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

Suggested 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 3 years, 6 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 23 times

Mdwro 3 years, 5 months ago
I think it is correct
upvoted 2 times

UWSFish 3 years, 5 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 3 years, 4 months ago
exclude the NOT, you need an auto-label policy for it to surface in MDCA
upvoted 1 times

cng Highly Voted 4 years, 1 month 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 20 times

blokechettri Most Recent 9 months, 2 weeks ago
auto label cannot be applied to cloud app security and non-publised cannot be appied. Therefore, it is only Sensitivity1. Answer is A
upvoted 1 times

doori88 1 year, 5 months ago
just tested it, only the published labels appear, labels with Auto-apply labeling policy dont appear in the governance actions of File policy in MDCA
upvoted 2 times

Davidf 1 year, 10 months ago
Selected Answer: A

Tested in a sandbox tenant, only sensitivity1 is available

upvoted 3 times

TeeKay_From_the_South 2 years 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 2 years, 1 month ago

just tested it, its Sensitivity label 1 only so answer is A

upvoted 1 times

dmoorthy 2 years, 2 months ago

Selected Answer: A

upvoted 1 times

xswe 2 years, 2 months 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

mcas 2 years, 8 months 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 2 times

mandragon 3 years 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 4 times

JamesM9 3 years, 2 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 3 years, 1 month 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 3 years, 5 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** 3 years, 1 month 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** 3 years, 9 months ago

Correct answer
upvoted 2 times

⊟ **MahmoudEldeep** 3 years, 11 months ago

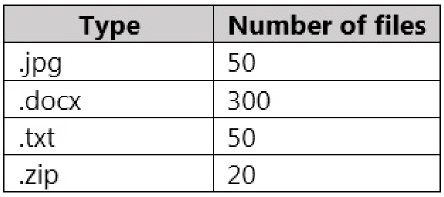
I think correct anser is B. As you can use any created sensitivity labels even if it is not published.
upvoted 1 times

⊟ **pheb** 3 years, 10 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.

Suggested Answer: *C*
Reference:
https://docs.microsoft.com/en-us/cloud-app-security/azip-integration

Community vote distribution
C (80%) B (20%)

jcgonzalez1978 Highly Voted 3 years, 10 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 25 times

sergioandreslq 3 years, 6 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 5 times

ca7859c Most Recent 1 month, 3 weeks ago

Selected Answer: C

https://learn.microsoft.com/en-us/purview/apply-sensitivity-label-automatically
On the Page:
Specific to auto-labeling for SharePoint and OneDrive:

PDF documents and Office files for Word (.docx), PowerPoint (.pptx), and Excel (.xlsx) are supported.

upvoted 1 times

joneszy 5 months ago

Selected Answer: B

https://learn.microsoft.com/en-us/defender-cloud-apps/data-protection-policies#file-filters The Defender for Cloud Apps engines perform content inspection by extracting text from all common file types (100+) including Office, Open Office, compressed files, various rich text formats, XML, HTML, and more.

upvoted 1 times

blokechettri 9 months, 2 weeks ago

A - It is correct presuming auto label in question is service side auto label. However, if auto-label for client side is applied then the answer will changed to S1 and S2

upvoted 1 times

taufiquzzaman 1 year, 3 months ago

Selected Answer: C

Answer is correct as of today, where Word, Excel, PowerPoint, PDF are the only supported file types for classification for now.

upvoted 1 times

Davidf 1 year, 10 months 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 2 years, 1 month ago

Qual e a resposta correta? rsrsrs Eu vou de C

upvoted 1 times

xswe 2 years, 2 months 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 2 years, 2 months ago

I mean ---- C

upvoted 1 times

wooyourdaddy 3 years, 1 month 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 3 years, 3 months ago

The answer is correct as of today.

upvoted 1 times

MahmoudEldeep 3 years, 11 months ago

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

upvoted 4 times

Eltooth 4 years ago

Answer appears to be correct.

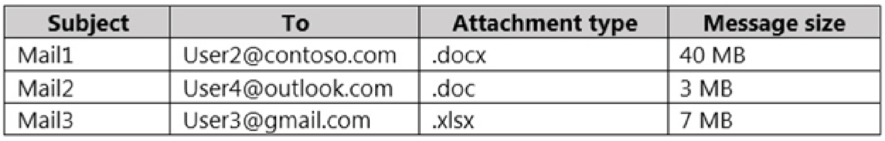
upvoted 3 times

Question #3 Topic 1

HOTSPOT -

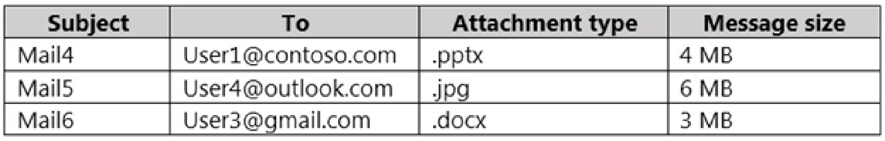
You have a Microsoft 365 tenant named contoso.com that contains two users named User1 and User2. The tenant uses Microsoft Office 365 Message Encryption
(OME).

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.

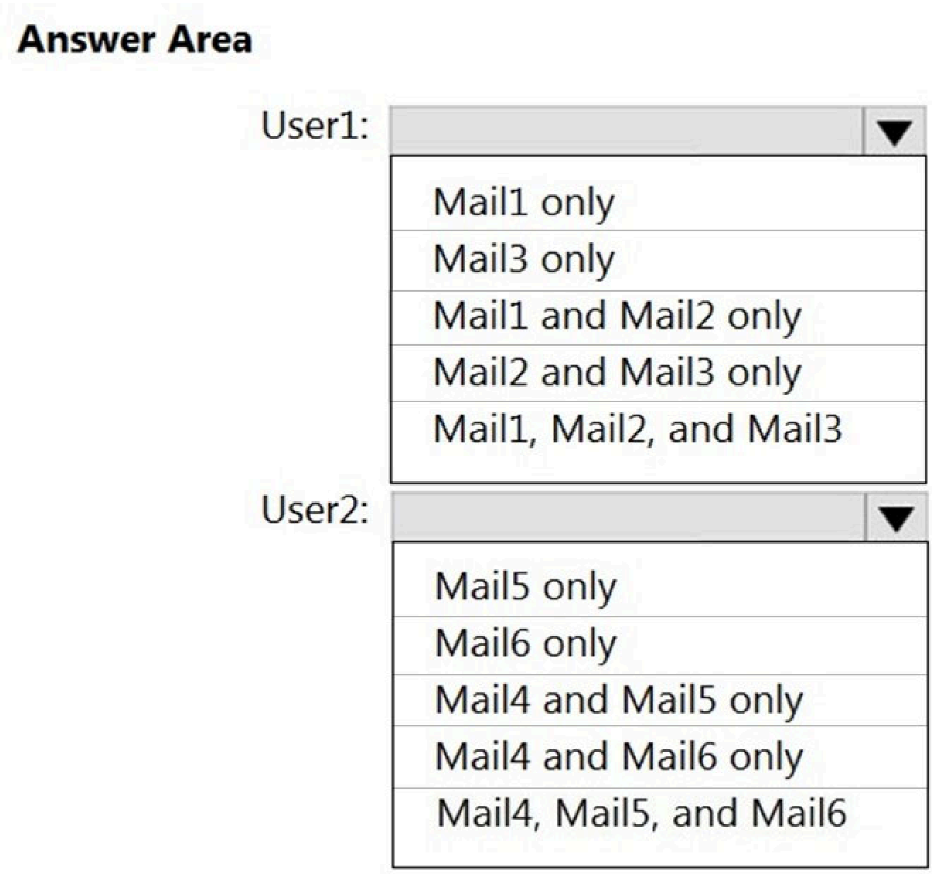


Subject	To	Attachment type	Message size
Mail4	User1@contoso.com	.pptx	4 MB
Mail5	User4@outlook.com	.jpg	6 MB
Mail6	User3@gmail.com	.docx	3 MB

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

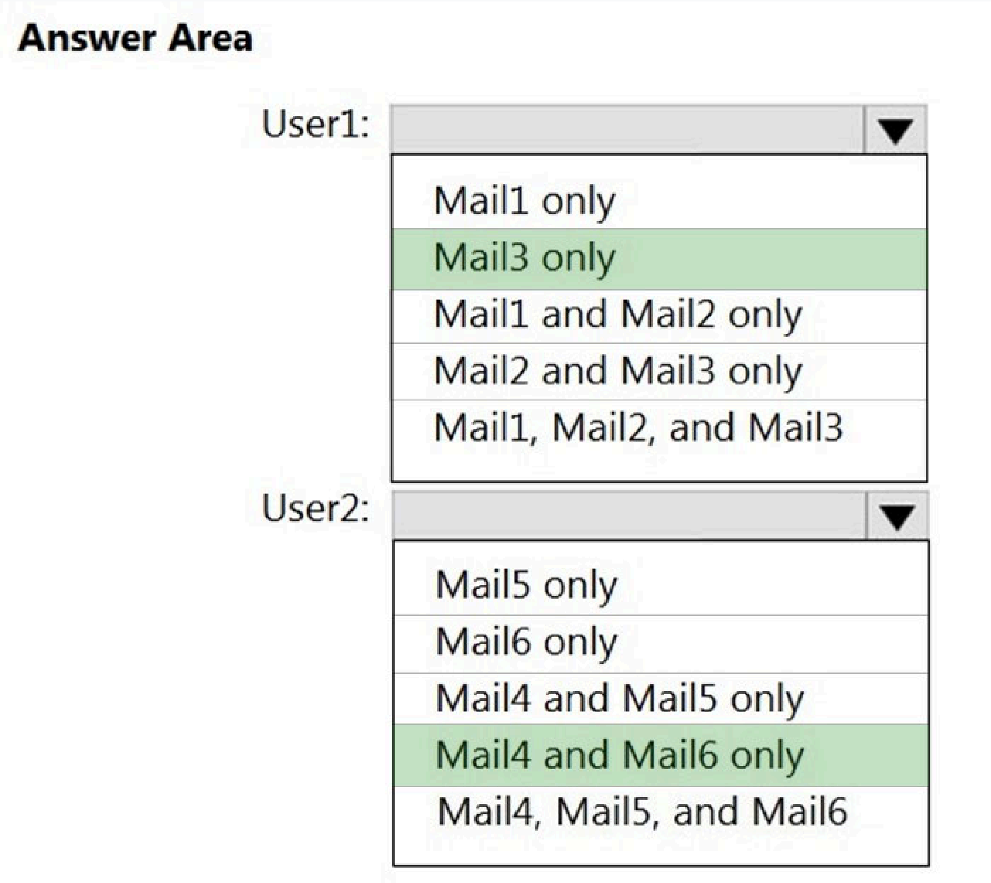
User1:

- 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

Suggested Answer:



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

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 3 years, 7 months ago

Mail1 Size is bigger than supported and JPG is not supported format

upvoted 26 times

sergioandreslq 3 years 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 7 times

BTAB 2 years, 7 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 3 years, 6 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 3 years, 6 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 3 years, 4 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

Futfuyfyjfj 11 months, 2 weeks ago

.doc doesn't show up at your Microsoft docs page (anymore)? https://learn.microsoft.com/en-us/purview/ome-faq?view=o365-worldwide#what-file-types-are-supported-as-attachments-in-protected-emails--do-attachments-inherit-the-protection-policies-and-permissions-associated-with-protected-emails-

upvoted 1 times

Topaz007 3 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 1 year, 3 months ago

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

upvoted 4 times

louisaok 11 months, 2 weeks ago

Organizations that were using OME should have transitioned to Microsoft Purview Message Encryption.

upvoted 3 times

xswe 1 year, 8 months 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 5 times

MartinSebek 1 year, 11 months 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 7 times

NinjaSchoolProfessor 2 years 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 3 times

Davidf 1 year, 4 months ago

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

upvoted 2 times

mimguy 12 months ago

Don't ignore this answer, if you follow this link: https://learn.microsoft.com/en-us/purview/ome?view=o365-worldwide
You'll find the section 'How Message Encryption works' which will bring you to this link which calls out that .doc is supported, among others.
https://support.office.com/article/bb643d33-4a3f-4ac7-9770-fd50d95f58dc#FileTypesforIRM

upvoted 1 times

Futfuyfyjfj 11 months, 2 weeks ago

You URL brings you to this page where the OME/Purview message encryption is still being mentioned as 25MB...?
https://learn.microsoft.com/en-us/office365/servicedescriptions/exchange-online-service-description/exchange-online-limits#message-

limits-1

upvoted 1 times

NinjaSchoolProfessor 2 years, 5 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 2 years, 9 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%20emai

upvoted 11 times

mimguy 12 months ago

.doc is supported https://support.microsoft.com/en-us/office/introduction-to-irm-for-email-messages-bb643d33-4a3f-4ac7-9770-fd50d95f58dc?ui=en-us
us&ad=us#FileTypesforIRM

upvoted 1 times

daavidsc400 2 years, 9 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 2 times

iJabu 2 years, 10 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 2 years, 10 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 2 years, 11 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 2 years, 11 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 2 years, 10 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 2 years, 11 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 2 years, 11 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 2 years, 11 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 3 years 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

samcool80 3 years, 5 months ago

User 1 Answer is correct

User 2 - Should be mail 6 only as the mail 4 is contoso.com domain and mail 5 is .jpg extensions which i guess is not supported

upvoted 3 times

Question #4 *Topic 1*

HOTSPOT -

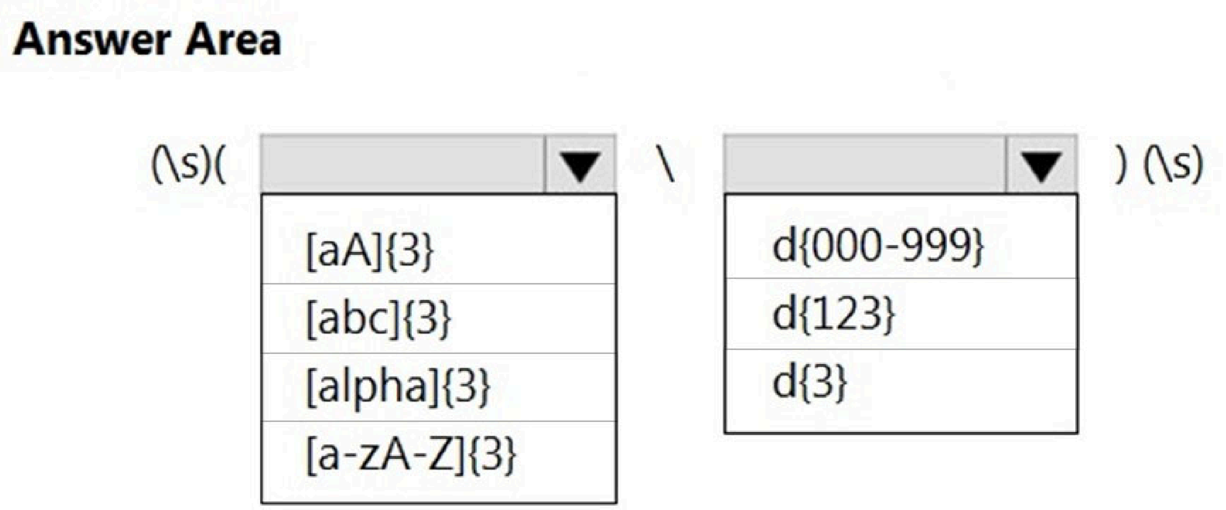
You use project codes that have a format of three alphabetical characters that represent the project type, followed by three digits, for example Abc123.

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:



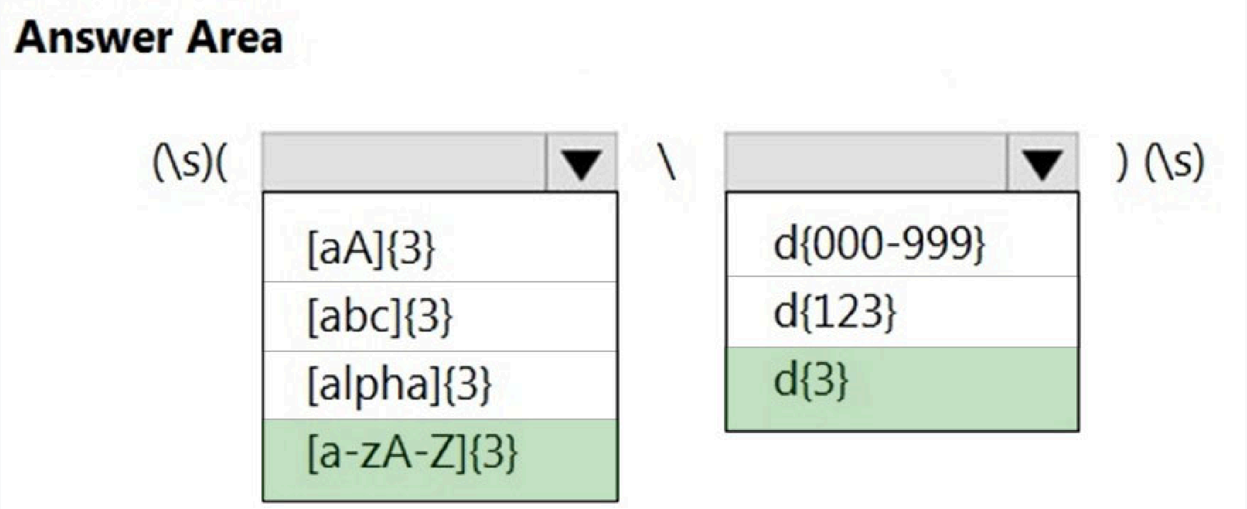
Answer Area

(\s)(▼ \ ▼) (\s)

- [aA]{3}
- [abc]{3}
- [alpha]{3}
- [a-zA-Z]{3}

- d{000-999}
- d{123}
- d{3}

Suggested Answer:



Answer Area

(\s)(▼ \ ▼) (\s)

- [aA]{3}
- [abc]{3}
- [alpha]{3}
- [✓ [a-zA-Z]{3}]

- d{000-999}
- d{123}
- [✓ d{3}]

Reference:

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

⊟ **liozuf** Highly Voted 2 years, 7 months ago

\d{3} correct answer

upvoted 26 times

⊟ **HardcodedCloud** Highly Voted 2 years 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

⊟ **xswe** Most Recent 8 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 3 times

⊟ **klosedotorg83** 2 years, 2 months ago

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

upvoted 3 times

⊟ **oberte007** 2 years, 2 months 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, 8 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, 5 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, 7 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 -

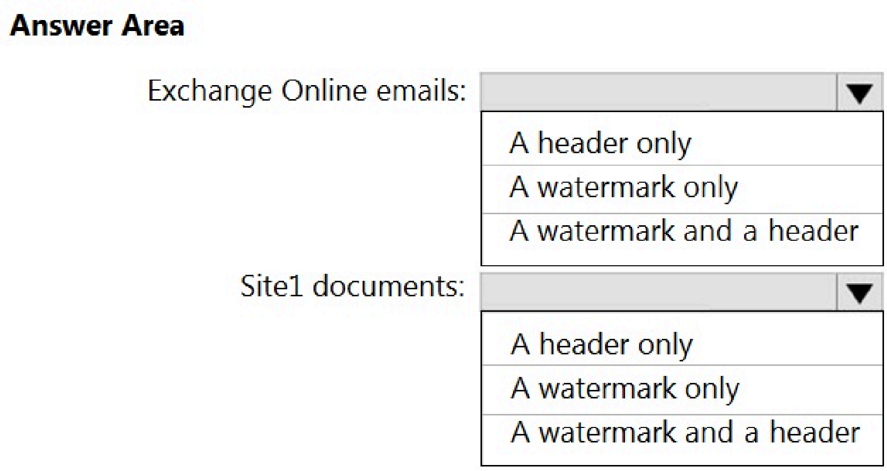
You have a Microsoft SharePoint Online site named Site1 and a sensitivity label named Sensitivity1. Sensitivity1 adds a watermark and a header to content.

