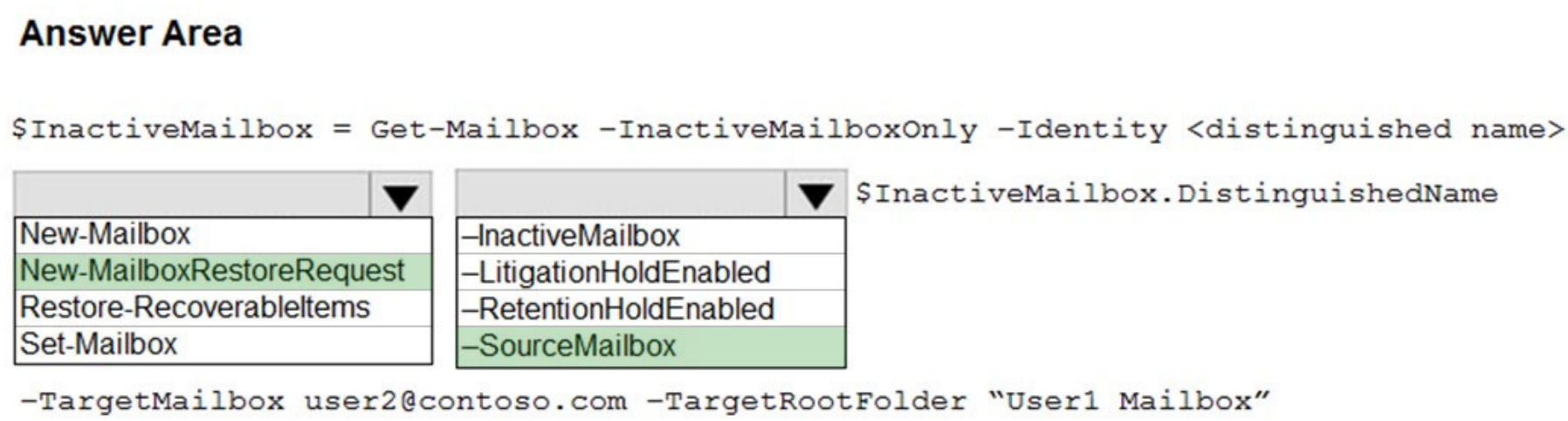
How should you complete the PowerShell command? To answer, select the appropriate options in the answer area.

NOTE: Each correct selection is worth one point.

Hot Area:



Correct Answer:



References:

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

wooyourdaddy 1 year, 5 months ago

I wrote the exam today, this question was on it, I choose the provided answers, scored 890!

upvoted 3 times

girikedar 1 year, 11 months ago

The answer is correct

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

upvoted 3 times

klosedotorg83 2 years, 1 month ago

Correct

upvoted 2 times

Question #29 *Topic 3*

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 files 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

Duncan Highly Voted 2 years ago
D; retention label policy of type auto-apply
See https://docs.microsoft.com/en-us/microsoft-365/compliance/apply-retention-labels-automatically?view=o365-worldwide
upvoted 6 times

xswe Most Recent 7 months, 3 weeks ago
A retention label policy will make sure that the documents with credit card numbers are retained for 7 years since you can take advantage of Sensitive info types or trainable classifiers
upvoted 1 times

Pravda 1 year, 10 months ago
On exam 1/20/2022
upvoted 1 times

girikedar 1 year, 11 months ago
A retention label policy of type auto-apply is the correct. Because we can create auto apply Policy based on sensitive info type of credit card number
upvoted 2 times

HOTSPOT
-

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

For Site1, users are assigned the roles shown in the following table.

Name	Role
User1	Owner
User2	Member

You publish retention labels to Site1 as shown in the following table.

Name	Retention period	During the retention period
Retention1	5 years	Mark items as a record
Retention2	5 years	Mark items as regulatory record

You have the files shown in the following table.

Name	Applied retention label
File1	Retention1
File2	Retention2

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	Yes	No
User1 can delete File2.	○	○
User2 can rename File1.	○	○
User1 can apply Retention2 to File1.	○	○

Answer Area

Correct Answer:

Statements	Yes	No
User1 can delete File2.	○	◉
User2 can rename File1.	◉	○
User1 can apply Retention2 to File1.	◉	○

Gesbie 3 months, 3 weeks ago
was on Exam August 9, 2023
upvoted 1 times

xswe 7 months, 3 weeks ago
Regulatory records is the most restrictive record and then comes "record".

User1 wont be able to delete File2 since its marked as regulatory record
User2 can rename File1 since its allowed if its marked as a record
User1 will be able to add retention 2 to File1 since File1 is only marked as a record
upvoted 4 times

wooyourdaddy 9 months, 1 week ago
Answers are correct and can be verified in the Action table at the following link:

https://learn.microsoft.com/en-us/microsoft-365/compliance/records-management?view=o365-worldwide#compare-restrictions-for-what-actions-are-allowed-or-blocked
upvoted 1 times

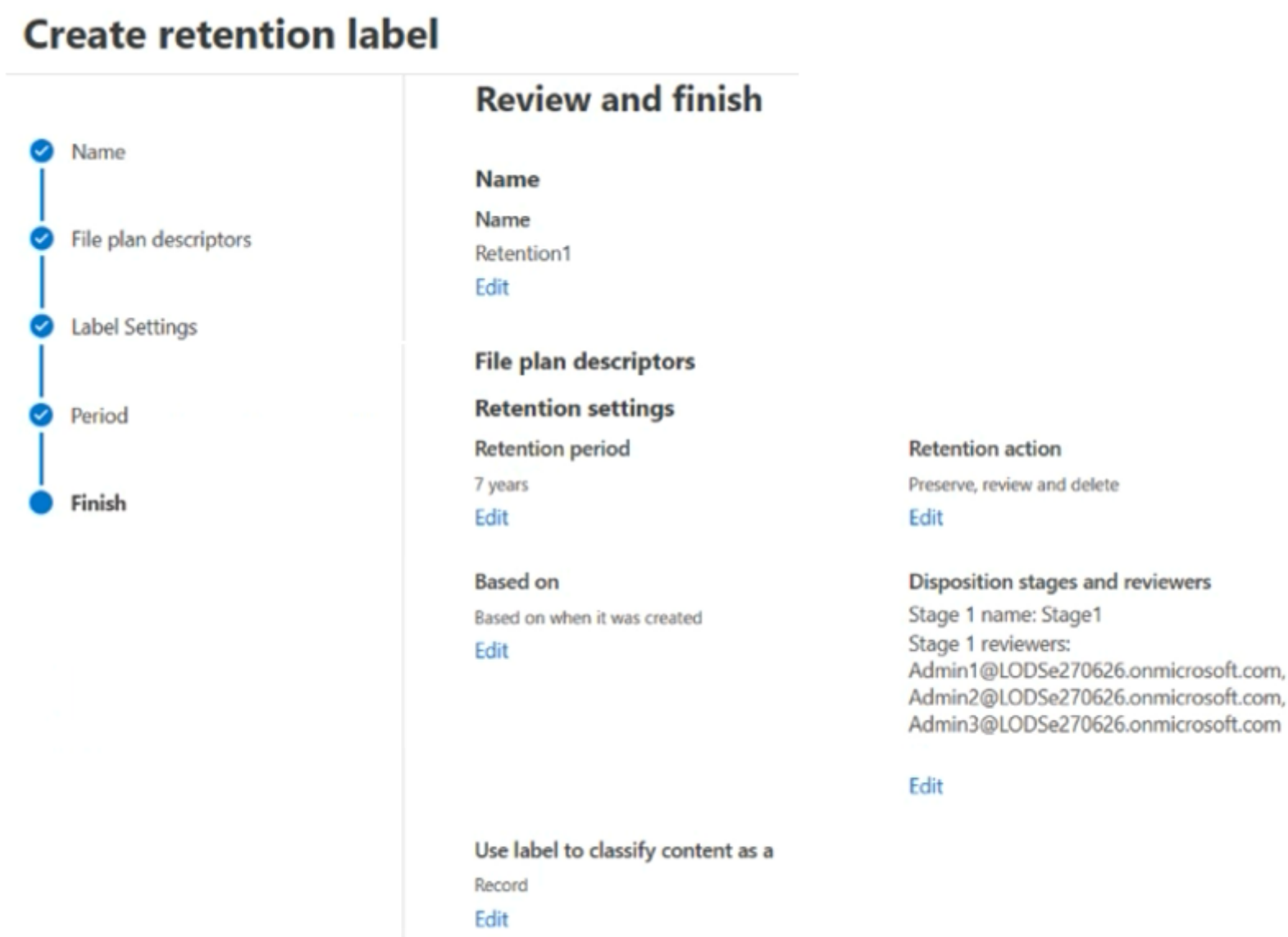
See_Es 10 months, 1 week ago
Correct.
upvoted 2 times

See_Es 10 months, 1 week ago
https://learn.microsoft.com/en-us/microsoft-365/compliance/records-management?view=o365-worldwide
upvoted 3 times

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

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

You create the retention label shown in the following exhibit.



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*

izgi43 3 weeks ago
on exam thu nov 9
upvoted 1 times

Brigg5 4 months ago
The stage one reviewer section lists: admin1, admin2, and admin3. I'm going with 'F'
upvoted 2 times

xswe 7 months, 3 weeks ago

Disposition review can only performed members of Disposition Management Role, by default both Compliance Administrator och Compliance Data Administrator have access to this but NOT GA.
Record management can also perform these reviews.
upvoted 1 times

See_Es 10 months, 1 week ago

So agreed with answer 'E' .... Global administrator does not have recordsmanagement permissions by default.
upvoted 2 times

See_Es 10 months, 1 week ago

Agreed. https://learn.microsoft.com/en-us/microsoft-365/compliance/disposition?view=o365-worldwide
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.

Records management is part of the compliance administrator roles
https://learn.microsoft.com/en-us/microsoft-365/security/office-365-security/scc-permissions?view=o365-worldwide
upvoted 3 times

Question #32 *Topic 3*

You have a Microsoft 365 E5 subscription.

You need to create static retention policies for the following locations:

- Teams chats
- Exchange email
- SharePoint sites
- Microsoft 365 Groups
- Teams channel messages

What is the minimum number of retention policies required?

A. 1

B. 2

C. 3

D. 4

E. 5

Correct Answer: *E*

NoOne24 3 months, 2 weeks ago

Selected Answer: B

is B you need minimum 2

upvoted 1 times

xswe 7 months, 3 weeks ago

We need 2 policies since we are going to retain data in Teams and more location, Teams cant be configured in a policy together with other locations choosed.
Try this out!

upvoted 3 times

wooyourdaddy 9 months, 1 week ago

This link:

https://learn.microsoft.com/en-us/microsoft-365/compliance/create-retention-policies?view=o365-worldwide&tabs=teams-retention#create-and-configure-a-retention-policy

has the following statement:

If you select the Teams or Yammer locations when you create a retention policy, the other locations are automatically excluded. This means that the instructions to follow depend on whether you need to include the Teams or Yammer locations.

So based on that, you would need 2 at minimum.

upvoted 2 times

mmexams 10 months, 1 week ago

Selected Answer: B

Agreed, Teams policies deselect when you select the others.

upvoted 4 times

See_Es 10 months, 1 week ago

Selected Answer: B

Should be 'B'...2 policies. 1 for Exchange mail, Sharepoint Sites and Microsoft 365 Groups. And 1 for teams chats and teams channel messages.

upvoted 4 times

Question #33 *Topic 3*

You have a Microsoft 365 tenant that uses records management.

You use a retention label to mark legal files stored in a Microsoft SharePoint Online document library as regulatory records.

What can you do to the legal files?

A. Remove the retention label of the files.

B. Edit the content of the files.

C. Move the files to a different folder within the document library.

D. Change the retention label of the files.

Correct Answer: *C*

Gesbie 3 months, 3 weeks ago
was on Exam August 9, 2023
upvoted 1 times

xswe 7 months, 3 weeks ago
Move the files to a different folder with in the container is one of the few things you can do to documents marked as regulatory records
upvoted 1 times

wooyourdaddy 9 months, 1 week ago
Chart summarizing options is available here:

https://learn.microsoft.com/en-us/microsoft-365/compliance/records-management?view=o365-worldwide#compare-restrictions-for-what-actions-are-allowed-or-blocked
upvoted 1 times

See_Es 10 months, 1 week ago
Selected Answer: C
Correct.
upvoted 2 times

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.

Answer 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:

Answer 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.	○	○

xswe 7 months, 3 weeks ago

Yes, since User1 is a included in both Retention1 and Retention2
No, User2 is not included in Retention1
Yes, since the user is included in Retention2

upvoted 1 times

Chris7910 9 months, 1 week ago

Why is second one no?

upvoted 1 times

wooyourdaddy 9 months, 1 week ago

The Retention1 label locations only allow user 1 to see the label in his his mailbox, while group 2 can only see it as part of an M365 group.

upvoted 2 times

See_Es 10 months, 1 week ago

I agree with the given answer.

upvoted 2 times

Question #35 *Topic 3*

HOTSPOT
-

While creating a retention label, you discover that the Mark items as a regulatory record option is unavailable.

You need to ensure that the options are available when you create retention labels 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 [ ▼ ]
```

- Az
- ExchangeOnlineManagement
- Microsoft.Online.SharePoint.PowerShell
- MicrosoftTeams

```
[ ▼ ] -Credential $UserCredential
```

- Connect-AadrmService
- Connect-AzureAD
- Connect-AzAccount
- Connect-IPPSSession

```
[ ▼ ] -Enabled $true
```

- Enable-ComplianceTagStorage
- New-ComplianceTag
- Set-RegulatoryComplianceUI
- Set-RetentionCompliancePolicy

Correct Answer:

Answer Area

```
$UserCredential = Get-Credential
Import-Module [ ▼ ]
```

- Az
- ExchangeOnlineManagement
- Microsoft.Online.SharePoint.PowerShell
- MicrosoftTeams

```
[ ▼ ] -Credential $UserCredential
```

- Connect-AadrmService
- Connect-AzureAD
- Connect-AzAccount
- Connect-IPPSSession

```
[ ▼ ] -Enabled $true
```

- Enable-ComplianceTagStorage
- New-ComplianceTag
- Set-RegulatoryComplianceUI
- Set-RetentionCompliancePolicy

izgi43 3 weeks ago
in exam thu nov 9

upvoted 1 times

wooyourdaddy 9 months, 1 week ago

Answer can be confirmed in these links:

https://learn.microsoft.com/en-us/powershell/module/exchange/connect-ippssession?view=exchange-ps

Where the Prerequisites for the Exchange Online PowerShell module hyperlink mentions the ExchangeOnlineManagement module being needed for the Connect-IPPSSession command.

And this link:

https://learn.microsoft.com/en-us/powershell/module/exchange/set-regulatorycomplianceui?view=exchange-ps

Which states:

Use the Set-RegulatoryComplianceUI cmdlet to display the UI option in retention label settings to mark content as a regulatory record.

upvoted 4 times

See_Es 10 months, 1 week ago

I agree with the given answer.

upvoted 3 times

Question #36 *Topic 3*

You have a Microsoft 365 E5 subscription that contains a Microsoft SharePoint Online site named Site1.

You need to implement a records management solution for the files stored on Site1. The solution must meet the following requirements:

• The files must be retained for seven years.
• Files older than seven years must be deleted automatically.

What should you use to manage the files?

A. a label policy

B. an adaptive scope

C. a file plan

D. a disposition review

Correct Answer: *C*

Domza 2 weeks, 3 days ago

Looks good~

upvoted 1 times

xswe 7 months, 3 weeks ago

File plan is used for use cases like this to manage retention labels, this is where you implement retention labels

upvoted 1 times

kvdvliert 8 months ago

Selected Answer: C

You can use File Plan to manage retention labels

https://learn.microsoft.com/en-us/microsoft-365/compliance/file-plan-manager?view=o365-worldwide

upvoted 1 times

See_Es 10 months, 1 week ago

Selected Answer: C

File plan is correct

upvoted 2 times

Question #37 *Topic 3*

You have a Microsoft 365 E5 tenant that contains a Microsoft SharePoint Online document library named Library1.

You need to declare a collection of files that are stored in Library1 as regulatory records.

What should you use?

A. a sensitivity label policy

B. a retention label policy

C. a retention policy

D. data loss prevention (DLP) policy

Correct Answer: *B*

heshmat2022 1 month ago

Retention labels help you retain what you need and delete what you don't at the item level (document or email). They're also used to declare an item as a record as part of a records management solution for your Microsoft 365 data.

Making retention labels available to people in your organization so that they can classify content is a two-step process:

Create the retention labels.

Publish the retention labels by using a retention label policy.

upvoted 1 times

js124 8 months ago

Answer is correct.
https://learn.microsoft.com/en-us/microsoft-365/compliance/create-apply-retention-labels?view=o365-worldwide

upvoted 1 times

Question #38 *Topic 3*

You have a Microsoft 365 E5 subscription that contains a Microsoft SharePoint Online site named Site1. Site1 contains a file named File1.

You have a retention policy named Retention1 that has the following settings:

• Retention items for a specific period
o Retention period: 5 years
o At the end of the retention period: Delete items automatically

Retention1 is applied to Site1.

You need to ensure that File1 is deleted automatically after seven years. The solution must NOT affect the retention of other files on Site1.

What should you do first?

A. Move File1 to a new folder and configure the access control list (ACL) entries for File1.

B. Create a new retention policy.

C. Create and publish a new retention label.

D. Move File1 to a new folder and list the excluded locations for Retention1.

Correct Answer: *C*

Romeokton 5 days, 13 hours ago

Selected Answer: D

For this question I was thinking about the word "first" regarding what should you do. I was thinking that the emergency is to keep the file first, so I would exclude it from the scope of the other policy, i.e. answer D. I am not sure about it however.

upvoted 1 times

izgi43 3 weeks ago

in exam thu nov 9

upvoted 1 times

xswe 7 months, 3 weeks ago

Create and publish a new retention label is a solution to this since we want to create a new rule for one file named FIle1 in Site1, this file will then get retained for 7 years instead of 5 yearswwwwwwwwwwwww

upvoted 1 times

CharlieGolf 8 months, 1 week ago

Selected Answer: C

Correct. Retention labels are for exceptions like this.

upvoted 1 times

Question #39 *Topic 3*

You have a Microsoft 365 E5 tenant that contains a Microsoft SharePoint Online site named Site1 and a user named User1. The tenant has auditing enabled.

You need to ensure that User1 can perform disposition reviews. The solution must use the principle of the least privilege.

What should you do?

A. Assign User1 the Compliance Data Administrator role.

B. Add User1 to the Records Management role group.

C. Assign User1 the Data Investigator role.

D. Add User1 to the Content Explorer Content Viewer role group.

Correct Answer: *B*

HDEIWDEOW 3 months, 2 weeks ago

Got this question on exam on 17th August

upvoted 1 times

xswe 7 months, 3 weeks ago

To be able to perform Disposition reviews you need to be a part of the Records Management role group or Disposition management role.

upvoted 3 times

js124 8 months ago

Answer is correct.
https://learn.microsoft.com/en-us/microsoft-365/compliance/disposition?view=o365-worldwide

upvoted 1 times

Question #40 *Topic 3*

You have a Microsoft 365 E5 subscription that contains a trainable classifier named Trainable1.

You plan to create the items shown in the following table.

Name	Type
Label1	Sensitivity label
Label2	Retention label
Policy1	Retention label policy
DLP1	Data loss prevention (DLP) policy

Which items can use Trainable1?

A. Label2 only

B. Label1 and Label2 only

C. Label1 and Policy1 only

D. Label2, Policy1, and DLP1 only

Correct Answer: *C*

HDEIWDEOW 3 months, 2 weeks ago
Got this question on exam on 17th August
upvoted 1 times

Davidf 3 months, 2 weeks ago
Selected Answer: D
https://learn.microsoft.com/en-us/microsoft-365/compliance/classifier-learn-about?view=o365-worldwide

Where you can use classifiers
Classifiers are available to use as a condition for:

Office auto-labeling with sensitivity labels
Auto-apply retention label policy based on a condition
Communication compliance
Sensitivity labels can use classifiers as conditions, see Apply a sensitivity label to content automatically.
Data loss prevention
upvoted 2 times

Gesbie 3 months, 3 weeks ago
was on Exam August 9, 2023
upvoted 1 times

ivzdf 5 months, 2 weeks ago
https://learn.microsoft.com/en-us/microsoft-365/compliance/classifier-learn-about?view=o365-worldwide

Where you can use classifiers
Classifiers are available to use as a condition for:

Office auto-labeling with sensitivity labels
Auto-apply retention label policy based on a condition
Communication compliance
Sensitivity labels can use classifiers as conditions, see Apply a sensitivity label to content automatically.
Data loss prevention
upvoted 2 times

pokus00132 7 months, 3 weeks ago
Selected Answer: C
C is right, but DLP can also use Trainable classifiers when Location is restricted to Exchange email, Sharepoint sites, OneDrive Accounts.
upvoted 2 times

xswe 7 months, 3 weeks ago
Trainable classsifers can only bve used when creating sensitivty labels and Retention label policies
upvoted 1 times

CharlieGolf 8 months, 1 week ago

Selected Answer: C

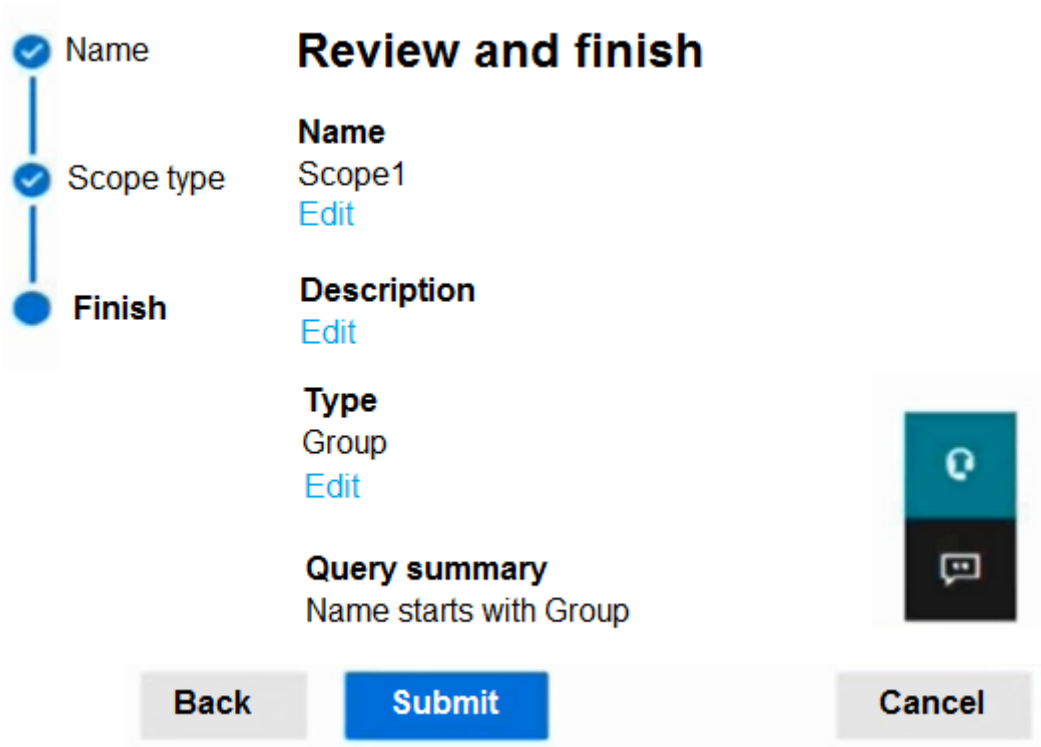
Agreed. https://learn.microsoft.com/en-us/microsoft-365/compliance/classifier-get-started-with?view=o365-worldwide

upvoted 1 times

HOTSPOT
-

You have a Microsoft 365 E5 subscription.

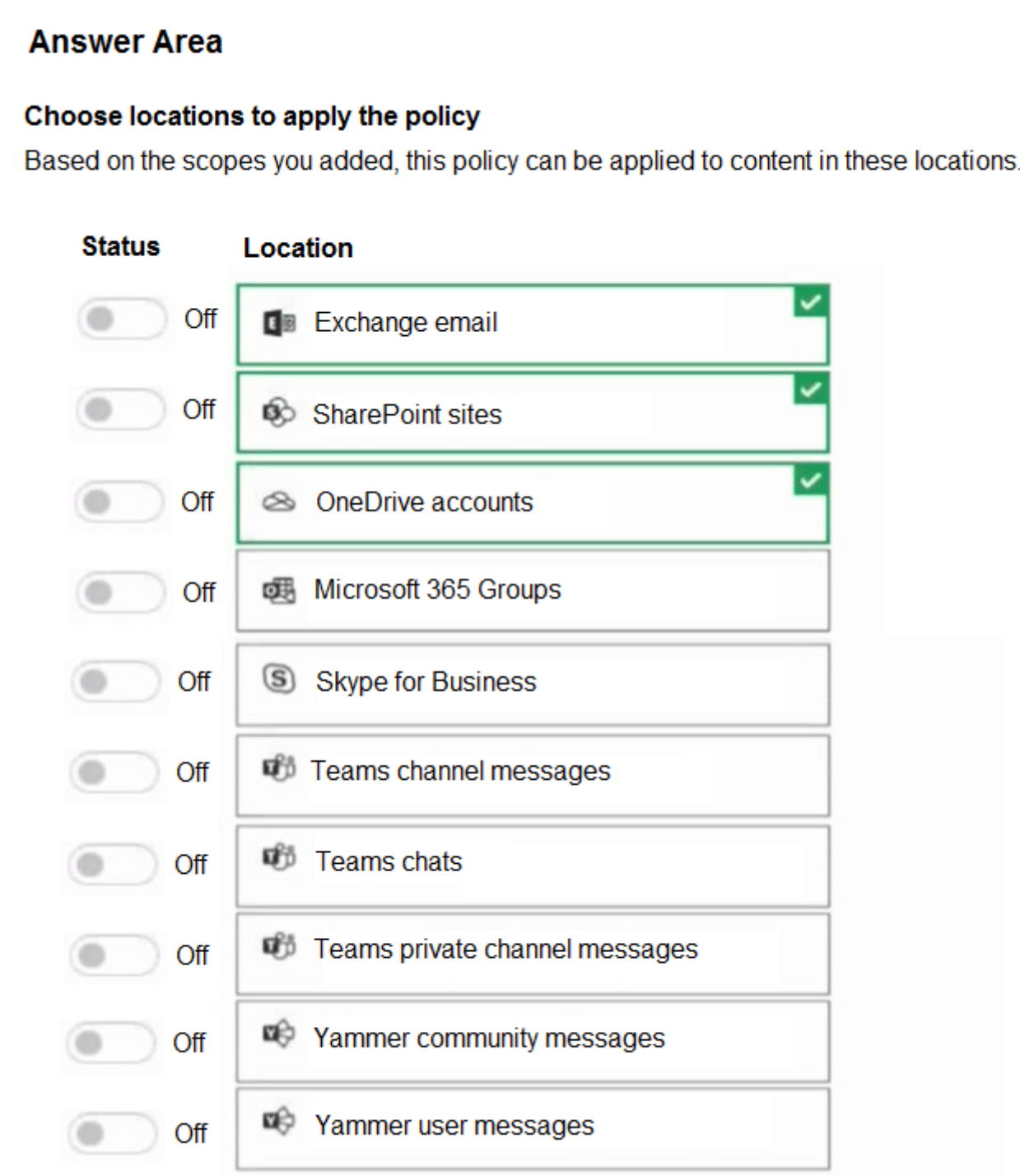
You create an adaptive scope named Scope1 as shown in the following exhibit.



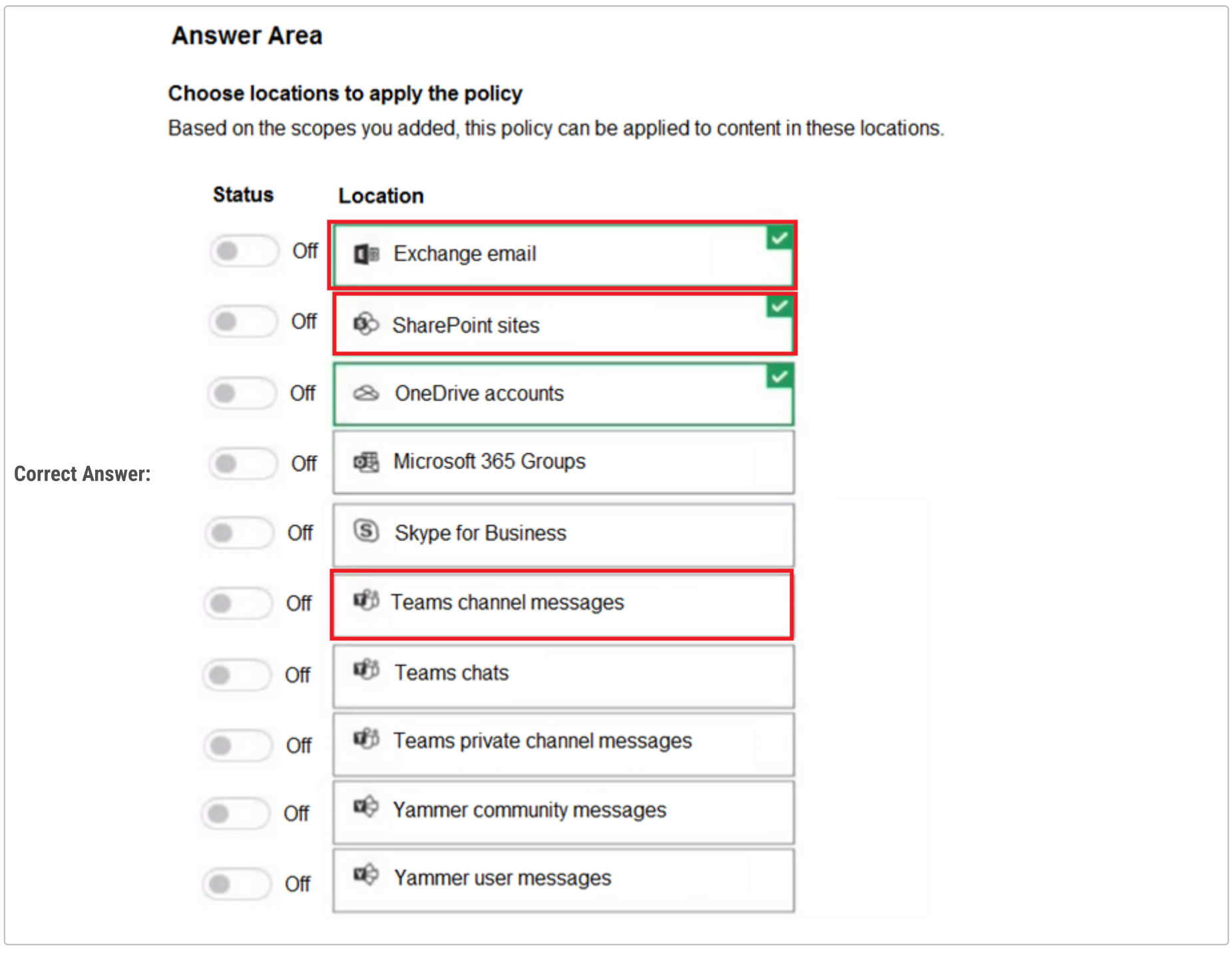
You create a retention policy named Policy1 that includes Scope1.

To which three locations can you apply Policy1? To answer, select the appropriate locations in the answer area.

NOTE: Each correct selection is worth one point.



Correct Answer:



Romeokton 5 days, 13 hours ago

So, given the comments, the underlined answers are not correct.

upvoted 1 times

Sango 3 months, 1 week ago

Using Group as a Scope there are only three options: Microsoft 365 Group mailboxes & sites, Teams channel messages and Yammer Community Messages.

upvoted 2 times

HDEIWDEOW 3 months, 2 weeks ago

Got this question on exam on 17th August

upvoted 1 times

xswe 7 months, 3 weeks ago

When you are configuring this by yourself in your tenant you will see that in the scope you can only add
Teams channel Message,
Yammer community messages,
M365 group mailboxses & sites

upvoted 3 times

pokus00132 7 months, 3 weeks ago

Right, If adaptiv scope is type "group" you have only following options:
Teams channel Message,
Yammer community messages,
M365 group mailboxses & sites

If adaptive scope type is "User":
Exchange mailboxes
OneDrive accounts
OR (cann't be together)
Teams chats
Teams private channel messages
Yammer user messages

If adaptive scope type is "Site":
SharePoint sites

upvoted 4 times

jacul 8 months ago

https://learn.microsoft.com/en-us/microsoft-365/compliance/retention?view=o365-worldwide

Microsoft 365 Groups - applies to:
- Microsoft 365 Group mailboxes & sites
- Teams channel messages (standard and shared)
- Yammer community messages

upvoted 2 times

Question #1 *Topic 4*

You have a Microsoft 365 tenant that has a retention label policy.

You need to configure the policy to meet the following requirements:

• Prevent the disabling or deletion of the policy.
• Ensure that new labels can be added.
• Prevent the removal of labels.

What should you do?

A. Import a file plan.

B. Enable insider risk management.

C. Enable the regulatory record option.

D. Create a preservation lock.

Correct Answer: *D*

martutene 4 weeks ago
Correct
upvoted 1 times

Question #2 *Topic 4*

You have a Microsoft 365 E5 subscription.

You create a role group named Role1.

You need to add a role to Role1 that will enable group members to view the metadata of records that were tagged for deletion automatically at the end of the records' retention period. The solution must use the principle of least privilege.

Which role should you add?

A. Review

B. View-Only Retention Management

C. Retention Management

D. Disposition Management

E. Record Management

Correct Answer: *E*

heshmat2022 1 week, 3 days ago

https://www.pass4success.com/microsoft/discussions/exam-sc-400-topic-4-question-66-discussion

upvoted 1 times

Softeng 2 weeks, 1 day ago

b

View-Only Retention Management role to the Role1 group. This role allows users to view retention policies, but not modify them, and view the metadata of records that were tagged for deletion automatically at the end of the records' retention period

upvoted 1 times

martutene 4 weeks, 1 day ago

Selected Answer: D

Should be D

To grant users just the permissions they need for disposition reviews without granting them permissions to view and configure other features for retention and records management, create a custom role group (for example, named "Disposition Reviewers") and grant this group the Disposition Management role.

https://learn.microsoft.com/en-us/purview/disposition

upvoted 1 times

Question #3 *Topic 4*

You have a Microsoft 365 E5 subscription that contains a Microsoft SharePoint Online site named Site1.

You need to implement Microsoft Purview data lifecycle management.

What should you create first?

A. a sensitivity label policy

B. a retention label

C. a data loss prevention (DLP) policy

D. an auto-labeling policy

Correct Answer: *B*

martutene 4 weeks ago

Correct

upvoted 1 times

Question #4 *Topic 4*

You have a Microsoft 365 E5 subscription.

You plan to implement retention policies for Microsoft Teams.

Which item types can be retained?

A. voice memos from the Teams mobile client

B. embedded images

C. code snippets

Correct Answer: *B*

martutene 4 weeks, 1 day ago

Selected Answer: B

Correct

Code snippets, recorded voice memos from the Teams mobile client, thumbnails, announcement images, and reactions from others in the form of emoticons aren't retained when you use retention policies for Teams.

https://learn.microsoft.com/en-us/purview/retention-policies-teams

upvoted 2 times

Domza 2 weeks, 3 days ago

Thanks for the link :)

upvoted 1 times

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

Name	Type	Query
Scope1	Users	`FirstName starts with User`
Scope2	SharePoint Online sites	`SiteTitle starts with Site`

You create the retention policies shown in the following table.

Name	Type	Location
RPolicy1	Adaptive	Scope1
RPolicy2	Adaptive	Scope2
RPolicy3	Static	Microsoft 365 groups

Which retention policies support a preservation lock?

A. RPolicy2 only

B. RPolicy3 only

C. RPolicy1 and RPolicy2 only

D. RPolicy1 and RPolicy3 only

E. RPolicy1, RPolicy2, and RPolicy3

Correct Answer: *B*

martutene 4 weeks, 1 day ago

Selected Answer: B

Currently, adaptive policy scopes don't support Preservation Lock.
https://learn.microsoft.com/en-us/purview/retention-preservation-lock

upvoted 2 times

Domza 2 weeks, 3 days ago

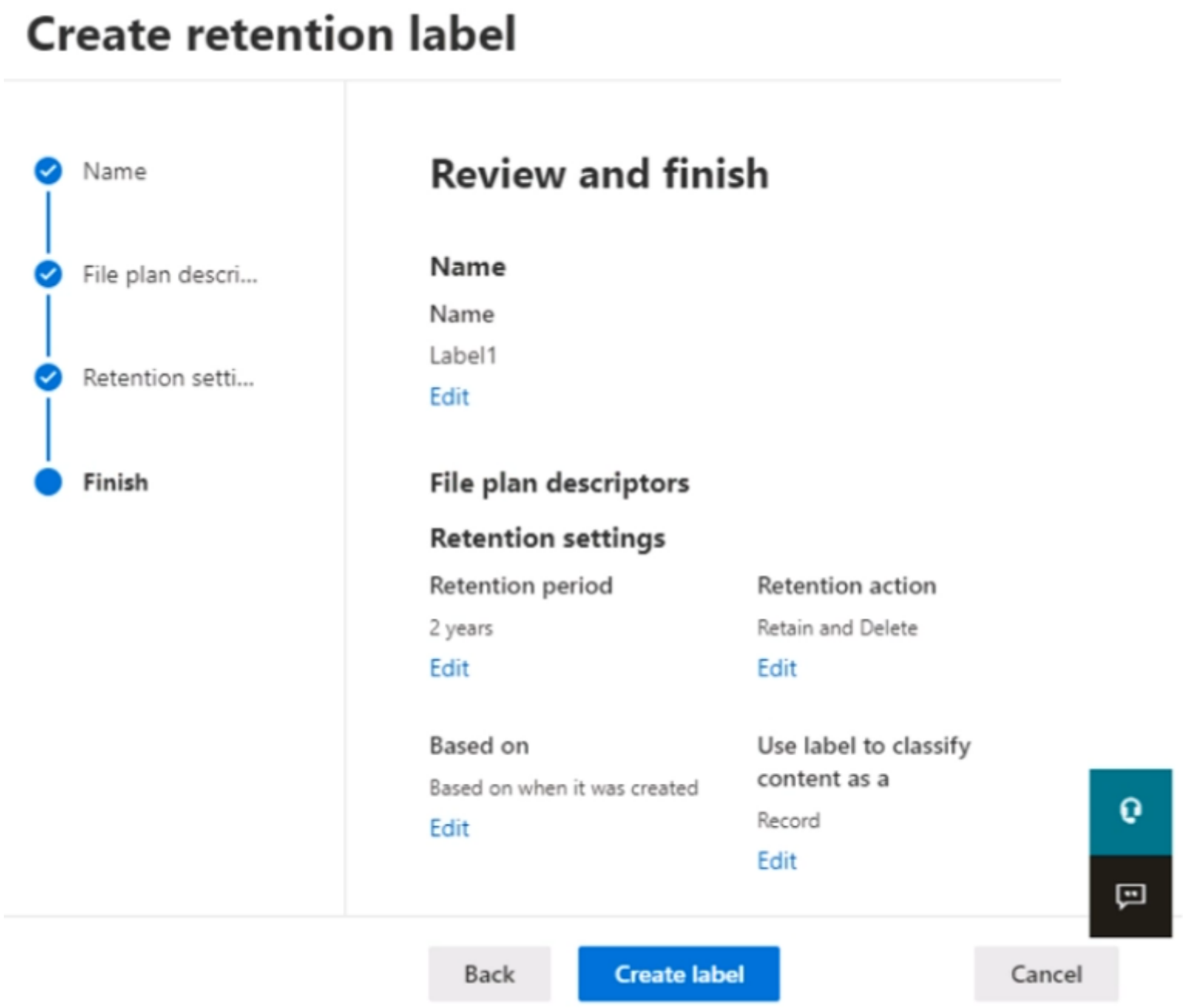
Thx for the link

upvoted 1 times

HOTSPOT
-

You have a Microsoft 365 subscription.

You create a retention label named Label1 as shown in the following exhibit.



You publish Label1 to SharePoint sites.

Use the drop-down menus to select the answer choice that completes each statement based on the information presented in the graphic.

NOTE: Each correct selection is worth one point.

Answer Area

If you create a file in a Microsoft SharePoint library on January 1, 2023, and apply Label1 to the file, you can **[answer choice]**.

- never delete the file
- delete the file before January 1, 2025
- delete the file after January 1, 2025

If you create a file in a Microsoft SharePoint library on March 15, 2023, and apply Label1 to the file, the file will **[answer choice]**.

- always remain in the library
- remain in the library until you delete the file
- be deleted automatically on March 15, 2025

Correct Answer:

Answer Area

If you create a file in a Microsoft SharePoint library on January 1, 2023, and apply Label1 to the file, you can **[answer choice]**.

- never delete the file
- delete the file before January 1, 2025
- delete the file after January 1, 2025

If you create a file in a Microsoft SharePoint library on March 15, 2023, and apply Label1 to the file, the file will **[answer choice]**.

- always remain in the library
- remain in the library until you delete the file
- be deleted automatically on March 15, 2025

Romeokton 5 days, 12 hours ago

I find the answer "Never delete the file" as absolutely wrong. It can be deleted after the retention period expires.

upvoted 1 times

Question #7 *Topic 4*

You have a Microsoft 365 subscription.

You need to ensure that users can apply retention labels to individual documents in their Microsoft SharePoint libraries.

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 a label.

B. From Microsoft Defender for Cloud Apps, create a file policy.

C. From the Microsoft Purview compliance portal, publish a label.

D. From the SharePoint admin center, modify the Site Settings.

E. From the SharePoint admin center, modify the records management settings.

Correct Answer: *BC*

Franc_Coetzee 15 hours, 37 minutes ago

Selected Answer: AC

Answer is A & C

upvoted 1 times

Romeokton 5 days, 12 hours ago

Selected Answer: AC

I don't know why B is suggested here. It doesn't make sense.

upvoted 1 times

Question #8 *Topic 4*

You have a Microsoft 365 E5 subscription that contains two Microsoft SharePoint Online sites named Site1 and Site2.

You plan to configure a retention label named Label1 and apply Label1 to all the files in Site1.

You need to ensure that two years after a file is created in Site1, the file moves automatically to Site2.

How should you configure the Choose what happens after the retention period setting for Label1?

A. Run a Power Automate flow

B. Change the label

C. Deactivate retention settings

D. Start a disposition review

Correct Answer: *A*

Question #9 *Topic 4*

HOTSPOT
-

You have a Microsoft 365 E5 subscription that contains two users named Admin1 and User1, a Microsoft SharePoint Online site named Site1, and a retention label named Retention1.

The role assignments for Site1 are shown in the following table.

Name	Role
Admin1	Owner
User1	Member

Site1 includes a file named File1.

Rentention1 has the following settings:

• Retain items for a specific period: Retention period: 7 years
• During the retention period: Mark items as a record
• At the end of the retention period: Delete items automatically

Rentention1 is published to Site1.

User1 applies Retention1 to File1.

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	Yes	No
User1 can rename File1.	○	○
Admin1 can modify the contents of File1.	○	○
User1 can remove Retention1 from File1.	○	○

Correct Answer:

Answer Area

Statements	Yes	No
User1 can rename File1.	○	☐
Admin1 can modify the contents of File1.	☐	○
User1 can remove Retention1 from File1.	○	☐

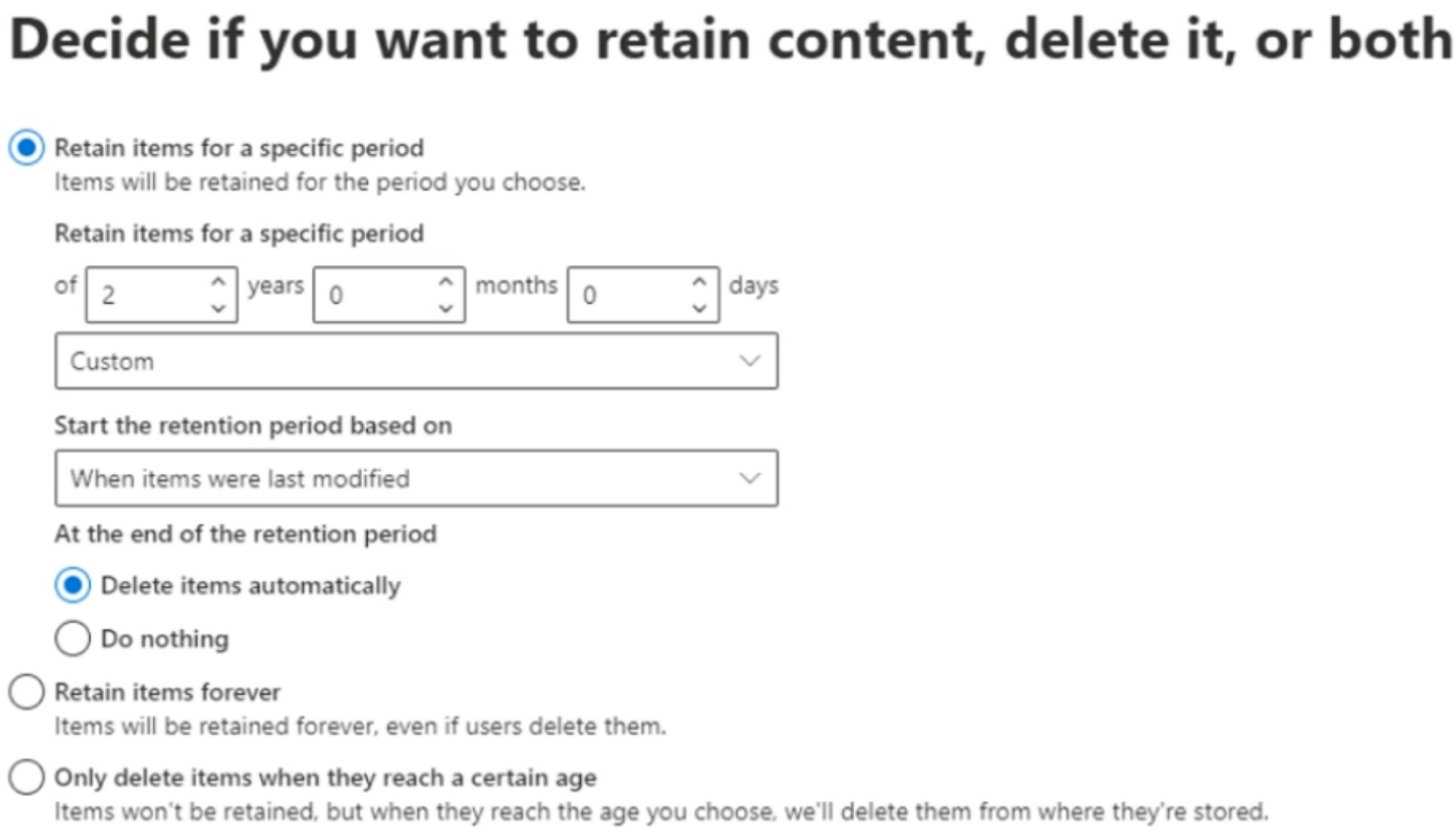
Romeokton 5 days, 12 hours ago
The provided answer does not seem correct. Here is a table that explains: https://learn.microsoft.com/en-us/purview/records-management

User 1 can Edit properties, including rename
Edit contents is allowed only for unlocked records, which is somewhat not specified in the question.
upvoted 1 times

HOTSPOT
-

You have a Microsoft 365 subscription.

You are creating a retention policy named Retention1 as shown in the exhibit. (Click the Exhibit tab.)



You apply Retention1 to SharePoint sites and OneDrive accounts.

Use the drop-down menus to select the answer choice that completes each statement based on the information presented in the graphic.

NOTE: Each correct selection is worth one point.

Answer Area

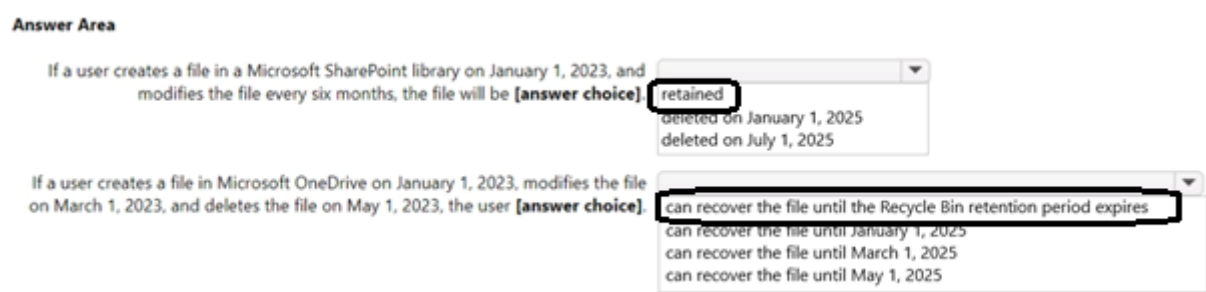
If a user creates a file in a Microsoft SharePoint library on January 1, 2023, and modifies the file every six months, the file will be **[answer choice]**.

- retained
- deleted on January 1, 2025
- deleted on July 1, 2025

If a user creates a file in Microsoft OneDrive on January 1, 2023, modifies the file on March 1, 2023, and deletes the file on May 1, 2023, the user **[answer choice]**.

- can recover the file until the Recycle Bin retention period expires
- can recover the file until January 1, 2025
- can recover the file until March 1, 2025
- can recover the file until May 1, 2025

Correct Answer:



Romeokton 5 days, 12 hours ago
Agreed with the answers.
upvoted 1 times

HOTSPOT
-

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

Name	Team membership
User1	Team1, Team2
User2	Team2

You have the retention policies shown in the following table.

Name	Location	Included	Retain items for	Start retention period	At the end of retention period
Policy1	Microsoft Teams channel messages	All teams	7 years	When items are created	Delete items automatically
	Microsoft Teams chats	User1			
Policy2	Microsoft Teams channel messages	Team1	5 years	When items are created	Delete items automatically
	Microsoft Teams chats	User2			

The users perform the actions shown in the following table.

User	Location	Action
User1	Team1 channel	Edits a message
User2	Private 1:1 chat with User1	Sends a message to User1
User1	Team2 channel	Deletes a message

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	Yes	No
The message edited by User1 will be deleted after five years.	○	○
User1 can see the message sent by User2 for up to seven years.	○	○
The message deleted by User1 will be moved to the SubstrateHolds folder.	○	○

Correct Answer:

Answer Area

Statements	Yes	No
The message edited by User1 will be deleted after five years.	○	○
User1 can see the message sent by User2 for up to seven years.	○	○
The message deleted by User1 will be moved to the SubstrateHolds folder.	○	○

Question #1 *Topic 5*

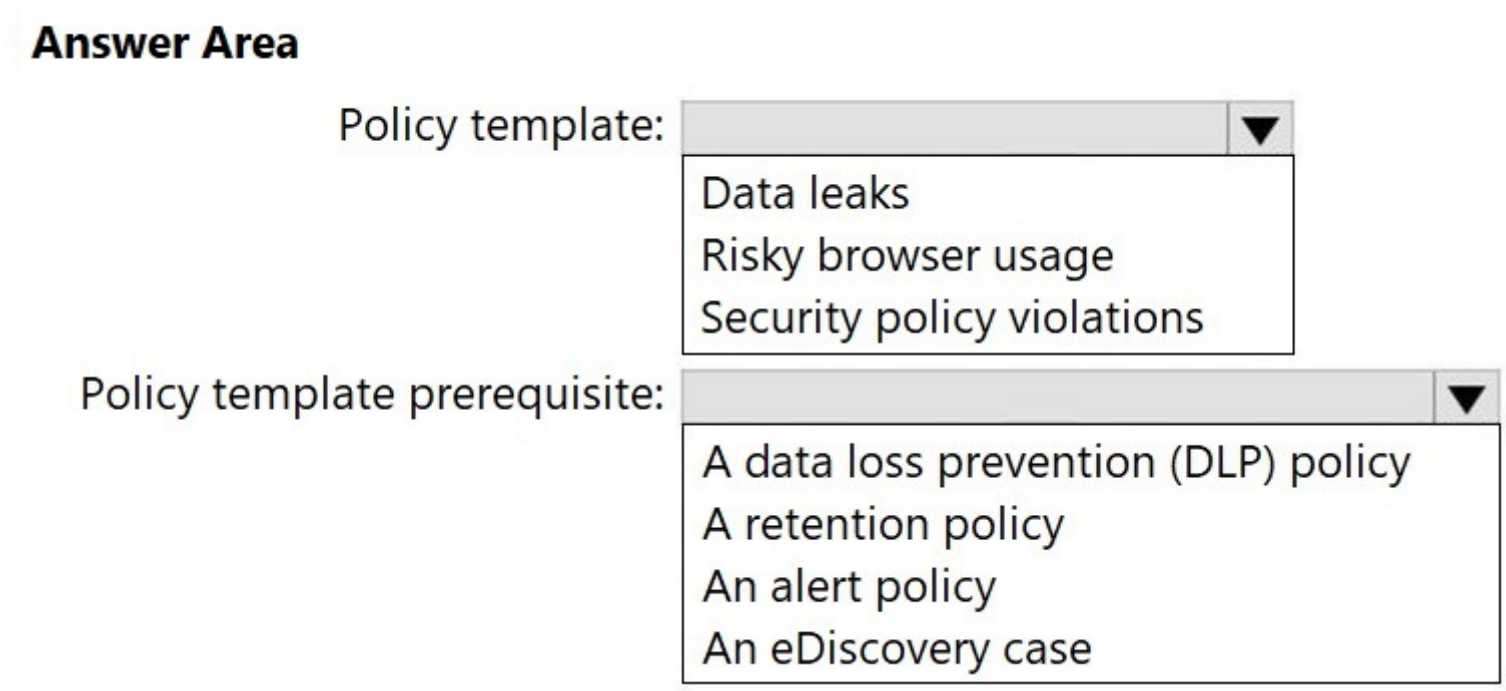
HOTSPOT
-

You have a Microsoft 365 E5 subscription that uses Microsoft Purview.

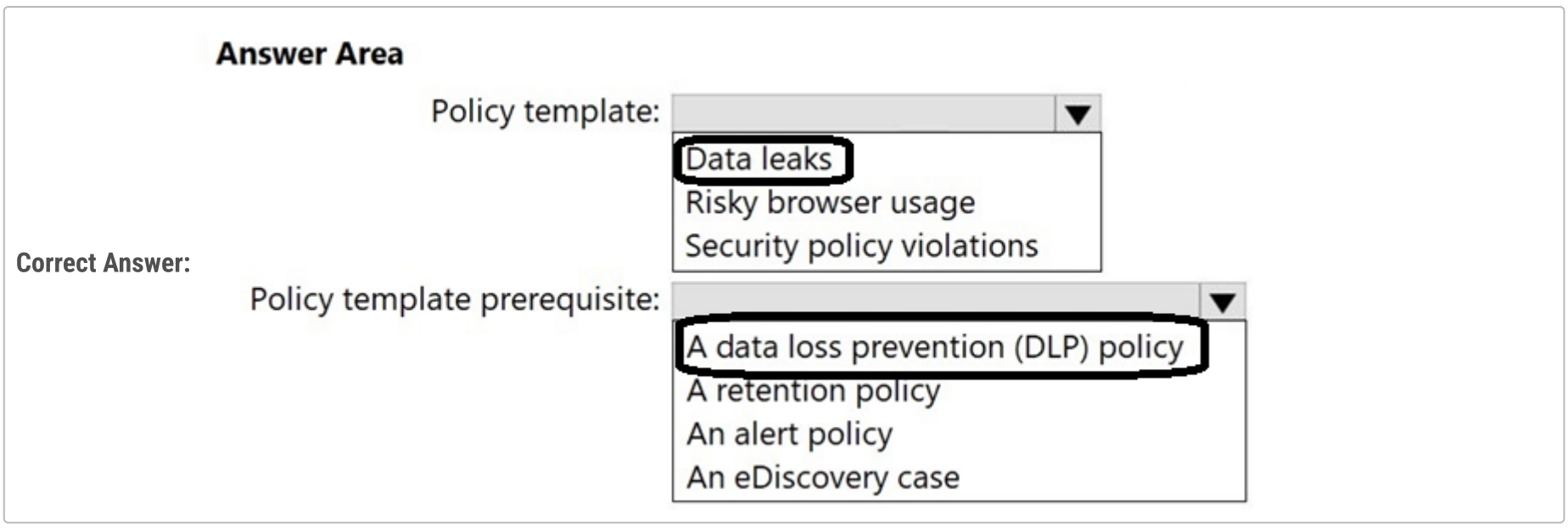
You need to deploy a compliance solution that will detect the accidental oversharing of information outside of an organization. The solution must minimize administrative effort.

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

NOTE: Each correct selection is worth one point.



Correct Answer:



izgi43 3 weeks ago
in exam thu nov 9
upvoted 1 times

Pablosanchez 3 weeks, 2 days ago
Agreed
upvoted 1 times

Question #2 *Topic 5*

HOTSPOT
-

You have a Microsoft 365 E5 subscription.

You are implementing insider risk management.

You need to create an insider risk management notice template and format the message body of the notice template.

How should you configure the template? To answer, select the appropriate options in the answer area.

NOTE: Each correct selection is worth one point.

Answer Area

Use the:
- Microsoft 365 admin center
- Microsoft 365 Defender portal
- Microsoft Entra admin center
- Microsoft Purview compliance portal

Format in:
- HTML
- Markdown
- RTF
- XML

Correct Answer:

Answer Area

Use the:
- Microsoft 365 admin center
- Microsoft 365 Defender portal
- Microsoft Entra admin center
- Microsoft Purview compliance portal

Format in:
- HTML
- Markdown
- RTF
- XML

martutene 4 weeks ago

Correct
https://learn.microsoft.com/en-us/purview/insider-risk-management-notices

upvoted 1 times

Question #3 *Topic 5*

You have a Microsoft 365 E5 subscription that contains a user named User1.

You need to ensure that all email messages that contain attachments are encrypted automatically by using Microsoft Purview Message Encryption.

What should you create?

A. a sensitivity label

B. an information barrier segment

C. a data loss prevention (DLP) policy

D. a mail flow rule

Correct Answer: *D*

Pablosanchez 3 weeks, 2 days ago

agreed

upvoted 1 times

Question #4 *Topic 5*

You have a Microsoft 365 E3 subscription.

You plan to audit all Microsoft Exchange Online user and admin activities.

You need to ensure that all the Exchange audit log records are retained for one year.

What should you do?

A. Modify the record type of the default audit retention policy.

B. Modify the retention period of the default audit retention policy.

C. Create a custom audit retention policy.

D. Assign Microsoft 365 Enterprise E5 licenses to all users.

Correct Answer: *D*

martutene 4 weeks ago

Correct, E3 only allows for 90 days

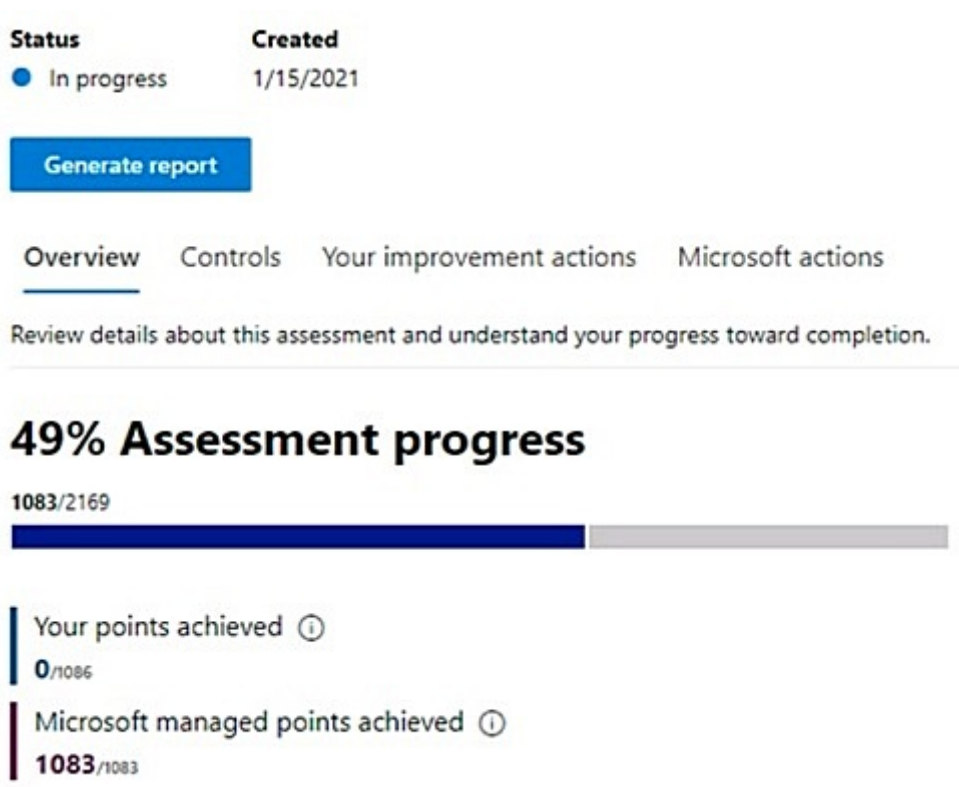
upvoted 3 times

HOTSPOT
-

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

Name	Microsoft 365 role	Role group
Admin1	Global Administrator	*None*
Admin2	Compliance Administrator	*None*
User3	User	Compliance Manager Contributors
User4	User	Compliance Manager Administrators
User5	User	*None*

You create an assessment named Assesment1 as shown in the following exhibit.



Which users can update the title of Assessment1, and which users can add User5 to the Compliance Manager Readers role group? To answer, select the appropriate options in the answer area.

NOTE: Each correct selection is worth one point.

Answer Area

Can update the Assessment1 title: [ ]
- User4 only
- Admin2 and User4 only
- Admin1, Admin2, and User4 only
- Admin1, Admin2, User3, and User4 only

Can add User5 to the Compliance Manager Readers role group: [ ]
- Admin1 only
- Admin1 and Admin2 only
- Admin1 and User4 only
- Admin1, Admin2, and User4 only

Correct Answer:

Answer Area

Can update the Assessment1 title:

- User4 only
- Admin2 and User4 only
- Admin1, Admin2, and User4 only
- Admin1, Admin2, User3, and User4 only

Can add User5 to the Compliance Manager Readers role group:

- Admin1 only
- Admin1 and Admin2 only
- Admin1 and User4 only
- Admin1, Admin2, and User4 only

Romeokton 5 days, 12 hours ago

Here is the link to answers: https://learn.microsoft.com/en-us/purview/compliance-manager-setup#role-types

upvoted 1 times

Question #6 *Topic 5*

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

Name	Role group
Admin1	eDiscovery Manager
Admin2	eDiscoverv Administrator
Admin3	*none*

You have the core eDiscovery cases shown in the following table.

Name	Created by	Members
Case1	Admin2	Admin
Case2	Admin1	Admin1, Admin3

You need to ensure that Admin3 can create holds in Case1 and Case2. The solution must use the principle of least privilege.

To what should you add Admin3?

A. the Global Administrator role

B. the eDiscovery Manager role group

C. the Compliance Manager Contributors role group

D. the eDiscovery Administrator role group

Correct Answer: *D*

phony 1 week, 6 days ago

eDiscovery Administrator role does not exist and eDiscovery Administrator (without role) is a member of the eDiscovery Manager role:

more info:
https://learn.microsoft.com/en-us/microsoft-365/security/office-365-security/scc-permissions?view=o365-worldwide

So I think the answer is B, because you cannot add Admin3 to a eDiscovery Administrator role group

upvoted 1 times

phony 1 week, 6 days ago

when looking deeper I see that within the eDiscovery Manager role you can choose between adding someone to eDiscovery Manager or eDiscovery Administrator. if you want to create a hold you need to be an eDiscovery Administrator (withoud role group). so the answer which fit the best is D.

upvoted 1 times

Domza 2 weeks, 3 days ago

Correct~

upvoted 1 times

HOTSPOT
-

You have a Microsoft 365 subscription that contains two groups named Group1 and Group2.

You have the compliance assessments shown in the following table.

Name	Group
Ca1	Group1
Ca2	Group1
Ca3	Group2

You have the improvement actions shown in the following table.

Action	Compliance assessment	Improvement action	Points	Action type
Action1	Ca1	Create and publish a retention label	5	Technical
Action2	Ca2	Create and publish a retention label	5	Technical
Action3	Ca3	Enable Windows 10 Security baseline	5	Technical
Action4	Ca1	Restrict access to privileged accounts	10	Operational
Action5	Ca2	Update security awareness training	10	Operational
Action6	Ca3	Update security awareness training	10	Operational

You perform the following actions:

• Create and publish a retention label.
• Implement security awareness training for all users.
• For Action4, change Implementation status to Implemented.

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	Yes	No
The compliance score for Ca1 will increase by 15 points.	○	○
The compliance score for Ca2 will increase by 15 points.	○	○
The compliance score for Ca3 will increase by 10 points.	○	○

Answer Area

Correct Answer:

Statements	Yes	No
The compliance score for Ca1 will increase by 15 points.	○	☒
The compliance score for Ca2 will increase by 15 points.	○	☒
The compliance score for Ca3 will increase by 10 points.	☒	○

Romeokton 5 days, 12 hours ago

The answer is correct as it is N-N-Y, because scoring is 25-25-10

upvoted 1 times

martutene 4 weeks, 1 day ago

I think it should be Y Y Y

upvoted 3 times

Question #8 *Topic 5*

HOTSPOT
-

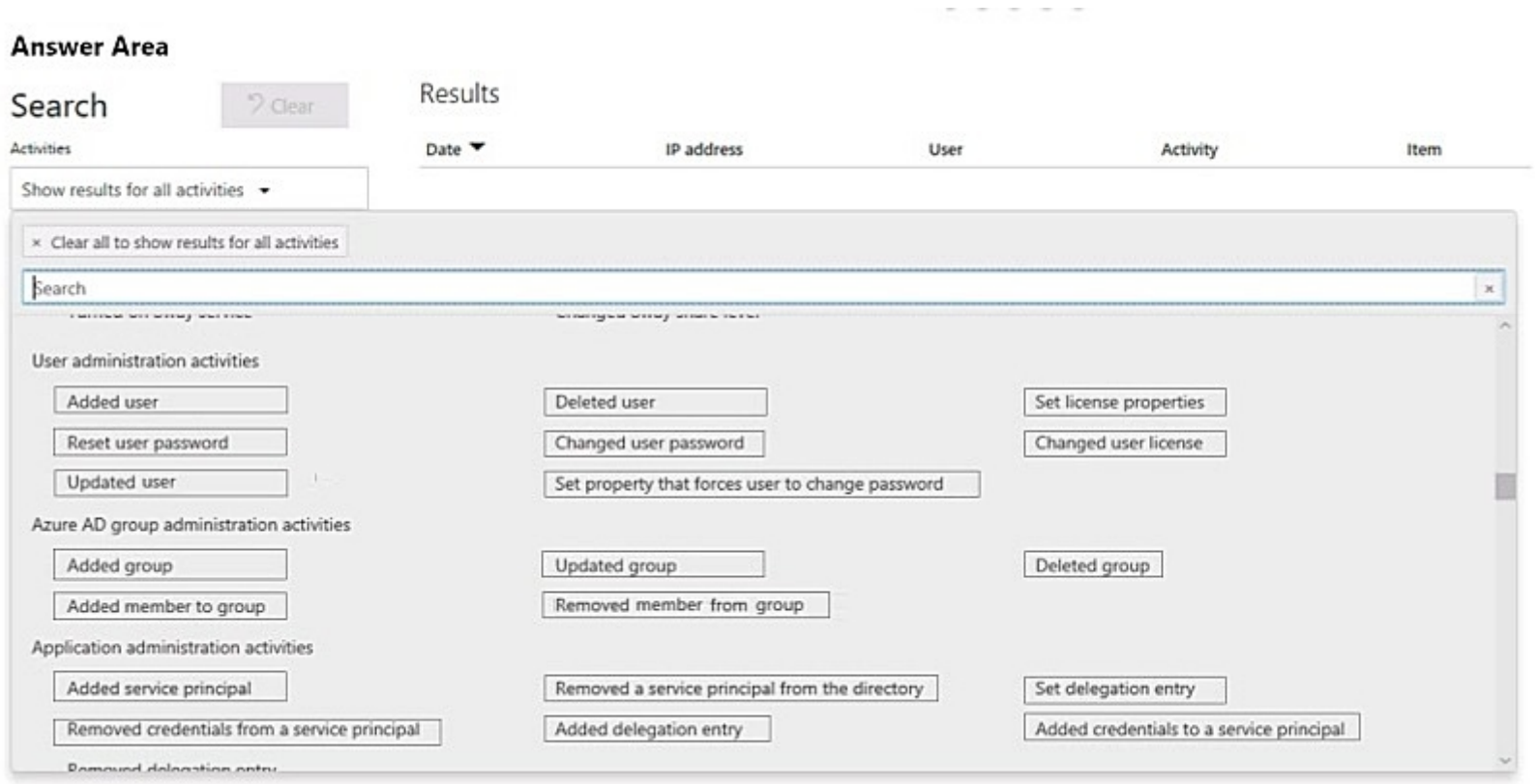
You have a Microsoft 365 subscription. Auditing is enabled.

A user named User1 is a member of a dynamic security group named Group1.

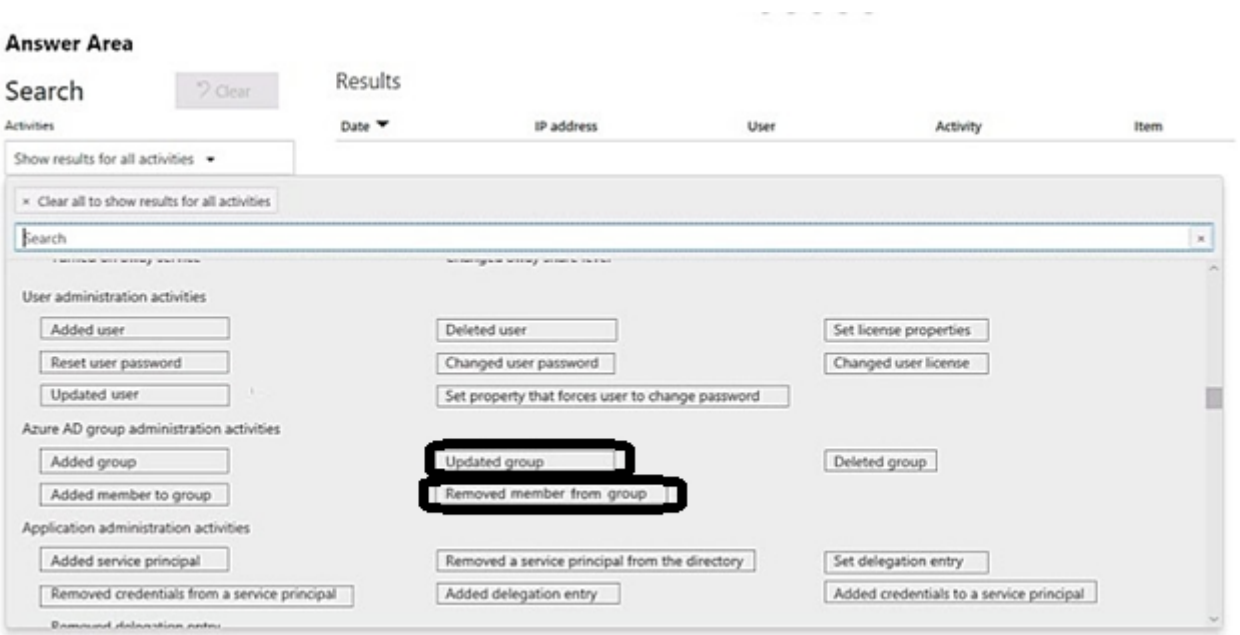
You discover that User1 is no longer a member of Group1.

You need to search the audit log to identify why User1 was removed from Group1.

Which two activities should you use in the search? To answer, select the appropriate activities in the answer area.



Correct Answer:



izgi43 3 weeks ago
on the exam thu nov 9
upvoted 1 times

Question #9 *Topic 5*

You have a Microsoft 365 E5 subscription.

You need to export the details of a retention label. The export must include the following information:

- Is record
- Is regulatory
- Disposition type

What should you do?

A. From the Microsoft Purview compliance portal, export Compliance Manager assessment actions.

B. From the Microsoft Purview compliance portal export a file plan.

C. From the Microsoft Purview compliance portal, export a disposition review.

D. From PowerShell, run the Export-ActivityExplorerData cmdlet.

E. From PowerShell, run the Get-RetentionEvent cmdlet.

Correct Answer: *B*

heshmat2022 1 week, 6 days ago

The file plan is correct, I have exported the file plan and the required records are present.

upvoted 1 times

Question #10 *Topic 5*

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 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-AdminAuditlogConfig -AdminAuditLogEnabled $true -AdminAuditLogCmdlets *Mailbox* command.

Does that meet the goal?

A. Yes

B. No

Correct Answer: *B*

izgi43 3 weeks ago
on the exam thu nov 9
upvoted 1 times

Question #11 *Topic 5*

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 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-AuditConfig -Workload Exchange command.

Does that meet the goal?

A. Yes

B. No

Correct Answer: *A*

izgi43 3 weeks ago

on the exam thu nov 9

upvoted 1 times

Question #12 *Topic 5*

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 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-MailboxFolderPermission -Identity "User1" -User User1@contoso.com -AccessRights Owner command.

Does that meet the goal?

A. Yes

B. No

Correct Answer: *B*

izgi43 3 weeks ago
on the exam thu nov 9
upvoted 1 times

Question #13 *Topic 5*

You have a Microsoft 365 subscription.