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:

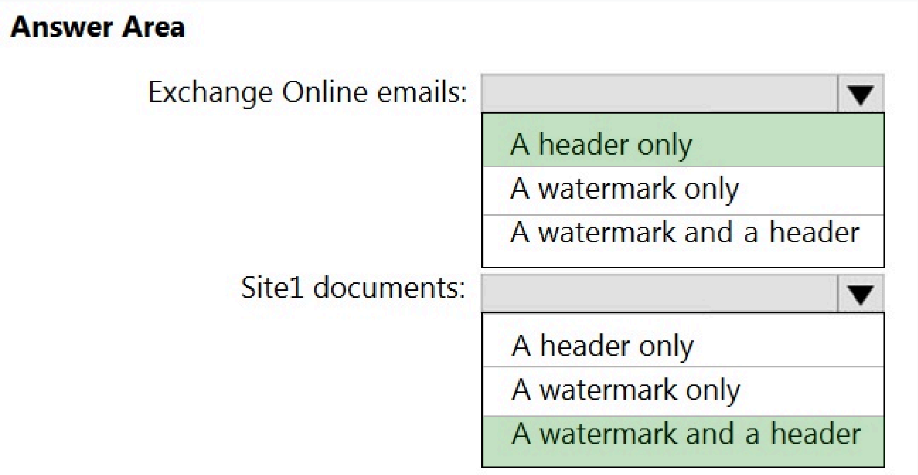


Answer Area

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

Suggested Answer:



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]

Reference:

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

pheb92 Highly Voted 3 years, 7 months ago

this is correct!

outlook does not support watermarks

upvoted 17 times

wooyourdaddy Highly Voted 2 years, 6 months ago

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

upvoted 5 times

Domza Most Recent 12 months ago

You all saying the same thing LOL why?

upvoted 2 times

xswe 1 year, 8 months 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

HardcodedCloud 3 years 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** 3 years, 3 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** 3 years, 5 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

Question #6 *Topic 1*

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.

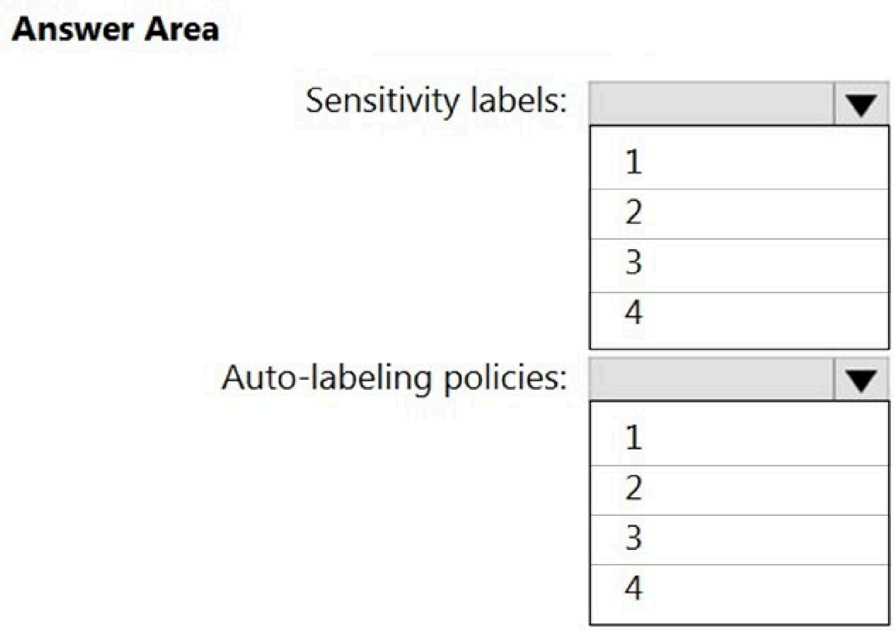
✑ When a user attempts to send an email or an attachment that contains a passport number, the user must receive a tooltip in Microsoft Outlook.

✑ 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:

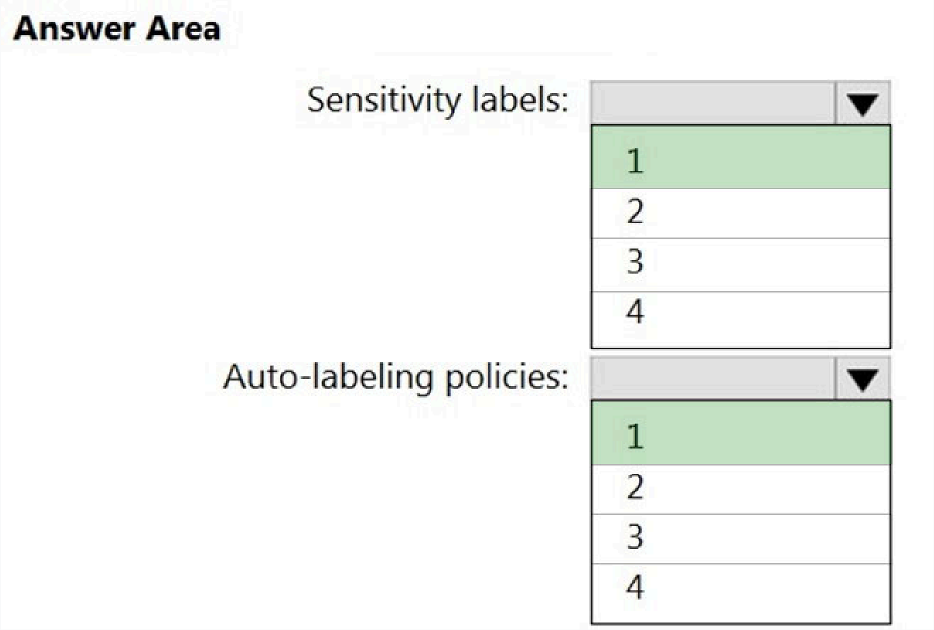


Answer Area

Sensitivity labels: ▼
- 1
- 2
- 3
- 4

Auto-labeling policies: ▼
- 1
- 2
- 3
- 4

Suggested Answer:



Answer Area

Sensitivity labels: ▼
- [✓ 1]
- 2
- 3
- 4

Auto-labeling policies: ▼
- [✓ 1]
- 2
- 3
- 4

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 3 years, 5 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 33 times

test123123 Highly Voted 3 years, 6 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 22 times

mbhasker Most Recent 1 year, 1 month ago

3 Sensitivty Label and 1 Auto Label Policy

upvoted 1 times

Domza 12 months ago

Nice one LOL

upvoted 1 times

hsinchang 1 year, 4 months 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 7 times

Softeng 11 months ago

Clear answer. Thank you.

upvoted 1 times

xswe 1 year, 8 months 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

klosedotorg83 3 years, 3 months ago

1 Sensitivty Label and 1 Auto Label Policy

upvoted 7 times

NW16 3 years, 5 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 3 years, 7 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 3 years, 7 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 7 times

dasha_an 3 years, 7 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

⊟ **Piper** 3 years, 7 months ago

So you think 1 Sensitivity label and 2 DLP policies?

upvoted 1 times

⊟ **pheb** 3 years, 4 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)

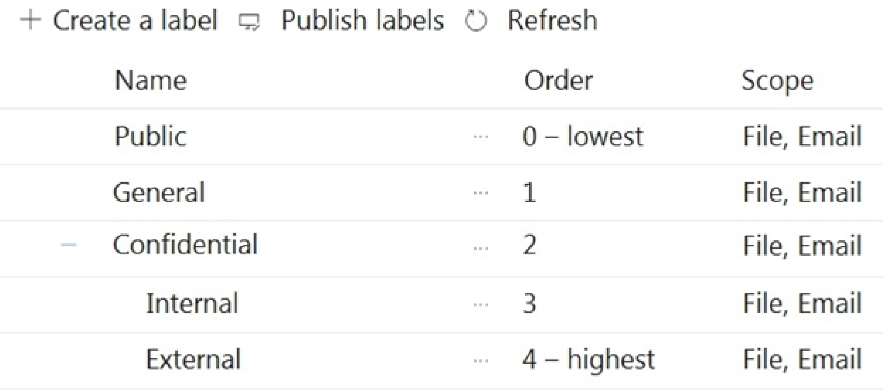
upvoted 3 times

Question #7 Topic 1

HOTSPOT -

You have a Microsoft 365 E5 tenant.

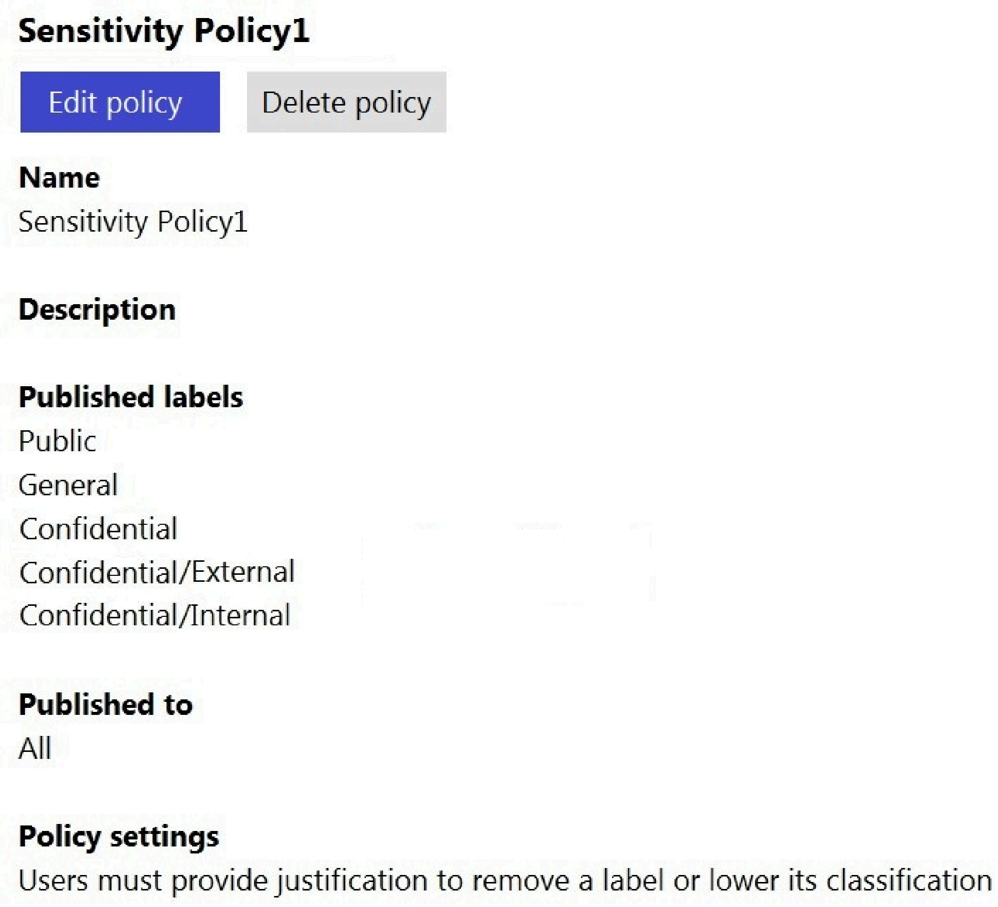
You create sensitivity labels as shown in the Sensitivity Labels exhibit.



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

Name

Sensitivity Policy1

Description

Published labels

Public
General
Confidential
Confidential/External
Confidential/Internal

Published to

All

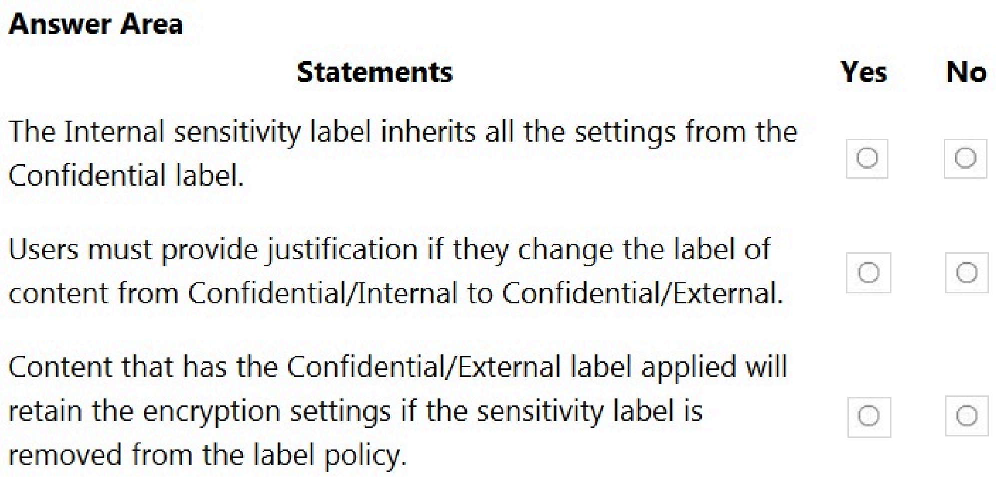
Policy settings

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.

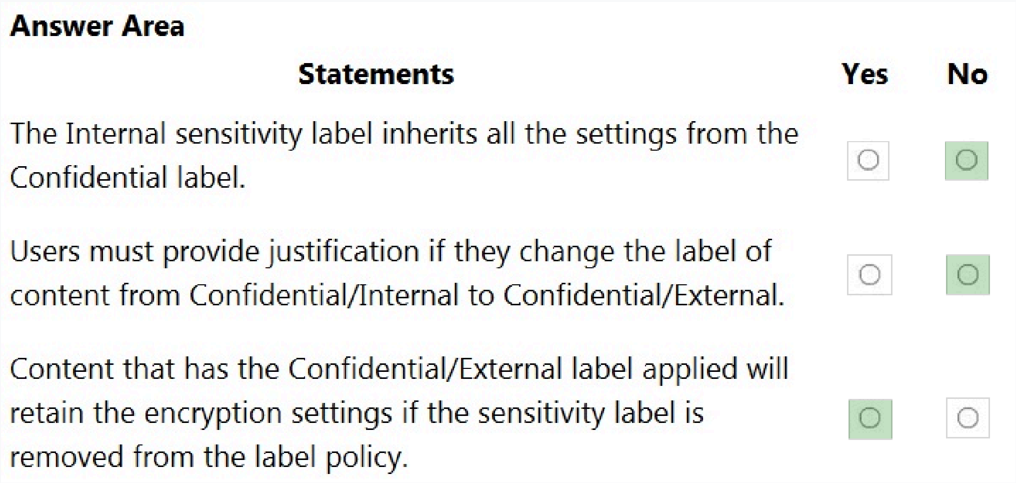
Hot Area:



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.	○	○

Suggested Answer:



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.	[✓ ○]	○

Reference:

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

Eltooth Highly Voted 4 years ago

No /No / Yes - correct

upvoted 20 times

fimbulvetrk Highly Voted 9 months, 1 week 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 17 times

UnitedKendom Most Recent 9 months, 1 week 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 3 years, 1 month 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]** 3 years, 1 month ago

Well said

upvoted 1 times

⊟ **prats005** 9 months, 1 week 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

⊟ **xswe** 9 months, 1 week 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 5 times

⊟ **RUPI04** 11 months, 1 week ago

Now we have track and revoke option, does that make option 3 as No as well

upvoted 1 times

⊟ **shanti0091** 3 years, 11 months ago

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

upvoted 4 times

⊟ **olsi** 4 years 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.

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

dasha_an Highly Voted 👍 2 years, 7 months ago
Resumes, Source code, Harassment, Profanity, Threat are pre-trained classifiers that exist already in Microsoft 365 -> Source code is correct
upvoted 23 times

JCkD4Ni3L 1 year 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 2 times

Anker 2 years, 6 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 11 times

xswe Most Recent 🕐 8 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 12 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

Eltooth 2 years, 6 months ago
Agreed - C.
upvoted 4 times

k4d4v4r 2 years, 7 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, 7 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, 6 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

Suggested 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%)

⊟ **dasha_an** Highly Voted 4 years, 1 month 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 14 times

⊟ **EM1234** 1 year ago
This link does not say anything about global admin anymore
upvoted 2 times

⊟ **Piper** 4 years, 1 month 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

⊟ **[Removed]** 1 year, 6 months ago
From the phrasing of the question it seems like it's asking what's required to opt in. Typical Microsoft trickery.

You need to "ENSURE" that custom trainable classifiers "CAN BE CREATED" in the tenant.

To ensure that the classifier can be created the tenant must be opted in. To opt in you must be a global admin. After opting in the creation and tanning of the classifiers can be delegated to "Compliance Administrators"
upvoted 1 times

⊟ **Anker** 4 years ago
Agreed, I would ere on the side of minimum required permissions as well and Compliance Administrator fits that criteria.
upvoted 2 times

⊟ **Eltooth** 4 years 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

⊟ **MahmoudEldeep** Highly Voted 3 years, 11 months ago
Based on my label test. the correct answer is Compliance administrator
upvoted 6 times

⊟ **Oujay** Most Recent 2 months ago
Selected Answer: D

Global Admin has the highest level of permissions across Microsoft 365, but it is not automatically granted permissions inside specialised portals like Microsoft Purview (compliance portal) for sensitive tasks such as data classification, DLP, or trainable classifiers.

upvoted 1 times

trut_hz 5 months, 1 week ago

Selected Answer: D

D. Compliance administrator

Explanation:

Custom trainable classifiers are part of Microsoft Purview compliance solutions.

The Compliance administrator role has the necessary permissions to configure and manage compliance settings, including trainable classifiers, data loss prevention policies, and more.

While the Global administrator (C) also has broad permissions across the tenant, the Compliance administrator is more targeted to this specific compliance functionality.

upvoted 2 times

Don_Barriga 8 months, 1 week ago

To ensure that custom trainable classifiers can be created in a Microsoft 365 tenant, you need to be assigned the Compliance Administrator role. This role has the necessary permissions to manage compliance features, including the ability to create and manage trainable classifiers within Microsoft Purview's Information Protection and Data Loss Prevention (DLP) functionalities.