You need to be notified by email whenever an administrator starts an eDiscovery search.

What should you do from the Microsoft Purview compliance portal?

A. From Records management create event type.

B. From eDiscovery, create an eDiscovery case.

C. From Content search, create a new search.

D. From Policies, create an alert policy.

Correct Answer: *D*

Question #14 *Topic 5*

You have a Microsoft 365 subscription that contains a user named User1.

You need to assign User1 permissions to search Microsoft Office 365 audit logs.

What should you use?

A. the Azure Active Directory admin center

B. the Microsoft Purview compliance portal

C. the Exchange admin center

D. the Microsoft 365 Defender portal

Correct Answer: *C*

Romeokton 5 days, 11 hours ago

Selected Answer: C

To search the audit log, administrators and members of investigation teams must be assigned the View-Only Audit Logs or Audit Logs role in Exchange Online.

upvoted 1 times

HOTSPOT
-

You have a Microsoft 365 E5 subscription that contains two users named User1 and User2.

You create the audit retention policies shown in the following table.

Priority	Policy name	Record type	Activities	Users	Duration
10	AuditRetention1	ExchangeItem	MailboxLogin	*None*	90 Days
20	AuditRetention2	ExchangeItem	Send, MailItemsAccesssed	User1	9 Months
30	AuditRetention3	Sharepoint	*None*	User1	6 Months
40	AuditRetention4	Sharepoint	SiteRenamed	User1	9 Months
50	AuditRetention5	Sharepoint	SiteRenamed	*None*	10 Years

The users perform the following actions:

• User1 renames a Microsoft SharePoint Online site.
• User2 sends an email message.

How long will the audit log records be retained for each action? To answer, select the appropriate options in the answer area.

NOTE: Each correct selection is worth one point.

Answer Area

User1 renames a SharePoint site:
90 days
6 months
9 months
1 year
10 years

User2 sends an email message:
90 days
6 months
9 months
1 year
10 years

Correct Answer:

Answer Area

User1 renames a SharePoint site:
90 days
6 months
9 months
1 year
10 years

User2 sends an email message:
90 days
6 months
9 months
1 year
10 years

Question #1 *Topic 6*

You have a Microsoft 365 E5 subscription that uses Microsoft Teams and contains a user named User1.

You configure Microsoft Purview Information Barriers.

You need to identify which information barrier policies apply to User1.

Which cmdlet should you use?

A. Get-OrganizationSegment

B. Get-InformationBarrierRecipientStatus

C. Get-InformationBarrierPolicy

D. Get-InformationBarrierPoliciesApplicationStatus

Correct Answer: *B*

Romeokton 5 days, 11 hours ago

Selected Answer: B

https://learn.microsoft.com/en-us/powershell/module/exchange/get-informationbarrierrecipientstatus?view=exchange-ps

upvoted 1 times

izgi43 3 weeks ago

on the exam thu nov 9

upvoted 1 times

martutene 4 weeks, 1 day ago

https://www.examtopics.com/discussions/microsoft/view/81523-exam-ms-500-topic-4-question-72-discussion/#:~:text=You%20can%20use%20this%20cmdlet,is%20not%20a%20valid%20cmdlet

upvoted 1 times

Question #2 *Topic 6*

You have a Microsoft 365 E5 subscription.

You are implementing insider risk management.

You need to maximize the amount of historical data that is collected when an event is triggered.

What is the maximum number of days that historical data can be collected?

A. 30

B. 60

C. 90

D. 180

Correct Answer: *D*

Romeokton 5 days, 11 hours ago

Selected Answer: C

I agree with C

upvoted 1 times

heshmat2022 1 week, 6 days ago

the maximum past activity detection period for emails in Microsoft 365 is 90 days. This means that certain actions or activities related to emails, such as message tracking, auditing, and eDiscovery, are typically retained for a maximum of 90 days. This retention period can vary based on specific configurations and policies set by administrators.

upvoted 1 times

martutene 4 weeks, 1 day ago

Selected Answer: C

Wrong
Activation window: The number of days, 1 to 30,
Past activity detection: The number of days, 0 to 90
For email activities, the past activity detection period is 10 days.

upvoted 4 times

phony 1 week, 6 days ago

if historical data means the same as Past activity detection
https://learn.microsoft.com/en-us/purview/insider-risk-management-settings-policy-timeframes
then the policy timeframe is max. 90. see slider in:
https://compliance.microsoft.com/insiderriskmgmt/globalsettings?viewid=overview

upvoted 1 times

Question #3 *Topic 6*

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.

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

izgi43 3 weeks ago
on the exam thu nov 9
upvoted 1 times

martutene 4 weeks, 1 day ago

correct
https://learn.microsoft.com/en-us/purview/communication-compliance-plan

upvoted 1 times

Question #4 *Topic 6*

HOTSPOT
-

You have a Microsoft 365 E5 subscription.

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

• Prevents users from performing data transfers that breach local regulations
• Minimizes effort to respond to requests for a user's personal data

What should you use in the Microsoft Purview compliance portal? To answer, select the appropriate options in the answer area.

NOTE: Each correct selection is worth one point.

Answer Area

To prevent users from performing data transfers that breach local regulations:

- Communication compliance
- Information barriers
- Incident risk management
- Privacy risk management

To minimize effort to respond to requests for a user's personal data:

- Data loss prevention (DLP)
- eDiscovery
- Records management
- Subject rights request

Correct Answer:

Answer Area

To prevent users from performing data transfers that breach local regulations:

- Communication compliance
- Information barriers
- Incident risk management
- Privacy risk management

To minimize effort to respond to requests for a user's personal data:

- Data loss prevention (DLP)
- eDiscovery
- Records management
- Subject rights request

Romeokton 5 days, 11 hours ago
The provided answer to the first question is wrong. Correct is Privacy risk management.
upvoted 1 times

izgi43 3 weeks ago
on the exam thu nov 9
upvoted 2 times

Pixan 3 weeks, 6 days ago
Hi Everyone!!
Join ET and get actual and valid study material: https://examstopics.quora.com/ and pass your exam in first attempt. Study Smart Not Hard
upvoted 1 times

martutene 4 weeks, 1 day ago
First one should be insider risk management
upvoted 1 times

martutene 4 weeks ago
my bad it should be Priva:
• Data transfers: This policy can detect personal data transfers across boundaries that you determine, which could involve transfers outside of your organization, or internal transfers across departments or geographic regions. When matches are found, you can set up notifications encouraging senders to revoke access to the content.
upvoted 3 times

Question #5 *Topic 6*

You have a Microsoft 365 E5 subscription that uses Microsoft Purview. The subscription contains two groups named Group1 and Group2.

You need to implement a policy to detect messages that present a conflict of interest between the users in Group1 and the users in Group2.

What should you use in the Microsoft Purview compliance portal?

A. Insider risk management

B. Privacy risk management

C. Information barriers

D. Communication compliance

Correct Answer: *D*

izgi43 3 weeks ago
on the exam thu nov 9
upvoted 2 times

SethuRam 3 weeks, 1 day ago
Information barriers is the correct answer
upvoted 4 times

BJack 2 weeks, 1 day ago
The requirement is to "detect" messages, which is Communication Compliance. Information Barriers will block communication.
upvoted 1 times

AndlMty 3 weeks ago
https://learn.microsoft.com/en-us/purview/information-barriers
upvoted 4 times

Domza 2 weeks, 3 days ago
Thx for the link
upvoted 1 times

Question #6 *Topic 6*

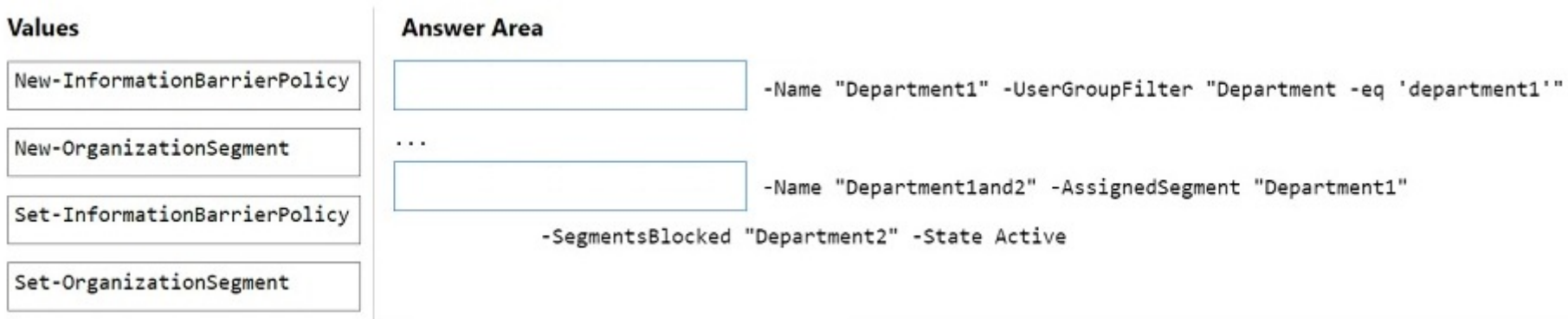
DRAG DROP
-

Your company has two departments named department1 and department2 and a Microsoft 365 E5 subscription.

You need to prevent communication between the users in department1 and the users in department2.

How should you complete the PowerShell script? To answer, drag the appropriate values to the correct targets. Each value 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.



Correct Answer:

phony 5 days, 1 hour ago
https://learn.microsoft.com/en-us/purview/information-barriers-policies#using-equals-and-not-equals-in-powershell-segment-definitions

first: New-OrganizationSegment
second: New-informationBarrierPolicy
upvoted 1 times

izgi43 3 weeks ago
on the exam thu nov 9
upvoted 3 times

Question #7 *Topic 6*

You have a Microsoft 365 E5 subscription.

You need to identify personal data stored in the subscription and control the transfer of personal data between users and groups.

Which type of license should you acquire?

A. Microsoft Purview Audit (Premium)

B. Priva Privacy Risk Management

C. Microsoft 365 E5 Compliance

D. Priva Subject Rights Requests

Correct Answer: *B*

Romeokton 5 days, 11 hours ago

Selected Answer: B

I also support B

upvoted 1 times

Question #8 *Topic 6*

You have a Microsoft 365 E5 subscription that contains a Microsoft SharePoint Online site named Site1.

You create an information barrier segment named Segment1.

You need to add Segment1 to Site1.

What should you do first?

A. Run the Set-SPOSite cmdlet.

B. Run the Set-SPOTenant cmdlet.

C. Create an information barrier policy.

D. Modify the permissions of Site1.

Correct Answer: *C*

HOTSPOT
-

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

Name	Member of
User1	Group2
User2	*None*
User3	*None*

The subscription contains the communication compliance policy shown in the following exhibit.

Review and finish

Name and description

Name
Policy1

Users and reviewers

Choose users and groups
group2@sk230415outlook.onmicrosoft.com

Excluded users and groups
None

Reviewers
user3@sk230415outlook.onmicrosoft.com

Locations

Scoped locations
Exchange

Conditions and percentage

Communication direction
Outbound, Internal

Optical character recognition(OCR)
Disabled

Filter email blasts
Enabled

Conditions
None

Percentage to review
100

Users send the email messages shown in the following table.

Name	Sender	Receiver
Mail1	User1	User2
Mail2	User1	friend@outlook.com
Mail3	friend@outlook.com	User2

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	Yes	No
User3 can review Mail1.	○	○
User3 can review Mail2.	○	○
User3 can review Mail3.	○	○

Answer Area

Correct Answer:

Statements	Yes	No
User3 can review Mail1.	☑	○
User3 can review Mail2.	○	☑
User3 can review Mail3.	○	☑

Romeokton 5 days, 11 hours ago
Agree with Y-Y-N
upvoted 2 times

MerajKhan 1 week, 2 days ago
Y,Y,N. First one is internal communication, second one is outbound communication and last one is inbound external communication.
upvoted 3 times

Question #10 *Topic 6*

You have a Microsoft 365 E5 subscription.

You plan to use insider risk management to collect and investigate forensic evidence.

You need to enable forensic evidence capturing.

What should you do first?

A. Enable Adaptive Protection.

B. Configure the information protection scanner.

C. Create priority user groups.

D. Claim capacity.

Correct Answer: *C*

ae88d96 2 weeks, 1 day ago

Selected Answer: D

D. Claim capacity.

Before you can enable forensic evidence capturing in insider risk management, you need to claim capacity for your organization. This ensures that adequate resources are reserved for evidence collection and investigation. After claiming capacity, you can proceed with configuring other aspects of insider risk management, such as creating policies and enabling evidence capture.

upvoted 3 times

martutene 4 weeks, 1 day ago

wrong:
Step 1: Confirm your subscription and configure data storage access
https://learn.microsoft.com/en-us/purview/insider-risk-management-forensic-evidence-configure

upvoted 1 times

izgi43 2 weeks, 3 days ago

so what is the right answer than?

upvoted 1 times

Romeokton 5 days, 11 hours ago

D is correct

upvoted 1 times

Domza 2 weeks, 3 days ago

You read and tell us the answer :)

upvoted 1 times

Question #11 *Topic 6*

You have a Microsoft 365 E5 subscription that uses Yammer.

You need to create a Microsoft Purview communication compliance policy that will detect inappropriate images in Yammer conversations.

What should you do first?

A. Configure Hybrid Mode for Yammer.

B. Configure Native Mode for Yammer.

C. Configure the Yammer network admin settings.

D. Assign each user a Yammer license.

Correct Answer: *B*

phony 5 days, 1 hour ago

https://learn.microsoft.com/en-us/viva/engage/overview-native-mode

upvoted 1 times

Romeokton 5 days, 11 hours ago

Selected Answer: B

Correct B

Yammer: Private messages and public community conversations in Yammer are supported in communication compliance policies. Yammer is an optional channel and must be in native mode to support checking of messages and attachments

upvoted 1 times

Question #12 *Topic 6*

You have a Microsoft 365 E5 subscription that uses Privacy Risk Management in Microsoft Priva.

You need to review the personal data type instances that were detected in the subscription.

What should you use in the Microsoft Purview compliance portal?

A. Content explorer

B. User data search

C. Content search

D. an eDiscovery case

Correct Answer: *A*

Romeokton 5 days, 11 hours ago

Selected Answer: A

Definitely A

upvoted 1 times

Question #13 *Topic 6*

DRAG DROP
-

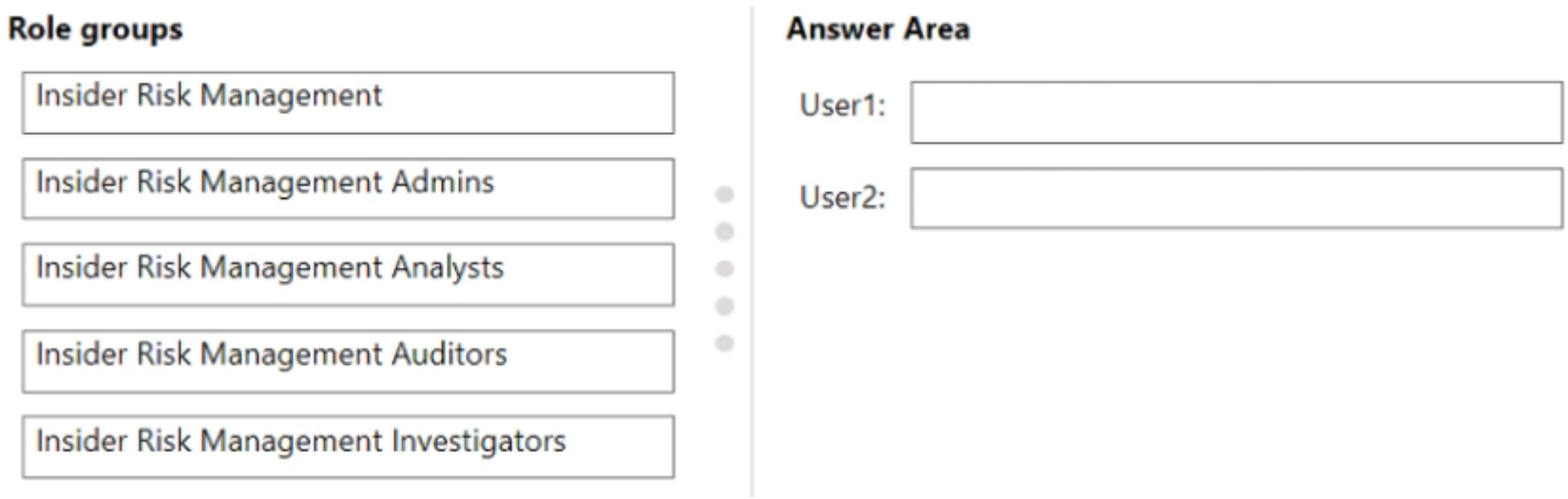
You have a Microsoft 365 E5 subscription that contains two users named User1 and User2.

You need to implement insider risk management. The solution must meet the following requirements:

• Ensure that User1 can create insider risk management policies.
• Ensure that User2 can use content captured by using insider risk management policies.
• Follow the principle of least privilege.

To which role group should you add each user? To answer, drag the appropriate role groups to the correct users. Each role group 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.



Correct Answer:

Question #14 *Topic 6*

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

Name	Department
User1	Finance
User2	Research
User3	Finance

You need to prevent users in the finance department from sharing files with users in the research department.

Which type of policy should you configure?

A. communication compliance

B. information barrier

C. Conditional Access

D. insider risk management

Correct Answer: *B*

HOTSPOT
-

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

Name	Type	User principal name (UPN)	Member of
User1	User	user1@sk220115outlook.onmicrosoft.com	Dist1
User2	User	user2@sk220115outlook.onmicrosoft.com	Dist1
User3	User	user3@sk220115outlook.onmicrosoft.com	Group1
User4	User	user4@sk220115outlook.onmicrosoft.com	none
Group1	Microsoft 365 group	group1@sk220115outlook.onmicrosoft.com	none
Dist1	Distribution group	dist1@sk220115outlook.onmicrosoft.com	none

You create the communication compliance policy as shown in the exhibit. (Click the Exhibit tab.)

Review and finish

Name and description

Name

CommCompliance1

Users and reviewers

Supervised users and groups

dist1@sk220115outlook.onmicrosoft.com,Group1@sk220115outlook.onmicrosoft.com

Excluded users and groups

User2@sk220115outlook.onmicrosoft.com

Reviewers

User4@sk220115outlook.onmicrosoft.com

Locations

Monitored locations

Exchange

Conditions and percentage

Communication direction

Inbound

Optical character recognition(OCR)

Disabled

Conditions

None

Percentage to review

100

Four emails are sent as shown in the following table.

Name	Description
Mail1	Sent by User3 to User1.
Mail2	Sent by User1 to User2.
Mail3	Sent by User2 to User1.

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	Yes	No
User4 can review Mail1.	○	○
User4 can review Mail2.	○	○
User4 can review Mail3.	○	○

Correct Answer:

Answer Area

Statements	Yes	No
User4 can review Mail1.	○	○
User4 can review Mail2.	○	○
User4 can review Mail3.	○	○

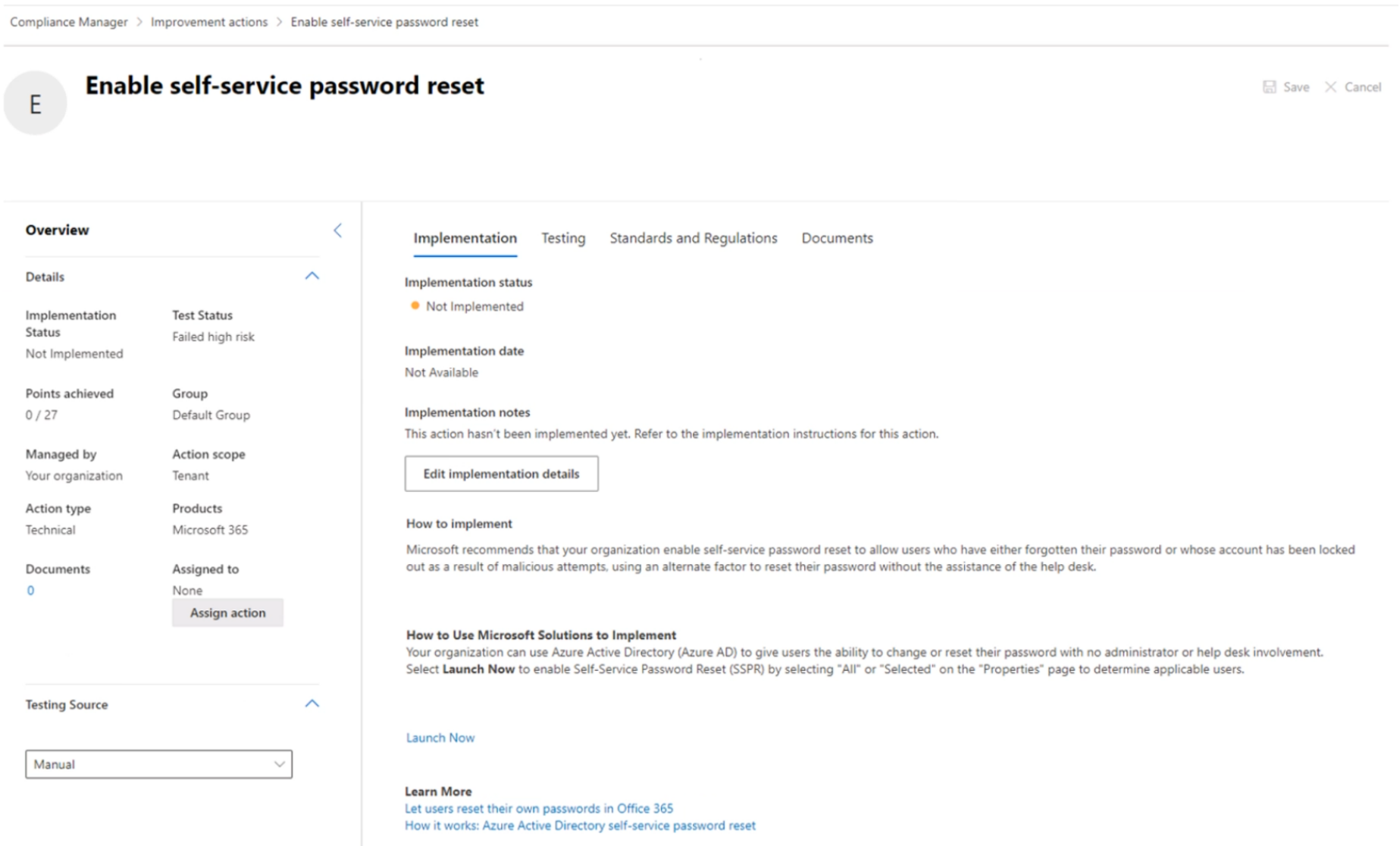
HOTSPOT

-

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	Security

You have the Compliance Manager improvement action shown in the following exhibit.



Use the drop-down menus to select the answer choice that completes each statement based on the information presented in the graphic.

NOTE: Each correct selection is worth one point.

Answer Area

The Enable self-service password reset improvement action can be assigned to **[answer choice]**.

- User1 only
- Group1 only
- User1 and Group1 only
- Group1 and Group2 only
- User1, Group1, and Group2

Twenty-four hours after self-service password reset (SSPR) is enabled for all users, Points achieved will be **[answer choice]**.

- 0 / 27
- 1 / 27
- 2 / 27
- 5 / 27
- 27 / 27

Correct Answer:

Answer Area

The Enable self-service password reset improvement action can be assigned to **[answer choice]**.

- User1 only
- Group1 only
- User1 and Group1 only
- Group1 and Group2 only
- User1, Group1, and Group2

Twenty-four hours after self-service password reset (SSPR) is enabled for all users, Points achieved will be **[answer choice]**.

- 0 / 27
- 1 / 27
- 2 / 27
- 5 / 27
- 27 / 27

HOTSPOT
-

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

Name	Mailbox	Cloud license
User1	On-premises Microsoft Exchange Server	Microsoft Teams
User2	On-premises Microsoft Exchange Server	Microsoft Exchange Online Plan 2
User3	On-premises Microsoft Exchange Server	Microsoft Teams, Exchange Online Plan 2
User4	Microsoft Exchange Online	Microsoft Teams, Exchange Online Plan 2

You need to perform an eDiscovery content search.

Which user's data can be included in the content search? To answer, select the appropriate options in the answer area.

NOTE: Each correct selection is worth one point.

Answer Area

Exchange mailboxes:
- User4 only
- User4 and User3 only
- User4, User3, and User2 only
- User4, User3, User2, and User1

Teams chat data:
- User4 only
- User4 and User3 only
- User4, User3, and User1 only
- User4, User3, User2, and User1

Answer Area

Exchange mailboxes:
- User4 only
- User4 and User3 only
- User4, User3, and User2 only
- User4, User3, User2, and User1

Correct Answer:

Teams chat data:
- User4 only
- User4 and User3 only
- User4, User3, and User1 only
- User4, User3, User2, and User1

HOTSPOT
-

You have a Microsoft 365 subscription that has Enable Security defaults set to No in Azure AD.

You have a custom compliance manager template named Regulation1.

You have the assessments shown in the following table.

Name	Score	Status	Group	Product	Regulation
Assessment1	1200	Incomplete	Group1	Microsoft 365	Regulation1
Assessment2	900	Incomplete	Group2	Microsoft 365	Regulation1

Assessment1 has the improvement actions shown in the following table.

Improvement action	Test status	Impact	Points achieved	Action type
Enable multi-factor authentication for admins	Failed high risk	+27 points	0/27	Technical
Enable multi-factor authentication for non-admins	Failed high risk	+27 points	0/27	Technical

Assessment2 has the improvement actions shown in the following table.

Improvement action	Test status	Impact	Points achieved	Action type
Establish a threat intelligence program	None	+9 points	0/9	Operational
Configure a privileged access policy	Failed high risk	+15 points	0/15	Technical

You perform the following actions:

- For Assessment2, change the Test status of Establish a threat intelligence program to Implemented.
- Enable multi-factor authentication (MFA) for all users.
- Configure a privileged access policy.

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	Yes	No
Establish a threat intelligence program will appear as Implemented in Assessment1.	○	○
The Assessment1 score will increase by only 54 points.	○	○
The Assessment2 score will increase by only 78 points.	○	○

Correct Answer:

Answer Area

Statements	Yes	No
Establish a threat intelligence program will appear as Implemented in Assessment1.	○	☒
The Assessment1 score will increase by only 54 points.	☒	○
The Assessment2 score will increase by only 78 points.	○	☒

Question #1 *Topic 7*

Introductory Info

Case study -

This is a case study. Case studies are not timed separately. You can use as much exam time as you would like to complete each case. However, there may be additional case studies and sections on this exam. You must manage your time to ensure that you are able to complete all questions included on this exam in the time provided.

To answer the questions included in a case study, you will need to reference information that is provided in the case study. Case studies might contain exhibits and other resources that provide more information about the scenario that is described in the case study. Each question is independent of the other questions in this case study.

At the end of this case study, a review screen will appear. This screen allows you to review your answers and to make changes before you move to the next section of the exam. After you begin a new section, you cannot return to this section.

To start the case study -

To display the first question in this case study, click the Next button. Use the buttons in the left pane to explore the content of the case study before you answer the questions. Clicking these buttons displays information such as business requirements, existing environment, and problem statements. If the case study has an All Information tab, note that the information displayed is identical to the information displayed on the subsequent tabs. When you are ready to answer a question, click the Question button to return to the question.

Overview -

Fabrikam, Inc. is a consulting company that has a main office in Montreal and six branch offices in New York, Seattle, Miami, Houston, Los Angeles, and
Vancouver.

Existing Environment -

Cloud Environment -

Fabrikam has a Microsoft 365 tenant that contains the following resources:

An on-premises Active Directory domain named corp.fabrikam.com that syncs to an Azure Active Directory (Azure AD) tenant

Microsoft Cloud App Security connectors configured for all supported cloud applications used by the company

Some users have company Dropbox accounts.

Compliance Configuration -

Fabrikam has the following in the Microsoft 365 compliance center:

A data loss prevention (DLP) policy is configured. The policy displays a tooltip to users. Users can provide a business justification to override a DLP policy violation.

The Azure Information Protection unified labeling scanner is installed and configured.

A sensitivity label named Fabrikam Confidential is configured.

An existing third-party records management system is managed by the compliance department.

Human Resources (HR) Management System

The HR department has an Azure SQL database that contains employee information. Each employee has a unique 12-character alphanumeric ID. The database contains confidential employee attributes including payroll information, date of birth, and personal contact details.

On-Premises Environment -

You have an on-premises file server that runs Windows Server 2019 and stores Microsoft Office documents in a shared folder named Data.

All end-user computers are joined to the corp.fabrikam.com domain and run a third-party antimalware application.

Business Processes -

Sales Contracts -

Users in the sales department receive draft sales contracts from customers by email. The sales contracts are written by the customers and are not in a standard format.

Employment Applications -

Employment applications and resumes are received by HR department managers and stored in either mailboxes, Microsoft SharePoint Online sites, OneDrive for
Business folders, or Microsoft Teams channels.
The employment application form is downloaded from SharePoint Online and a serial number is assigned to each application.
The resumes are written by the applicants and are in any format.

Requirements -

HR Requirements -
You need to create a DLP policy that will notify the HR department of a DLP policy violation if a document that contains confidential employee attributes is shared externally. The DLP policy must use an Exact Data Match (EDM) classification derived from a CSV export of the HR department database.
The HR department identifies the following requirements for handling employment applications:
Resumes must be identified automatically based on similarities to other resumes received in the past.
Employment applications and resumes must be deleted automatically two years after the applications are received.
Documents and emails that contain an application serial number must be identified automatically and marked as an employment application.

Sales Requirements -
A sensitivity label named Sales Contract must be applied automatically to all draft and finalized sales contracts.

Compliance Requirements -
Fabrikam identifies the following compliance requirements:
All DLP policies must be applied to computers that run Windows 10, with the least possible changes to the computers.
Users in the compliance department must view the justification provided when a user receives a tooltip notification for a DLP violation.
If a document that has the Fabrikam Confidential sensitivity label applied is uploaded to Dropbox, the file must be deleted automatically.
The Fabrikam Confidential sensitivity label must be applied to existing Microsoft Word documents in the Data shared folder that have a document footer containing the following string: Company use only.
Users must be able to manually select that email messages are sent encrypted. The encryption will use Office 365 Message Encryption (OME) v2.
Any email containing an attachment that has the Fabrikam Confidential sensitivity label applied must be encrypted automatically by using OME.
Existing policies configured in the third-party records management system must be replaced by using Records management in the Microsoft 365 compliance center. The compliance department plans to export the existing policies, and then produce a CSV file that contains matching labels and policies that are compatible with records management in Microsoft 365. The CSV file must be used to configure records management in Microsoft 365.

Executive Requirements -
You must be able to restore all email received by Fabrikam executives for up to three years after an email is received, even if the email was deleted permanently.

Question
You need to recommend a solution that meets the Data Loss Prevention requirements for the HR department.
Which three actions should you perform? Each correct answer presents part of the solution. (Choose three.)
NOTE: Each correct selection is worth one point.

A. Schedule EdmUploadAgent.exe to hash and upload a data file that contains employee information.

B. Create a sensitive info type rule package that contains the EDM classification.

C. Define the sensitive information database schema in the XML format.

D. Create a sensitive info type rule package that contains regular expressions.

E. Define the sensitive information database schema in the CSV format.

Correct Answer: *ABC*
Reference:
https://docs.microsoft.com/en-us/microsoft-365/compliance/create-a-custom-sensitive-information-type?view=o365-worldwide

wooyourdaddy 9 months, 1 week ago
Answer confirmed at this link:

https://learn.microsoft.com/en-us/microsoft-365/compliance/sit-get-started-exact-data-match-hash-upload?view=o365-worldwide#hash-and-upload-the-sensitive-information-source-table

upvoted 2 times

wooyourdaddy 1 year, 5 months ago

Selected Answer: ABC

I wrote the exam today, this question was on it, I choose ABC, scored 890!

upvoted 2 times

Pravda 1 year, 10 months ago

On exam 1/20/2022

upvoted 1 times

Ali_557 1 year, 11 months ago

Confirmed case study

upvoted 1 times

MrGarak1 2 years ago

It should be ABE because HR department is using CSV format

upvoted 2 times

MrGarak1 2 years ago

no, it's ABC.
https://docs.microsoft.com/en-us/microsoft-365/compliance/create-custom-sensitive-information-types-with-exact-data-match-based-classification?view=o365-worldwide#define-the-schema-for-your-database-of-sensitive-information
sorry

upvoted 6 times

sergioandreslq 1 year, 11 months ago

Agreed: ABC:
A: EdmUploadAgent.exe to hash
B: Create SIT using the EDM classification
C: You can create the exact data match (EDM) sensitive information type (SIT) by using the the EDM schema and SIT wizard in the Compliance center or create the rule package XML file manually. You can also combine both by using one method to create the schema and later edit it using the other method.
Whether you will be creating an EDM sensitive information type using the wizard or the rule package XML file via PowerShell, you must have Global admin or Compliance admin permissions to create, test, and deploy a custom sensitive information type through the UI.
reference:
https://docs.microsoft.com/en-us/microsoft-365/compliance/sit-get-started-exact-data-match-create-rule-package?view=o365-worldwide

upvoted 2 times

Mastersin 2 years ago

https://docs.microsoft.com/en-us/microsoft-365/compliance/sit-get-started-exact-data-match-create-rule-package?view=o365-worldwide

upvoted 1 times

Introductory Info

Case study -

This is a case study. Case studies are not timed separately. You can use as much exam time as you would like to complete each case. However, there may be additional case studies and sections on this exam. You must manage your time to ensure that you are able to complete all questions included on this exam in the time provided.