Alternatively, the Security Administrator or Global Administrator roles may also have permissions to perform these actions, but Compliance Administrator is the most directly aligned role for this task.

upvoted 2 times

MKnight25 8 months, 2 weeks ago

Selected Answer: D

D is correct, tested in a demo tenant

upvoted 3 times

belyo 8 months, 3 weeks ago

Selected Answer: D

https://learn.microsoft.com/en-us/purview/trainable-classifiers-get-started-with?view=o365-worldwide#:~:text=either%20Compliance%20admin%20or%20Security%20admin

requirements to create trainable classifiers are either CA or SA

GA is not relevant

upvoted 2 times

[Removed] 9 months, 1 week ago

Selected Answer: C

From the phrasing of the question it seems like it's asking what's required to opt in. Typical Microsoft trickery.

You need to "ENSURE" that custom trainable classifiers "CAN BE CREATED" in the tenant.

To ensure that the classifier can be created the tenant must be opted in. To opt in you must be a global admin. After opting in the creation and tanning of the classifiers can be delegated to "Compliance Administrators"

upvoted 1 times

SDiwan 9 months, 1 week ago

Selected Answer: C

Who can create trainable classifier? Compliance admin and global admin.

Who can enable trainable classifier? Global admin.

The questions asks "You need to ensure that custom trainable classifiers can be created in the tenant." . So it the answer is C, global admin need to enable the settings so that compliance admin can create the trainable classifier.

upvoted 3 times

Oujay 2 months ago

Who can create a trainable classifier? Compliance admin

Who can enable a trainable classifier? Compliance admin

Just being a Global Admin is not enough to perform that task immediately without extra steps. A Global Admin will have to assign themselves the Compliance Administrator role and then enable a trainable classifier on the tenant, and then create custom trainable classifiers.

The compliance Administrator role is enough because it includes permissions to configure tenant-level compliance features (including opting in to trainable classifiers).

upvoted 1 times

JimboJones99 11 months, 2 weeks ago

Selected Answer: D

https://learn.microsoft.com/en-us/purview/trainable-classifiers-get-started-with#how-to-create-a-trainable-classifier

Need Compliance Admin or Security Admin. Compliance is the role with the least privilege of the 2.

upvoted 1 times

PsiCzar 11 months, 2 weeks ago

As someone who does this for a living, for customers. The answer is D. Compliance Administrator. I'm never given GA access to a company's environment.

upvoted 1 times

perrito_css 1 year ago

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

Choose the Trainable classifiers tab.

upvoted 1 times

milosp 1 year, 3 months ago

Selected Answer: D

To perform the configuration and ensure that custom trainable classifiers can be created in the tenant, you should be assigned to the Compliance administrator (Option D) role.

upvoted 2 times

SSL2 1 year, 3 months ago

Selected Answer: D

To configure custom trainable classifiers in your new Microsoft 365 tenant, you should be assigned the **Compliance administrator** role. This role provides the necessary permissions to manage compliance features, including trainable classifiers. By having this role, you'll be able to create and configure custom classifiers to enhance data loss prevention (DLP) and other compliance-related tasks within your organization. Remember to assign this role to the appropriate user account to perform the necessary configuration tasks.

upvoted 1 times

Ruslan23 1 year, 4 months ago

Selected Answer: D

Principle of the least privilege, also C is correct.

upvoted 1 times

mbhasker 1 year, 7 months ago

D. Compliance administrator

upvoted 1 times

Davidf 1 year, 10 months ago

Selected Answer: C

NEW tenant - Global admin is required to opt in

upvoted 5 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

Suggested 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 (90%) 10%

⊟ **k4d4v4r** Highly Voted 4 years, 1 month 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 20 times

⊟ **Jideakin** 3 months ago

You'll also need a Label, right? otherwise, what are you auto-applying?

upvoted 1 times

⊟ **lime568** 3 years, 9 months ago

what about "... and configuration information."?

upvoted 1 times

⊟ **josepedroche** Highly Voted 4 years ago

I'd say B & F

B: custom trainable to identify identify computers name, ip adress, etc..

F: sensitivity label with auto-labeling for files and mail support as condition sensitivity info and trainable classifies (information protection auto-labeling) does not support trainable classifiers

upvoted 6 times

⊟ **Contactfornitish** Most Recent 1 month ago

Selected Answer: AC

E. for structured data like IP addresses and computer names, regular expressions (C) are far more effective and less prone to false positives or negatives.

F. sensitivity label that has auto-labeling is non-existent

B. Trainable classifiers are excellent for identifying types of content based on examples, rather than rigid patterns. Here we talking about machine names and IP Address which would follow easy pattern so trainable classifiers are overkill.

D. DLP policies can leverage sensitive info types, but they don't directly apply sensitivity labels for classification in the way an auto-labeling policy does.

upvoted 1 times

⊟ **trut_hz** 5 months ago

Selected Answer: AF

To automatically apply a sensitivity label to documents containing network information like computer names and IP addresses, you need two key components: a policy to enforce the label based on content detection and the sensitivity label itself.

A. An Information protection auto-labeling policy is required to define the conditions (e.g., sensitive information types) that trigger the label application. This policy specifies how content is scanned and which label to apply.

F. A sensitivity label that has auto-labeling is necessary because the label must be configured to be applied automatically through the policy. The label defines the classification and protection settings for the document.

upvoted 2 times

⊟ **NikPat3125** 6 months, 1 week ago

Selected Answer: AB

A = Keyword "autolabeling policy". in order to apply label you need auto-labelling policy.

B = Keyword "Configuration information" . You cannot use sensitive info type for cofiguration info.

upvoted 1 times

⊟ **Fren686478** 6 months, 3 weeks ago

Selected Answer: AC

C to match the content. A to auto apply

upvoted 1 times

⊟ **uilloz** 8 months ago

sensitivity label that has auto-labeling can be applied only to content you create or edit, so we need a policy here! to apply lòabels to at rest docs (shareopint for example). The second part can be done with regex or keywords so A + C or E

upvoted 2 times

⊟ **blokechettri** 9 months, 2 weeks ago

It is misleading with custom STI over tainable SIT. trainable SIT requires document seeding

upvoted 1 times

⊟ **narenbabu.chintu** 11 months, 3 weeks ago

AE -

First create Sensitive type info based on key words

Then

Create a auto labelling policy and call this sensitive info type.

upvoted 1 times

⊟ **narenbabu.chintu** 11 months, 3 weeks ago

How a customer trainable classifier is created when there are IP address, Computer names etc?

Customer trainable classifiers is mainly for documents. the classifier needs 50 to 500 positive sample documents and some negetive sample documents to train the classifier.

Although the questions says documents, the trick is a document can contain IP address, computer names etc in any place or in any format.

So, create sensitive type info based on key words.

then create auto labelling policy

upvoted 1 times

⊟ **EM1234** 1 year ago

Selected Answer: CF

I can only imagine the many, many meetings it would take to agree on what "configuration" information" is and how to identify it....

The real answer would be to argue about it for three years until you get your next role.

upvoted 3 times

> ⊟ **EM1234** 1 year ago
>
> Also, I really have no idea on what the answer is for this one. I am going with C and F for now, as I think you could do it with those.
>
> What even (precisely) is an "information protection auto labeling policy"? Do they mean sensitivity label auto labeling?
>
> upvoted 1 times

⊟ **Sinaes** 1 year, 4 months ago

A & F "You need to automatically apply"

upvoted 1 times

⊟ **mbhasker** 1 year, 7 months ago

correct answer: AB

upvoted 3 times

⊟ **dmoorthy** 2 years, 2 months 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 3 times

xswe 2 years, 2 months 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

trut_hz 5 months, 1 week ago
Isnt there a builtin classifier for that kind of stuff? So then A F?
upvoted 1 times

NinjaSchoolProfessor 2 years, 6 months 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

prats005 2 years, 11 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

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

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

olsi Highly Voted 4 years, 1 month ago
correct, has to be SP Online folder
upvoted 13 times

sergioandreslq 3 years, 6 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 4 times

fiksarion Most Recent 6 months, 3 weeks ago
Selected Answer: A
In preview: The following process automates the testing of trainable classifiers and shortens the creation workflow from 12 days to two days. (In some cases, the process can take only a few hours.)

Collect between 50-500 seed content items that strongly represent the data you want the classifier to positively identify as being in the category. For a list of supported file types, see Default crawled file name extensions and parsed file types in SharePoint Server.

Collect a second set of seed content (from 150 - 1500 items) that represents data that don't belong in the category.

Place the positive and negative seed content in separate SharePoint folders. Each folder must be dedicated to holding only the seed content. Make note of the site, library, and folder URL for each set.
upvoted 1 times

blokechettri 9 months, 2 weeks ago
SPO folder location A is correct
upvoted 1 times

xswe 2 years, 2 months 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 3 times

Bluebaron520 2 years, 7 months ago
valid 24/11/2022
upvoted 2 times

Pravda 3 years, 5 months ago
On exam 1/20/2022
upvoted 2 times

⊟ **examkid** 3 years, 8 months 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.

Suggested 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 3 years, 8 months 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 11 times

sergioandreslq 3 years, 6 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 10 times

husamshahin Highly Voted 11 months, 1 week ago
on Exam 28-7-2024
upvoted 5 times

blokechettri Most Recent 9 months, 2 weeks ago
D. New-OMEConfiguration cmdlet. (OME encryption is the only encryption that allows branding)
upvoted 1 times

hsinchang 1 year, 10 months 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 2 years, 2 months 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 2 years, 7 months ago

valid 24/11/2022

upvoted 3 times

wooyourdaddy 3 years 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 3 years, 6 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

jcgonzalez1978 3 years, 10 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

Piper 4 years, 1 month 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

Suggested 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 3 years, 11 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

⊟ **VitaliLuca** 4 months, 3 weeks ago
Old, now it's 5 times per day
https://learn.microsoft.com/en-us/purview/sit-use-exact-data-refresh-data
upvoted 2 times

⊟ **cris_exam** Highly Voted 2 years 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 17 times

⊟ **NikPat3125** Most Recent 6 months, 1 week ago
Selected Answer: C
https://learn.microsoft.com/en-us/purview/sit-use-exact-data-refresh-data.
It will be 5 times per day. the nearest is 6 hours. This question needs to be changed.
upvoted 4 times

⊟ **blokechettri** 9 months, 2 weeks ago
B. twice per day
upvoted 1 times

⊟ **ShrawanBhat1991** 1 year, 2 months ago
EDMUploadAgent can be used 5 times per day
Correct Answer : C
This question is old : before new update it used to be only twice per day
upvoted 2 times

⊟ **damconsult** 1 year, 5 months ago

since you can use this function up to 5 times a day surely C would be a correct answer because you can use it every 6 hours 4 times a day rather than B twice a day - every 12 hours

upvoted 1 times

mbhasker 1 year, 7 months ago

A. twice per week

upvoted 2 times

RChahal 1 year, 7 months ago

changed to five times per day

upvoted 1 times

JacoH 1 year, 7 months 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 1 year, 10 months ago

was on Exam August 9, 2023

upvoted 2 times

slick_orange 2 years, 1 month 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 2 years, 2 months 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 2 years, 7 months ago

valid 24/11/2022

upvoted 3 times

hapthompson88 2 years, 9 months ago

B is correct

upvoted 3 times

prabhjot 2 years, 9 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 2 years, 10 months ago

Selected Answer: B

Correct Answer

upvoted 3 times

palciny 2 years, 10 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

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:

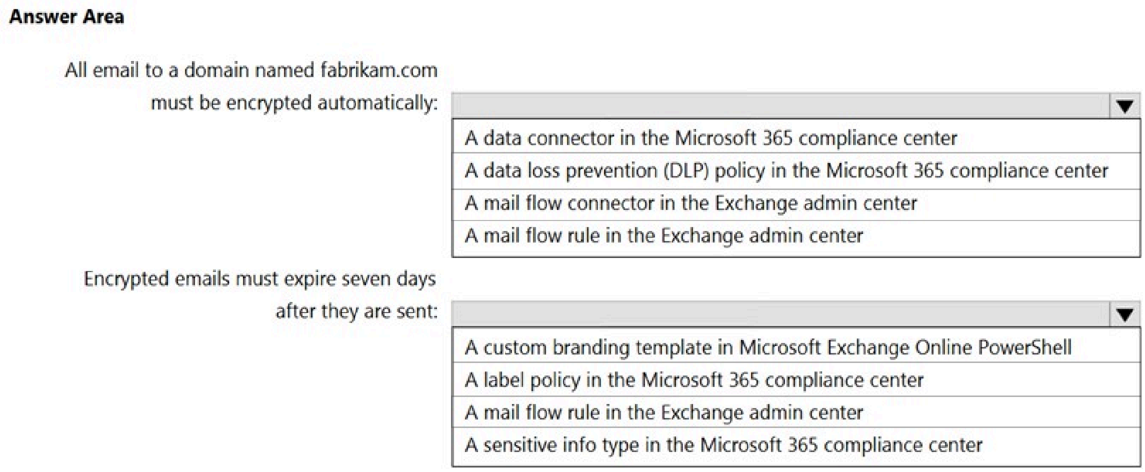
✑ All email to a domain named fabrikam.com must be encrypted automatically.

✑ 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

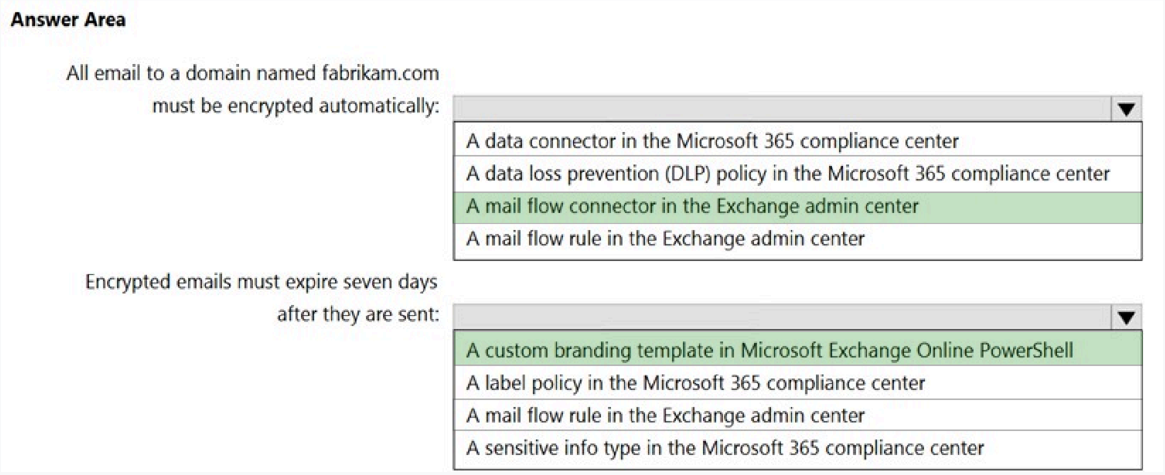
All email to a domain named fabrikam.com must be encrypted automatically: ▼

- 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

Suggested 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 3 years, 12 months ago

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

upvoted 57 times

⊟ **Rockalm** 2 years, 5 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 4 times

⊟ **ccKane** 2 years, 10 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

⊟ **JakubK64** Highly Voted 3 years, 12 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 3 years, 12 months ago

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

upvoted 2 times

Nivos300 Most Recent 5 months ago

A Mail Flow Rule in the Exchange admin center
And
A Custom Branding Template

https://learn.microsoft.com/en-us/purview/define-mail-flow-rules-to-encrypt-email

https://learn.microsoft.com/en-us/purview/ome-advanced-expiration

upvoted 1 times

Boeroe 8 months, 3 weeks ago

DLP would be the correct answer at this time, as all mail rules are to be migrated to Purview DLP as the message in EO mentions:
"DLP policies and DLP-related conditions and actions in Mail flow rules are no longer supported and can no longer be created or edited in the Exchange Admin Center (EAC) or using Exchange Online PowerShell. We recommend migrating all DLP-related rules to Microsoft Purview DLP in the compliance center as soon as possible. Once you have migrated these rules please delete them here in the EAC or via PowerShell"

upvoted 3 times

ca7859c 1 month, 3 weeks ago

Yes!!!

upvoted 1 times

ShrawanBhat1991 1 year, 2 months ago

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

upvoted 1 times

Domza 1 year, 5 months ago

New info:
~You can force recipients to use the encrypted message portal to view and reply to encrypted emails sent from your organization by using a custom branded template that specifies an expiration date in Microsoft PowerShell.

upvoted 1 times

dmoorthy 2 years, 2 months ago

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

upvoted 1 times

xswe 2 years, 2 months 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 2 years, 7 months 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 2 years, 7 months ago

valid 24/11/2022

upvoted 1 times

wooyourdaddy 3 years ago

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

upvoted 3 times

⊟ **junior6995** 3 years ago

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

upvoted 2 times

⊟ **ChaBum** 3 years, 5 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** 2 years, 11 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** 3 years, 10 months ago

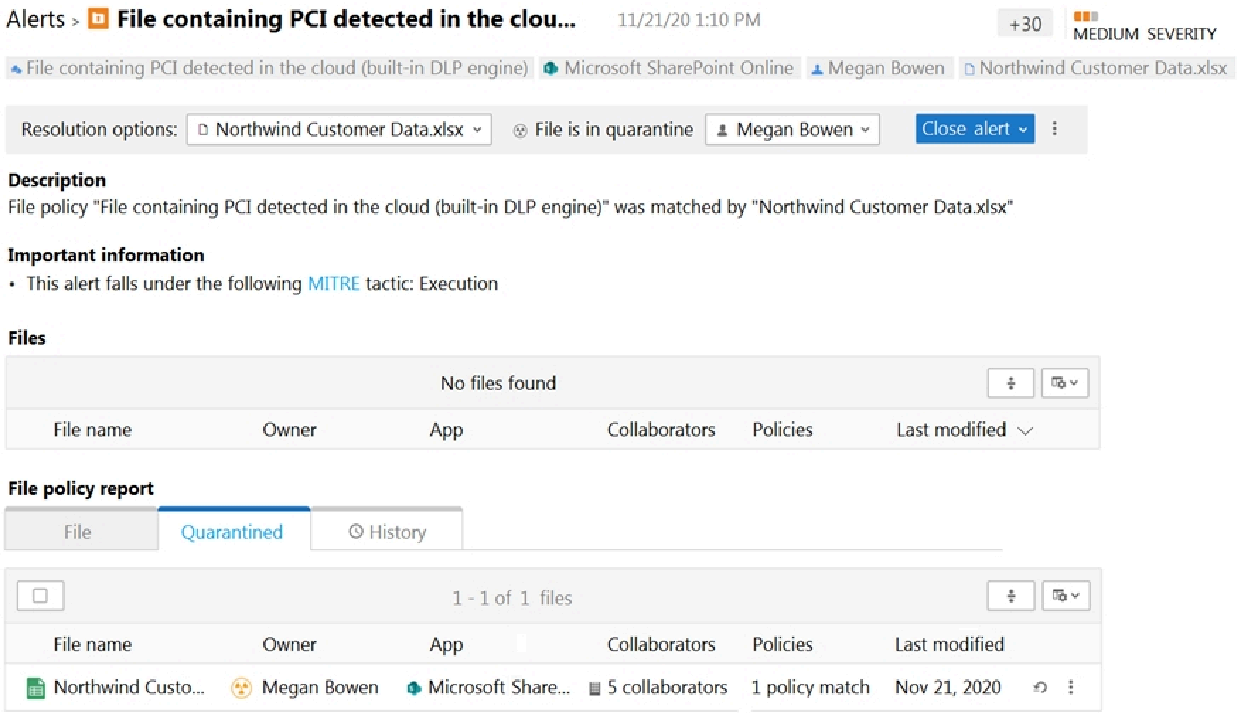
Correct. for the mailflow rule go to the exchange admin center to enable it. and for the powershell follow the example in this piece of documentation:
https://docs.microsoft.com/en-us/microsoft-365/compliance/ome-advanced-expiration

upvoted 3 times

Question #15 Topic 1

A user reports that she can no longer access a Microsoft Excel file named Northwind Customer Data.xlsx.

From the Cloud App Security portal, you discover the alert shown in the exhibit.



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

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

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

Description

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

Important information

- This alert falls under the following MITRE tactic: Execution

Files

No files found

File name	Owner	App	Collaborators	Policies	Last modified

File policy report

File | Quarantined | History

1 - 1 of 1 files

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

You restore the file from quarantine.

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

What should you do?

A. Modify the policy template.

B. Assign the Global reader role to the file owners.

C. Exclude file matching by using a regular expression.

D. Update the governance action.

Suggested 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 3 years, 4 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 11 times

wooyourdaddy Highly Voted 2 years, 6 months ago

Selected Answer: D

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

upvoted 11 times

Vangelis_1980 8 months, 4 weeks ago

So it may be wrong since you haven't scored 1000, right?

upvoted 6 times

xswe Most Recent 1 year, 8 months 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 3 years, 4 months ago

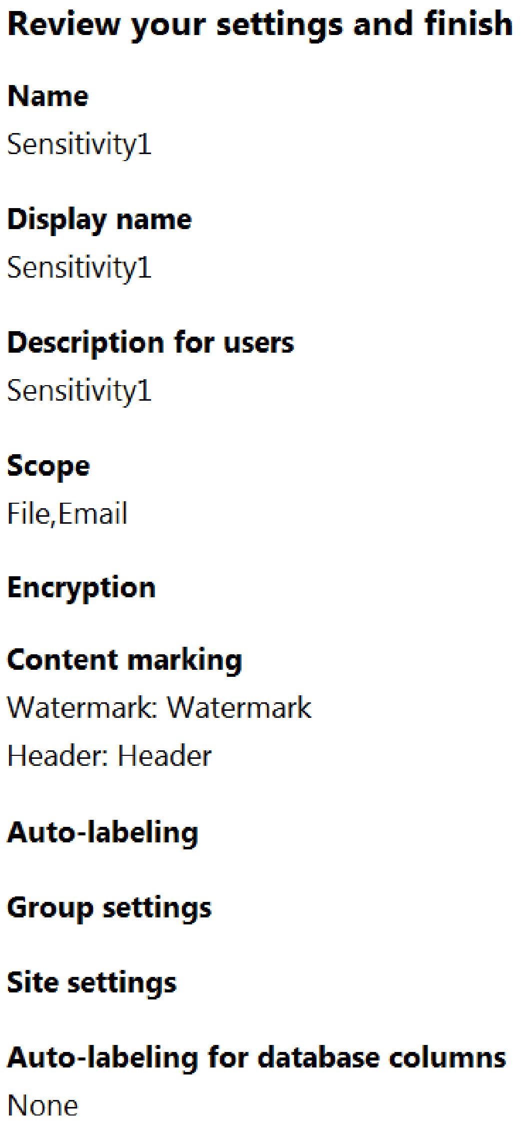
correct. The wrong governance action is being executed. if you only want an alert you should not enable the quarantine option

upvoted 6 times

Question #16 *Topic 1*

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

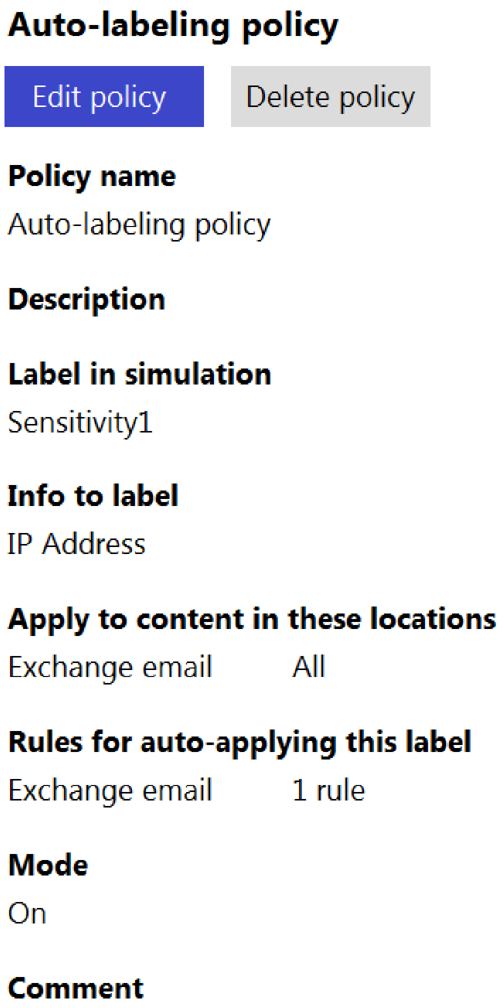
Group settings

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 -

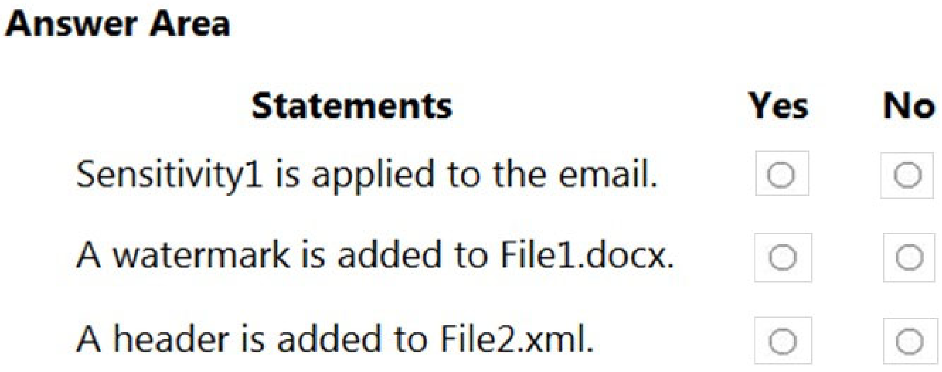
To: user2@fabrikam.com -

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.

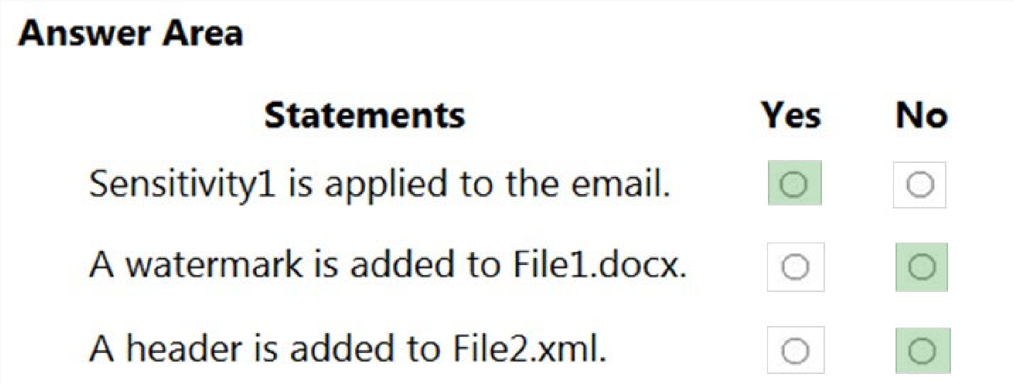
Hot Area:



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.	○	○

Suggested Answer:



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.	○	[✓ ○]

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 3 years, 9 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 26 times

Topaz007 3 years, 9 months ago

This is correct indeed. A very tricking question this one.

upvoted 3 times

klosedotorg83 3 years, 8 months 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 3 times

Topaz007 3 years, 8 months 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 7 times

CalST 3 years, 4 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

shanti0091 Highly Voted 3 years, 11 months ago

correct

upvoted 6 times

ca7859c Most Recent 1 month, 3 weeks ago

https://learn.microsoft.com/en-us/purview/apply-sensitivity-label-automatically
If the labels you want to use for auto-labeling are configured to use visual markings (headers, footers, watermarks), note that these aren't applied to documents. *****

Auto labeling only supports these
PDF documents and Office files for Word (.docx), PowerPoint (.pptx), and Excel (.xlsx) are supported.

\\same page

upvoted 1 times

husamshahin 11 months, 1 week ago

on Exam 28-7-2024

upvoted 3 times

emartiy 1 year, 3 months ago

Read Carefully.. Correct YES - NO - NO because auto-labeling policy will label only email when Sensivity1 sit conditions match. Any attachment in email can be with policy rule. +point from this question read carefully.

If the labels you want to use for auto-labeling are configured to use visual markings (headers, footers, watermarks), note that these aren't applied to documen https://learn.microsoft.com/en-us/purview/apply-sensitivity-label-automatically?view=o365-worldwide.#:~:text=If%20the%20labels%20you%20want%20to%20use%20for%20auto%2Dlabeling%20are%20configured%20to%20use%20visual%20markings

upvoted 3 times

mbhasker 1 year, 7 months ago

yes, yes, No

upvoted 1 times

Azurefox79 2 years, 4 months ago

Only email is in scope per exhibit, answer is correct

upvoted 1 times

wooyourdaddy 3 years ago

I wrote the exam today, this question was on it, I choose Yes / No / No, scored 890!

upvoted 3 times

Pravda 3 years, 5 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 3 years, 5 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 3 years, 8 months 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 3 years, 5 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 3 years, 12 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

Suggested 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, 4 months ago
Yes, can be TXT- or a CVS-File --> the answer is correct
upvoted 13 times

trut_hz Most Recent 5 months ago
Selected Answer: D
To create a keyword dictionary for a sensitive information type, the list of words must be saved in a CSV file with each word separated by commas. This is the supported format for importing a keyword dictionary in Microsoft 365 compliance tools.
upvoted 2 times

luissaro 8 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 8 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 10 months, 1 week ago
Given answer correct, CSV or TXT file. Upload via portal or powershell
upvoted 1 times

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

Abhishek1610 1 year, 1 month ago

Selected Answer: D

most commonly from a file (such as a .csv or .txt list)

upvoted 1 times

chrissempai 1 year, 3 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, 3 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, 3 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, 4 months ago

On Microsoft ESI practice test ....option selected is C

an XML file

C

upvoted 1 times

prats005 1 year, 5 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, 5 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, 6 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, 6 months ago
>
> csv ---> comma-separated values
>
> upvoted 1 times

> **Harry0300** 1 year, 6 months ago
>
> XML is for keyword list.
>
> upvoted 1 times

JamesM9 1 year, 8 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, 4 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, 9 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, 9 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, 11 months ago

On exam 1/20/2022

upvoted 1 times

⊟ **Ali_557** 2 years ago

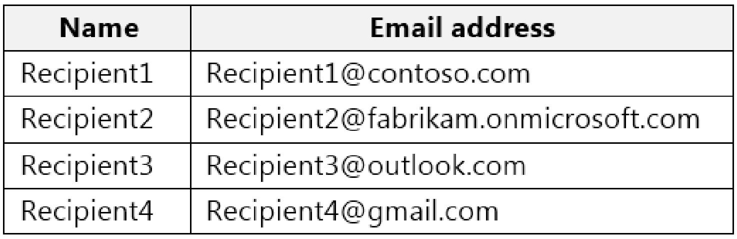
The keywords for your dictionary could come from various sources, most commonly from a file (such as a .csv or .txt list) imported in the service or by PowerShell cmdlet, from a list you enter directly in the PowerShell cmdlet, or from an existing dictionary.

upvoted 1 times

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

Suggested 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 3 years, 10 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 23 times

wooyourdaddy Highly Voted 3 years ago

Selected Answer: A

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

upvoted 14 times

rajatn 1 year ago

You sound like someone paid you to say this !

upvoted 2 times

NidaH 1 year, 10 months ago

Stop commening this in every question.

upvoted 8 times

Joipanom 1 year, 8 months ago

I like him

upvoted 6 times

thetootall 10 months, 3 weeks ago

I too appreciate the affirmation 😁

upvoted 1 times

EM1234 1 year ago

Me too

upvoted 1 times

plm_gv Most Recent 10 months, 1 week ago

The correct answer should be C as the email used link-based experience https://learn.microsoft.com/en-us/purview/revoke-ome-encrypted-mail#encrypted-emails-that-you-can-revoke

upvoted 2 times

Domza 1 year, 6 months ago

Correct: A

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

upvoted 1 times

Gesbie 1 year, 10 months ago

was on Exam August 9, 2023

upvoted 3 times

TeeKay_From_the_South 2 years ago

Microsoft doesn't play with google.

upvoted 4 times

xswe 2 years, 2 months 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 2 years, 6 months 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 3 years, 3 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 3 years, 3 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 3 years, 3 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 3 years, 5 months ago
On exam 1/20/2022
upvoted 1 times

jkklim 3 years, 9 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 3 years, 6 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 3 years, 11 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 3 years, 11 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 3 years, 11 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

Suggested 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, 8 months 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 16 times

⊟ **xswe** Highly Voted 👍 1 year, 2 months 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 6 times

⊟ **fiksarion** Most Recent ⏲ 6 months, 3 weeks ago

Selected Answer: D

The Test-IRMConfiguration command is used to test the configuration of the IRM (Information Rights Management) service, which is crucial for Microsoft Office 365 Message Encryption (OME). This command allows you to verify the correctness of encryption and decryption settings, as well as check if the IRM service is active and functioning correctly for both the sender and the recipient.

This command helps verify the following:

Activation of the IRM service.

Status of encryption and decryption verification.

Other commands, such as Test-ClientAccessRule, Test-Mailflow, and Test-OAuthConnectivity, are not directly related to testing message encryption features in OME.

upvoted 2 times

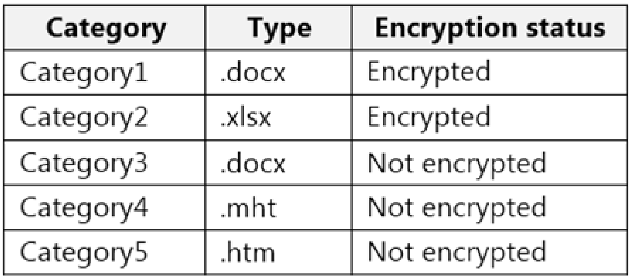
Question #20 *Topic 1*

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

Suggested 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 1 year, 10 months 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 10 times

tlgrittz Most Recent 8 months, 3 weeks ago

On test 9Apr24

upvoted 2 times

Domza 1 year ago

Correct~ B

.htm is supported

upvoted 1 times

Rohit_Panchal 1 year, 5 months 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 4 times

217f3c9 1 year, 7 months ago

mht is supported (now)

upvoted 4 times

xswe 1 year, 8 months 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** 1 year, 11 months 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 2 times

⊟ **NinjaSchoolProfessor** 2 years 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** 2 years, 1 month ago

Answer is correct .htm and docx

upvoted 2 times

⊟ **Harry008** 2 years, 1 month 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.

Suggested 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 3 years, 8 months ago
Option C - Right Answer
upvoted 10 times

Domza Highly Voted 1 year, 6 months ago
New Updates:
Office 365 Message Encryption will be retired in July 2023 and replaced by Microsoft Purview Message Encryption. Starting May 2023, all existing rules that use Office 365 Message Encryption will automatically start using Microsoft Purview Message Encryption

DLP policies and DLP-related conditions and actions in Mail flow rules are no longer supported and can no longer be created or edited in the Exchange Admin Center (EAC) or using Exchange Online PowerShell. We recommend migrating all DLP-related rules to Microsoft Purview DLP in the compliance center as soon as possible
upvoted 7 times

Boeroe 8 months, 3 weeks ago
Correct, OME is depricated and DLP is to be used (which isn't an answer in this question).
Link: https://learn.microsoft.com/en-us/purview/ome#how-message-encryption-works
upvoted 1 times

heshmat2022 Most Recent 1 year, 8 months ago
IT WAS ON EXAM OCTOBER 18 2023
upvoted 1 times

xswe 2 years, 2 months 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 2 years, 6 months ago
Selected Answer: C
Mail Flow rule will fit the bill.
upvoted 2 times

wooyourdaddy 3 years ago
Selected Answer: C
I wrote the exam today, this question was on it, I choose C, scored 890!
upvoted 2 times

crista_ 3 years, 3 months ago

C is correct

upvoted 2 times

Pravda 3 years, 5 months ago

On exam 1/20/2022

upvoted 1 times

pixuefei 3 years, 6 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.

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

Community vote distribution
D (79%) C (19%)

Topaz007 Highly Voted 3 years, 8 months 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 22 times

sergioandreslq 3 years, 6 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 3 years, 6 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 11 times

MahmoudEldeep 3 years, 7 months ago
Agree, You can not create a new sensitivity label for Groups & Sites unless you enable this option.
upvoted 4 times

zaqwsx 3 years, 6 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 9 times

Pravda Highly Voted 3 years, 5 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 12 times

JCkD4Ni3L 2 years, 6 months 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

trut_hz Most Recent 5 months, 1 week ago

Selected Answer: B

The reason why NOT option D, "Configure the EnableMIPLabels Azure Active Directory (Azure AD) setting," is not the first step is because you need to create a new sensitivity label scoped to Groups & sites before you can configure the EnableMIPLabels setting. The sensitivity label must exist and be properly scoped to Groups & sites to ensure that it can be applied to new Microsoft Teams sites

Once the sensitivity label is created, you can then proceed to configure the EnableMIPLabels setting in Azure AD to enable the feature and ensure that the labels can be applied to Microsoft Teams sites

upvoted 1 times

trut_hz 5 months, 1 week ago

Selected Answer: B

Two different Co-pilots and ChatGPT 4o
Before sensitivity labels can be applied to Microsoft Teams sites, you need to create and configure sensitivity labels specifically scoped for "Groups & sites." This configuration allows the labels to be applicable to containers like Teams, Microsoft 365 groups, and SharePoint sites.
MICROSOFT LEARN

After creating the sensitivity label, you must publish it to the necessary users or groups.