To answer the questions included in a case study, you will need to reference information that is provided in the case study. Case studies might contain exhibits and other resources that provide more information about the scenario that is described in the case study. Each question is independent of the other questions in this case study.

At the end of this case study, a review screen will appear. This screen allows you to review your answers and to make changes before you move to the next section of the exam. After you begin a new section, you cannot return to this section.

To start the case study -

To display the first question in this case study, click the Next button. Use the buttons in the left pane to explore the content of the case study before you answer the questions. Clicking these buttons displays information such as business requirements, existing environment, and problem statements. If the case study has an All Information tab, note that the information displayed is identical to the information displayed on the subsequent tabs. When you are ready to answer a question, click the Question button to return to the question.

Overview -

Fabrikam, Inc. is a consulting company that has a main office in Montreal and six branch offices in New York, Seattle, Miami, Houston, Los Angeles, and
Vancouver.

Existing Environment -

Cloud Environment -

Fabrikam has a Microsoft 365 tenant that contains the following resources:

An on-premises Active Directory domain named corp.fabrikam.com that syncs to an Azure Active Directory (Azure AD) tenant

Microsoft Cloud App Security connectors configured for all supported cloud applications used by the company

Some users have company Dropbox accounts.

Compliance Configuration -

Fabrikam has the following in the Microsoft 365 compliance center:

A data loss prevention (DLP) policy is configured. The policy displays a tooltip to users. Users can provide a business justification to override a DLP policy violation.

The Azure Information Protection unified labeling scanner is installed and configured.

A sensitivity label named Fabrikam Confidential is configured.

An existing third-party records management system is managed by the compliance department.

Human Resources (HR) Management System

The HR department has an Azure SQL database that contains employee information. Each employee has a unique 12-character alphanumeric ID. The database contains confidential employee attributes including payroll information, date of birth, and personal contact details.

On-Premises Environment -

You have an on-premises file server that runs Windows Server 2019 and stores Microsoft Office documents in a shared folder named Data.

All end-user computers are joined to the corp.fabrikam.com domain and run a third-party antimalware application.

Business Processes -

Sales Contracts -

Users in the sales department receive draft sales contracts from customers by email. The sales contracts are written by the customers and are not in a standard format.

Employment Applications -

Employment applications and resumes are received by HR department managers and stored in either mailboxes, Microsoft SharePoint Online sites, OneDrive for
Business folders, or Microsoft Teams channels.

The employment application form is downloaded from SharePoint Online and a serial number is assigned to each application.
The resumes are written by the applicants and are in any format.

Requirements -

HR Requirements -
You need to create a DLP policy that will notify the HR department of a DLP policy violation if a document that contains confidential employee attributes is shared externally. The DLP policy must use an Exact Data Match (EDM) classification derived from a CSV export of the HR department database.
The HR department identifies the following requirements for handling employment applications:
Resumes must be identified automatically based on similarities to other resumes received in the past.
Employment applications and resumes must be deleted automatically two years after the applications are received.
Documents and emails that contain an application serial number must be identified automatically and marked as an employment application.

Sales Requirements -
A sensitivity label named Sales Contract must be applied automatically to all draft and finalized sales contracts.

Compliance Requirements -
Fabrikam identifies the following compliance requirements:
All DLP policies must be applied to computers that run Windows 10, with the least possible changes to the computers.
Users in the compliance department must view the justification provided when a user receives a tooltip notification for a DLP violation.
If a document that has the Fabrikam Confidential sensitivity label applied is uploaded to Dropbox, the file must be deleted automatically.
The Fabrikam Confidential sensitivity label must be applied to existing Microsoft Word documents in the Data shared folder that have a document footer containing the following string: Company use only.
Users must be able to manually select that email messages are sent encrypted. The encryption will use Office 365 Message Encryption (OME) v2.
Any email containing an attachment that has the Fabrikam Confidential sensitivity label applied must be encrypted automatically by using OME.
Existing policies configured in the third-party records management system must be replaced by using Records management in the Microsoft 365 compliance center. The compliance department plans to export the existing policies, and then produce a CSV file that contains matching labels and policies that are compatible with records management in Microsoft 365. The CSV file must be used to configure records management in Microsoft 365.

Executive Requirements -
You must be able to restore all email received by Fabrikam executives for up to three years after an email is received, even if the email was deleted permanently.

Question
You need to recommend a solution that meets the compliance requirements for protecting the documents in the Data shared folder.
What should you recommend?

A. From the Microsoft 365 compliance center, configure an auto-labeling policy.

B. From Azure Information Protection, configure a content scan job.

C. From the Microsoft 365 compliance center, configure a Content Search query.

D. From the Microsoft 365 compliance center, configure a DLP policy.

Correct Answer: *B*
Reference:
https://docs.microsoft.com/en-us/azure/information-protection/deploy-aip-scanner

eezzykel Highly Voted 2 years, 5 months ago
The answer is correct. You run an AIP scanner on premise. You cannot configure auto labeling from compliance center on premise
upvoted 13 times

xswe Most Recent 7 months, 3 weeks ago
Since we are going to place sensitivty labels on exisiting on Data shared folder we have to use unified scanner which is called content scan job now
upvoted 2 times

wooyourdaddy 1 year, 5 months ago
Selected Answer: B

I wrote the exam today, this question was on it, I choose B, scored 890!
upvoted 2 times

Pravda 1 year, 10 months ago
On exam 1/20/2022
upvoted 1 times

Eltooth 2 years, 4 months ago
Agreed - B. Run AIP scan job to classify and auto label with policy created from Compliance Centre.
upvoted 4 times

Che1 2 years, 5 months ago
Answer is correct. It can't be "A" because the data share is located on-premise and needs to have unified labeling client installed which is from Azure Information protection.

If the document is online then auto-labeling can be applied using M365 compliance center.
upvoted 4 times

Johnnien 2 years, 5 months ago
The answer could be A
upvoted 1 times

sergioandreslq 1 year, 11 months ago
Nop, Auto-labeling can't apply to the on-premise file share.
Auto-labeling apply to SPO, OneDrive for Business and Exchange online for Email in transit
upvoted 1 times

Banzaaai 2 years, 6 months ago
why not A or D ?
upvoted 3 times

MIRo0002 2 years, 5 months ago
To inspect your files, the scanner uses IFilters installed on the computer. To determine whether the files need labeling, the scanner uses the Microsoft 365 built-in data loss prevention (DLP) sensitivity information types and pattern detection, or Microsoft 365 regex patterns.
upvoted 1 times

sergioandreslq 1 year, 11 months ago
Nop, Auto-labeling can't apply to the on-premise file share. and data in on-premise
Auto-labeling apply to SPhttps://www.examtopics.com/exams/microsoft/sc-400/view/4/#O, OneDrive for Business and Exchange online for Email in transit
upvoted 1 times

Introductory Info

Case study -

This is a case study. Case studies are not timed separately. You can use as much exam time as you would like to complete each case. However, there may be additional case studies and sections on this exam. You must manage your time to ensure that you are able to complete all questions included on this exam in the time provided.

To answer the questions included in a case study, you will need to reference information that is provided in the case study. Case studies might contain exhibits and other resources that provide more information about the scenario that is described in the case study. Each question is independent of the other questions in this case study.

At the end of this case study, a review screen will appear. This screen allows you to review your answers and to make changes before you move to the next section of the exam. After you begin a new section, you cannot return to this section.

To start the case study -

To display the first question in this case study, click the Next button. Use the buttons in the left pane to explore the content of the case study before you answer the questions. Clicking these buttons displays information such as business requirements, existing environment, and problem statements. If the case study has an All Information tab, note that the information displayed is identical to the information displayed on the subsequent tabs. When you are ready to answer a question, click the Question button to return to the question.

Overview -

Fabrikam, Inc. is a consulting company that has a main office in Montreal and six branch offices in New York, Seattle, Miami, Houston, Los Angeles, and
Vancouver.

Existing Environment -

Cloud Environment -

Fabrikam has a Microsoft 365 tenant that contains the following resources:

An on-premises Active Directory domain named corp.fabrikam.com that syncs to an Azure Active Directory (Azure AD) tenant

Microsoft Cloud App Security connectors configured for all supported cloud applications used by the company

Some users have company Dropbox accounts.

Compliance Configuration -

Fabrikam has the following in the Microsoft 365 compliance center:

A data loss prevention (DLP) policy is configured. The policy displays a tooltip to users. Users can provide a business justification to override a DLP policy violation.

The Azure Information Protection unified labeling scanner is installed and configured.

A sensitivity label named Fabrikam Confidential is configured.

An existing third-party records management system is managed by the compliance department.

Human Resources (HR) Management System

The HR department has an Azure SQL database that contains employee information. Each employee has a unique 12-character alphanumeric ID. The database contains confidential employee attributes including payroll information, date of birth, and personal contact details.

On-Premises Environment -

You have an on-premises file server that runs Windows Server 2019 and stores Microsoft Office documents in a shared folder named Data.

All end-user computers are joined to the corp.fabrikam.com domain and run a third-party antimalware application.

Business Processes -

Sales Contracts -

Users in the sales department receive draft sales contracts from customers by email. The sales contracts are written by the customers and are not in a standard format.

Employment Applications -

Employment applications and resumes are received by HR department managers and stored in either mailboxes, Microsoft SharePoint Online sites, OneDrive for
Business folders, or Microsoft Teams channels.

The employment application form is downloaded from SharePoint Online and a serial number is assigned to each application.
The resumes are written by the applicants and are in any format.

Requirements -

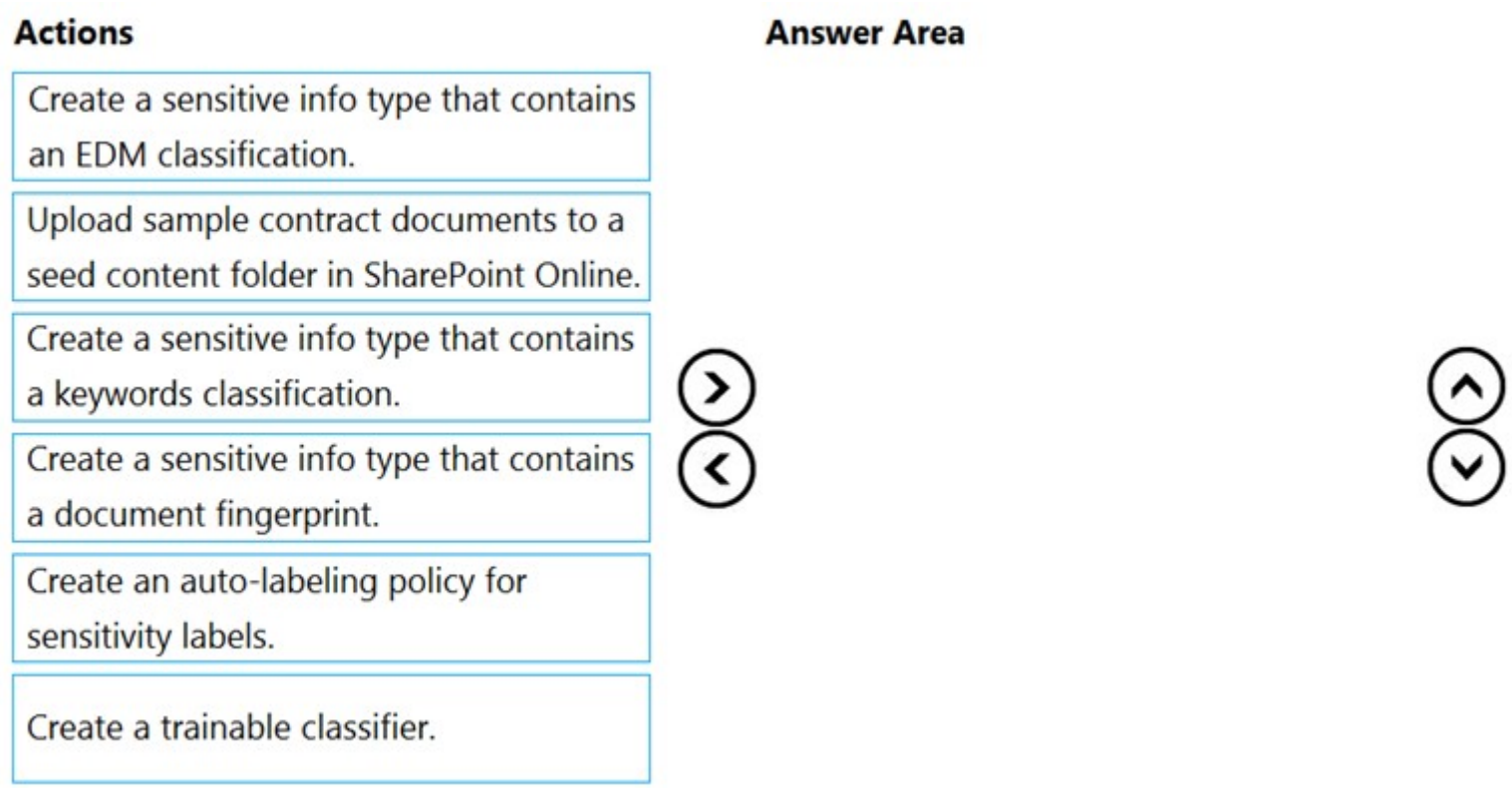
HR Requirements -
You need to create a DLP policy that will notify the HR department of a DLP policy violation if a document that contains confidential employee attributes is shared externally. The DLP policy must use an Exact Data Match (EDM) classification derived from a CSV export of the HR department database.
The HR department identifies the following requirements for handling employment applications:
Resumes must be identified automatically based on similarities to other resumes received in the past.
Employment applications and resumes must be deleted automatically two years after the applications are received.
Documents and emails that contain an application serial number must be identified automatically and marked as an employment application.

Sales Requirements -
A sensitivity label named Sales Contract must be applied automatically to all draft and finalized sales contracts.

Compliance Requirements -
Fabrikam identifies the following compliance requirements:
All DLP policies must be applied to computers that run Windows 10, with the least possible changes to the computers.
Users in the compliance department must view the justification provided when a user receives a tooltip notification for a DLP violation.
If a document that has the Fabrikam Confidential sensitivity label applied is uploaded to Dropbox, the file must be deleted automatically.
The Fabrikam Confidential sensitivity label must be applied to existing Microsoft Word documents in the Data shared folder that have a document footer containing the following string: Company use only.
Users must be able to manually select that email messages are sent encrypted. The encryption will use Office 365 Message Encryption (OME) v2.
Any email containing an attachment that has the Fabrikam Confidential sensitivity label applied must be encrypted automatically by using OME.
Existing policies configured in the third-party records management system must be replaced by using Records management in the Microsoft 365 compliance center. The compliance department plans to export the existing policies, and then produce a CSV file that contains matching labels and policies that are compatible with records management in Microsoft 365. The CSV file must be used to configure records management in Microsoft 365.

Executive Requirements -
You must be able to restore all email received by Fabrikam executives for up to three years after an email is received, even if the email was deleted permanently.

Question
DRAG DROP -
You need to recommend a solution that meets the sales requirements.
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. (Choose three.)
Select and Place:



Correct Answer:

Actions	Answer Area
Create a sensitive info type that contains an EDM classification.	Upload sample contract documents to a seed content folder in SharePoint Online.
	Create a trainable classifier.
Create a sensitive info type that contains a keywords classification.	Create an auto-labeling policy for sensitivity labels.
Create a sensitive info type that contains a document fingerprint.	

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

Eltooth Highly Voted 2 years, 4 months ago

Answer looks correct as sales contracts are received in multiple formats via email. A sample set should be upload into SPO then using trainable classifieds to identify trends, auto apply a sensitivity label.

"Users in the sales department receive draft sales contracts from customers by email. The sales contracts are written by the customers and are not in a standard format."

upvoted 16 times

xswe Most Recent 7 months, 3 weeks ago

We have to know how to detect and classify the sales contract, these contracts are written by customers and they are not in a standard format so a Fingerprint wont work.
We need a trainable classifier.

Upload the samples of the contracts in SharePoint Online as seed content.
Create a trainable classifier that will use the seed content to detect the contracts.
Create an auto-labeling policy to automatically apply the sensitvity label.

upvoted 4 times

mcas 1 year, 1 month ago

I was put off by this "applied automatically to all draft and finalized sales contracts."
how do you configure this condition in the policy?

upvoted 2 times

Introductory Info

Case study -

This is a case study. Case studies are not timed separately. You can use as much exam time as you would like to complete each case. However, there may be additional case studies and sections on this exam. You must manage your time to ensure that you are able to complete all questions included on this exam in the time provided.

To answer the questions included in a case study, you will need to reference information that is provided in the case study. Case studies might contain exhibits and other resources that provide more information about the scenario that is described in the case study. Each question is independent of the other questions in this case study.

At the end of this case study, a review screen will appear. This screen allows you to review your answers and to make changes before you move to the next section of the exam. After you begin a new section, you cannot return to this section.

To start the case study -

To display the first question in this case study, click the Next button. Use the buttons in the left pane to explore the content of the case study before you answer the questions. Clicking these buttons displays information such as business requirements, existing environment, and problem statements. If the case study has an All Information tab, note that the information displayed is identical to the information displayed on the subsequent tabs. When you are ready to answer a question, click the Question button to return to the question.

Overview -

Fabrikam, Inc. is a consulting company that has a main office in Montreal and six branch offices in New York, Seattle, Miami, Houston, Los Angeles, and
Vancouver.

Existing Environment -

Cloud Environment -

Fabrikam has a Microsoft 365 tenant that contains the following resources:

An on-premises Active Directory domain named corp.fabrikam.com that syncs to an Azure Active Directory (Azure AD) tenant

Microsoft Cloud App Security connectors configured for all supported cloud applications used by the company

Some users have company Dropbox accounts.

Compliance Configuration -

Fabrikam has the following in the Microsoft 365 compliance center:

A data loss prevention (DLP) policy is configured. The policy displays a tooltip to users. Users can provide a business justification to override a DLP policy violation.

The Azure Information Protection unified labeling scanner is installed and configured.

A sensitivity label named Fabrikam Confidential is configured.

An existing third-party records management system is managed by the compliance department.

Human Resources (HR) Management System

The HR department has an Azure SQL database that contains employee information. Each employee has a unique 12-character alphanumeric ID. The database contains confidential employee attributes including payroll information, date of birth, and personal contact details.

On-Premises Environment -

You have an on-premises file server that runs Windows Server 2019 and stores Microsoft Office documents in a shared folder named Data.

All end-user computers are joined to the corp.fabrikam.com domain and run a third-party antimalware application.

Business Processes -

Sales Contracts -

Users in the sales department receive draft sales contracts from customers by email. The sales contracts are written by the customers and are not in a standard format.

Employment Applications -

Employment applications and resumes are received by HR department managers and stored in either mailboxes, Microsoft SharePoint Online sites, OneDrive for
Business folders, or Microsoft Teams channels.

The employment application form is downloaded from SharePoint Online and a serial number is assigned to each application.
The resumes are written by the applicants and are in any format.

Requirements -

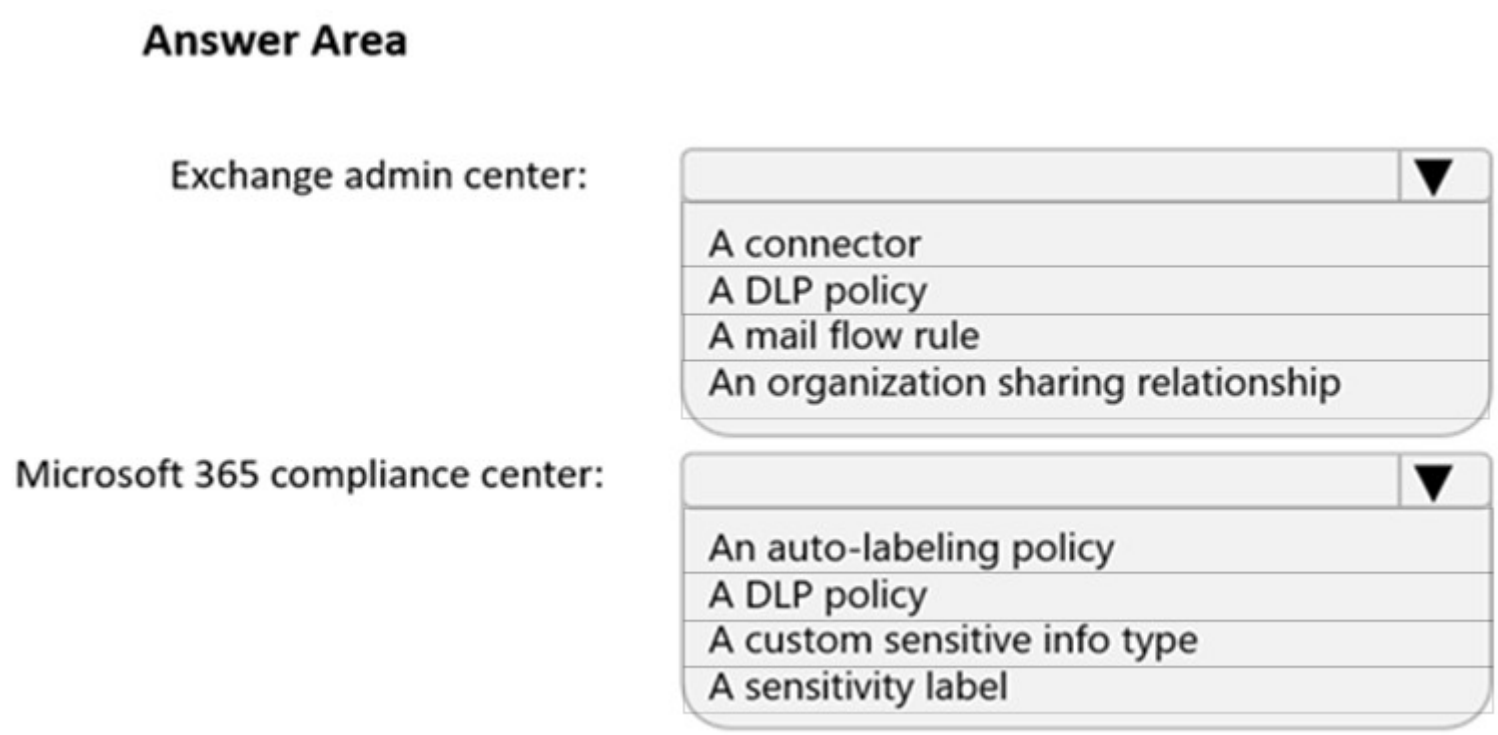
HR Requirements -
You need to create a DLP policy that will notify the HR department of a DLP policy violation if a document that contains confidential employee attributes is shared externally. The DLP policy must use an Exact Data Match (EDM) classification derived from a CSV export of the HR department database.
The HR department identifies the following requirements for handling employment applications:
Resumes must be identified automatically based on similarities to other resumes received in the past.
Employment applications and resumes must be deleted automatically two years after the applications are received.
Documents and emails that contain an application serial number must be identified automatically and marked as an employment application.

Sales Requirements -
A sensitivity label named Sales Contract must be applied automatically to all draft and finalized sales contracts.

Compliance Requirements -
Fabrikam identifies the following compliance requirements:
All DLP policies must be applied to computers that run Windows 10, with the least possible changes to the computers.
Users in the compliance department must view the justification provided when a user receives a tooltip notification for a DLP violation.
If a document that has the Fabrikam Confidential sensitivity label applied is uploaded to Dropbox, the file must be deleted automatically.
The Fabrikam Confidential sensitivity label must be applied to existing Microsoft Word documents in the Data shared folder that have a document footer containing the following string: Company use only.
Users must be able to manually select that email messages are sent encrypted. The encryption will use Office 365 Message Encryption (OME) v2.
Any email containing an attachment that has the Fabrikam Confidential sensitivity label applied must be encrypted automatically by using OME.
Existing policies configured in the third-party records management system must be replaced by using Records management in the Microsoft 365 compliance center. The compliance department plans to export the existing policies, and then produce a CSV file that contains matching labels and policies that are compatible with records management in Microsoft 365. The CSV file must be used to configure records management in Microsoft 365.

Executive Requirements -
You must be able to restore all email received by Fabrikam executives for up to three years after an email is received, even if the email was deleted permanently.

Question
HOTSPOT -
You need to implement a solution to encrypt email. The solution must meet the compliance requirements.
What should you create in the Exchange admin center and the Microsoft 365 compliance center? To answer, select the appropriate options in the answer area.
NOTE: Each correct selection is worth one point.
Hot Area:



Answer Area

Exchange admin center:

- A connector
- A DLP policy
- A mail flow rule
- An organization sharing relationship

Correct Answer:

Microsoft 365 compliance center:

- An auto-labeling policy
- A DLP policy
- A custom sensitive info type
- A sensitivity label

Users must be able to manually select that email messages are sent encrypted. The encryption will use Office 365 Message Encryption (OME) v2. Any email containing an attachment that has the Fabrikam Confidential sensitivity label applied must be encrypted automatically by using OME.

Reference:

https://docs.microsoft.com/en-us/microsoft-365/compliance/ome-sensitive-info-types?view=o365-worldwide

sergioandreslq Highly Voted 1 year, 11 months ago

1. A mail flow rule
2. A DLP Policy that includes locations ODfB, SPO, and Exchange Online.
Condition: If Sensitivity Label "Fabrikam Confidential" is present
Action: Encrypt

upvoted 21 times

SnottyPudding 1 year, 8 months ago

I agree.
Step 1: Choose what you want to monitor (sensitivity label).
Step 2: Choose where you want to monitor (Exchange, SP, OD, etc)
Step 3: Choose condition that must be matched (item has specific sensitivity label "Fabrikam Confidential")
Step 4: Action: Encrypt
https://docs.microsoft.com/en-us/microsoft-365/compliance/dlp-learn-about-dlp?view=o365-worldwide
https://gcits.com/office-365-message-encryption-encrypt-only-template-available-in-office-365-unified-dlp/#:~:text=Enabling%20Encrypt%2DOnly%20via%20a,%3A%2F%2Fprotection.office.com.

upvoted 2 times

HardcodedCloud Highly Voted 1 year, 11 months ago

Should be Mail Flow & an auto-labeling Policy.
As mentioned in the case study that "A sensitivity label named Fabrikam Confidential is configured." So you need an auto-labeling policy to apply the label to al documents, then the mail flow in Exchange Online will encrypt automatically any email with attachment that has "Fabrikam Confidential" label applied.

upvoted 11 times

omnomsnom Most Recent 1 month ago

Surely you need the mail flow rule or DLP policy, but not both?

upvoted 1 times

HDEIWDEOW 3 months, 2 weeks ago

Got this question on exam on 17th August

upvoted 1 times

xswe 7 months, 3 weeks ago

To configure encrypted email message we need,
Exchange = Mail flow rule
M365 compliance center = DLP rule

upvoted 1 times

luissaro 7 months, 2 weeks ago

also auto-labeling policy is set in microsoft purview compliance portal and it is indeed the requested action since they have already the label and they need to establish a process in which if there is that label ome encryption will be triggered. the only way to apply a label is through policy

upvoted 1 times

mcas 1 year, 1 month ago

For this part "Any email containing an attachment that has the Fabrikam Confidential sensitivity label applied must be encrypted automatically by using OME."

you don't need a custom sensitive info type, you can use a Mail Flow Rule where you block attachments that use a sensitivity label MSIP_Label_ ed4411cc-bec4-444a-b279-c404aaad79d6_Enabled=true

upvoted 2 times

mcas 1 year, 1 month ago

To satisfy this condition "Users must be able to manually select that email messages are sent encrypted" you need a sensitivity label. You would create one for items (files and emails) with the encryption settings

Sensitivity labels are used to classify email messages, documents, sites, and more. When a label is applied (automatically or by the user), the content or site is protected based on the settings you choose. For example, you can create labels that encrypt files, add content marking, and control user access to specific sites

upvoted 3 times

mcas 1 year, 1 month ago

this is the example directly from Microsoft

https://learn.microsoft.com/en-us/previous-versions/azure/information-protection/configure-exo-rules#example-2-rule-that-applies-the-encrypt-only-option-to-emails-when-they-have-attachments-that-are-labeled-confidential--partners-and-these-emails-are-sent-outside-the-organization

upvoted 2 times

JamesM9 1 year, 7 months ago

I have tested this today and the answer is Mail Flow/DLP. The case study states that a sensitivity label has already been created, so all we need to do is find a way to apply this and encrypt.

When creating a DLP policy we can specify the locations, select the (already created) "Fabrikam Confidential" label and then add an action to restrict/encrypt.

When attempting to create an auto-labelling policy, we are asked to add a sensitive info type, which would need to be created. Since we have everything all ready to go in a DLP policy (and the label has already been created) then this is the quickest method.

Therefore, the answer is - Mail Flow/DLP.

upvoted 5 times

nupagazi 1 year, 10 months ago

Customer sensivetive info typeis correct ! To configure DLP you have to use sensitive label. In order to creat sensitive label you need sensiive info type

upvoted 1 times

PrettyFlyWifi 1 year, 9 months ago

This will confuse people, this isn't correct. You do not NEED a sensitive info type to create a sensitivity label. You can create whatever labels you want and let users manually apply them for labelling purposes. Go and create a general label with no settings until you get to the end and you'll see you can simply create a label. No SIT needed.

upvoted 1 times

Pravda 1 year, 10 months ago

On exam 1/20/2022

upvoted 1 times

Question #1 *Topic 8*

Introductory Info

Case study -

This is a case study. Case studies are not timed separately. You can use as much exam time as you would like to complete each case. However, there may be additional case studies and sections on this exam. You must manage your time to ensure that you are able to complete all questions included on this exam in the time provided.

To answer the questions included in a case study, you will need to reference information that is provided in the case study. Case studies might contain exhibits and other resources that provide more information about the scenario that is described in the case study. Each question is independent of the other questions in this case study.

At the end of this case study, a review screen will appear. This screen allows you to review your answers and to make changes before you move to the next section of the exam. After you begin a new section, you cannot return to this section.

To start the case study -

To display the first question in this case study, click the Next button. Use the buttons in the left pane to explore the content of the case study before you answer the questions. Clicking these buttons displays information such as business requirements, existing environment, and problem statements. If the case study has an All Information tab, note that the information displayed is identical to the information displayed on the subsequent tabs. When you are ready to answer a question, click the Question button to return to the question.

Overview -

Contoso, Ltd. is a consulting company that has a main office in Montreal and three branch offices in Seattle, Boston, and Johannesburg.

Existing Environment -

Microsoft 365 Environment -

Contoso has a Microsoft 365 E5 tenant. The tenant contains the administrative user accounts shown in the following table.

Name	Role
Admin1	Global Reader
Admin2	Compliance data administrator
Admin3	Compliance administrator
Admin4	Security operator
Admin5	Security administrator

Users store data in the following locations:

SharePoint sites

OneDrive accounts

Exchange email

Exchange public folders

Teams chats

Teams channel messages

When users in the research department create documents, they must add a 10-digit project code to each document. Project codes that start with the digits 999 are confidential.

SharePoint Online Environment -

Contoso has four Microsoft SharePoint Online sites named Site1, Site2, Site3, and Site4.

Site2 contains the files shown in the following table.

Name	Number of SWIFT codes in the file
File1.docx	1
File2.bmp	4
File3.txt	3
File4.xlsx	7

Two users named User1 and User2 are assigned roles for Site2 as shown in the following table.

User	Role
User1	Site owner
User2	Site visitor

Site3 stores documents related to the company's projects. The documents are organized in a folder hierarchy based on the project.
Site4 has the following two retention policies applied:
Name: Site4RetentionPolicy1
- Locations to apply the policy: Site4
- Delete items older than: 2 years
- Delete content based on: When items were created
Name: Site4RetentionPolicy2
- Locations to apply the policy: Site4
- Retain items for a specific period: 4 years
- Start the retention period based on: When items were created
- At the end of the retention period: Do nothing

Problem Statements -
Management at Contoso is concerned about data leaks. On several occasions, confidential research department documents were leaked.

Requirements -

Planned Changes -
Contoso plans to create the following data loss prevention (DLP) policy:
Name: DLPpolicy1
Locations to apply the policy: Site2
Conditions:
- Content contains any of these sensitive info types: SWIFT Code
- Instance count: 2 to any
Actions: Restrict access to the content

Technical Requirements -
Contoso must meet the following technical requirements:
All administrative users must be able to review DLP reports.
Whenever possible, the principle of least privilege must be used.
For all users, all Microsoft 365 data must be retained for at least one year.
Confidential documents must be detected and protected by using Microsoft 365.
Site1 documents that include credit card numbers must be labeled automatically.
All administrative users must be able to create Microsoft 365 sensitivity labels.
After a project is complete, the documents in Site3 that relate to the project must be retained for 10 years.

Question
HOTSPOT -
You need to meet the technical requirements for the confidential documents.
What should you create 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:

Answer Area

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

Answer Area

Create first:

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

Correct Answer:

Use for detection method:

- Dictionary
- File type
- Keywords
- Regular expression

Reference:
https://docs.microsoft.com/en-us/microsoft-365/compliance/create-a-custom-sensitive-information-type?view=o365-worldwide

Neil_Liu Highly Voted 2 years, 4 months ago
The given answer is correct.
Sensitive information types :
Identifies sensitive data by using built-in or custom regular expressions or a function. Corroborative evidence includes keywords, confidence levels, and proximity.
https://docs.microsoft.com/en-us/microsoft-365/compliance/information-protection?view=o365-worldwide
upvoted 12 times

izgi43 Most Recent 3 weeks ago
on the exam thu nov 9
upvoted 1 times

Gesbie 3 months, 3 weeks ago
was on Exam August 9, 2023
upvoted 1 times

xswe 7 months, 3 weeks ago
To be able to detect these documents in order to protect these files we need to first of create a sensitive info type and regex to detect the files
upvoted 2 times

wooyourdaddy 1 year, 5 months ago
I wrote the exam today, this question was on it, I choose the provided answers, scored 890!
upvoted 3 times

Pravda 1 year, 10 months ago
On exam 1/20/2022
upvoted 1 times

ZZIN 2 years, 5 months ago
Correct answer?
Create first:A DLP policy
Use for detection method:Keywords
OK?
upvoted 1 times

Anker 2 years, 5 months ago
I don't understand why this can't be a DLP policy. If it's asking for detection and protection DLP to me looks to be the only one to fit that protection requirement. Unless I'm reading into this differently. Not sure why this would require you to create a new sensitive info type since its looking for SWIFT codes and credit card numbers both of these are available as built in sensitive info types already.
upvoted 1 times

test123123 2 years, 5 months ago
To detect the sensitiv confidential (999) data in the 10 digit code, you must first make a sensitive information type with the method regular expression.
upvoted 12 times

olsi 2 years, 6 months ago
it has to be keywords, as "confidential research department documents were leaked". Thus keywords
upvoted 1 times

Introductory Info

Case study -

This is a case study. Case studies are not timed separately. You can use as much exam time as you would like to complete each case. However, there may be additional case studies and sections on this exam. You must manage your time to ensure that you are able to complete all questions included on this exam in the time provided.

To answer the questions included in a case study, you will need to reference information that is provided in the case study. Case studies might contain exhibits and other resources that provide more information about the scenario that is described in the case study. Each question is independent of the other questions in this case study.

At the end of this case study, a review screen will appear. This screen allows you to review your answers and to make changes before you move to the next section of the exam. After you begin a new section, you cannot return to this section.

To start the case study -

To display the first question in this case study, click the Next button. Use the buttons in the left pane to explore the content of the case study before you answer the questions. Clicking these buttons displays information such as business requirements, existing environment, and problem statements. If the case study has an All Information tab, note that the information displayed is identical to the information displayed on the subsequent tabs. When you are ready to answer a question, click the Question button to return to the question.

Overview -

Contoso, Ltd. is a consulting company that has a main office in Montreal and three branch offices in Seattle, Boston, and Johannesburg.

Existing Environment -

Microsoft 365 Environment -

Contoso has a Microsoft 365 E5 tenant. The tenant contains the administrative user accounts shown in the following table.

Name	Role
Admin1	Global Reader
Admin2	Compliance data administrator
Admin3	Compliance administrator
Admin4	Security operator
Admin5	Security administrator

Users store data in the following locations:

SharePoint sites

OneDrive accounts

Exchange email

Exchange public folders

Teams chats

Teams channel messages

When users in the research department create documents, they must add a 10-digit project code to each document. Project codes that start with the digits 999 are confidential.

SharePoint Online Environment -

Contoso has four Microsoft SharePoint Online sites named Site1, Site2, Site3, and Site4.

Site2 contains the files shown in the following table.

Name	Number of SWIFT codes in the file
File1.docx	1
File2.bmp	4
File3.txt	3
File4.xlsx	7

Two users named User1 and User2 are assigned roles for Site2 as shown in the following table.

User	Role
User1	Site owner
User2	Site visitor

Site3 stores documents related to the company's projects. The documents are organized in a folder hierarchy based on the project.

Site4 has the following two retention policies applied:

Name: Site4RetentionPolicy1
- Locations to apply the policy: Site4
- Delete items older than: 2 years
- Delete content based on: When items were created
Name: Site4RetentionPolicy2
- Locations to apply the policy: Site4
- Retain items for a specific period: 4 years
- Start the retention period based on: When items were created
- At the end of the retention period: Do nothing

Problem Statements -
Management at Contoso is concerned about data leaks. On several occasions, confidential research department documents were leaked.

Requirements -

Planned Changes -
Contoso plans to create the following data loss prevention (DLP) policy:
Name: DLPpolicy1
Locations to apply the policy: Site2
Conditions:
- Content contains any of these sensitive info types: SWIFT Code
- Instance count: 2 to any
Actions: Restrict access to the content

Technical Requirements -
Contoso must meet the following technical requirements:
All administrative users must be able to review DLP reports.
Whenever possible, the principle of least privilege must be used.
For all users, all Microsoft 365 data must be retained for at least one year.
Confidential documents must be detected and protected by using Microsoft 365.
Site1 documents that include credit card numbers must be labeled automatically.
All administrative users must be able to create Microsoft 365 sensitivity labels.
After a project is complete, the documents in Site3 that relate to the project must be retained for 10 years.

Question
You need to meet the technical requirements for the Site3 documents.
What should you create?

A. a retention policy that has Only delete items when they reach a certain age selected

B. a retention label policy and a retention label that uses an event

C. a sensitive info type that uses a regular expression and a sensitivity label

D. a sensitive info type that uses a dictionary and a sensitivity label

Correct Answer: *B*
Reference:
https://docs.microsoft.com/en-us/microsoft-365/compliance/event-driven-retention?view=o365-worldwide

shanti0091 Highly Voted 2 years, 4 months ago
correct
upvoted 5 times

Gesbie Most Recent 3 months, 3 weeks ago
was on Exam August 9, 2023
upvoted 1 times

xswe 7 months, 3 weeks ago
To be able to trigger a retention period on a specific event such as end of a project we need to create a retention label poilicy and a retention label that uses an event as trigger

upvoted 1 times

wooyourdaddy 1 year, 5 months ago

Selected Answer: B

I wrote the exam today, this question was on it, I choose B, scored 890!

upvoted 3 times

Pravda 1 year, 10 months ago

On exam 1/20/2022

upvoted 1 times

ExamReviewerIZ 2 years, 1 month ago

I get the retention label policy for the 10 years retention of confidential documents.

But why the "event" type?

upvoted 2 times

[Removed] 2 years ago

The "trigger" of the event is when the project is completed. This is the Event Type.

upvoted 6 times

Eltooth 2 years, 4 months ago

Correct - B.

upvoted 4 times

Introductory Info

Case study -

This is a case study. Case studies are not timed separately. You can use as much exam time as you would like to complete each case. However, there may be additional case studies and sections on this exam. You must manage your time to ensure that you are able to complete all questions included on this exam in the time provided.

To answer the questions included in a case study, you will need to reference information that is provided in the case study. Case studies might contain exhibits and other resources that provide more information about the scenario that is described in the case study. Each question is independent of the other questions in this case study.

At the end of this case study, a review screen will appear. This screen allows you to review your answers and to make changes before you move to the next section of the exam. After you begin a new section, you cannot return to this section.

To start the case study -

To display the first question in this case study, click the Next button. Use the buttons in the left pane to explore the content of the case study before you answer the questions. Clicking these buttons displays information such as business requirements, existing environment, and problem statements. If the case study has an All Information tab, note that the information displayed is identical to the information displayed on the subsequent tabs. When you are ready to answer a question, click the Question button to return to the question.

Overview -

Contoso, Ltd. is a consulting company that has a main office in Montreal and three branch offices in Seattle, Boston, and Johannesburg.

Existing Environment -

Microsoft 365 Environment -

Contoso has a Microsoft 365 E5 tenant. The tenant contains the administrative user accounts shown in the following table.

Name	Role
Admin1	Global Reader
Admin2	Compliance data administrator
Admin3	Compliance administrator
Admin4	Security operator
Admin5	Security administrator

Users store data in the following locations:

SharePoint sites

OneDrive accounts

Exchange email

Exchange public folders

Teams chats

Teams channel messages

When users in the research department create documents, they must add a 10-digit project code to each document. Project codes that start with the digits 999 are confidential.

SharePoint Online Environment -

Contoso has four Microsoft SharePoint Online sites named Site1, Site2, Site3, and Site4.

Site2 contains the files shown in the following table.

Name	Number of SWIFT codes in the file
File1.docx	1
File2.bmp	4
File3.txt	3
File4.xlsx	7

Two users named User1 and User2 are assigned roles for Site2 as shown in the following table.

User	Role
User1	Site owner
User2	Site visitor

Site3 stores documents related to the company's projects. The documents are organized in a folder hierarchy based on the project.

Site4 has the following two retention policies applied:

Name: Site4RetentionPolicy1
- Locations to apply the policy: Site4
- Delete items older than: 2 years
- Delete content based on: When items were created
Name: Site4RetentionPolicy2
- Locations to apply the policy: Site4
- Retain items for a specific period: 4 years
- Start the retention period based on: When items were created
- At the end of the retention period: Do nothing

Problem Statements -
Management at Contoso is concerned about data leaks. On several occasions, confidential research department documents were leaked.

Requirements -

Planned Changes -
Contoso plans to create the following data loss prevention (DLP) policy:
Name: DLPpolicy1
Locations to apply the policy: Site2
Conditions:
- Content contains any of these sensitive info types: SWIFT Code
- Instance count: 2 to any
Actions: Restrict access to the content

Technical Requirements -
Contoso must meet the following technical requirements:
All administrative users must be able to review DLP reports.
Whenever possible, the principle of least privilege must be used.
For all users, all Microsoft 365 data must be retained for at least one year.
Confidential documents must be detected and protected by using Microsoft 365.
Site1 documents that include credit card numbers must be labeled automatically.
All administrative users must be able to create Microsoft 365 sensitivity labels.
After a project is complete, the documents in Site3 that relate to the project must be retained for 10 years.

Question
You need to meet the technical requirements for the creation of the sensitivity labels.
To which user or users must you grant the Sensitivity label administrator role?

A. Admin1, Admin2, Admin4, and Admin5 only

B. Admin1, Admin2, and Admin3 only

C. Admin1 only

D. Admin1 and Admin4 only

E. Admin1 and Admin5 only

Correct Answer: *D*
Compliance Data Administrator, Compliance Administrator, and Security Administrator already have the required permissions to create the labels.
Reference:
https://docs.microsoft.com/en-us/microsoft-365/compliance/get-started-with-sensitivity-labels?view=o365-worldwide#permissions-required-to-create-and-manage- sensitivity-labels

HDEIWDEOW 3 months, 2 weeks ago
Got this question on exam on 17th August
upvoted 1 times

Gesbie 3 months, 3 weeks ago
was on Exam August 9, 2023

upvoted 1 times

xswe 7 months, 3 weeks ago

Since administrative users must be able to create sensitivity labels we need to grant Global reader and Security Operator with role Sensitivity label administrator role. Both Compliance data administrator, compliance administrator and security administrator can already create sensitivity labels

upvoted 2 times

JCkD4Ni3L 11 months, 2 weeks ago

Selected Answer: D

Interesting enough, none of the answers are good.

The correct answer would be Admin1, Admin4 and Admin5 as only the Compliance Administrator, Compliance Data Administrator and Global Administrator role have the necessary rights to manage and create Labels in the Compliance Center.

Simply search for the right "microsoft.office365.complianceManager/allEntities/allTasks" within the following right section: https://learn.microsoft.com/en-us/azure/active-directory/roles/permissions-reference

Closest answer would be Admin1 and Admin4, thus D.

upvoted 1 times

mcas 1 year, 1 month ago

there is no such thing as "sensitivity label administrator"

upvoted 2 times

JCkD4Ni3L 11 months, 2 weeks ago

https://learn.microsoft.com/en-us/microsoft-365/compliance/get-started-with-sensitivity-labels?view=o365-worldwide#permissions-required-to-create-and-manage-sensitivity-labels

upvoted 3 times

mcas 9 months, 3 weeks ago

I stand corrected

upvoted 2 times

wooyourdaddy 1 year, 5 months ago

Selected Answer: D

I wrote the exam today, this question was on it, I choose D, scored 890!

upvoted 1 times

mcas 1 year, 1 month ago

this is a fake review like it appears all over other questions, because this site is run by dodgy people

upvoted 6 times

PrettyFlyWifi 1 year, 9 months ago

Looks correct. Both Global Reader and Security Operator do NOT have the sensitivity label admin role, (check the roles in protection.office.com) and the requirement is to grant all admins the rights to create sensitivity labels. So Admin 1 and Admin 4 need to be granted the sensitivity label admin role.

upvoted 3 times

MSROCKS 1 year, 10 months ago

Permissions required to create and manage sensitivity labels
Members of your compliance team who will create sensitivity labels need permissions to the Microsoft 365 compliance center.

By default, global administrators for your tenant have access to this admin center and can give compliance officers and other people access, without giving them all of the permissions of a tenant admin. For this delegated limited admin access, add users to the Compliance Data Administrator, Compliance Administrator, or Security Administrator role group.

Alternatively to using the default roles, you can create a new role group and add either Sensitivity Label Administrator or Organization Configuration roles to this group. For a read-only role, use Sensitivity Label Reader.

https://docs.microsoft.com/en-us/microsoft-365/compliance/get-started-with-sensitivity-labels?view=o365-worldwide

upvoted 2 times

Pravda 1 year, 10 months ago

On exam 1/20/2022

upvoted 1 times

xofowi5140 2 years, 4 months ago

Compliance Administrator don't have
Sensitivity Label Administrator role

upvoted 2 times

ExamReviewerIZ 2 years, 1 month ago

Yes, they do have it. Complaince Administrator and Compliance Data Administrador can create Sensitivity Labels, thus they don't need to any other permissions assigned

upvoted 2 times

pheb 2 years, 3 months ago

correct, it should be Admin 1, 3 and 4

upvoted 2 times

jcgonzalez1978 2 years, 3 months ago

You sure? Per the link provided in the answer:
By default, global administrators for your tenant have access to this admin center and can give compliance officers and other people access, without giving them all of the permissions of a tenant admin. For this delegated limited admin access, add users to the Compliance Data Administrator, Compliance Administrator, or Security Administrator role group.

upvoted 5 times

shanti0091 2 years, 4 months ago

True, correct

upvoted 4 times

Introductory Info

Case study -

This is a case study. Case studies are not timed separately. You can use as much exam time as you would like to complete each case. However, there may be additional case studies and sections on this exam. You must manage your time to ensure that you are able to complete all questions included on this exam in the time provided.

To answer the questions included in a case study, you will need to reference information that is provided in the case study. Case studies might contain exhibits and other resources that provide more information about the scenario that is described in the case study. Each question is independent of the other questions in this case study.

At the end of this case study, a review screen will appear. This screen allows you to review your answers and to make changes before you move to the next section of the exam. After you begin a new section, you cannot return to this section.

To start the case study -

To display the first question in this case study, click the Next button. Use the buttons in the left pane to explore the content of the case study before you answer the questions. Clicking these buttons displays information such as business requirements, existing environment, and problem statements. If the case study has an All Information tab, note that the information displayed is identical to the information displayed on the subsequent tabs. When you are ready to answer a question, click the Question button to return to the question.

Overview -

Contoso, Ltd. is a consulting company that has a main office in Montreal and three branch offices in Seattle, Boston, and Johannesburg.

Existing Environment -

Microsoft 365 Environment -

Contoso has a Microsoft 365 E5 tenant. The tenant contains the administrative user accounts shown in the following table.

Name	Role
Admin1	Global Reader
Admin2	Compliance data administrator
Admin3	Compliance administrator
Admin4	Security operator
Admin5	Security administrator

Users store data in the following locations:

SharePoint sites

OneDrive accounts

Exchange email

Exchange public folders

Teams chats

Teams channel messages

When users in the research department create documents, they must add a 10-digit project code to each document. Project codes that start with the digits 999 are confidential.

SharePoint Online Environment -

Contoso has four Microsoft SharePoint Online sites named Site1, Site2, Site3, and Site4.

Site2 contains the files shown in the following table.

Name	Number of SWIFT codes in the file
File1.docx	1
File2.bmp	4
File3.txt	3
File4.xlsx	7

Two users named User1 and User2 are assigned roles for Site2 as shown in the following table.

User	Role
User1	Site owner
User2	Site visitor

Site3 stores documents related to the company's projects. The documents are organized in a folder hierarchy based on the project.

Site4 has the following two retention policies applied:

Name: Site4RetentionPolicy1
- Locations to apply the policy: Site4
- Delete items older than: 2 years
- Delete content based on: When items were created
Name: Site4RetentionPolicy2
- Locations to apply the policy: Site4
- Retain items for a specific period: 4 years
- Start the retention period based on: When items were created
- At the end of the retention period: Do nothing

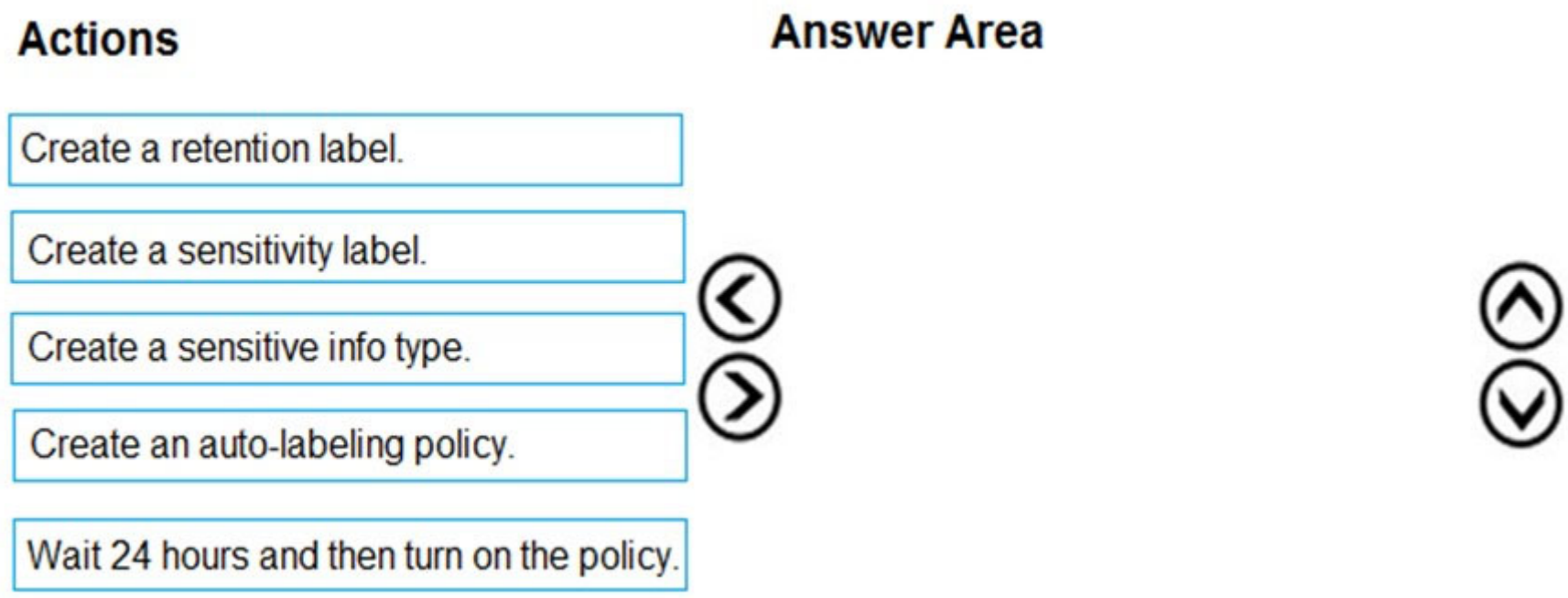
Problem Statements -
Management at Contoso is concerned about data leaks. On several occasions, confidential research department documents were leaked.

Requirements -

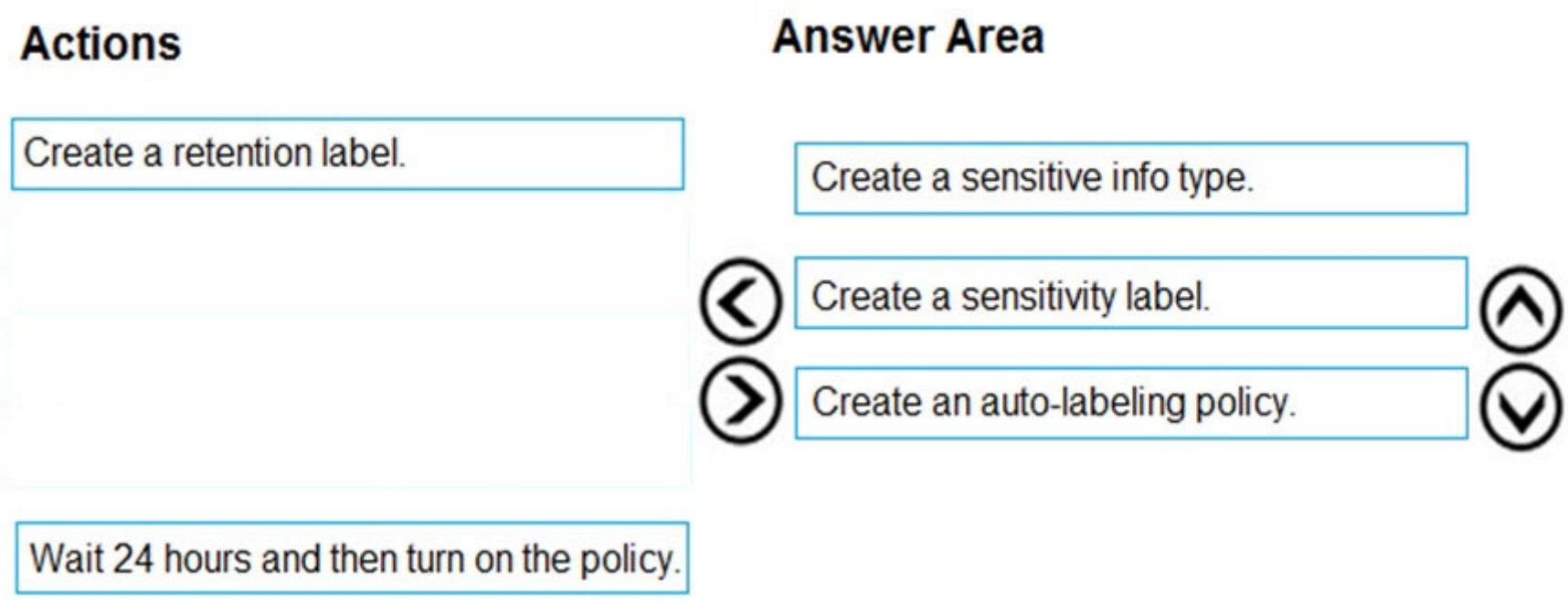
Planned Changes -
Contoso plans to create the following data loss prevention (DLP) policy:
Name: DLPpolicy1
Locations to apply the policy: Site2
Conditions:
- Content contains any of these sensitive info types: SWIFT Code
- Instance count: 2 to any
Actions: Restrict access to the content

Technical Requirements -
Contoso must meet the following technical requirements:
All administrative users must be able to review DLP reports.
Whenever possible, the principle of least privilege must be used.
For all users, all Microsoft 365 data must be retained for at least one year.
Confidential documents must be detected and protected by using Microsoft 365.
Site1 documents that include credit card numbers must be labeled automatically.
All administrative users must be able to create Microsoft 365 sensitivity labels.
After a project is complete, the documents in Site3 that relate to the project must be retained for 10 years.

Question
DRAG DROP -
You need to meet the technical requirements for the Site1 documents.
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.
Select and Place:



Correct Answer:



Reference:
https://docs.microsoft.com/en-us/microsoft-365/compliance/apply-sensitivity-label-automatically?view=o365-worldwide#how-to-configure-auto-labeling-policies-for- sharepoint-onedrive-and-exchange

[Removed] Highly Voted 2 years ago
Wrong, Microsoft 365 already has the confidential information type "Credit Card Number", so it is not necessary to create a new one. Correct sequence:

1- Create a Sensitivity label
2- Crate an auto-labeling policy
3- Wait 24 hours and then turn on the policy (from the simulation mode).
upvoted 33 times

mcas 1 year, 1 month ago
agree but there is no need to wait 24h before turning on the policy, it doesn't make any different to turn it on right away.
upvoted 2 times

us3r 1 year, 11 months ago
Agree.

Also on MS-101
upvoted 2 times

Romeokton Most Recent 4 days, 19 hours ago
On exam November 2023
upvoted 1 times

HDEIWDEOW 3 months, 2 weeks ago
Got this question on exam on 17th August
upvoted 1 times

Gesbie 3 months, 3 weeks ago
was on Exam August 9, 2023
upvoted 1 times

CharlieGolf 8 months, 1 week ago
Should be the following based on link below (see how simulation is required and takes at least 12 hours; only auto-turns on if ignored for 7 days):
1 - Create sensitivity label
2 - Create auto-labeling policy (requires sim mode before enabling)
3 - Wait 24 hours and then turn on (after sim mode runs)
Ref: https://learn.microsoft.com/en-us/microsoft-365/compliance/apply-sensitivity-label-automatically?view=o365-worldwide#how-to-configure-auto-labeling-policies-for-sharepoint-onedrive-and-exchange
upvoted 2 times

nupagazi 1 year, 10 months ago
agreed
upvoted 1 times

Pravda 1 year, 10 months ago
On exam 1/20/2022
upvoted 1 times

Question #1 *Topic 9*

Introductory Info

Case study -

This is a case study. Case studies are not timed separately. You can use as much exam time as you would like to complete each case. However, there may be additional case studies and sections on this exam. You must manage your time to ensure that you are able to complete all questions included on this exam in the time provided.

To answer the questions included in a case study, you will need to reference information that is provided in the case study. Case studies might contain exhibits and other resources that provide more information about the scenario that is described in the case study. Each question is independent of the other questions in this case study.

At the end of this case study, a review screen will appear. This screen allows you to review your answers and to make changes before you move to the next section of the exam. After you begin a new section, you cannot return to this section.

To start the case study -

To display the first question in this case study, click the Next button. Use the buttons in the left pane to explore the content of the case study before you answer the questions. Clicking these buttons displays information such as business requirements, existing environment, and problem statements. If the case study has an All Information tab, note that the information displayed is identical to the information displayed on the subsequent tabs. When you are ready to answer a question, click the Question button to return to the question.

Overview -

Fabrikam, Inc. is a consulting company that has a main office in Montreal and six branch offices in New York, Seattle, Miami, Houston, Los Angeles, and
Vancouver.

Existing Environment -

Cloud Environment -

Fabrikam has a Microsoft 365 tenant that contains the following resources:

An on-premises Active Directory domain named corp.fabrikam.com that syncs to an Azure Active Directory (Azure AD) tenant

Microsoft Cloud App Security connectors configured for all supported cloud applications used by the company

Some users have company Dropbox accounts.

Compliance Configuration -

Fabrikam has the following in the Microsoft 365 compliance center:

A data loss prevention (DLP) policy is configured. The policy displays a tooltip to users. Users can provide a business justification to override a DLP policy violation.

The Azure Information Protection unified labeling scanner is installed and configured.