Additionally, ensure that sensitivity labels are enabled for containers and synchronized with Microsoft Entra ID (formerly Azure Active Directory). This process involves running the Execute-AzureAdLabelSync cmdlet to synchronize the labels.
MICROSOFT LEARN

By creating and configuring a sensitivity label scoped to "Groups & sites," and ensuring proper synchronization, you enable the application of these labels to new Microsoft Teams sites.

upvoted 1 times

HeirrBourne 5 months, 1 week ago

Selected Answer: B

To ensure that you can view and apply sensitivity labels to new Microsoft Teams sites, the correct first step is to:

B. Create a new sensitivity label scoped to Groups & sites.
D. Configure the EnableMIPLabels Azure Active Directory (Azure AD) setting:
This setting is related to Microsoft Information Protection (MIP) integration with Azure AD. However, this setting does not directly affect the ability to apply sensitivity labels to Teams sites. Configuring labels first, as described in option B, is the correct approach.
Conclusion:
To enable sensitivity labels for Microsoft Teams sites, you must first create a new sensitivity label scoped to Groups & Sites. This ensures the label can be applied to both Microsoft Teams (which is built on Groups) and SharePoint sites (used by Teams for file storage

upvoted 1 times

belyo 8 months, 3 weeks ago

Selected Answer: D

https://learn.microsoft.com/en-us/entra/identity/users/groups-assign-sensitivity-labels?tabs=microsoft#sensitivity-labels-arent-available-for-assignment-on-a-group

1st is to enable EnableMIPLabels in AAD templates
2nd is to start sync across Entra ID Execute-AzureAdLabelSync
upvoted 1 times

EM1234 1 year ago

Selected Answer: B

It is B.
I know everyone is going on about the powershell and they do have a point but please read the very beginning of this link:
https://learn.microsoft.com/en-us/entra/identity/users/groups-assign-sensitivity-labels

It says:
Microsoft Entra ID supports applying sensitivity labels to Microsoft 365 groups when those labels are published in the Microsoft Purview portal or the Microsoft Purview compliance portal and the labels are configured for groups and sites.

Yes, you do need to enable them with powershell but you need to do this first. C is kind of right but it is a different module and D is needed too as you can see in the troubleshooting part of the link I added.

I am going with B. Good luck out there, may we all get 890s.
upvoted 1 times

ShrawanBhat1991 1 year, 2 months ago

First step is to ensure EnableMIPLabels is enabled and set to True
Correct Answer D
upvoted 1 times

emartiy 1 year, 3 months ago

Selected Answer: D

Yes it is D.
upvoted 1 times

emartiy 1 year, 3 months ago

Selected Answer: C

Be carefore.. Groups and Sites options there in the policy but it is gray-out. you can't select it until you enable labels for containers etc. To enable it, you need to "Execute-AzureAdLabelSync" Then you will be able to apply labels to Groups and sites..
upvoted 1 times

emartiy 1 year, 4 months ago

ensure that you can view and apply sensitivity labels to new Microsoft Teams sites. - Answer is C. In order to apply label to Groups & Site, you need to ensure you are able to see this option. So, you need to sync labels to azure. -- C --
https://learn.microsoft.com/en-us/purview/sensitivity-labels-teams-groups-sites
"Then run the following command to ensure your sensitivity labels can be used with Microsoft 365 groups:"
upvoted 1 times

Domza 1 year, 6 months ago

Got it: here is the link:
https://learn.microsoft.com/en-us/entra/identity/users/groups-assign-sensitivity-labels#enable-sensitivity-label-support-in-powershell

Enjoy :)
upvoted 1 times

bhadolaa29 2 years ago

D is the correct Answer. Tested
upvoted 2 times

dmoorthy 2 years, 2 months ago

Answers is D.
upvoted 1 times

luissaro 2 years, 2 months 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 2 years, 2 months 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 2 years, 4 months 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

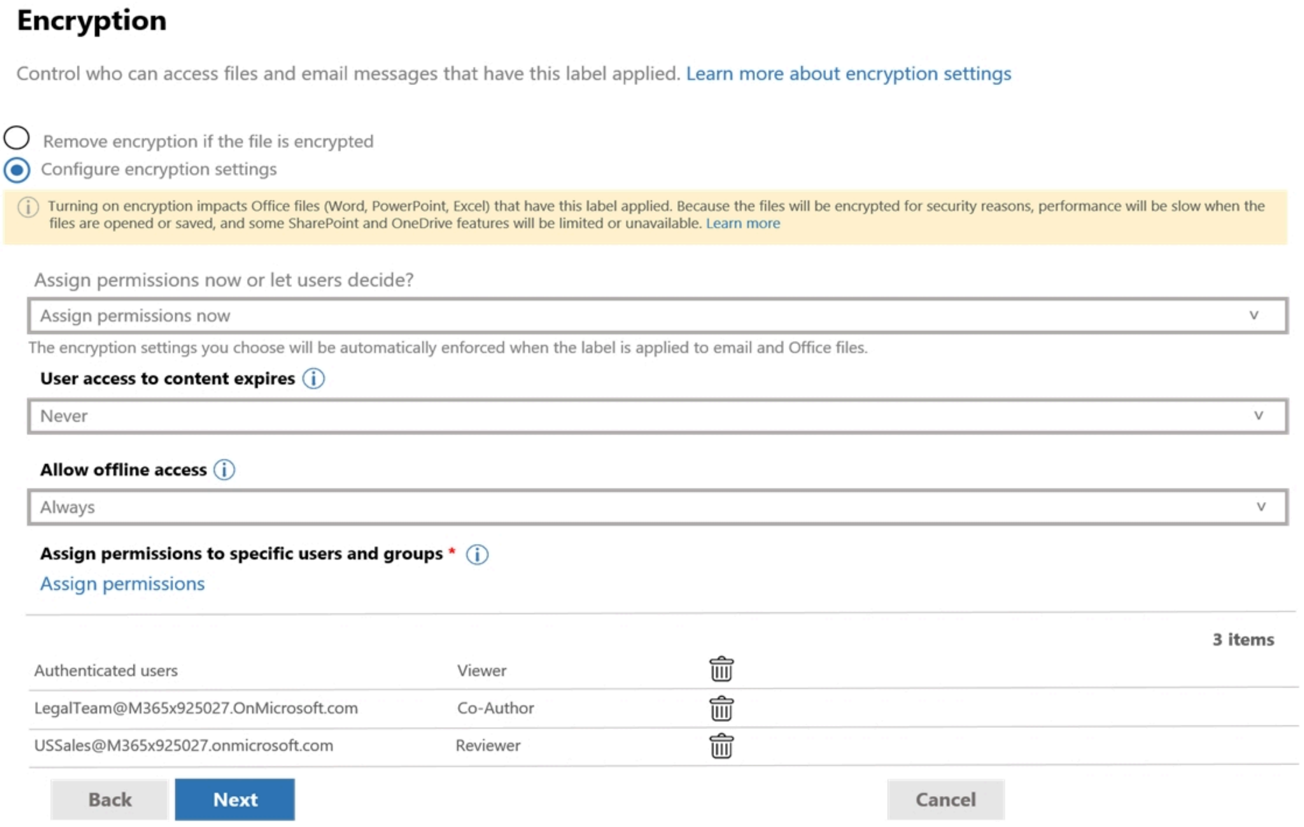
Question #23 Topic 1

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.



Encryption

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

○ Remove encryption if the file 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 ⓘ

Never

Allow offline access ⓘ

Always

Assign permissions to specific users and groups * ⓘ

Assign permissions

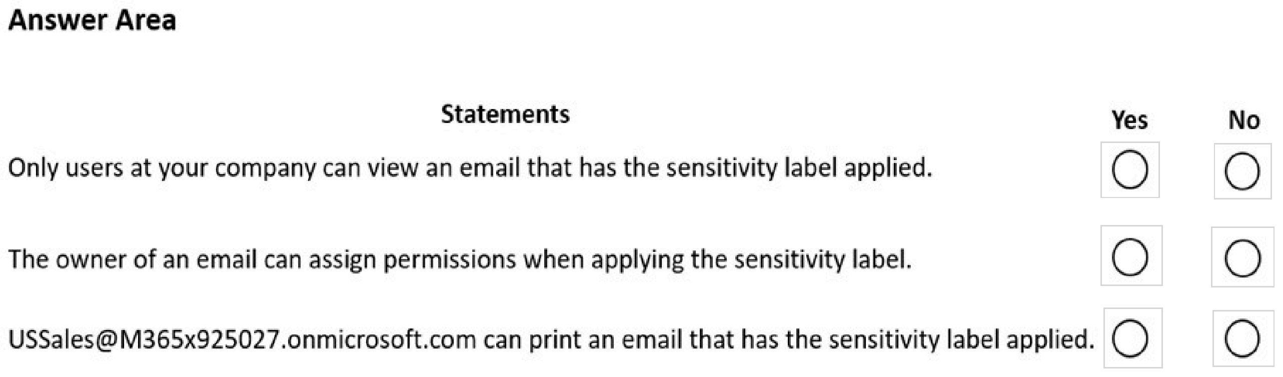
3 items

Authenticated users	Viewer	🗑
LegalTeam@M365x925027.OnMicrosoft.com	Co-Author	🗑
USSales@M365x925027.onmicrosoft.com	Reviewer	🗑

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

NOTE: Each correct selection is worth one point.

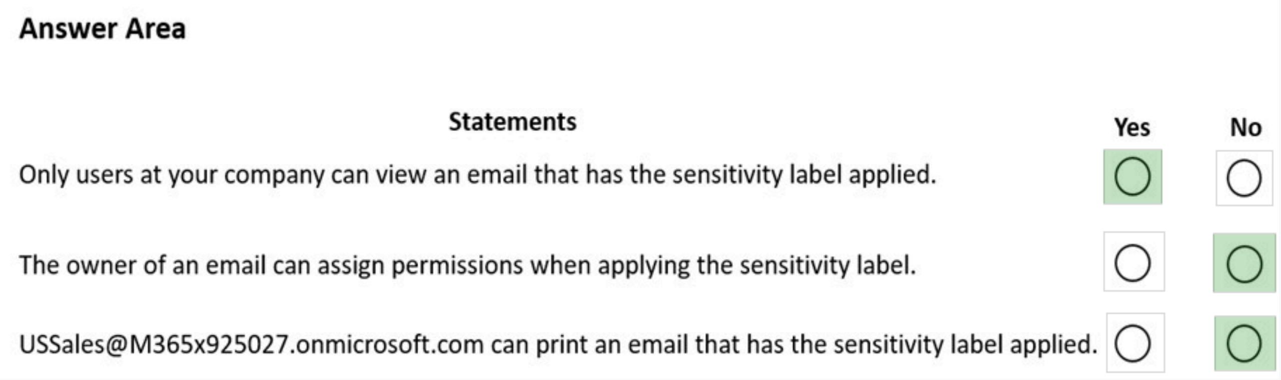
Hot Area:



Answer Area

Statements	Yes	No
Only users at your company can view an email that has the sensitivity label applied.	○	○
The owner of an email can assign permissions when applying the sensitivity label.	○	○
USSales@M365x925027.onmicrosoft.com can print an email that has the sensitivity label applied.	○	○

Suggested Answer:



Answer Area

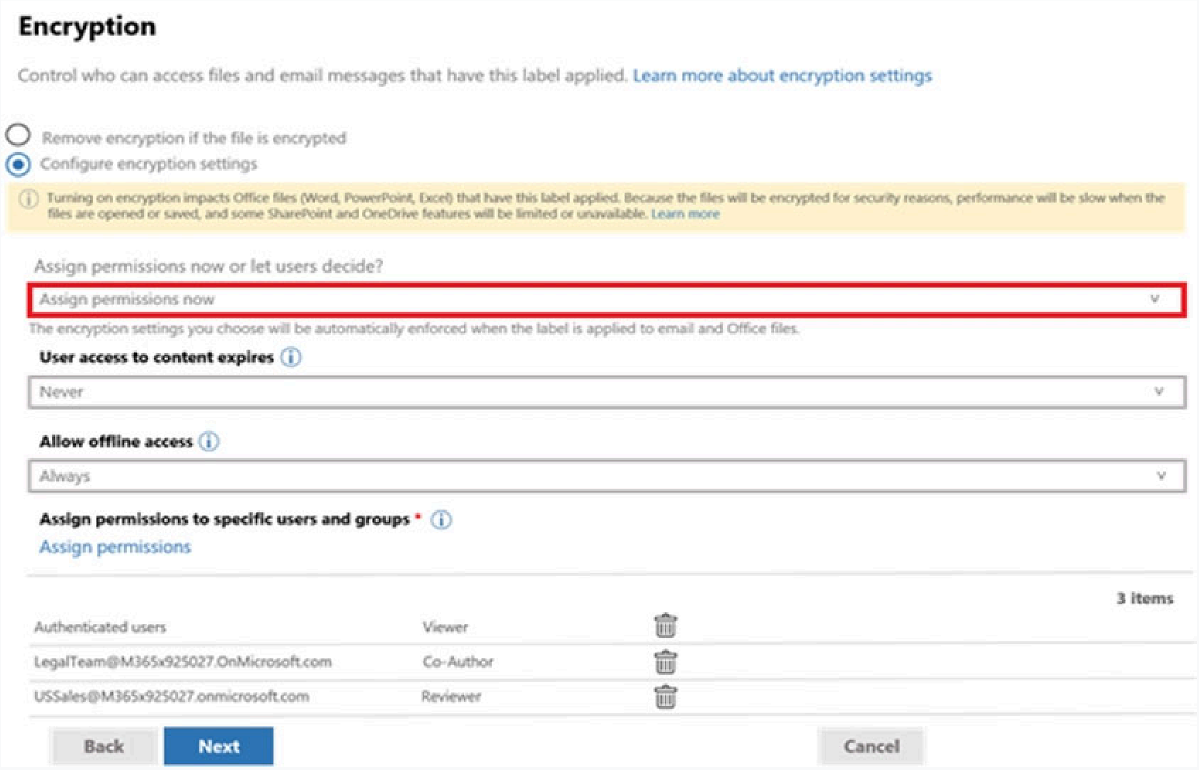
Statements	Yes	No
Only users at your company can view an email that has the sensitivity label applied.	[✓ ○]	○
The owner of an email can assign permissions when applying the sensitivity label.	○	[✓ ○]
USSales@M365x925027.onmicrosoft.com can print an email that has the sensitivity label applied.	○	[✓ ○]

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.



Encryption

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

○ Remove encryption if the file 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 ⓘ

Never

Allow offline access ⓘ

Always

Assign permissions to specific users and groups * ⓘ

Assign permissions

3 items

Authenticated users	Viewer	🗑
LegalTeam@M365x925027.OnMicrosoft.com	Co-Author	🗑
USSales@M365x925027.onmicrosoft.com	Reviewer	🗑

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 3 years, 8 months 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 21 times

⊟ **McAlec** 3 years, 8 months 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 10 times

⊟ **BTAB** 3 years, 1 month ago

Yes, No, No. Authenticated Users has Viewer permissions, which will allow them to view emails based upon the policy settings

upvoted 6 times

⊟ **BTAB** 3 years, 1 month 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

⊟ **Ras1364** Highly Voted 3 years, 6 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

⊟ **Bakkia** 6 months, 1 week ago

yes no no for me,.. This looks very tricky .. but if you think deeply..

why would you create a label to make someone view the mail ?
who should view the mail will be decided by the user who composes the email.
So let me say I create a mail ABC (encrypted) and send it to XYZ (same company) .. and if XYZ is inside the org they can view the message.
but further if the XYZ is part of legal group then they get the extra permissions (copy, edit / print) as they are the co-author ..

upvoted 1 times

⊟ **Ras1364** 3 years, 6 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** 2 years, 6 months ago

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

upvoted 1 times

⊟ **Mdwro** 3 years, 5 months ago

Hmm, but there is a viewer permission assigned to all authenticated users

upvoted 2 times

⊟ **mimguy** 1 year, 5 months ago

Authenticated users can include guest accounts

upvoted 3 times

⊟ **uilloz** Most Recent 8 months ago

"any authenticated users" includes any user who:
Has an email account that's authenticated by Microsoft Entra ID or a federated social provider.
Is authenticated by a Microsoft account.
Uses a one-time passcode for email only.

upvoted 1 times

⊟ **Cubalibre69** 1 year, 1 month ago

Only users within your organization can open a confidential document or email is No because you would see tenantname.onmicrosoft.com in the assign permissions section

upvoted 1 times

⊟ **emartiy** 1 year, 3 months ago

This question's correct answer is N, N, N!
Only users at your company can view.... - No: Reason:
"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). However, the application opening the encrypted content must be able to support the authentication being used.

Other 2 sentences are also NO based on the policy deifications you can read. Tricky part of this question is granting authenticated users with Viewer..

Please read this pharagraph
https://learn.microsoft.com/en-us/purview/encryption-sensitivity-labels#requirements-and-limitations-for-add-any-authenticated-users

upvoted 1 times

⊟ **emartiy** 1 year, 4 months ago

As BTAB sadi below, Yes, NO NO, there is 3 selection for granted for that policy. Authenticated users is an option so, all users in domain can see document and others NO based on the descriptions.. Be careful while readin and scanning informaiton on the question ::)

upvoted 2 times

⊟ **Domza** 1 year, 5 months ago

Did anyone read the provided link? LOL

upvoted 1 times

⊟ **heshmat2022** 1 year, 8 months ago

IT WAS ON EXAM OCTOBER 18 2023

upvoted 1 times

⊟ **Gesbie** 1 year, 10 months ago

was on Exam August 9, 2023

upvoted 1 times

⊟ **bhadolaa29** 2 years ago

Correct Answer No, No, Yes

Co Author permission includes print

upvoted 1 times

⊟ **Sategi** 1 year, 11 months ago

USSales us reviewer

upvoted 3 times

⊟ **Jonclark** 2 years, 3 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 4 times

⊟ **JCkD4Ni3L** 2 years, 7 months 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** 3 years, 2 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** 3 years, 5 months ago

On exam 1/20/2022

upvoted 1 times

⊟ **UWSFish** 3 years, 5 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** 3 years, 5 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** 3 years, 4 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** 3 years, 5 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

Question #24 *Topic 1*

HOTSPOT -

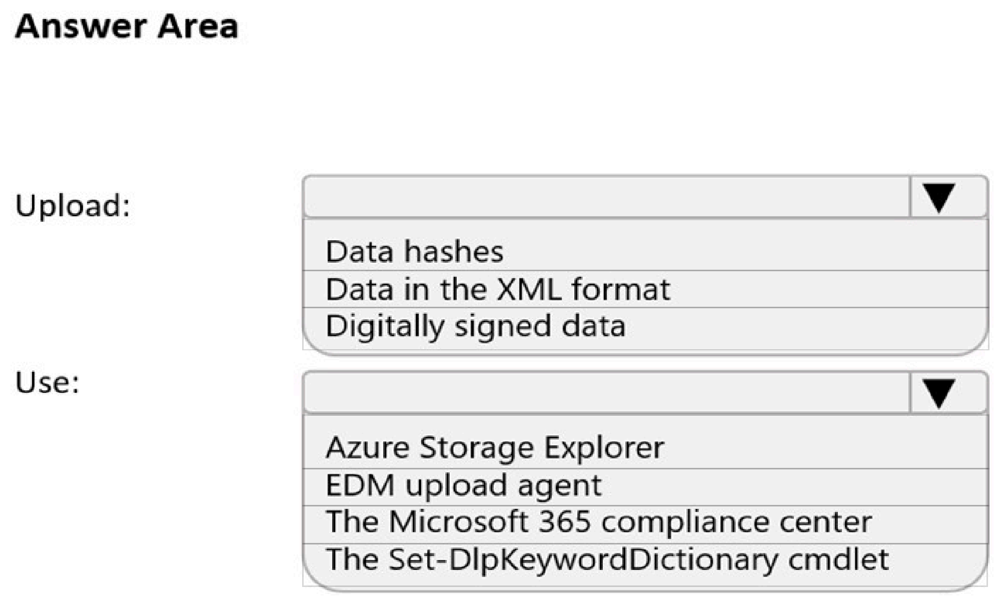
You plan to create a custom sensitive information type that will use Exact Data Match (EDM).

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:

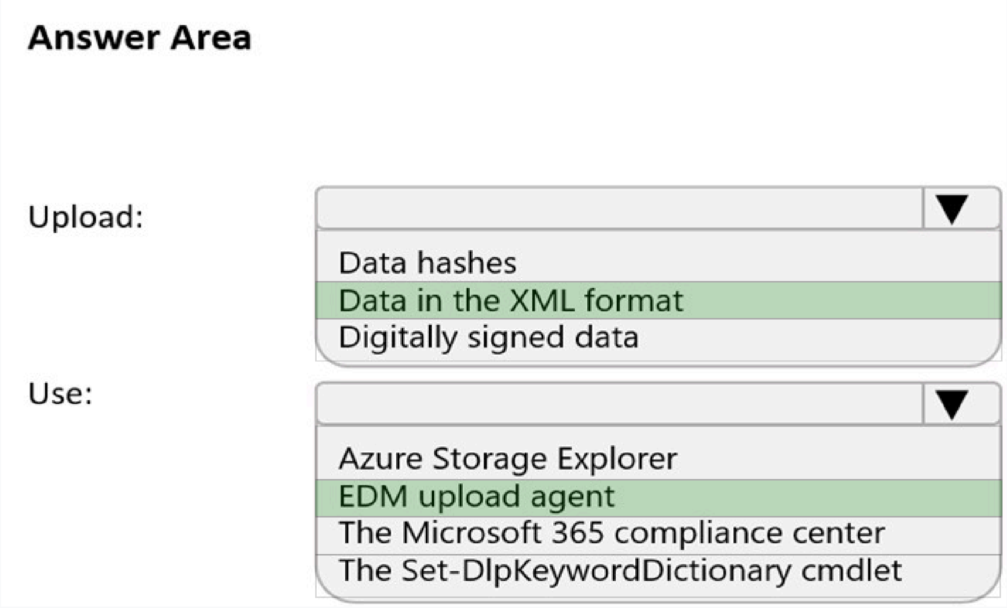


Answer Area

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

Suggested 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 3 years, 2 months 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 21 times

⊟ **sergioandreslq** 3 years 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 2 years, 11 months ago

How do you hash the XML file containing the data?
I believe it's with the EDM agent...

upvoted 1 times

Holii 2 years, 7 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

McAlec 3 years, 1 month 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 16 times

Jonclark Highly Voted 1 year, 10 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 7 times

emartiy Most Recent 10 months, 2 weeks ago

It asks what to upload and what is the method to be able to upload data.. Don' confuse with background of process.. You are able to select one the listed data type.. Are you able upload data hash by yourself? by using EDM agent, you chose data and agent perform what is needed during upload progress.. Displayed selections are correct :)

upvoted 1 times

emartiy 10 months, 2 weeks ago

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

https://learn.microsoft.com/en-us/purview/sit-get-started-exact-data-match-hash-upload

upvoted 1 times

Bakkia 6 months, 1 week ago

but edm.xml is just the schema here.. the actual data is patientRecords.csv
The option "Data in XML format" option itself is wrong here.. if "Schema in XML format " is the option then probably you are right ..
And here the question is what will you upload to O365 .. using which tool.. we upload hashed data using EDMuploadagent tool.

I took a day to analyze this alone :| hope this is right

upvoted 1 times

Domza 12 months ago

New Info here: Hash Data
https://mslearn.cloudguides.com/guides/Identify%20data%20using%20exact%20data%20match-based%20classification%20in%20Microsoft%20Purview%20Information%20Protection

with love

upvoted 3 times

Tzu_Hsien 11 months ago

thanks!!!

upvoted 1 times

heshmat2022 1 year, 2 months 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 2 years 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 2 years, 1 month 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 2 years, 6 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 2 times

Srd 1 year, 9 months ago

This is a spam bot. Same answer under most questions.

upvoted 5 times

JCkD4Ni3L 2 years ago

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

upvoted 4 times

dostras 3 years 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 3 years, 2 months 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 3 years, 2 months 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 2 years, 7 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 -

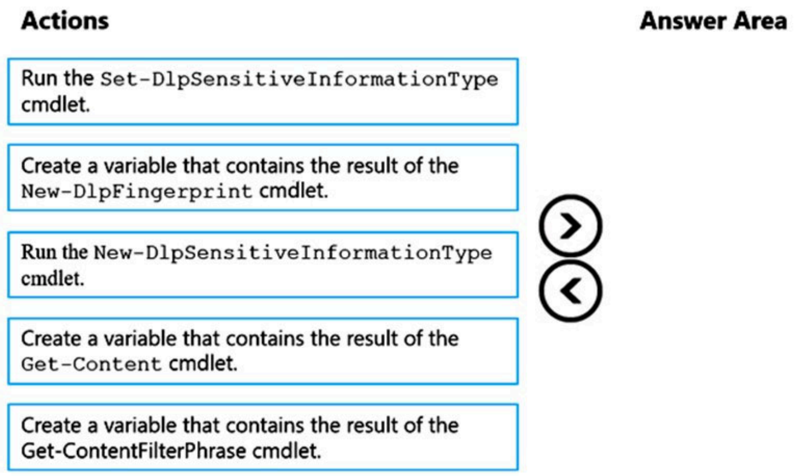
You have a Microsoft 365 tenant that uses data loss prevention (DLP).

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:

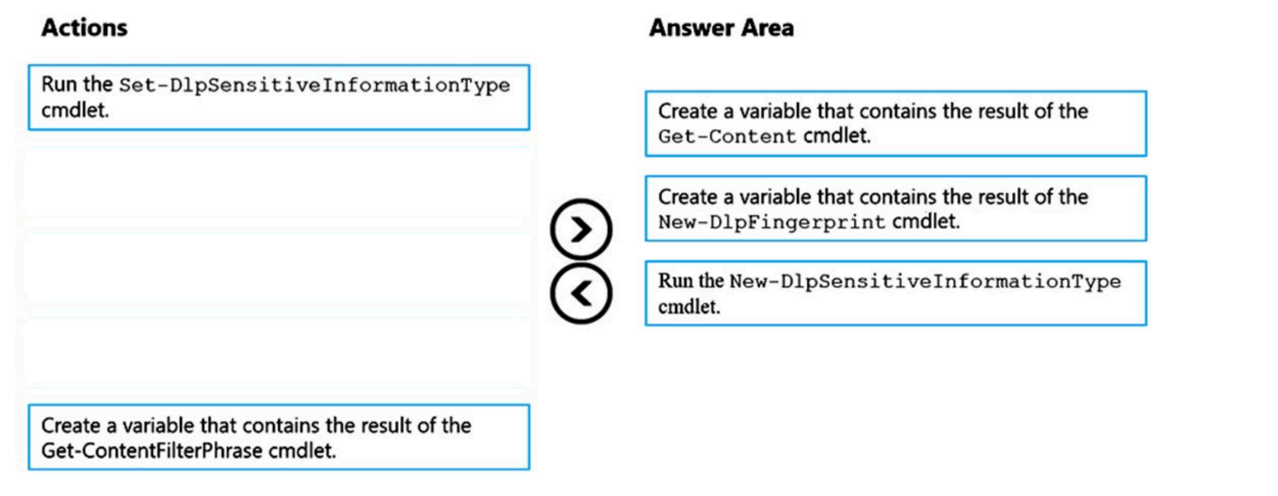


Actions

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

Answer Area

Suggested Answer:



Actions

- Run the `Set-DlpSensitiveInformationType` cmdlet.
- Create a variable that contains the result of the Get-ContentFilterPhrase cmdlet.

Answer Area

- Create a variable that contains the result of the `Get-Content` cmdlet.
- Create a variable that contains the result of the `New-DlpFingerprint` cmdlet.
- Run the `New-DlpSensitiveInformationType` cmdlet.

Reference:

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

kochunnee Highly Voted 3 years, 2 months 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 15 times

sergioandreslq 3 years ago

Agreed, reviewed on the web site

upvoted 1 times

Jonclark Highly Voted 1 year, 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 14 times

⊟ **Co123** 1 year ago

Thanks You!!!!

upvoted 1 times

⊟ **Domza** Most Recent 12 months ago

Nice work all. ~

upvoted 2 times

⊟ **PrettyFlyWifi** 3 years 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 4 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.

Suggested Answer: *A*

Community vote distribution

B (67%) A (33%)

researched_answer_boi Highly Voted 3 years, 7 months 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 3 years, 5 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 14 times

MatExam Most Recent 4 months ago

Selected Answer: A

None is correct....
You can't revoke an encrypted message which is sent to an office account, only revocation from social mailboxes such gmail will work....
Ref: https://learn.microsoft.com/en-us/entra/identity/users/groups-assign-sensitivity-labels?tabs=microsoft#sensitivity-labels-arent-available-for-assignment-on-a-group

Quote:
"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 Microsoft 365 or a user that uses a Microsoft account, for example, an outlook.com account."

upvoted 1 times

plm_gv 10 months, 1 week ago

The message revocation feature isn't that a Advance Message Encryption feature that's not available in OME ?

upvoted 1 times

ShrawanBhat1991 1 year, 2 months ago

Step 1: Run the Message Trace first and capture Message ID

Step 2 : Set-OMEMessageRevocation -"MessageId " -Revoke $true

Tricky

upvoted 3 times

EM1234 1 year ago

There are other ways to get the message ID. I think B is the answer

upvoted 2 times

Wildz 1 year, 3 months ago

hot take use new-compliance search and do a hard delete of the result there u go mail just went houdini

upvoted 1 times

emartiy 1 year, 4 months ago

Selected Answer: A

In the question, it says contoso.com alreasy uses OME. In order to prevent fabrikam.com user to reach emails sent by user1 in contoso, you can use following cmdlet.

Set-OMEMessageRevocation -MessageId "<d96****4c-127b-4**a-ae2e-fa7df****9d@DM3NAM06BG401.Eop-nam06.prod.protection.outlook.com>" -Revoke $true

So, do you know all MessagID information by yourself? :) No, you need to find it to be able use above cmdlet. As a part of progress, you need to start with get message trace in order to find Mail ID's (for all emails was sent to user2 in fabrikam.com by user1 in contoso.com domain in order to be able use Set-OMEMessageRevocation -MessageId <message-id> :) Isn't it clear?

upvoted 2 times

Domza 1 year, 6 months ago

Hello,
Please read the question. It says<You need to prevent user2@fabrikam.com from accessing the email.>

Correct is B

upvoted 1 times

heshmat2022 1 year, 8 months ago

IN EXAM OCTOBER 18TH 2023

upvoted 4 times

Mpho_S 2 years 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 2 years, 2 months 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 2 years, 6 months 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 2 years, 9 months ago

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

upvoted 1 times

Lion007 2 years, 10 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 3 years ago

Selected Answer: B

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

upvoted 1 times

sunilkms 3 years, 1 month ago

Selected Answer: B

Set-OMEMessageRevocation

upvoted 2 times

JamesM9 3 years, 2 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 7 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.

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

Community vote distribution
C (67%) A (33%)

Juancho Highly Voted 3 years, 1 month 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 14 times

sergioandreslq 3 years 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

Amin4799 Most Recent 7 months, 2 weeks ago
Selected Answer: C
Azure Rights Management (Azure RMS) is a key component for OME. Activating Azure RMS enables your organization to apply rights protection to emails, documents, and other data, including the encryption provided by OME. Once Azure RMS is activated, you can configure and apply OME policies to encrypt sensitive emails and protect their content.
upvoted 1 times

emartiy 10 months, 1 week ago
Selected Answer: C
Correct one.
upvoted 1 times

emartiy 10 months, 1 week ago
Selected Answer: A
Correct.
upvoted 1 times

emartiy 10 months, 1 week ago
mistakenly selected. please ignore.
upvoted 2 times

xswe 1 year, 8 months ago
Azure RMS are needed for OME
upvoted 1 times

NinjaSchoolProfessor 2 years 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** 2 years, 5 months ago

Activate Azure Rights Management (Azure RMS).

upvoted 2 times

⊟ **Pravda** 2 years, 11 months ago

On exam 1/20/2022

upvoted 2 times

⊟ **klosedotorg83** 3 years, 2 months ago

Correct

upvoted 1 times

Question #28 Topic 1

HOTSPOT -

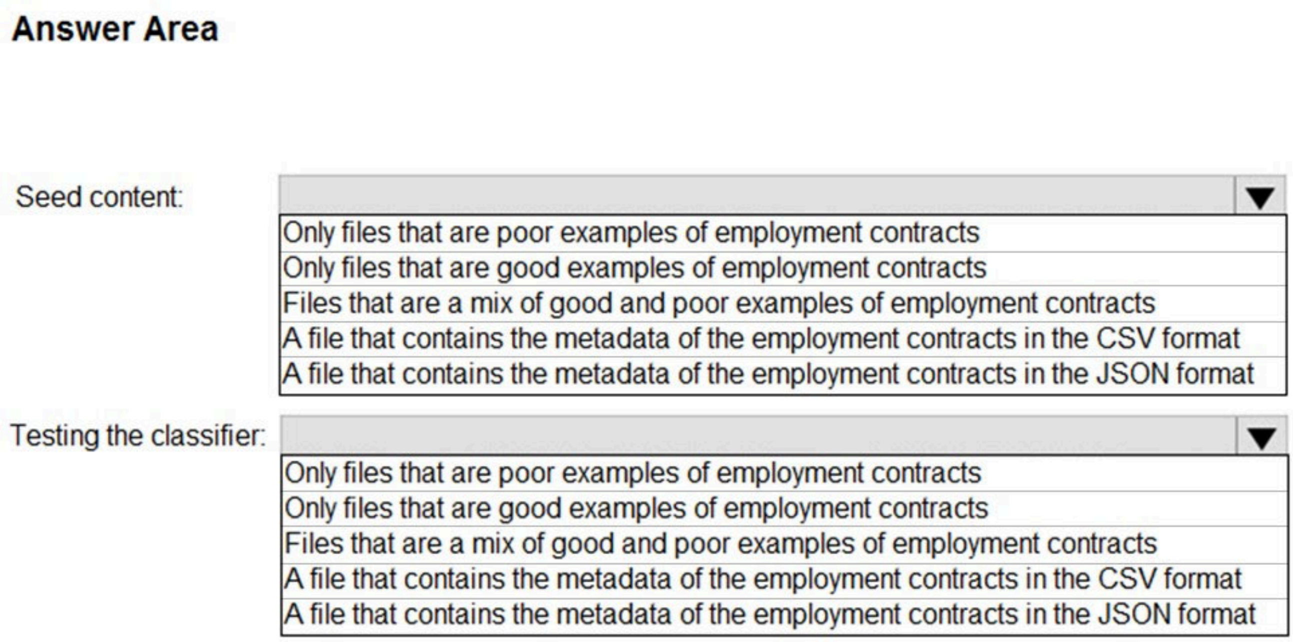
You plan to implement a sensitive information type based on a trainable classifier. The sensitive information type will identify employment contracts.