A sensitivity label named Fabrikam Confidential is configured.

An existing third-party records management system is managed by the compliance department.

Human Resources (HR) Management System

The HR department has an Azure SQL database that contains employee information. Each employee has a unique 12-character alphanumeric ID. The database contains confidential employee attributes including payroll information, date of birth, and personal contact details.

On-Premises Environment -

You have an on-premises file server that runs Windows Server 2019 and stores Microsoft Office documents in a shared folder named Data.

All end-user computers are joined to the corp.fabrikam.com domain and run a third-party antimalware application.

Business Processes -

Sales Contracts -

Users in the sales department receive draft sales contracts from customers by email. The sales contracts are written by the customers and are not in a standard format.

Employment Applications -

Employment applications and resumes are received by HR department managers and stored in either mailboxes, Microsoft SharePoint Online sites, OneDrive for
Business folders, or Microsoft Teams channels.
The employment application form is downloaded from SharePoint Online and a serial number is assigned to each application.
The resumes are written by the applicants and are in any format.

Requirements -

HR Requirements -
You need to create a DLP policy that will notify the HR department of a DLP policy violation if a document that contains confidential employee attributes is shared externally. The DLP policy must use an Exact Data Match (EDM) classification derived from a CSV export of the HR department database.
The HR department identifies the following requirements for handling employment applications:
Resumes must be identified automatically based on similarities to other resumes received in the past.
Employment applications and resumes must be deleted automatically two years after the applications are received.
Documents and emails that contain an application serial number must be identified automatically and marked as an employment application.

Sales Requirements -
A sensitivity label named Sales Contract must be applied automatically to all draft and finalized sales contracts.

Compliance Requirements -
Fabrikam identifies the following compliance requirements:
All DLP policies must be applied to computers that run Windows 10, with the least possible changes to the computers.
Users in the compliance department must view the justification provided when a user receives a tooltip notification for a DLP violation.
If a document that has the Fabrikam Confidential sensitivity label applied is uploaded to Dropbox, the file must be deleted automatically.
The Fabrikam Confidential sensitivity label must be applied to existing Microsoft Word documents in the Data shared folder that have a document footer containing the following string: Company use only.
Users must be able to manually select that email messages are sent encrypted. The encryption will use Office 365 Message Encryption (OME) v2.
Any email containing an attachment that has the Fabrikam Confidential sensitivity label applied must be encrypted automatically by using OME.
Existing policies configured in the third-party records management system must be replaced by using Records management in the Microsoft 365 compliance center. The compliance department plans to export the existing policies, and then produce a CSV file that contains matching labels and policies that are compatible with records management in Microsoft 365. The CSV file must be used to configure records management in Microsoft 365.

Executive Requirements -
You must be able to restore all email received by Fabrikam executives for up to three years after an email is received, even if the email was deleted permanently.

Question
You need to recommend a solution that meets the compliance requirements for viewing DLP tooltip justifications.
What should you recommend?

A. Instruct the compliance department users to review the False positive and override report.

B. Configure a Microsoft Power Automate workflow to route DLP notification emails to the compliance department.

C. Instruct the compliance department users to review the DLP incidents report.

D. Configure an Azure logic app to route DLP notification emails to the compliance department.

Correct Answer: *A*
Reference:
https://docs.microsoft.com/en-us/microsoft-365/compliance/view-the-dlp-reports?view=o365-worldwide

JCkD4Ni3L 11 months, 2 weeks ago
Selected Answer: A
Correct !
upvoted 2 times

wooyourdaddy 1 year, 5 months ago

Selected Answer: A

I wrote the exam today, this question was on it, I choose A, scored 890!

upvoted 3 times

HardcodedCloud 1 year, 11 months ago

DLP false positives and overrides If your DLP policy allows users to override it or report a false positive, this report shows a count of such instances over time.

upvoted 3 times

Introductory Info

Case study -

This is a case study. Case studies are not timed separately. You can use as much exam time as you would like to complete each case. However, there may be additional case studies and sections on this exam. You must manage your time to ensure that you are able to complete all questions included on this exam in the time provided.

To answer the questions included in a case study, you will need to reference information that is provided in the case study. Case studies might contain exhibits and other resources that provide more information about the scenario that is described in the case study. Each question is independent of the other questions in this case study.

At the end of this case study, a review screen will appear. This screen allows you to review your answers and to make changes before you move to the next section of the exam. After you begin a new section, you cannot return to this section.

To start the case study -

To display the first question in this case study, click the Next button. Use the buttons in the left pane to explore the content of the case study before you answer the questions. Clicking these buttons displays information such as business requirements, existing environment, and problem statements. If the case study has an All Information tab, note that the information displayed is identical to the information displayed on the subsequent tabs. When you are ready to answer a question, click the Question button to return to the question.

Overview -

Fabrikam, Inc. is a consulting company that has a main office in Montreal and six branch offices in New York, Seattle, Miami, Houston, Los Angeles, and
Vancouver.

Existing Environment -

Cloud Environment -

Fabrikam has a Microsoft 365 tenant that contains the following resources:

An on-premises Active Directory domain named corp.fabrikam.com that syncs to an Azure Active Directory (Azure AD) tenant

Microsoft Cloud App Security connectors configured for all supported cloud applications used by the company

Some users have company Dropbox accounts.

Compliance Configuration -

Fabrikam has the following in the Microsoft 365 compliance center:

A data loss prevention (DLP) policy is configured. The policy displays a tooltip to users. Users can provide a business justification to override a DLP policy violation.

The Azure Information Protection unified labeling scanner is installed and configured.

A sensitivity label named Fabrikam Confidential is configured.

An existing third-party records management system is managed by the compliance department.

Human Resources (HR) Management System

The HR department has an Azure SQL database that contains employee information. Each employee has a unique 12-character alphanumeric ID. The database contains confidential employee attributes including payroll information, date of birth, and personal contact details.

On-Premises Environment -

You have an on-premises file server that runs Windows Server 2019 and stores Microsoft Office documents in a shared folder named Data.

All end-user computers are joined to the corp.fabrikam.com domain and run a third-party antimalware application.

Business Processes -

Sales Contracts -

Users in the sales department receive draft sales contracts from customers by email. The sales contracts are written by the customers and are not in a standard format.

Employment Applications -

Employment applications and resumes are received by HR department managers and stored in either mailboxes, Microsoft SharePoint Online sites, OneDrive for
Business folders, or Microsoft Teams channels.

The employment application form is downloaded from SharePoint Online and a serial number is assigned to each application.
The resumes are written by the applicants and are in any format.

Requirements -

HR Requirements -
You need to create a DLP policy that will notify the HR department of a DLP policy violation if a document that contains confidential employee attributes is shared externally. The DLP policy must use an Exact Data Match (EDM) classification derived from a CSV export of the HR department database.
The HR department identifies the following requirements for handling employment applications:
Resumes must be identified automatically based on similarities to other resumes received in the past.
Employment applications and resumes must be deleted automatically two years after the applications are received.
Documents and emails that contain an application serial number must be identified automatically and marked as an employment application.

Sales Requirements -
A sensitivity label named Sales Contract must be applied automatically to all draft and finalized sales contracts.

Compliance Requirements -
Fabrikam identifies the following compliance requirements:
All DLP policies must be applied to computers that run Windows 10, with the least possible changes to the computers.
Users in the compliance department must view the justification provided when a user receives a tooltip notification for a DLP violation.
If a document that has the Fabrikam Confidential sensitivity label applied is uploaded to Dropbox, the file must be deleted automatically.
The Fabrikam Confidential sensitivity label must be applied to existing Microsoft Word documents in the Data shared folder that have a document footer containing the following string: Company use only.
Users must be able to manually select that email messages are sent encrypted. The encryption will use Office 365 Message Encryption (OME) v2.
Any email containing an attachment that has the Fabrikam Confidential sensitivity label applied must be encrypted automatically by using OME.
Existing policies configured in the third-party records management system must be replaced by using Records management in the Microsoft 365 compliance center. The compliance department plans to export the existing policies, and then produce a CSV file that contains matching labels and policies that are compatible with records management in Microsoft 365. The CSV file must be used to configure records management in Microsoft 365.

Executive Requirements -
You must be able to restore all email received by Fabrikam executives for up to three years after an email is received, even if the email was deleted permanently.

Question
You need to recommend a solution that meets the compliance requirements for Dropbox.
What should you recommend?

A. Create a file policy in Cloud App Security that uses the built-in DLP inspection method.

B. Edit an existing retention label that enforces the item deletion settings.

C. Create a retention label that enforces the item deletion settings.

D. Create a DLP policy that applies to devices.

Correct Answer: *A*
Reference:
https://docs.microsoft.com/en-us/microsoft-365/compliance/dlp-use-policies-non-microsoft-cloud-apps?view=o365-worldwide

Eltooth Highly Voted 2 years, 4 months ago
A. Correct.
upvoted 6 times

JCkD4Ni3L Most Recent 11 months, 2 weeks ago
Selected Answer: A
A is the correct Answer, mcas is required to fit the bill.
upvoted 1 times

wooyourdaddy 1 year, 5 months ago

Selected Answer: A

I wrote the exam today, this question was on it, I choose A, scored 890!

upvoted 1 times

IAGirl 1 year, 8 months ago

A is correct

upvoted 1 times

AJ2021 1 year, 9 months ago

NO, I think it's D. Create a DLP policy that applies to devices..
DLP policies applied to non-Microsoft apps use Microsoft Defender for Cloud Apps. When the DLP policy for a non-Microsoft app is created, the same policy will be automatically created in Microsoft Defender for Cloud Apps.

upvoted 1 times

PrettyFlyWifi 1 year, 9 months ago

I don't think this is correct. A is still best fit for the answer. If you scope the location of a DLP policy to just Devices, then you don't get any conditions that would allow you to check if any docs have been uploaded to Dropbox. You only get "content contains, file extension is, file type is". So yes you can have a condition on the label, but no Dropbox condition, so this isn't a good fit.
Better fit is still the file policy, when you go to the "Apply to" filter you see the statement "Currently supports SharePoint, OneDrive for Business, Box, Dropbox.". You can use the built-in DLP and do a few things with it, so just seems a better fit here.

upvoted 1 times

Pravda 1 year, 10 months ago

On exam 1/20/2022

upvoted 1 times

Introductory Info

Case study -

This is a case study. Case studies are not timed separately. You can use as much exam time as you would like to complete each case. However, there may be additional case studies and sections on this exam. You must manage your time to ensure that you are able to complete all questions included on this exam in the time provided.

To answer the questions included in a case study, you will need to reference information that is provided in the case study. Case studies might contain exhibits and other resources that provide more information about the scenario that is described in the case study. Each question is independent of the other questions in this case study.

At the end of this case study, a review screen will appear. This screen allows you to review your answers and to make changes before you move to the next section of the exam. After you begin a new section, you cannot return to this section.

To start the case study -

To display the first question in this case study, click the Next button. Use the buttons in the left pane to explore the content of the case study before you answer the questions. Clicking these buttons displays information such as business requirements, existing environment, and problem statements. If the case study has an All Information tab, note that the information displayed is identical to the information displayed on the subsequent tabs. When you are ready to answer a question, click the Question button to return to the question.

Overview -

Fabrikam, Inc. is a consulting company that has a main office in Montreal and six branch offices in New York, Seattle, Miami, Houston, Los Angeles, and
Vancouver.

Existing Environment -

Cloud Environment -

Fabrikam has a Microsoft 365 tenant that contains the following resources:

An on-premises Active Directory domain named corp.fabrikam.com that syncs to an Azure Active Directory (Azure AD) tenant

Microsoft Cloud App Security connectors configured for all supported cloud applications used by the company

Some users have company Dropbox accounts.

Compliance Configuration -

Fabrikam has the following in the Microsoft 365 compliance center:

A data loss prevention (DLP) policy is configured. The policy displays a tooltip to users. Users can provide a business justification to override a DLP policy violation.

The Azure Information Protection unified labeling scanner is installed and configured.

A sensitivity label named Fabrikam Confidential is configured.

An existing third-party records management system is managed by the compliance department.

Human Resources (HR) Management System

The HR department has an Azure SQL database that contains employee information. Each employee has a unique 12-character alphanumeric ID. The database contains confidential employee attributes including payroll information, date of birth, and personal contact details.

On-Premises Environment -

You have an on-premises file server that runs Windows Server 2019 and stores Microsoft Office documents in a shared folder named Data.

All end-user computers are joined to the corp.fabrikam.com domain and run a third-party antimalware application.

Business Processes -

Sales Contracts -

Users in the sales department receive draft sales contracts from customers by email. The sales contracts are written by the customers and are not in a standard format.

Employment Applications -

Employment applications and resumes are received by HR department managers and stored in either mailboxes, Microsoft SharePoint Online sites, OneDrive for
Business folders, or Microsoft Teams channels.

The employment application form is downloaded from SharePoint Online and a serial number is assigned to each application.
The resumes are written by the applicants and are in any format.

Requirements -

HR Requirements -
You need to create a DLP policy that will notify the HR department of a DLP policy violation if a document that contains confidential employee attributes is shared externally. The DLP policy must use an Exact Data Match (EDM) classification derived from a CSV export of the HR department database.
The HR department identifies the following requirements for handling employment applications:
Resumes must be identified automatically based on similarities to other resumes received in the past.
Employment applications and resumes must be deleted automatically two years after the applications are received.
Documents and emails that contain an application serial number must be identified automatically and marked as an employment application.

Sales Requirements -
A sensitivity label named Sales Contract must be applied automatically to all draft and finalized sales contracts.

Compliance Requirements -
Fabrikam identifies the following compliance requirements:
All DLP policies must be applied to computers that run Windows 10, with the least possible changes to the computers.
Users in the compliance department must view the justification provided when a user receives a tooltip notification for a DLP violation.
If a document that has the Fabrikam Confidential sensitivity label applied is uploaded to Dropbox, the file must be deleted automatically.
The Fabrikam Confidential sensitivity label must be applied to existing Microsoft Word documents in the Data shared folder that have a document footer containing the following string: Company use only.
Users must be able to manually select that email messages are sent encrypted. The encryption will use Office 365 Message Encryption (OME) v2.
Any email containing an attachment that has the Fabrikam Confidential sensitivity label applied must be encrypted automatically by using OME.
Existing policies configured in the third-party records management system must be replaced by using Records management in the Microsoft 365 compliance center. The compliance department plans to export the existing policies, and then produce a CSV file that contains matching labels and policies that are compatible with records management in Microsoft 365. The CSV file must be used to configure records management in Microsoft 365.

Executive Requirements -
You must be able to restore all email received by Fabrikam executives for up to three years after an email is received, even if the email was deleted permanently.

Question
You need to implement a solution that meets the compliance requirements for the Windows 10 computers.
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. Deploy a Microsoft 365 Endpoint data loss prevention (Endpoint DLP) configuration package to the computers.

B. Configure the Microsoft Intune device enrollment settings.

C. Configure hybrid Azure AD join for all the computers.

D. Configure a compliance policy in Microsoft Intune.

E. Enroll the computers in Microsoft Defender for Endpoint protection.

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

GY23 Highly Voted 2 years, 2 months ago
Why choose E instead of A? Why do we need to enroll the computers in Defender for Endpoint (so that they appear in Endpoint DLP dashboard automatically), where in fact we can download the package of Endpoint DLP directly and onboard it on the endpoints?
E doesn't make any sense to me. By answering E, you are adding another solution (MDE) which is not even required.

Answer is AC
upvoted 13 times

oberte007 2 years, 1 month ago

Answer A is also another solution. but given answser is (C and E) the simplest way because enrolling devices in defender for endpoint, you will be able to deploy centrally all DLP policies on them by group as devices enrolled in defender for endpoint can be managed from microsoft 365 compliance center where you set your DLP policies. so CE are good answers.

upvoted 2 times

BieLey 1 year, 8 months ago

But that will cause more changes, since the devices already have a third party malware solution. More administrative effort is the right answer in this question.

AC

upvoted 3 times

Shachar_Nativ Most Recent 1 month, 2 weeks ago

Selected Answer: AC

If I'm interpreting this correctly;
A- Deploy package to endpoints (can be achieved via GPO in this case since endpoints are domain joined).
C- Hybrid AD join is configured via AD Connect, which doesn't impact devices directly.

Only way that has no impact on endpoints and both A and C directly correlate as C is a requirement for A to work.

upvoted 2 times

phony 5 days, 1 hour ago

i think you are right because of this sentence in the testlet:
-All DLP policies must be applied to computers that run Windows 10, with the least possible changes to the computers.

upvoted 1 times

Davidf 3 months, 2 weeks ago

The answer is AC - why? If you onboard the devices to Defender for Endpoint then you need to add exclusionss to DFE for the current AV, and for DFE to the current AV, hence there are additional changes required to the client devices

upvoted 1 times

ivzdf 5 months, 2 weeks ago

Device onboarding is shared across Microsoft 365 and Microsoft Defender for Endpoint (MDE). If you've already onboarded devices to MDE, they will appear in the managed devices list and no further steps are necessary to onboard those specific devices.

ll devices must be one of these:

Azure Active Directory (Azure AD) joined
Hybrid Azure AD joined
AAD registered

https://learn.microsoft.com/en-us/microsoft-365/compliance/device-onboarding-overview?view=o365-worldwide#onboard-windows-10-and-windows-11-devices-into-microsoft-365-overview

upvoted 1 times

JCkD4Ni3L 11 months, 2 weeks ago

Selected Answer: CE

Here is my take on this,

In order to deploy and manage endpoint DLP you require a trust type (Hybrid Azure AD joined, AADJ or AADR)(https://learn.microsoft.com/en-us/microsoft-365/compliance/device-onboarding-overview?view=o365-worldwide#prepare-your-windows-devices), since Fabrikam already syncs with AAD, the changes required to achieve Hybrid AADJ is minimal. (C)

MDE is not configured by default, but in this scenario it should be done to minimize the changes required to achive the solution. Fabrikam already has MCAS deployed with all the necessary connectors to their cloud applications. One of the requirement for MCAS, Cloud Discovery, requires Defender for Endpoint (https://learn.microsoft.com/en-us/defender-cloud-apps/get-started#step-4-set-up-cloud-discovery) (E)

So answers are good (CE)

upvoted 2 times

wooyourdaddy 1 year, 5 months ago

Selected Answer: AC

I wrote the exam today, this question was on it, I choose AC, scored 890!

upvoted 2 times

jkklim 2 years, 2 months ago

ANSWER IS CE.

All DLP policies must be applied to computers that run Windows 10, with the least possible changes to the computers.

Requirement is LEAST POSSIBLE CHANGES

Enroll into MS DEFENDER FOR ENDPOINT PROTECTION IS FASTER AND EFFORTLESS COMPARE TO USING DEPLOYMENT PACKAGE WHICH IS WHY I CHOOSE - E

for C - is it common sense

upvoted 2 times

ExamReviewerIZ 2 years, 1 month ago

Answer is AC.

As you said "LEAST POSSIBLE CHANGES" and no "LEAST ADMINISTRATION EFFORT OR OVERHEAD".

These computers already have a third party malware solution, if you add then to Microsoft Defender for Endpoint that's going to cause a lot of changes. That's not what we want.

upvoted 11 times

Senior 1 year, 10 months ago

You are totally right.

The answers are A and C.

The enrollment of devices into MS Defender for Endpoint is using the same steps as DLP for endpoint (https://docs.microsoft.com/en-us/microsoft-365/security/defender-endpoint/onboarding?view=o365-worldwide).

So why would you enroll a device into MS Defender for Endpoint to achieve the enrollment of the device in Endpoint DLP???

upvoted 2 times

pheb 2 years, 3 months ago

It states, that Azure AD Connect is set up - by default there is no Hybrid Azure AD join. So i would say, the answer is correct: Hybrid Azure AD join followed by the enrollment in Defender for Endpoint.

upvoted 3 times

MahmoudEldeep 2 years, 3 months ago

I think correct answer is A,C

upvoted 3 times

Introductory Info

Case study -

This is a case study. Case studies are not timed separately. You can use as much exam time as you would like to complete each case. However, there may be additional case studies and sections on this exam. You must manage your time to ensure that you are able to complete all questions included on this exam in the time provided.

To answer the questions included in a case study, you will need to reference information that is provided in the case study. Case studies might contain exhibits and other resources that provide more information about the scenario that is described in the case study. Each question is independent of the other questions in this case study.

At the end of this case study, a review screen will appear. This screen allows you to review your answers and to make changes before you move to the next section of the exam. After you begin a new section, you cannot return to this section.

To start the case study -

To display the first question in this case study, click the Next button. Use the buttons in the left pane to explore the content of the case study before you answer the questions. Clicking these buttons displays information such as business requirements, existing environment, and problem statements. If the case study has an All Information tab, note that the information displayed is identical to the information displayed on the subsequent tabs. When you are ready to answer a question, click the Question button to return to the question.

Overview -

Fabrikam, Inc. is a consulting company that has a main office in Montreal and six branch offices in New York, Seattle, Miami, Houston, Los Angeles, and
Vancouver.

Existing Environment -

Cloud Environment -

Fabrikam has a Microsoft 365 tenant that contains the following resources:

An on-premises Active Directory domain named corp.fabrikam.com that syncs to an Azure Active Directory (Azure AD) tenant

Microsoft Cloud App Security connectors configured for all supported cloud applications used by the company

Some users have company Dropbox accounts.

Compliance Configuration -

Fabrikam has the following in the Microsoft 365 compliance center:

A data loss prevention (DLP) policy is configured. The policy displays a tooltip to users. Users can provide a business justification to override a DLP policy violation.

The Azure Information Protection unified labeling scanner is installed and configured.

A sensitivity label named Fabrikam Confidential is configured.

An existing third-party records management system is managed by the compliance department.

Human Resources (HR) Management System

The HR department has an Azure SQL database that contains employee information. Each employee has a unique 12-character alphanumeric ID. The database contains confidential employee attributes including payroll information, date of birth, and personal contact details.

On-Premises Environment -

You have an on-premises file server that runs Windows Server 2019 and stores Microsoft Office documents in a shared folder named Data.

All end-user computers are joined to the corp.fabrikam.com domain and run a third-party antimalware application.

Business Processes -

Sales Contracts -

Users in the sales department receive draft sales contracts from customers by email. The sales contracts are written by the customers and are not in a standard format.

Employment Applications -

Employment applications and resumes are received by HR department managers and stored in either mailboxes, Microsoft SharePoint Online sites, OneDrive for
Business folders, or Microsoft Teams channels.

The employment application form is downloaded from SharePoint Online and a serial number is assigned to each application.
The resumes are written by the applicants and are in any format.

Requirements -

HR Requirements -
You need to create a DLP policy that will notify the HR department of a DLP policy violation if a document that contains confidential employee attributes is shared externally. The DLP policy must use an Exact Data Match (EDM) classification derived from a CSV export of the HR department database.
The HR department identifies the following requirements for handling employment applications:
Resumes must be identified automatically based on similarities to other resumes received in the past.