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

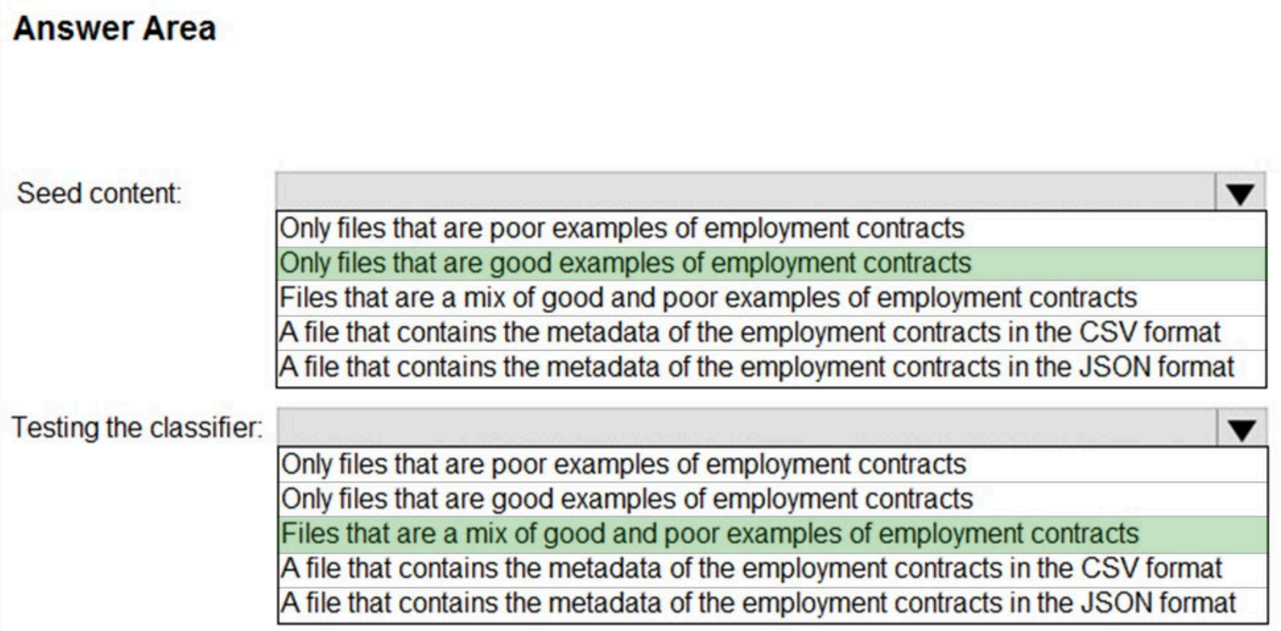
Seed content: ▼

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

Suggested 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 2 years, 2 months 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 10 times

JS_Jasey Highly Voted 11 months, 2 weeks ago

Looks like alot has changed in 2 years. Now you need to give positive and negative samples at the same time.

upvoted 7 times

Pravda Most Recent 3 years, 5 months ago

On exam 1/20/2022

upvoted 1 times

Ali_557 3 years, 6 months ago

In Seed content why its not the 3rd option?

upvoted 2 times

Dreamhaxx 3 years, 5 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 3 years, 6 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 3 years, 6 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

kochunnee 3 years, 8 months 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

Question #29 *Topic 1*

HOTSPOT -

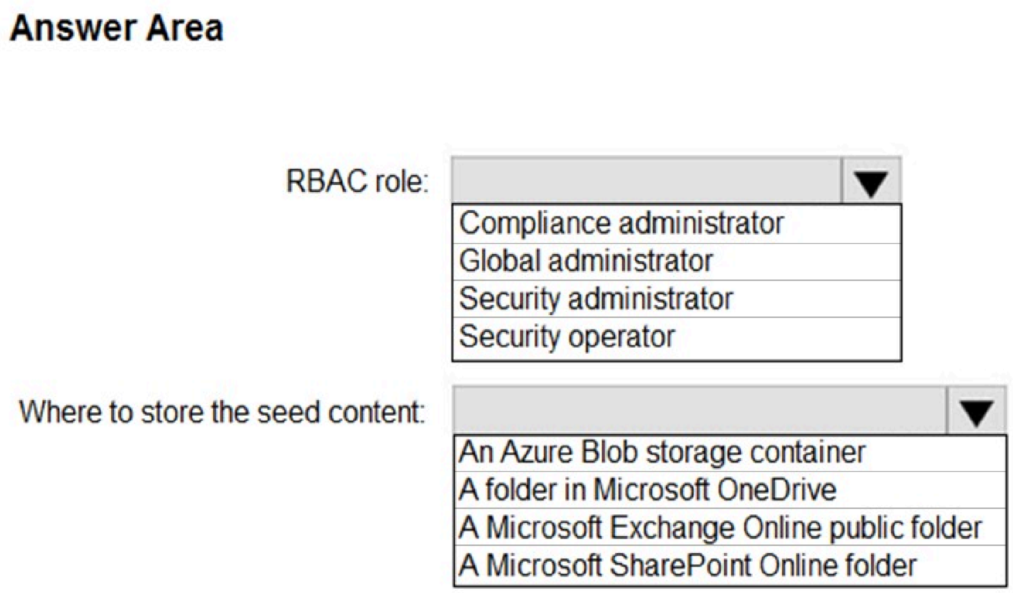
You plan to create a custom trainable classifier based on an organizational from template.

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:



Answer Area

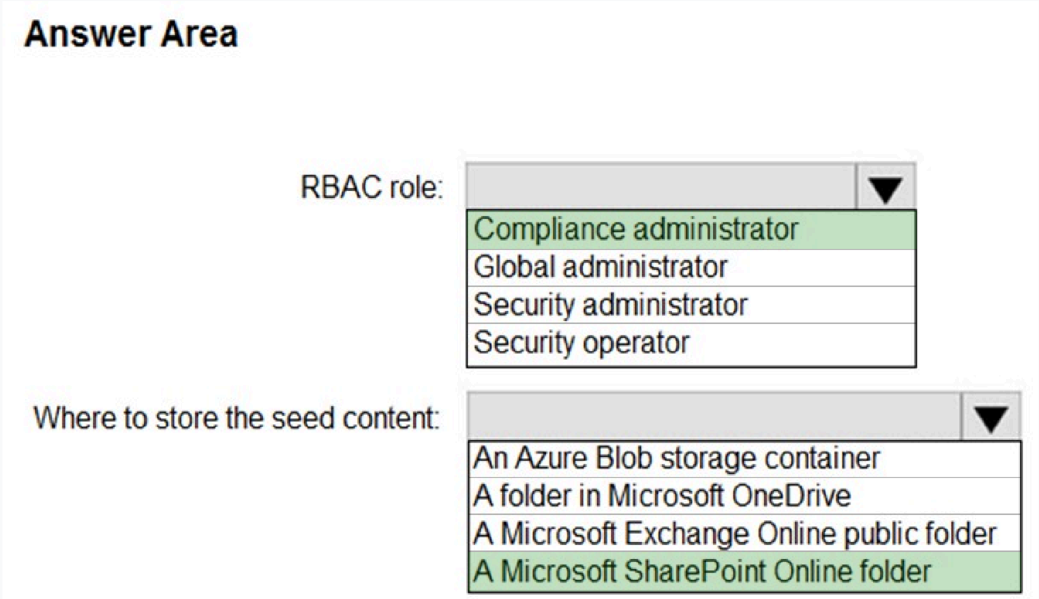
RBAC role:

- Compliance administrator
- Global administrator
- Security administrator
- Security operator

Where to store the seed content:

- An Azure Blob storage container
- A folder in Microsoft OneDrive
- A Microsoft Exchange Online public folder
- A Microsoft SharePoint Online folder

Suggested Answer:



Answer Area

RBAC role:

- [✓ Compliance administrator]
- Global administrator
- Security administrator
- Security operator

Where to store the seed content:

- An Azure Blob storage container
- A folder in Microsoft OneDrive
- A Microsoft Exchange Online public folder
- [✓ A Microsoft SharePoint Online folder]

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 2 years, 11 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 12 times

NinjaSchoolProfessor Highly Voted 2 years 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 9 times

ehommes Most Recent 1 year, 1 month 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

Futfuyfyjfj 11 months ago

Security admin can create them as well, but security admin is more powerful than compliance admin. -> least privileges.
upvoted 2 times

xswe 1 year, 8 months 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 2 years, 11 months ago

On exam 1/20/2022
upvoted 4 times

Ali_557 3 years 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 3 years 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 3 years 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 3 years 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] 3 years, 1 month ago

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

upvoted 1 times

⊟ **MahmoudEldeep** 3 years, 1 month ago

Tested, Compliance administrator can also create trainable classifier.

upvoted 7 times

⊟ **Mdwro** 2 years, 11 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 2 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.

Suggested 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 👍 2 years, 11 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 12 times

oberte007 Highly Voted 👍 3 years, 2 months ago

Yes! right! Simulation mode allows you to test the policy's efficiency and to make some adjustments as necessary

upvoted 7 times

sergioandreslq 3 years 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

Bakkia Most Recent 🕒 6 months, 1 week ago

Selected Answer: D

what should you do first ? .. ha ha .. thats the trick in this question.

Answer is D

upvoted 1 times

emartiy 10 months, 1 week ago

Selected Answer: D

Other options does not provite information in order to be ensured if auto-labeling policy can apply label to files. So, you need to figure out if policy run correctly and you can see it in simulation mode :) Thanks.

upvoted 1 times

VictoryLovesPrep07 1 year ago

Selected Answer: D

Best practice according to MS is the always test it out

upvoted 2 times

xswe 1 year, 8 months 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 2 years, 3 months ago

Selected Answer: D

It needs to be an auto label

upvoted 2 times

⊟ **Pravda** 2 years, 11 months ago

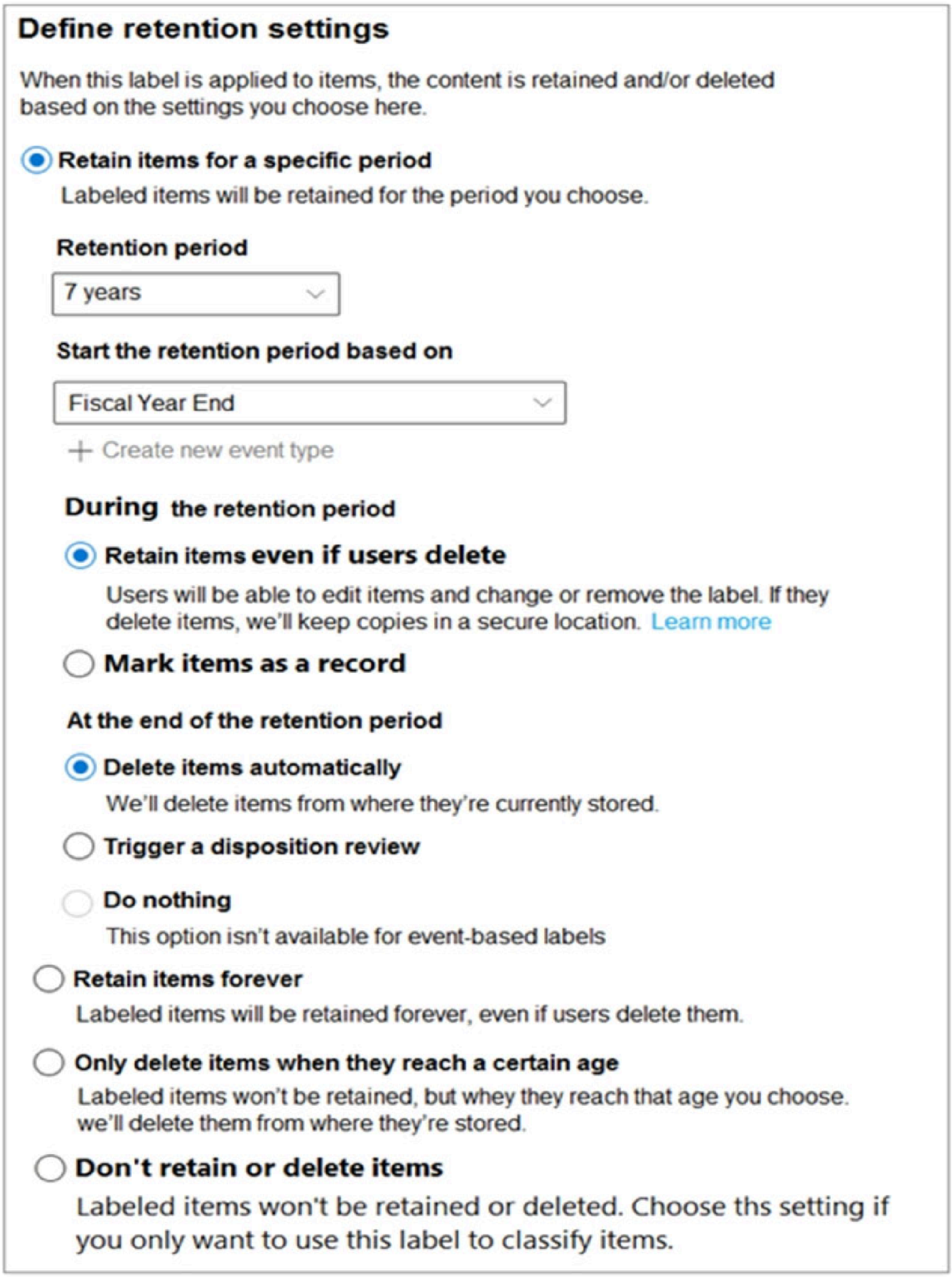
On exam 1/20/2022

upvoted 1 times

Question #31 *Topic 1*

HOTSPOT -

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



Define retention settings

When this label is applied to items, the content is retained and/or deleted based on the settings you choose here.

● **Retain items for a specific period**
Labeled items will be retained for the period you choose.

Retention period

7 years

Start the retention period based on

Fiscal Year End

+ Create new event type

During the retention period

● **Retain items even if users delete**
Users will be able to edit items and change or remove the label. If they delete items, we'll keep copies in a secure location. Learn more

○ **Mark items as a record**

At the end of the retention period

● **Delete items automatically**
We'll delete items from where they're currently stored.

○ **Trigger a disposition review**

○ **Do nothing**
This option isn't available for event-based labels

○ **Retain items forever**
Labeled items will be retained forever, even if users delete them.

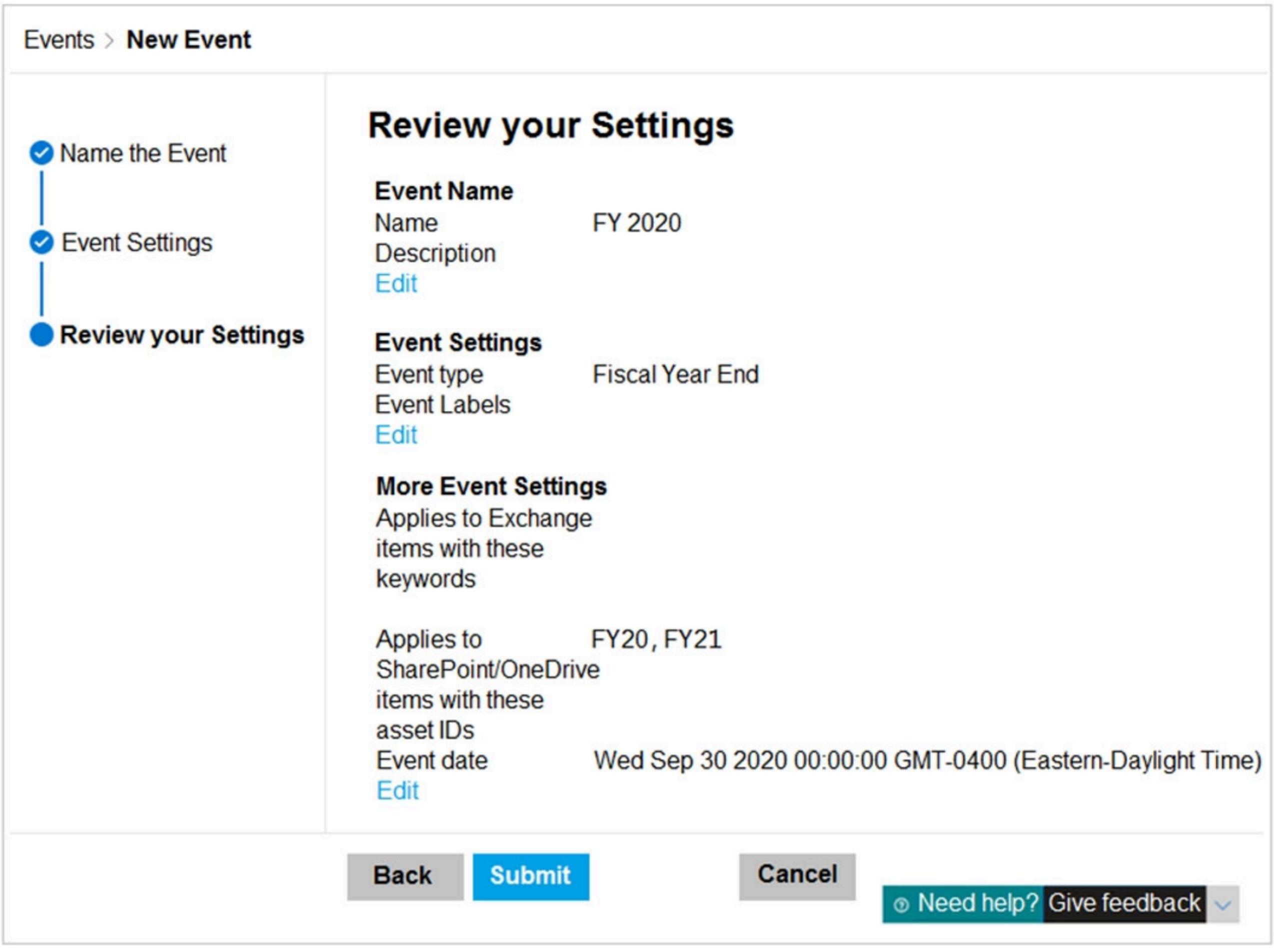
○ **Only delete items when they reach a certain age**
Labeled items won't be retained, but whey they reach that age you choose. we'll delete them from where they're stored.

○ **Don't retain or delete items**
Labeled items won't be retained or deleted. Choose ths setting if you only want to use this label to classify items.

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.)



Events > New Event

- Name the Event
- Event Settings
- Review your Settings

Review your Settings

Event Name

Name FY 2020
Description
Edit

Event Settings

Event type Fiscal Year End
Event Labels
Edit

More Event Settings

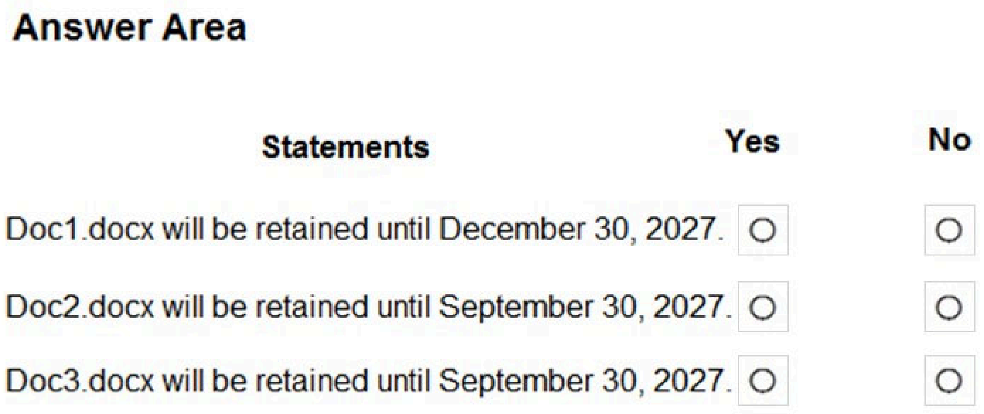
Applies to Exchange items with these keywords

Applies to SharePoint/OneDrive items with these asset IDs FY20, FY21
Event date Wed Sep 30 2020 00:00:00 GMT-0400 (Eastern-Daylight Time)
Edit

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

NOTE: Each correct selection is worth one point.