Employment applications and resumes must be deleted automatically two years after the applications are received.
Documents and emails that contain an application serial number must be identified automatically and marked as an employment application.

Sales Requirements -
A sensitivity label named Sales Contract must be applied automatically to all draft and finalized sales contracts.

Compliance Requirements -
Fabrikam identifies the following compliance requirements:
All DLP policies must be applied to computers that run Windows 10, with the least possible changes to the computers.
Users in the compliance department must view the justification provided when a user receives a tooltip notification for a DLP violation.
If a document that has the Fabrikam Confidential sensitivity label applied is uploaded to Dropbox, the file must be deleted automatically.
The Fabrikam Confidential sensitivity label must be applied to existing Microsoft Word documents in the Data shared folder that have a document footer containing the following string: Company use only.
Users must be able to manually select that email messages are sent encrypted. The encryption will use Office 365 Message Encryption (OME) v2.
Any email containing an attachment that has the Fabrikam Confidential sensitivity label applied must be encrypted automatically by using OME.
Existing policies configured in the third-party records management system must be replaced by using Records management in the Microsoft 365 compliance center. The compliance department plans to export the existing policies, and then produce a CSV file that contains matching labels and policies that are compatible with records management in Microsoft 365. The CSV file must be used to configure records management in Microsoft 365.

Executive Requirements -
You must be able to restore all email received by Fabrikam executives for up to three years after an email is received, even if the email was deleted permanently.

Question
You need to recommend a solution to configure the Microsoft 365 Records management settings by using the CSV file. The solution must meet the compliance requirements.
What should you recommend?

A. Use EdmUploadAgent.exe to upload a hash of the CSV to a datastore.

B. Use a PowerShell command that pipes the Import-Csv cmdlet to the New-RetentionPolicy cmdlet.

C. From the Microsoft 365 compliance center, import the CSV file to a file plan.

D. Use a PowerShell command that pipes the Import-Csv cmdlet to the New-Label cmdlet.

Correct Answer: *C*
Reference:
https://docs.microsoft.com/en-us/microsoft-365/compliance/file-plan-manager?view=o365-worldwide#import-retention-labels-into-your-file-plan

HardcodedCloud Highly Voted 1 year, 11 months ago

The file plan template is a comma separated value (CSV) file. You download it from the file plan page of the records management solution.

upvoted 5 times

Pravda Most Recent 1 year, 10 months ago

On exam 1/20/2022

upvoted 2 times

Question #1 *Topic 10*

Introductory Info

Case study -

This is a case study. Case studies are not timed separately. You can use as much exam time as you would like to complete each case. However, there may be additional case studies and sections on this exam. You must manage your time to ensure that you are able to complete all questions included on this exam in the time provided.

To answer the questions included in a case study, you will need to reference information that is provided in the case study. Case studies might contain exhibits and other resources that provide more information about the scenario that is described in the case study. Each question is independent of the other questions in this case study.

At the end of this case study, a review screen will appear. This screen allows you to review your answers and to make changes before you move to the next section of the exam. After you begin a new section, you cannot return to this section.

To start the case study -

To display the first question in this case study, click the Next button. Use the buttons in the left pane to explore the content of the case study before you answer the questions. Clicking these buttons displays information such as business requirements, existing environment, and problem statements. If the case study has an All Information tab, note that the information displayed is identical to the information displayed on the subsequent tabs. When you are ready to answer a question, click the Question button to return to the question.

Overview -

Contoso, Ltd. is a consulting company that has a main office in Montreal and three branch offices in Seattle, Boston, and Johannesburg.

Existing Environment -

Microsoft 365 Environment -

Contoso has a Microsoft 365 E5 tenant. The tenant contains the administrative user accounts shown in the following table.

Name	Role
Admin1	Global Reader
Admin2	Compliance data administrator
Admin3	Compliance administrator
Admin4	Security operator
Admin5	Security administrator

Users store data in the following locations:

SharePoint sites

OneDrive accounts

Exchange email

Exchange public folders

Teams chats

Teams channel messages

When users in the research department create documents, they must add a 10-digit project code to each document. Project codes that start with the digits 999 are confidential.

SharePoint Online Environment -

Contoso has four Microsoft SharePoint Online sites named Site1, Site2, Site3, and Site4.

Site2 contains the files shown in the following table.

Name	Number of SWIFT codes in the file
File1.docx	1
File2.bmp	4
File3.txt	3
File4.xlsx	7

Two users named User1 and User2 are assigned roles for Site2 as shown in the following table.

User	Role
User1	Site owner
User2	Site visitor

Site3 stores documents related to the company's projects. The documents are organized in a folder hierarchy based on the project.
Site4 has the following two retention policies applied:
Name: Site4RetentionPolicy1
- Locations to apply the policy: Site4
- Delete items older than: 2 years
- Delete content based on: When items were created
Name: Site4RetentionPolicy2
- Locations to apply the policy: Site4
- Retain items for a specific period: 4 years
- Start the retention period based on: When items were created
- At the end of the retention period: Do nothing

Problem Statements -
Management at Contoso is concerned about data leaks. On several occasions, confidential research department documents were leaked.

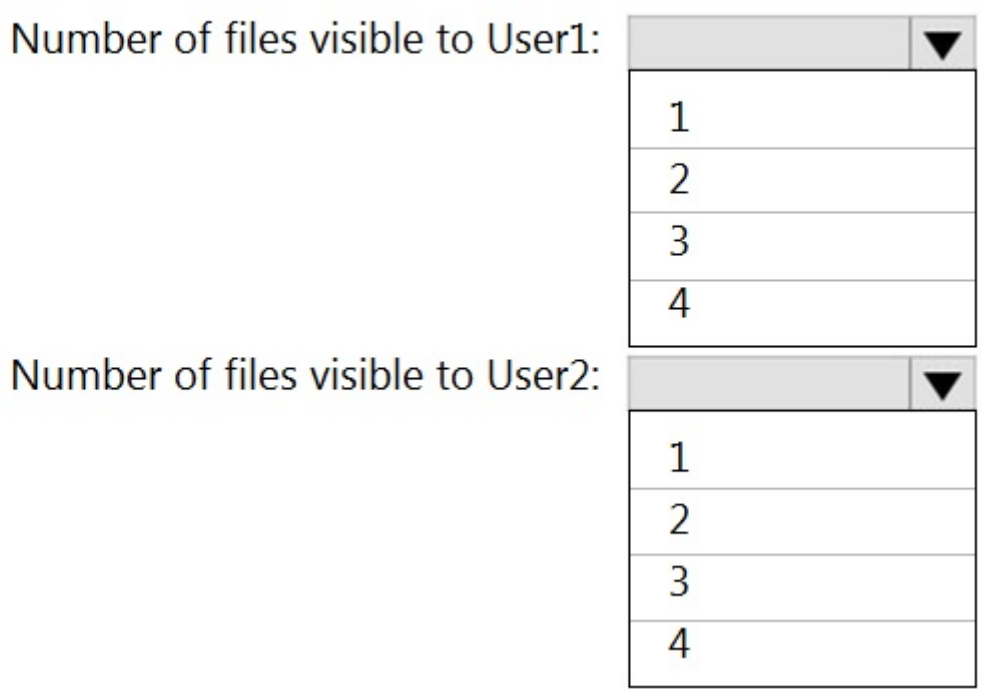
Requirements -

Planned Changes -
Contoso plans to create the following data loss prevention (DLP) policy:
Name: DLPpolicy1
Locations to apply the policy: Site2
Conditions:
- Content contains any of these sensitive info types: SWIFT Code
- Instance count: 2 to any
Actions: Restrict access to the content

Technical Requirements -
Contoso must meet the following technical requirements:
All administrative users must be able to review DLP reports.
Whenever possible, the principle of least privilege must be used.
For all users, all Microsoft 365 data must be retained for at least one year.
Confidential documents must be detected and protected by using Microsoft 365.
Site1 documents that include credit card numbers must be labeled automatically.
All administrative users must be able to create Microsoft 365 sensitivity labels.
After a project is complete, the documents in Site3 that relate to the project must be retained for 10 years.

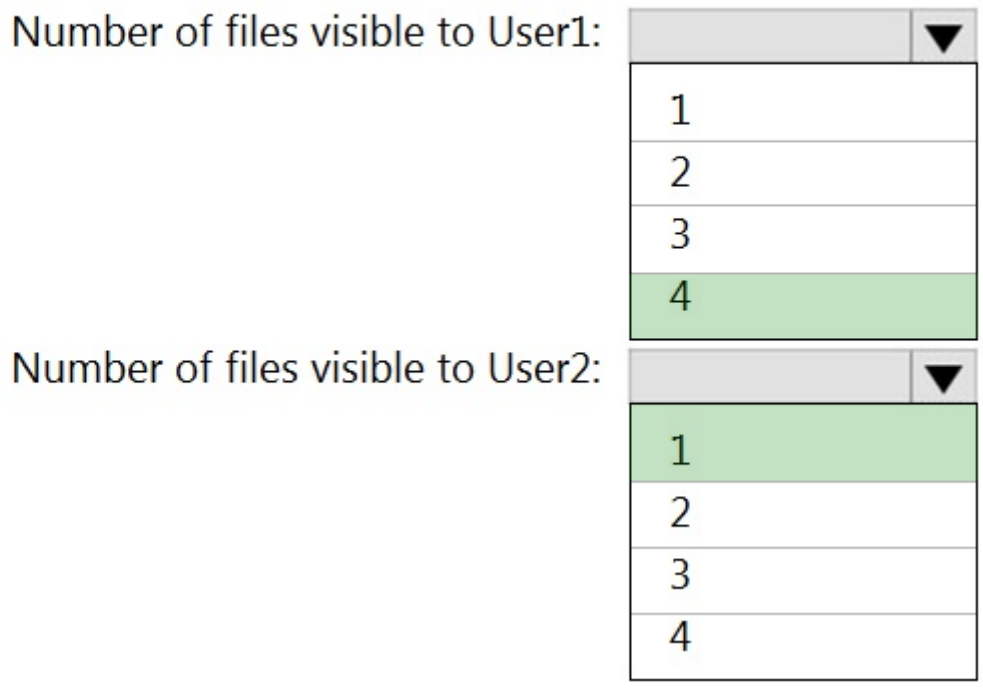
Question
HOTSPOT -
How many files in Site2 will be visible to User1 and User2 after you turn on DLPpolicy1? To answer, select the appropriate options in the answer area.
NOTE: Each correct selection is worth one point.
Hot Area:

Answer Area



Answer Area

Correct Answer:



Reference:
https://social.technet.microsoft.com/wiki/contents/articles/36527.implement-data-loss-prevention-dlp-in-sharepoint-online.aspx

pheb Highly Voted 2 years, 3 months ago
Should be: 4 and 2.
- .bmp is not a supported file type
- the first document contains only 1 swift code (DLP rule matches if "Instance count: 2 to any" applies).
upvoted 19 times

jcgonzalez1978 2 years, 3 months ago
Supported file types in DLP are documented here: https://docs.microsoft.com/en-gb/exchange/security-and-compliance/mail-flow-rules/inspect-message-attachments
upvoted 3 times

ExamReviewerIZ 2 years, 1 month ago
Wrong resource, we are looking into auto-apply for SharePoint not Email.
upvoted 1 times

zaspamer 1 year, 11 months ago
That is the right one and txt files are crawled https://docs.microsoft.com/en-us/SharePoint/technical-reference/default-crawled-file-name-extensions-and-parsed-file-types
upvoted 6 times

BTAB 1 year, 6 months ago
Correct .bmp is the only file type not crawled. According to the link for SharePoint crawled files.

Answer is 4 and 2
upvoted 4 times

ExamReviewerIZ 2 years, 1 month ago
.txt is not supported either
upvoted 2 times

ExamReviewerIZ Highly Voted 2 years, 1 month ago
Only the .docx and .xlsx files could be labeled. (.txt nor .BPM are supported)

That being clarified, only the .xlsx file will be labeled based on the conditions specified in the DLP Policy.

User1-Owner: will be able to see all files includes those blocked by a DLP policy.
User2-Visitor: All files except the one blocked by the DLP Policy.

Answer: 4 and 3
upvoted 19 times

wyindualizer 1 year, 3 months ago
Txt is supported aswell
https://docs.microsoft.com/en-us/sharepoint/technical-reference/default-crawled-file-name-extensions-and-parsed-file-types
upvoted 3 times

SnottyPudding 1 year, 8 months ago
You are correct. Others, including ExamTopics, are misreading the question. The only file blocked to User2 is File4.xlsx; the other three will be available. Therefore, the correct answer is 4 and 3.
upvoted 2 times

HDEIWDEOW Most Recent 3 months, 2 weeks ago

Got this question on exam on 17th August

upvoted 1 times

JCkD4Ni3L 11 months, 2 weeks ago

Answer should be 4 and 2.
- DLP Policy will trigger if the SWIFT Code count is 2 or higher.
- Only .BMP file extension isn't supported.
(and yes, .txt file type IS supported: https://learn.microsoft.com/en-us/microsoft-365/compliance/endpoint-dlp-learn-about?view=o365-worldwide#monitored-files)

upvoted 3 times

chrissempai 1 year, 2 months ago

the good answer is
user 1 : 4
user2 : 2
the extension supported for the security is docx, txt, xlsx. bmp not supported

upvoted 5 times

JamesM9 1 year, 7 months ago

The group owner will see all files by default.
The DLP policy will allow user 2 to see all files that match the policy. The instance count is 2 to any, which rules out File 1 as there is only 1 instance count for File 1.

Therefore, the answer here is 4 & 3.

upvoted 1 times

daavidsc400 1 year, 8 months ago

.bmp is not supported...
"Microsoft 365 uses the search crawler to identify and classify sensitive information in SharePoint Online and OneDrive for Business sites. To identify your new custom sensitive information type in existing content, the content must be re-crawled. "

here is the list of crawled file types...
https://docs.microsoft.com/en-us/sharepoint/technical-reference/default-crawled-file-name-extensions-and-parsed-file-types

.bmp is not on the list

upvoted 2 times

Pravda 1 year, 10 months ago

On exam 1/20/2022

upvoted 1 times

MahmoudEldeep 2 years, 3 months ago

What are the supported file types by O365 DLP?

upvoted 1 times

Eltooth 2 years, 4 months ago

" Currently evaluating" means yet to be implemented therefore no changes made.

Correct answer should be Admin 2, 3 & 5.

upvoted 1 times

Eltooth 2 years, 4 months ago

Answer for next question...

upvoted 1 times

Eltooth 2 years, 4 months ago

4 and 1. Correct answer.

upvoted 2 times

Introductory Info

Case study -

This is a case study. Case studies are not timed separately. You can use as much exam time as you would like to complete each case. However, there may be additional case studies and sections on this exam. You must manage your time to ensure that you are able to complete all questions included on this exam in the time provided.

To answer the questions included in a case study, you will need to reference information that is provided in the case study. Case studies might contain exhibits and other resources that provide more information about the scenario that is described in the case study. Each question is independent of the other questions in this case study.

At the end of this case study, a review screen will appear. This screen allows you to review your answers and to make changes before you move to the next section of the exam. After you begin a new section, you cannot return to this section.

To start the case study -

To display the first question in this case study, click the Next button. Use the buttons in the left pane to explore the content of the case study before you answer the questions. Clicking these buttons displays information such as business requirements, existing environment, and problem statements. If the case study has an All Information tab, note that the information displayed is identical to the information displayed on the subsequent tabs. When you are ready to answer a question, click the Question button to return to the question.

Overview -

Contoso, Ltd. is a consulting company that has a main office in Montreal and three branch offices in Seattle, Boston, and Johannesburg.

Existing Environment -

Microsoft 365 Environment -

Contoso has a Microsoft 365 E5 tenant. The tenant contains the administrative user accounts shown in the following table.

Name	Role
Admin1	Global Reader
Admin2	Compliance data administrator
Admin3	Compliance administrator
Admin4	Security operator
Admin5	Security administrator

Users store data in the following locations:

SharePoint sites

OneDrive accounts

Exchange email

Exchange public folders

Teams chats

Teams channel messages

When users in the research department create documents, they must add a 10-digit project code to each document. Project codes that start with the digits 999 are confidential.

SharePoint Online Environment -

Contoso has four Microsoft SharePoint Online sites named Site1, Site2, Site3, and Site4.

Site2 contains the files shown in the following table.

Name	Number of SWIFT codes in the file
File1.docx	1
File2.bmp	4
File3.txt	3
File4.xlsx	7

Two users named User1 and User2 are assigned roles for Site2 as shown in the following table.

User	Role
User1	Site owner
User2	Site visitor

Site3 stores documents related to the company's projects. The documents are organized in a folder hierarchy based on the project.

Site4 has the following two retention policies applied:

Name: Site4RetentionPolicy1
- Locations to apply the policy: Site4
- Delete items older than: 2 years
- Delete content based on: When items were created
Name: Site4RetentionPolicy2
- Locations to apply the policy: Site4
- Retain items for a specific period: 4 years
- Start the retention period based on: When items were created
- At the end of the retention period: Do nothing

Problem Statements -
Management at Contoso is concerned about data leaks. On several occasions, confidential research department documents were leaked.

Requirements -

Planned Changes -
Contoso plans to create the following data loss prevention (DLP) policy:
Name: DLPpolicy1
Locations to apply the policy: Site2
Conditions:
- Content contains any of these sensitive info types: SWIFT Code
- Instance count: 2 to any
Actions: Restrict access to the content

Technical Requirements -
Contoso must meet the following technical requirements:
All administrative users must be able to review DLP reports.
Whenever possible, the principle of least privilege must be used.
For all users, all Microsoft 365 data must be retained for at least one year.
Confidential documents must be detected and protected by using Microsoft 365.
Site1 documents that include credit card numbers must be labeled automatically.
All administrative users must be able to create Microsoft 365 sensitivity labels.
After a project is complete, the documents in Site3 that relate to the project must be retained for 10 years.

Question
You are evaluating the technical requirements for the DLP reports.
Which user can currently view the DLP reports?

A. Admin4

B. Admin1

C. Admin5

D. Admin2

E. Admin3

Correct Answer: *E*

GY23 Highly Voted 2 years, 2 months ago
The answer is "compliance administrator", admin 3.
https://docs.microsoft.com/en-us/microsoft-365/compliance/view-the-dlp-reports?view=o365-worldwide
upvoted 8 times

ExamReviewerIZ Highly Voted 2 years, 1 month ago
There's someone wrong with this question. Obviously more that one currently has access to the DLP reports.

I believe this should be a "Select three" type of question.
upvoted 6 times

Gesbie Most Recent 3 months, 3 weeks ago
was on Exam August 9, 2023

upvoted 1 times

Ciapek 1 year, 6 months ago

Selected Answer: E

Admin3

upvoted 1 times

Pravda 1 year, 10 months ago

On exam 1/20/2022

upvoted 1 times

GY23 2 years, 2 months ago

Guys, it clearly says "Which user can currently view the DLP reports?".
User is without an "s", so stop saying all admins or giving several options. You'll be confusing everyone who sees your comments.

upvoted 4 times

fangeel 1 year, 12 months ago

Admin3 best answer...

upvoted 2 times

sergioandreslq 1 year, 11 months ago

Agreed, the question is asking for "USER" not "USERS".
The best answer for compliance roles is the Compliance administrator

upvoted 2 times

xofowi5140 2 years, 4 months ago

DLP Compliance Management role: View and edit settings and reports for data loss prevention (DLP) policies.

View-Only DLP Compliance Management role: View the settings and reports for data loss prevention (DLP) policies.

DLP Compliance Management or View-Only DLP Compliance Management:
- Compliance Administrator
- Compliance Data Administrator
- Security Administrator
- Security Operator
- Security Reader
- Global Reader
- Organization Management

So, all admin users

upvoted 6 times

xofowi5140 2 years, 4 months ago

Not all admins.

To view DLP reports in the Security & Compliance Center, you have to be assigned the:

Security Reader role in the Exchange admin center. By default, this role is assigned to the Organization Management and Security Reader role groups in the Exchange admin center.

View-Only DLP Compliance Management role in the Security & Compliance Center. By default, this role is assigned to the Compliance Administrator, Organization Management, Security Administrator, and Security Reader role groups in the Security & Compliance Center.

View-Only Recipients role in the Exchange admin center. By default, this role is assigned to the Compliance Management, Organization Management, and View-Only Organization Management role groups in the Exchange admin center.

upvoted 3 times

Eltooth 2 years, 4 months ago

"Currently evaluating" means yet to be implemented therefore no changes made.

To view DLP reports in the Security & Compliance Center, you have to be assigned the:

* Security Reader role in the Exchange admin center. By default, this role is assigned to the Organization Management and Security Reader role groups in the Exchange admin center.

* View-Only DLP Compliance Management role in the Security & Compliance Center. By default, this role is assigned to the Compliance Administrator, Organization Management, Security Administrator, and Security Reader role groups in the Security & Compliance Center.

*View-Only Recipients role in the Exchange admin center. By default, this role is assigned to the Compliance Management, Organization Management, and View-Only Organization Management role groups in the Exchange admin center.

https://docs.microsoft.com/en-us/microsoft-365/compliance/view-the-dlp-reports?view=o365-worldwide#permissions-for-dlp-reports

https://docs.microsoft.com/en-us/microsoft-365/security/office-365-security/permissions-in-the-security-and-compliance-center?view=o365-worldwide#roles-in-the-security--compliance-center

Correct answer should be Admin 2, 3 & 5.

upvoted 3 times

nupagazi 1 year, 10 months ago

From the link I think only Security Administrator and Compliance Administrator, right ?

upvoted 3 times

Question #1 *Topic 11*

Introductory Info

Case study -

This is a case study. Case studies are not timed separately. You can use as much exam time as you would like to complete each case. However, there may be additional case studies and sections on this exam. You must manage your time to ensure that you are able to complete all questions included on this exam in the time provided.

To answer the questions included in a case study, you will need to reference information that is provided in the case study. Case studies might contain exhibits and other resources that provide more information about the scenario that is described in the case study. Each question is independent of the other questions in this case study.

At the end of this case study, a review screen will appear. This screen allows you to review your answers and to make changes before you move to the next section of the exam. After you begin a new section, you cannot return to this section.

To start the case study -

To display the first question in this case study, click the Next button. Use the buttons in the left pane to explore the content of the case study before you answer the questions. Clicking these buttons displays information such as business requirements, existing environment, and problem statements. If the case study has an All Information tab, note that the information displayed is identical to the information displayed on the subsequent tabs. When you are ready to answer a question, click the Question button to return to the question.

Overview -

Contoso, Ltd. is a consulting company that has a main office in Montreal and three branch offices in Seattle, Boston, and Johannesburg.

Existing Environment -

Microsoft 365 Environment -

Contoso has a Microsoft 365 E5 tenant. The tenant contains the administrative user accounts shown in the following table.

Name	Role
Admin1	Global Reader
Admin2	Compliance data administrator
Admin3	Compliance administrator
Admin4	Security operator
Admin5	Security administrator

Users store data in the following locations:

SharePoint sites

OneDrive accounts

Exchange email

Exchange public folders

Teams chats

Teams channel messages

When users in the research department create documents, they must add a 10-digit project code to each document. Project codes that start with the digits 999 are confidential.

SharePoint Online Environment -

Contoso has four Microsoft SharePoint Online sites named Site1, Site2, Site3, and Site4.

Site2 contains the files shown in the following table.

Name	Number of SWIFT codes in the file
File1.docx	1
File2.bmp	4
File3.txt	3
File4.xlsx	7

Two users named User1 and User2 are assigned roles for Site2 as shown in the following table.

User	Role
User1	Site owner
User2	Site visitor

Site3 stores documents related to the company's projects. The documents are organized in a folder hierarchy based on the project.
Site4 has the following two retention policies applied:
Name: Site4RetentionPolicy1
- Locations to apply the policy: Site4
- Delete items older than: 2 years
- Delete content based on: When items were created
Name: Site4RetentionPolicy2
- Locations to apply the policy: Site4
- Retain items for a specific period: 4 years
- Start the retention period based on: When items were created
- At the end of the retention period: Do nothing

Problem Statements -
Management at Contoso is concerned about data leaks. On several occasions, confidential research department documents were leaked.

Requirements -

Planned Changes -
Contoso plans to create the following data loss prevention (DLP) policy:
Name: DLPpolicy1
Locations to apply the policy: Site2
Conditions:
- Content contains any of these sensitive info types: SWIFT Code
- Instance count: 2 to any
Actions: Restrict access to the content

Technical Requirements -
Contoso must meet the following technical requirements:
All administrative users must be able to review DLP reports.
Whenever possible, the principle of least privilege must be used.
For all users, all Microsoft 365 data must be retained for at least one year.
Confidential documents must be detected and protected by using Microsoft 365.
Site1 documents that include credit card numbers must be labeled automatically.
All administrative users must be able to create Microsoft 365 sensitivity labels.
After a project is complete, the documents in Site3 that relate to the project must be retained for 10 years.

Question
HOTSPOT -
You are reviewing policies for the SharePoint Online environment.
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:

Answer Area

Statements	Yes	No
If a user creates a file in Site4 on January 1, 2021, users will be able to access the file on January 15, 2023.	○	○
If a user deletes a file from Site4 that was created on January 1, 2021, an administrative user will be able to recover the file on April 15, 2023.	○	○
If a user deletes a file from Site4 that was created on January 1, 2021, an administrative user will be able to recover the file on April 15, 2026.	○	○

Correct Answer:

Answer Area

Statements	Yes	No
If a user creates a file in Site4 on January 1, 2021, users will be able to access the file on January 15, 2023.	○	○
If a user deletes a file from Site4 that was created on January 1, 2021, an administrative user will be able to recover the file on April 15, 2023.	○	○
If a user deletes a file from Site4 that was created on January 1, 2021, an administrative user will be able to recover the file on April 15, 2026.	○	○

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

hydrillo Highly Voted 2 years, 3 months ago
Retention wins over Deletion. So Yes, Yes, Yes
upvoted 12 times

jimmyjose 1 year, 2 months ago
The 3rd answer statement indirectly states that the user deleted the file on April 15, 2026, which is well beyond the 4 years of retention, and admins will not be able to recover the file.

Hence, the answer should be Yes, Yes, No.
upvoted 4 times

ExamReviewerIZ 2 years, 1 month ago
Yes, Yes, No. There's no way for an admin to recover a file after 4 years.
upvoted 10 times

sergioandreslq 1 year, 11 months ago
Answer is Yes, Yes, No
When configuring a retention policy you can set, [At the end of the retention period "Do Nothing"]. Isn't this the same thing as "retain items forever"?
NO: No, it's actually the opposite. Retain forever means take steps to ensure the item is never permanently deleted (will always be returned in eDiscovery searches). Whereas "do nothing" at the end of the retention period means no longer take steps to ensure the item isn't permanently deleted - in other words, the item can now be deleted by a user or system-initiated action & they won't be returned by eDiscovery searches. So, there is no way to recover the file after 4 years, for 2026 the file will be deleted.
upvoted 10 times

pheb 2 years, 3 months ago
You are correct: https://docs.microsoft.com/en-us/microsoft-365/compliance/retention?view=o365-worldwide#the-principles-of-retention-or-what-takes-precedence
upvoted 6 times

HDEIWDEOW Most Recent 3 months, 2 weeks ago
Got this question on exam on 17th August
upvoted 1 times

Gesbie 3 months, 3 weeks ago
was on Exam August 9, 2023
upvoted 1 times

chrissempai 1 year, 1 month ago
the answer is : YES /YES / YES
at the end of retention do nothing
upvoted 1 times

jacul 8 months, 3 weeks ago
but the file was deleted 5 years ago
upvoted 1 times

Pravda 1 year, 10 months ago
On exam 1/20/2022
upvoted 1 times

oberte007 2 years, 1 month ago
Alright! Priority to retention policies over deletion policies
upvoted 2 times

Introductory Info

Case study -

This is a case study. Case studies are not timed separately. You can use as much exam time as you would like to complete each case. However, there may be additional case studies and sections on this exam. You must manage your time to ensure that you are able to complete all questions included on this exam in the time provided.

To answer the questions included in a case study, you will need to reference information that is provided in the case study. Case studies might contain exhibits and other resources that provide more information about the scenario that is described in the case study. Each question is independent of the other questions in this case study.

At the end of this case study, a review screen will appear. This screen allows you to review your answers and to make changes before you move to the next section of the exam. After you begin a new section, you cannot return to this section.

To start the case study -

To display the first question in this case study, click the Next button. Use the buttons in the left pane to explore the content of the case study before you answer the questions. Clicking these buttons displays information such as business requirements, existing environment, and problem statements. If the case study has an All Information tab, note that the information displayed is identical to the information displayed on the subsequent tabs. When you are ready to answer a question, click the Question button to return to the question.

Overview -

Contoso, Ltd. is a consulting company that has a main office in Montreal and three branch offices in Seattle, Boston, and Johannesburg.

Existing Environment -

Microsoft 365 Environment -

Contoso has a Microsoft 365 E5 tenant. The tenant contains the administrative user accounts shown in the following table.

Name	Role
Admin1	Global Reader
Admin2	Compliance data administrator
Admin3	Compliance administrator
Admin4	Security operator
Admin5	Security administrator

Users store data in the following locations:

SharePoint sites

OneDrive accounts

Exchange email

Exchange public folders

Teams chats

Teams channel messages

When users in the research department create documents, they must add a 10-digit project code to each document. Project codes that start with the digits 999 are confidential.

SharePoint Online Environment -

Contoso has four Microsoft SharePoint Online sites named Site1, Site2, Site3, and Site4.

Site2 contains the files shown in the following table.

Name	Number of SWIFT codes in the file
File1.docx	1
File2.bmp	4
File3.txt	3
File4.xlsx	7

Two users named User1 and User2 are assigned roles for Site2 as shown in the following table.

User	Role
User1	Site owner
User2	Site visitor

Site3 stores documents related to the company's projects. The documents are organized in a folder hierarchy based on the project.

Site4 has the following two retention policies applied:

Name: Site4RetentionPolicy1
- Locations to apply the policy: Site4
- Delete items older than: 2 years
- Delete content based on: When items were created
Name: Site4RetentionPolicy2
- Locations to apply the policy: Site4
- Retain items for a specific period: 4 years
- Start the retention period based on: When items were created
- At the end of the retention period: Do nothing

Problem Statements -
Management at Contoso is concerned about data leaks. On several occasions, confidential research department documents were leaked.

Requirements -

Planned Changes -
Contoso plans to create the following data loss prevention (DLP) policy:
Name: DLPpolicy1
Locations to apply the policy: Site2
Conditions:
- Content contains any of these sensitive info types: SWIFT Code
- Instance count: 2 to any
Actions: Restrict access to the content

Technical Requirements -
Contoso must meet the following technical requirements:
All administrative users must be able to review DLP reports.
Whenever possible, the principle of least privilege must be used.
For all users, all Microsoft 365 data must be retained for at least one year.
Confidential documents must be detected and protected by using Microsoft 365.
Site1 documents that include credit card numbers must be labeled automatically.
All administrative users must be able to create Microsoft 365 sensitivity labels.
After a project is complete, the documents in Site3 that relate to the project must be retained for 10 years.

Question
You need to meet the retention requirement for the users' Microsoft 365 data.
What is the minimum number of retention policies that you should use?

A. 1

B. 2

C. 3

D. 4

E. 6

Correct Answer: *A*
Reference:
https://docs.microsoft.com/en-us/microsoft-365/compliance/retention?view=o365-worldwide

k4d4v4r Highly Voted 2 years, 6 months ago
B is correct."If you select the Teams or Yammer locations when you create a retention policy, the other locations are automatically excluded. This means that the instructions to follow depend on whether you need to include the Teams or Yammer locations:" https://docs.microsoft.com/en-us/microsoft-365/compliance/create-retention-policies?view=o365-worldwide#create-and-configure-a-retention-policy
upvoted 17 times

sergioandreslq 1 year, 11 months ago
Nop,
One for Teams Private Channel Messages

One for Teams chats
One for everything else.
One for Yammer (preview) If Yammer user messages Preview is considered , then One policy more for Yammer.
It could be 3 or 4, depend on what Microsoft think when they created this question.
I tested and I need 3
upvoted 5 times

mcas 1 year, 1 month ago
teams private message is not in the list where users store data

SharePoint sites
OneDrive accounts
Exchange email
Exchange public folders
Teams chats
Teams channel messages
upvoted 1 times

mcas 1 year, 1 month ago
teams private channel I mean
upvoted 1 times

Piper Highly Voted 2 years, 6 months ago
Similar to an earlier question, this must be B because 2 retention policies will be needed
upvoted 9 times

dasha_an 2 years, 6 months ago
Why?
Here https://docs.microsoft.com/en-us/microsoft-365/compliance/retention?view=o365-worldwide it is mentionned that "Retention label policies specify the locations to publish the retention labels. The same location can be included in multiple retention label policies."

1 policy is enough
upvoted 3 times

Lineup 2 years, 6 months ago
But could this be a tricky one beacause all information in Teams chats are saved in OneDrive which is covered and then all information in Teams channels are saved in Sharepoint?
upvoted 1 times

Johnnien 2 years, 4 months ago
What about Yammer?
upvoted 1 times

shanti0091 2 years, 4 months ago
Well true, you make a point but yammer is still in preview mode
upvoted 1 times

Sam12 1 year, 10 months ago
This scenario does not mention "Teams private channel messages" nor any yammer worloads.
upvoted 2 times

dasha_an 2 years, 6 months ago
I checked again and I agree with you
upvoted 3 times

HDEIWDEOW Most Recent 3 months, 2 weeks ago
Got this question on exam on 17th August
upvoted 1 times

Gesbie 3 months, 3 weeks ago
was on Exam August 9, 2023
upvoted 1 times

CharlieGolf 8 months, 1 week ago
Selected Answer: B
Answer is 2. Ignore all the noise/debate about Yammer and Teams Private because they are not in the scope of the case study's user data locations.
upvoted 3 times

See_Es 10 months, 1 week ago
Selected Answer: B
1 for
-SharePoint sites
-OneDrive accounts
-Exchange email
-Exchange public folders

and one for
-Teams chats
-Teams channel messages
upvoted 3 times

mcas 1 year, 1 month ago

Selected Answer: B

teams private message is not in the list where users store data

SharePoint sites
OneDrive accounts
Exchange email
Exchange public folders
Teams chats
Teams channel messages
upvoted 2 times

chrissempai 1 year, 1 month ago

Selected Answer: D

you need at least 4 policies for covering all MS365, I check the configuration
upvoted 1 times

RamenIsDelicious 1 year, 3 months ago

Selected Answer: D

As of 8/15/22 you need 4 policies, 1 teams channel and chat messages, 1 for teams private messages, 1 for Yammer + User messages, 1 for everything else.
upvoted 1 times

odbjegli 1 year, 7 months ago

Selected Answer: B

For me B. 2 policies
Users store data in the following locations:
[SharePoint sites, OneDrive accounts, Exchange email, Exchange public folders] 1'st policy
[Teams chats, Teams channel messages] 2'nd policy
upvoted 3 times

g2s 1 year, 4 months ago

agree, simple as that
upvoted 2 times

JamesM9 1 year, 7 months ago

Another tricky question. Based on the locations specifically mentioned in the question, we are being asked to create 2 retention policies.

Retention policy 1 - SharePoint, Onedrive, Exchange, Exchange Public Folders.
Retention policy 2 - Teams chat, Teams Channel messages.

The question does not ask for any more than this, so for me the answer is B (2).
upvoted 2 times

ranc1d 1 year, 8 months ago

Selected Answer: B

2 policies:
Users store data in the following locations:
Policy1:
SharePoint sites
OneDrive accounts
Exchange email
Exchange public folders
Policiy2:
Teams chats
Teams channel messages
upvoted 3 times

nupagazi 1 year, 10 months ago

Agreed 1 policy. Since the requirements for retention do not specify whether delete documents, then 1 policy for logest retention can meet requirements
upvoted 1 times

nupagazi 1 year, 10 months ago

3 is correct because retention periods are 3: 4 years for site 4; 10 years for project document and 1 year for remaining site, I think
upvoted 1 times

Sam12 1 year, 10 months ago

Users store data in the following locations:
[One for]
SharePoint sites

OneDrive accounts
Exchange email
Exchange public folders
[another one for]
Teams chats
Teams channel messages

So, 2.
upvoted 6 times

Sam12 1 year, 10 months ago
In this scenario there is no mention to "Teams private channel messages", which would need its own policy, nor does it mention "Yammer community message" or "Yammer user messages" which would need another sigle policy for both yammer workloads.
So, for this scenario you just net 2, but if it mention all of the M365 workloads then you would need 4.
upvoted 3 times

UWSFish 1 year, 9 months ago
Yes two is the correct answer. There is no mention of "Teams private channel messages". 100% correct. Go try it yourself.
upvoted 1 times

Robert__Susin 1 year, 11 months ago
Selected Answer: D
Take a look at ExamReviewerIZ answer
upvoted 2 times

ExamReviewerIZ 2 years, 1 month ago
You need 3(of not taking Yammer Messages into account) otherwise you need 4 policies.

People saying you only need 2 is incorrect.

Remember you need to activate only those that let you select "Users" (as that it Microsoft 365 Data of user).

One for Teams Private Channel Messages
One for Teams chats
One for everything else.
(If Yammer user messages Preview is considered , then One policy more for this)
upvoted 6 times

Robert__Susin 1 year, 11 months ago
Correct
upvoted 1 times

IAGirl 1 year, 8 months ago
The question does no mention private channel, the answer is two
upvoted 1 times

girikedar 1 year, 11 months ago
Tested , It requires 4 retention policy to retain all Microsoft 365 data
upvoted 3 times

Sam12 1 year, 10 months ago
This scenario does not mention "Teams private channel messages" nor any yammer worloads. so 2 is enough.
upvoted 2 times

PrettyFlyWifi 1 year, 9 months ago
This is the correct answer, look at the workloads it lists. There is nothing about Teams private channels, which would normally need it's own policy, but not here at all. You need 1 policy for Exchange, SPO, OneDrive, etc, and then 1 policy purely for Teams chats and channel messages. 2 in total is the correct answer.
upvoted 2 times

sergioandreslq 1 year, 11 months ago
Very good answer, I tested in my M365 and I need min 3, If I want to add Yammer, then, I will need 4.
upvoted 3 times

Question #1 *Topic 12*

Introductory Info

Case study -

This is a case study. Case studies are not timed separately. You can use as much exam time as you would like to complete each case. However, there may be additional case studies and sections on this exam. You must manage your time to ensure that you are able to complete all questions included on this exam in the time provided.

To answer the questions included in a case study, you will need to reference information that is provided in the case study. Case studies might contain exhibits and other resources that provide more information about the scenario that is described in the case study. Each question is independent of the other questions in this case study.

At the end of this case study, a review screen will appear. This screen allows you to review your answers and to make changes before you move to the next section of the exam. After you begin a new section, you cannot return to this section.

To start the case study -

To display the first question in this case study, click the Next button. Use the buttons in the left pane to explore the content of the case study before you answer the questions. Clicking these buttons displays information such as business requirements, existing environment, and problem statements. If the case study has an All Information tab, note that the information displayed is identical to the information displayed on the subsequent tabs. When you are ready to answer a question, click the Question button to return to the question.

Overview -

Fabrikam, Inc. is a consulting company that has a main office in Montreal and six branch offices in New York, Seattle, Miami, Houston, Los Angeles, and
Vancouver.

Existing Environment -

Cloud Environment -

Fabrikam has a Microsoft 365 tenant that contains the following resources:

An on-premises Active Directory domain named corp.fabrikam.com that syncs to an Azure Active Directory (Azure AD) tenant.

Microsoft Cloud App Security connectors configured for all supported cloud applications used by the company.

Some users have company Dropbox accounts.

Compliance Configuration -

Fabrikam has the following in the Microsoft 365 compliance center:

A data loss prevention (DLP) policy is configured. The policy displays a tooltip to users. Users can provide a business justification to override a DLP policy violation.

The Azure Information Protection unified labeling scanner is installed and configured.

A sensitivity label named Fabrikam Confidential is configured.

An existing third-party records management system is managed by the compliance department.

Human Resources (HR) Management System

The HR department has an Azure SQL database that contains employee information. Each employee has a unique 12-character alphanumeric ID. The database contains confidential employee attributes including payroll information, date of birth, and personal contact details.

On-Premises Environment -

You have an on-premises file server that runs Windows Server 2019 and stores Microsoft Office documents in a shared folder named Data.

All end-user computers are joined to the corp.fabrikam.com domain and run a third-party antimalware application.

Business Processes -

Sales Contracts -

Users in the sales department receive draft sales contracts from customers by email. The sales contracts are written by the customers and are not in a standard format.

Employment Applications -

Employment applications and resumes are received by HR department managers and stored in either mailboxes, Microsoft SharePoint Online sites, OneDrive for
Business folders, or Microsoft Teams channels.
The employment application form is downloaded from SharePoint Online and a serial number is assigned to each application.
The resumes are written by the applicants and are in any format.

Requirements -

HR Requirements -
You need to create a DLP policy that will notify the HR department of a DLP policy violation if a document that contains confidential employee attributes is shared externally. The DLP policy must use an Exact Data Match (EDM) classification derived from a CSV export of the HR department database.
The HR department identifies the following requirements for handling employment applications:
Resumes must be identified automatically based on similarities to other resumes received in the past.
Employment applications and resumes must be deleted automatically two years after the applications are received.
Documents and emails that contain an application serial number must be identified automatically and marked as an employment application.

Sales Requirements -
A sensitivity label named Sales Contract must be applied automatically to all draft and finalized sales contracts.

Compliance Requirements -
Fabrikam identifies the following compliance requirements:
All DLP policies must be applied to computers that run Windows 10, with the least possible changes to the computers.
Users in the compliance department must view the justification provided when a user receives a tooltip notification for a DLP violation.
If a document that has the Fabrikam Confidential sensitivity label applied is uploaded to Dropbox, the file must be deleted automatically.
The Fabrikam Confidential sensitivity label must be applied to existing Microsoft Word documents in the Data shared folder that have a document footer containing the following string: Company use only.
Users must be able to manually select that email messages are sent encrypted. The encryption will use Office 365 Message Encryption (OME) v2.
Any email containing an attachment that has the Fabrikam Confidential sensitivity label applied must be encrypted automatically by using OME.
Existing policies configured in the third-party records management system must be replaced by using Records management in the Microsoft 365 compliance center. The compliance department plans to export the existing policies, and then produce a CSV file that contains matching labels and policies that are compatible with records management in Microsoft 365. The CSV file must be used to configure records management in Microsoft 365.

Executive Requirements -
You must be able to restore all email received by Fabrikam executives for up to three years after an email is received, even if the email was deleted permanently.

Question
You need to recommend a solution that meets the executive requirements.
What should you recommend?

A. From the Microsoft 365 compliance center, create a DLP policy.

B. From the Exchange admin center, enable archive mailboxes.

C. From the Microsoft 365 compliance center, create a retention label.

D. From the Microsoft 365 compliance center, create a retention policy.

Correct Answer: *C*
Reference:
https://docs.microsoft.com/en-us/microsoft-365/compliance/create-apply-retention-labels?view=o365-worldwide

ExamReviewerIZ Highly Voted 2 years, 1 month ago
Retention Policy from Compliance Center.
upvoted 13 times

klosedotorg83 Highly Voted 2 years, 1 month ago
Create a retention policy should be the correct answer

upvoted 7 times

Sango Most Recent 3 months, 1 week ago

Agree. It's Policy. Use a retention policy to assign the same retention settings for content at a site or mailbox level, and use a retention label to assign retention settings at an item level (folder, document, email).

upvoted 1 times

luissaro 7 months ago

Selected Answer: D

"Example: Emails and OneDrive documents for executives require a longer retention period than standard users. You create a retention policy with an adaptive scope that uses the Azure AD attribute job title of "Executive", and then select the Exchange email and OneDrive accounts locations for the policy. There's no need to specify email addresses or OneDrive URLs for these users because the adaptive scope automatically retrieves these values. For new executives, there's no need to reconfigure the retention policy because these new users with their corresponding values for email and OneDrive are automatically picked up." source: https://learn.microsoft.com/en-us/microsoft-365/compliance/retention?view=o365-worldwide Adaptive or static policy scopes for retention

upvoted 2 times

CharlieGolf 8 months, 1 week ago

Selected Answer: D

Retention policy b/c "all email" in the exec mailboxes. No need to label individual emails in their mailboxes.

upvoted 1 times

See_Es 10 months, 1 week ago

Selected Answer: D

Retention Policy for sure

upvoted 1 times

mitho 10 months, 2 weeks ago

Retention Policy from Compliance Center.

upvoted 1 times

Rockalm 11 months ago

Answer is C. After you have created a retention label, then you can create a retention policy. So, this must be the first step. I agree, the policy will then execute this.

upvoted 1 times

Fcnet 11 months ago

Hi
Answer is C
-retention policy : settings at a site or mailbox level,
-retention label : settings at item level (folder, document, email).
we want to do a retention for emails so we need a retention label
https://learn.microsoft.com/en-us/microsoft-365/compliance/retention

upvoted 2 times

mcas 1 year, 1 month ago

Selected Answer: D

Retention policy https://learn.microsoft.com/en-us/microsoft-365/compliance/retention-policies-exchange?view=o365-worldwide#how-retention-works-for-exchange

upvoted 1 times

wooyourdaddy 1 year, 5 months ago

Selected Answer: D

I wrote the exam today, this question was on it, I choose D, scored 890!

upvoted 1 times

Pravda 1 year, 10 months ago

On exam 1/20/2022

upvoted 1 times

Sam12 1 year, 10 months ago

Selected Answer: D

retention policy

upvoted 1 times

Robert__Susin 1 year, 10 months ago

Selected Answer: D

Retention Policy

upvoted 1 times

mmendozaf 2 years, 1 month ago

According to https://docs.microsoft.com/en-us/microsoft-365/compliance/retention?view=o365-worldwide#adaptive-or-static-policy-scopes-for-retention in the example, should be a retention policy based on a dynamic group.

upvoted 6 times

Coop1234 1 year, 2 months ago

Docs support retention policy as the correct answer for this question... see mmendozaf's link.

upvoted 1 times

Introductory Info

Case study -

This is a case study. Case studies are not timed separately. You can use as much exam time as you would like to complete each case. However, there may be additional case studies and sections on this exam. You must manage your time to ensure that you are able to complete all questions included on this exam in the time provided.

To answer the questions included in a case study, you will need to reference information that is provided in the case study. Case studies might contain exhibits and other resources that provide more information about the scenario that is described in the case study. Each question is independent of the other questions in this case study.

At the end of this case study, a review screen will appear. This screen allows you to review your answers and to make changes before you move to the next section of the exam. After you begin a new section, you cannot return to this section.

To start the case study -

To display the first question in this case study, click the Next button. Use the buttons in the left pane to explore the content of the case study before you answer the questions. Clicking these buttons displays information such as business requirements, existing environment, and problem statements. If the case study has an All Information tab, note that the information displayed is identical to the information displayed on the subsequent tabs. When you are ready to answer a question, click the Question button to return to the question.

Overview -

Fabrikam, Inc. is a consulting company that has a main office in Montreal and six branch offices in New York, Seattle, Miami, Houston, Los Angeles, and
Vancouver.

Existing Environment -

Cloud Environment -

Fabrikam has a Microsoft 365 tenant that contains the following resources:

An on-premises Active Directory domain named corp.fabrikam.com that syncs to an Azure Active Directory (Azure AD) tenant.

Microsoft Cloud App Security connectors configured for all supported cloud applications used by the company.

Some users have company Dropbox accounts.

Compliance Configuration -

Fabrikam has the following in the Microsoft 365 compliance center:

A data loss prevention (DLP) policy is configured. The policy displays a tooltip to users. Users can provide a business justification to override a DLP policy violation.

The Azure Information Protection unified labeling scanner is installed and configured.

A sensitivity label named Fabrikam Confidential is configured.

An existing third-party records management system is managed by the compliance department.

Human Resources (HR) Management System

The HR department has an Azure SQL database that contains employee information. Each employee has a unique 12-character alphanumeric ID. The database contains confidential employee attributes including payroll information, date of birth, and personal contact details.

On-Premises Environment -

You have an on-premises file server that runs Windows Server 2019 and stores Microsoft Office documents in a shared folder named Data.

All end-user computers are joined to the corp.fabrikam.com domain and run a third-party antimalware application.

Business Processes -

Sales Contracts -

Users in the sales department receive draft sales contracts from customers by email. The sales contracts are written by the customers and are not in a standard format.

Employment Applications -

Employment applications and resumes are received by HR department managers and stored in either mailboxes, Microsoft SharePoint Online sites, OneDrive for
Business folders, or Microsoft Teams channels.

The employment application form is downloaded from SharePoint Online and a serial number is assigned to each application.
The resumes are written by the applicants and are in any format.

Requirements -

HR Requirements -
You need to create a DLP policy that will notify the HR department of a DLP policy violation if a document that contains confidential employee attributes is shared externally. The DLP policy must use an Exact Data Match (EDM) classification derived from a CSV export of the HR department database.
The HR department identifies the following requirements for handling employment applications:
Resumes must be identified automatically based on similarities to other resumes received in the past.
Employment applications and resumes must be deleted automatically two years after the applications are received.
Documents and emails that contain an application serial number must be identified automatically and marked as an employment application.

Sales Requirements -
A sensitivity label named Sales Contract must be applied automatically to all draft and finalized sales contracts.

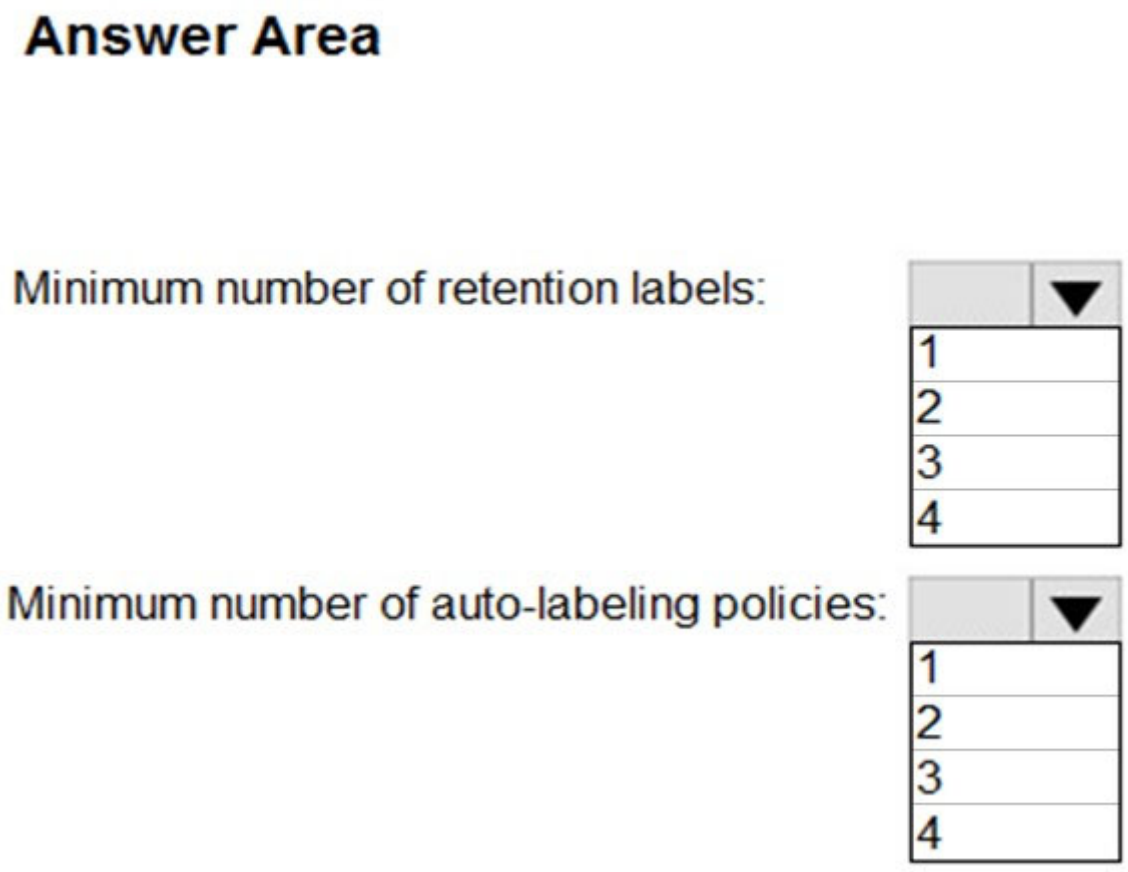
Compliance Requirements -
Fabrikam identifies the following compliance requirements:
All DLP policies must be applied to computers that run Windows 10, with the least possible changes to the computers.
Users in the compliance department must view the justification provided when a user receives a tooltip notification for a DLP violation.
If a document that has the Fabrikam Confidential sensitivity label applied is uploaded to Dropbox, the file must be deleted automatically.
The Fabrikam Confidential sensitivity label must be applied to existing Microsoft Word documents in the Data shared folder that have a document footer containing the following string: Company use only.
Users must be able to manually select that email messages are sent encrypted. The encryption will use Office 365 Message Encryption (OME) v2.
Any email containing an attachment that has the Fabrikam Confidential sensitivity label applied must be encrypted automatically by using OME.
Existing policies configured in the third-party records management system must be replaced by using Records management in the Microsoft 365 compliance center. The compliance department plans to export the existing policies, and then produce a CSV file that contains matching labels and policies that are compatible with records management in Microsoft 365. The CSV file must be used to configure records management in Microsoft 365.

Executive Requirements -
You must be able to restore all email received by Fabrikam executives for up to three years after an email is received, even if the email was deleted permanently.

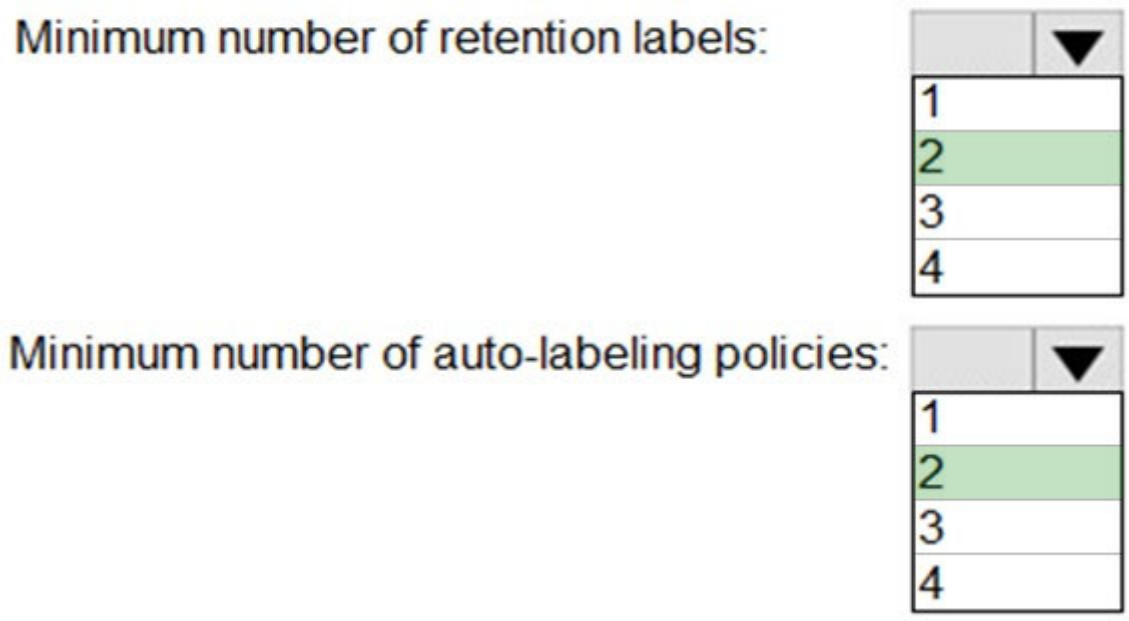
Question
HOTSPOT -
You need to recommend an information governance solution that meets the HR requirements for handling employment applications and resumes. What is the minimum number of information governance solution components that you should create? To answer, select the appropriate options in the answer area.

NOTE: Each correct selection is worth one point.

Hot Area:



Correct Answer:



Reference:

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

Senior Highly Voted 1 year, 10 months ago

1 and 2.

Why do you need to create two retention labels? You can apply the same retention label to both the application and resumes. So create one retention label and 2 auto-apply label policies.

Or am I missing something?

upvoted 11 times

klosedotorg83 Highly Voted 2 years, 1 month ago

It should be 1 and 1

upvoted 7 times

fangeel 1 year, 11 months ago

2 ret. labels and 2 auto-lab. policies would be correct (1 each for both empl. applic. and resumes)

upvoted 3 times

Valavan Most Recent 11 months, 3 weeks ago

Retention Label -1 and Auto labelling Policy - 2

upvoted 1 times

RamenIsDelicious 1 year, 3 months ago

8/15/22, tested should be 1/2:
"Resumes must be identified automatically based on similarities to other resumes received in the past." - Trainable classifier can handle this
"Employment applications and resumes must be deleted automatically two years after the applications are received." - 1 retention label set to two yr retention + 1 auto label policy pointing to the trainer
"Documents and emails that contain an application serial number must be identified automatically and marked as an employment application." - 1 auto labeling policy can satisfy this condition. (also need a sensitive information type but not needed for this question)
upvoted 6 times

PrettyFlyWifi 1 year, 9 months ago
The employment application form is downloaded from SharePoint Online and a serial number is assigned to each application.
The resumes are written by the applicants and are in any format.

Based off this you cannot use the same auto-label policy for both doc types, so you would need to choose 2 auto-label policies so one can "Apply label to content that contains words or phrases..." and another policy to "Apply label to content that matches trainable classifier", which there is a built-in "Resume" classifier for.
upvoted 4 times

PrettyFlyWifi 1 year, 9 months ago
Employment applications and resumes must be deleted automatically two years after the applications are received.

From this requirement, as the retention time is the same, you can use just 1 retention label on both of the retention auto-label policies, so the answer for me is...

1 label
2 auto-label policies
upvoted 1 times

Pravda 1 year, 10 months ago
On exam 1/20/2022
upvoted 1 times

Sam12 1 year, 10 months ago
a sensitive info trainable classifier for the resumes
a sensitive info type for the application, can be EDM, Keywordlist or Regex.
one auto-retention-label policy for each sensitive info type.

so 2 and 2
upvoted 1 times

Sam12 1 year, 10 months ago
my bad, for the first part it is asking for a retention label and not sensitivity label/type.
So 1 and 2(assuming that both sensitive info types were previously created.)
upvoted 2 times