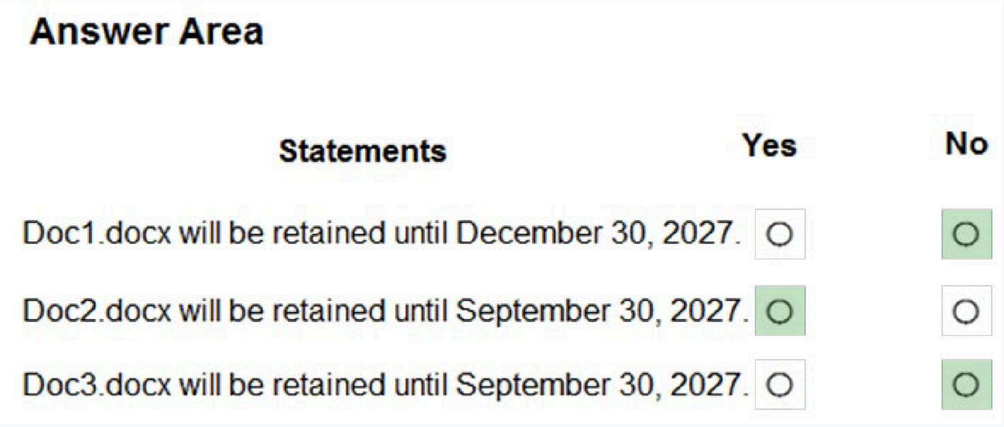
Hot Area:



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.	○	○

Suggested 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 2 years, 9 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 22 times

fimbulvetrk 2 years, 7 months ago
I don't get the answer too, I agree with you.
upvoted 2 times

wooyourdaddy 2 years, 4 months 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 2 times

Nickname 2 years, 1 month 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] 1 year, 6 months ago
But the Event Date is Sept 30th 2020. So does it apply to a file that wasn't created Oct 15 2020?
upvoted 1 times

[Removed] 1 year, 6 months ago
*a file that wasn't created until Oct 15 2020?
upvoted 1 times

[Removed] Highly Voted 2 years, 4 months 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 14 times

Ruslan23 1 year, 4 months ago
I'm agree cause asset ID is for FY 2021 + 7 = 2028
upvoted 1 times

kanag1 Most Recent 1 year ago
One needs to understand what a fiscal year means in the US to correctly answer the question. The given answers are correct.
upvoted 1 times

emartiy 1 year, 4 months ago
Advised answer is Correct. "No - Yes - No"
file 1: Won't be retained until December 30, because it is created at 1 sept and could be reatined until 20 sept 2027 based on how event configured (30 sept. 2020)
file 2: will be retained until September 30, because it is created at 20 sept and could be reatined until 30 sept 2027 based on how event configured (30 sept. 2020 last day keeping file)
file 3: It is created in October after Sept. So, based on the event and retention policy, this file will be retained after even after 30 sept. 2027 but option says until 30 sept. 2027 which is wrong and earlier date for deletion based on creation date and policy defined.
upvoted 1 times

Kodoi 1 year, 4 months ago
N, Y, N is correct.
Policy applies only to content that has already been created.
Doc3.docx was created later, so the policy does not apply to it.
upvoted 1 times

Chairborne33 1 year, 4 months ago
It was created before the Event though. Doc3 was created in October, and the event in December. It existed when the event was created.
upvoted 1 times

⊟ **heshmat2022** 1 year, 8 months ago

IT WAS ON EXAM OCTOBER 18TH 2023

upvoted 5 times

⊟ **Gesbie** 1 year, 10 months ago

was on Exam August 9, 2023

upvoted 2 times

⊟ **R3xx** 2 years 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** 2 years, 2 months 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 2 times

⊟ **_Nickname_** 2 years, 1 month 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** 2 years, 3 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 7 times

⊟ **mcas** 2 years, 8 months 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** 2 years, 8 months 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** 2 years, 7 months 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** 2 years, 9 months ago

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

upvoted 4 times

⊟ **avr** 2 years, 6 months ago

N, Y, N

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

upvoted 4 times

⊟ **_Nickname_** 2 years, 1 month 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

Suggested 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 3 years, 8 months 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 9 times

JimboJones99 Highly Voted 11 months, 1 week ago
This looks to have changed and from the question it is unclear if the trainable classifier has been published (i'm assuming it has).

"Retraining published custom classifiers is no longer supported. If you need to improve the accuracy of a trainable classifier you've published, remove the classifier and start over with larger sample sets.

To improve the accuracy of an unpublished classifier, review the test results, update the data set with additional data, and restart the training."

https://learn.microsoft.com/en-us/purview/trainable-classifiers-learn-about#retraining-classifiers
upvoted 5 times

belyo Most Recent 8 months, 3 weeks ago
Selected Answer: C
obsolete question as this is no longer supported
but during its time C was the correct option

https://learn.microsoft.com/en-us/purview/trainable-classifiers-learn-about#retraining-classifiers
upvoted 1 times

emartiy 1 year, 4 months ago
Selected Answer: C
Aggreed.
upvoted 1 times

xswe 2 years, 2 months 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 2 years, 3 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 4 times

⊟ **wooyourdaddy** 3 years ago

Selected Answer: C

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

upvoted 1 times

⊟ **ayush0312** 3 years, 3 months ago

GOOD please look in to the doc

upvoted 1 times

⊟ **PrettyFlyWifi** 3 years, 5 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

Suggested 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%)

emartiy 10 months, 1 week ago
Selected Answer: D
You can upload a csv or txt file..
upvoted 3 times

xswe 1 year, 8 months ago
When creating keyword dictionaries for sensitive info types you can only use txt and csv documents.
upvoted 2 times

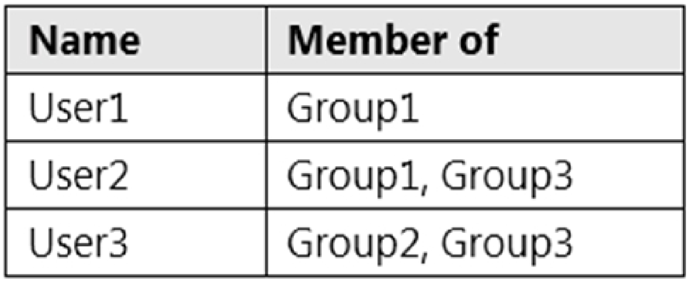
chrissempai 2 years, 3 months ago
Selected Answer: D
Basic steps to creating a keyword dictionary
The keywords for your dictionary could come from various sources, most commonly from a file (such as a .csv or .txt list) imported in the service or by PowerShell cmdlet, from a list you enter directly in the PowerShell cmdlet, or from an existing dictionary.
upvoted 4 times

Question #34 *Topic 1*

HOTSPOT -

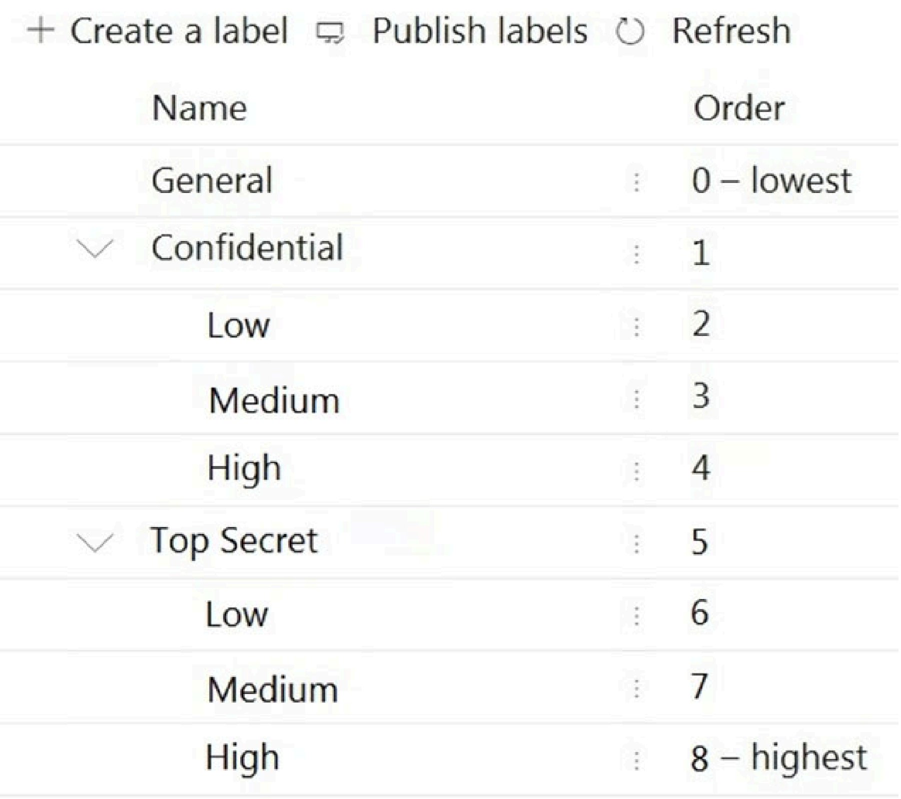
You have a Microsoft 365 E5 tenant that contains three groups named Group1, Group2, and Group3.

You have the users shown in the following table.



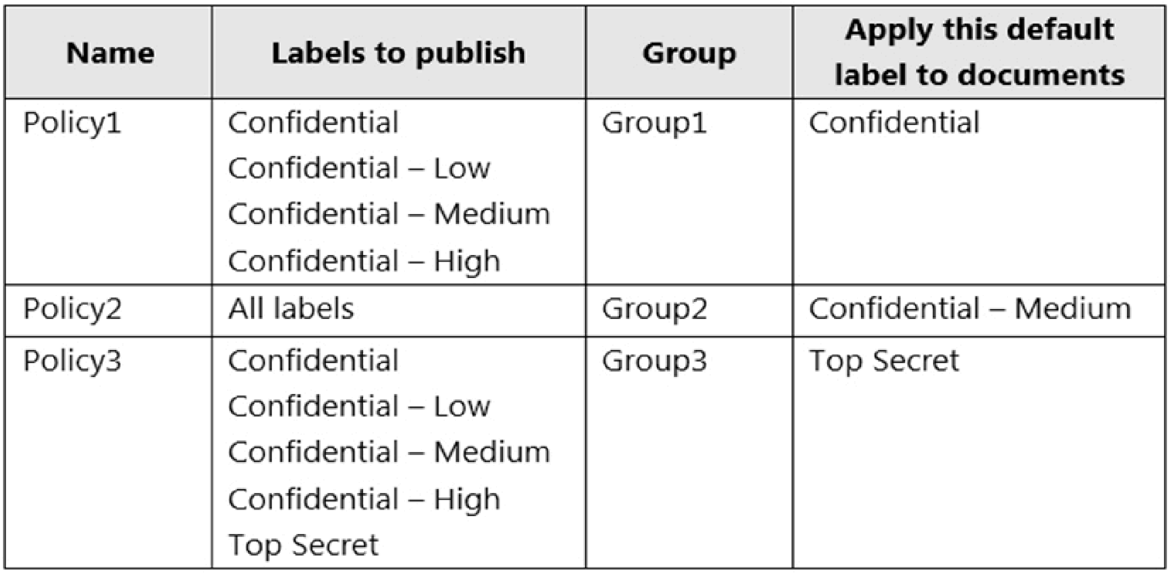
Name	Member of
User1	Group1
User2	Group1, Group3
User3	Group2, Group3

You have the sensitivity labels shown in the following exhibit.



Name	Order
General	0 – lowest
Confidential	1
Low	2
Medium	3
High	4
Top Secret	5
Low	6
Medium	7
High	8 – highest

You have the label policies shown in the following table.

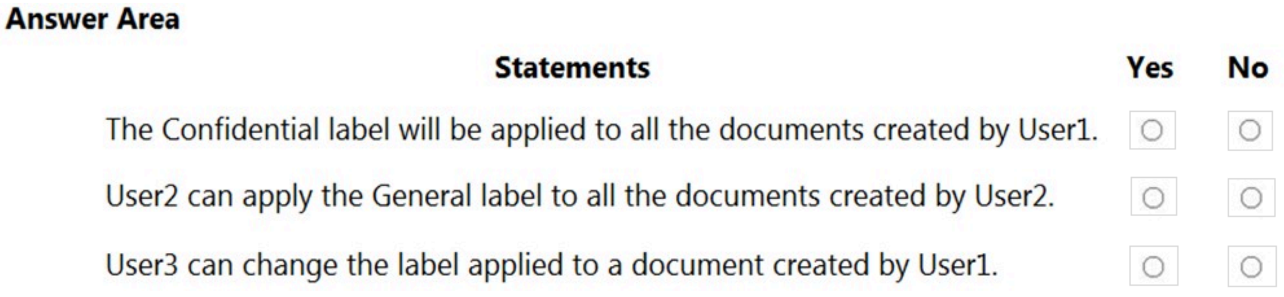


Name	Labels to publish	Group	Apply this default label to documents
Policy1	Confidential Confidential – Low Confidential – Medium Confidential – High	Group1	Confidential
Policy2	All labels	Group2	Confidential – Medium
Policy3	Confidential Confidential – Low Confidential – Medium Confidential – High Top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

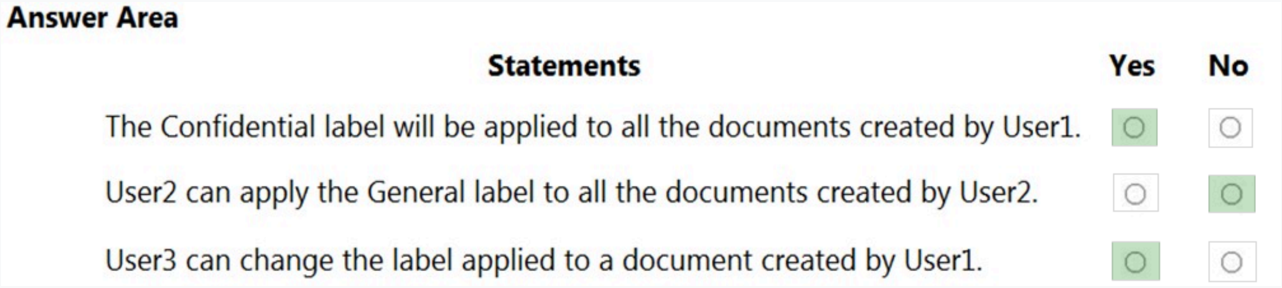
Hot Area:



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.	○	○

Suggested 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 2 years, 10 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 14 times

aashuboss 2 years, 8 months 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 10 times

xswe Highly Voted 2 years, 2 months 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 9 times

narenbabu.chintu Most Recent 11 months, 3 weeks ago

It is not possible to apply label "Confidential" as it has sub labels. these sub labels can only be assigned. Hence the first one is "NO".

upvoted 1 times

wesley223 1 year, 2 months ago

1. (YES) The confidential label will be applied to all documents created by user1, because group 1 has policy1 that applies the confidential label by default.

2. (No) User2's groups do not have "General" labels published

3- (No) User3 cannot change the label of documents created by user1 because user3 is not in group1 and consequently does not have access to the files.

upvoted 1 times

Elangamban 1 year, 6 months ago

No for first option

Reference:

https://learn.microsoft.com/en-us/purview/apply-sensitivity-label-automatically#considerations-for-label-configurations

Don't configure a parent label to be applied automatically or recommended

Remember, you can't apply a parent label (a label with sublabels) to content. Make sure that you don't configure a parent label to be auto-applied or recommended in Office apps, and don't select a parent label for an auto-labeling policy. If you do, the parent label won't be applied to content.
To use automatic labeling with sublabels, make sure you publish both the parent label and the sublabel.
For more information on parent labels and sublabels, see Sublabels (grouping labels).
upvoted 3 times

⊟ **Jonclark** 2 years, 3 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 6 times

⊟ **iUser123** 2 years, 5 months ago
Yes (https://m365admin.handsontek.net/updated-change-in-display-of-hierarchical-sensitivity-labels/)
No
Yes
upvoted 1 times

⊟ **fr54fr** 2 years, 8 months 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** 2 years, 8 months 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** 2 years, 8 months ago
Answer 2 = No,
Label General is not published for Group 1 & Group 3 of which User2 is member of
upvoted 2 times

Question #35 *Topic 1*

HOTSPOT -

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

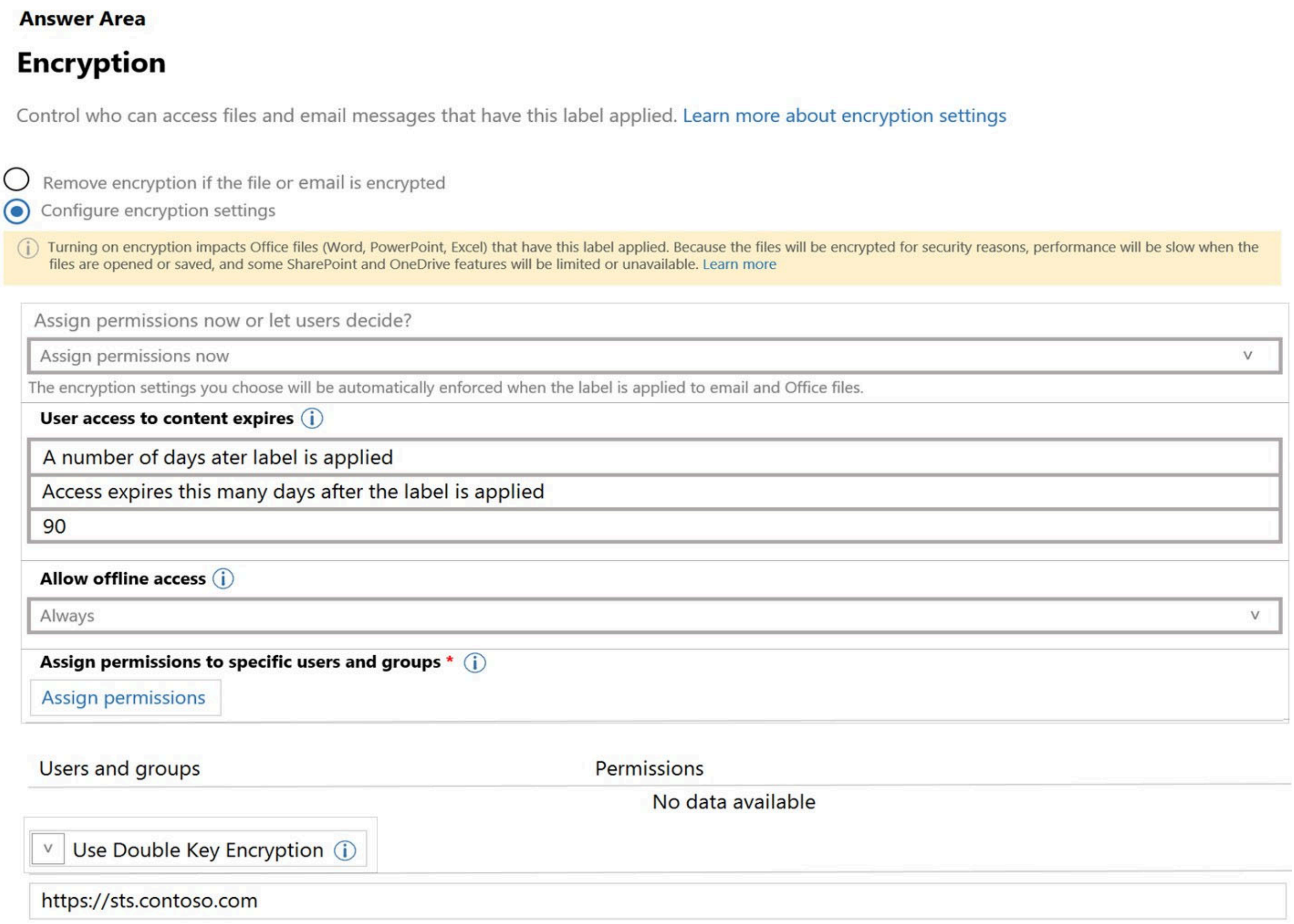
You plan to enable co-authoring for encrypted files.

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:



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 * ⓘ

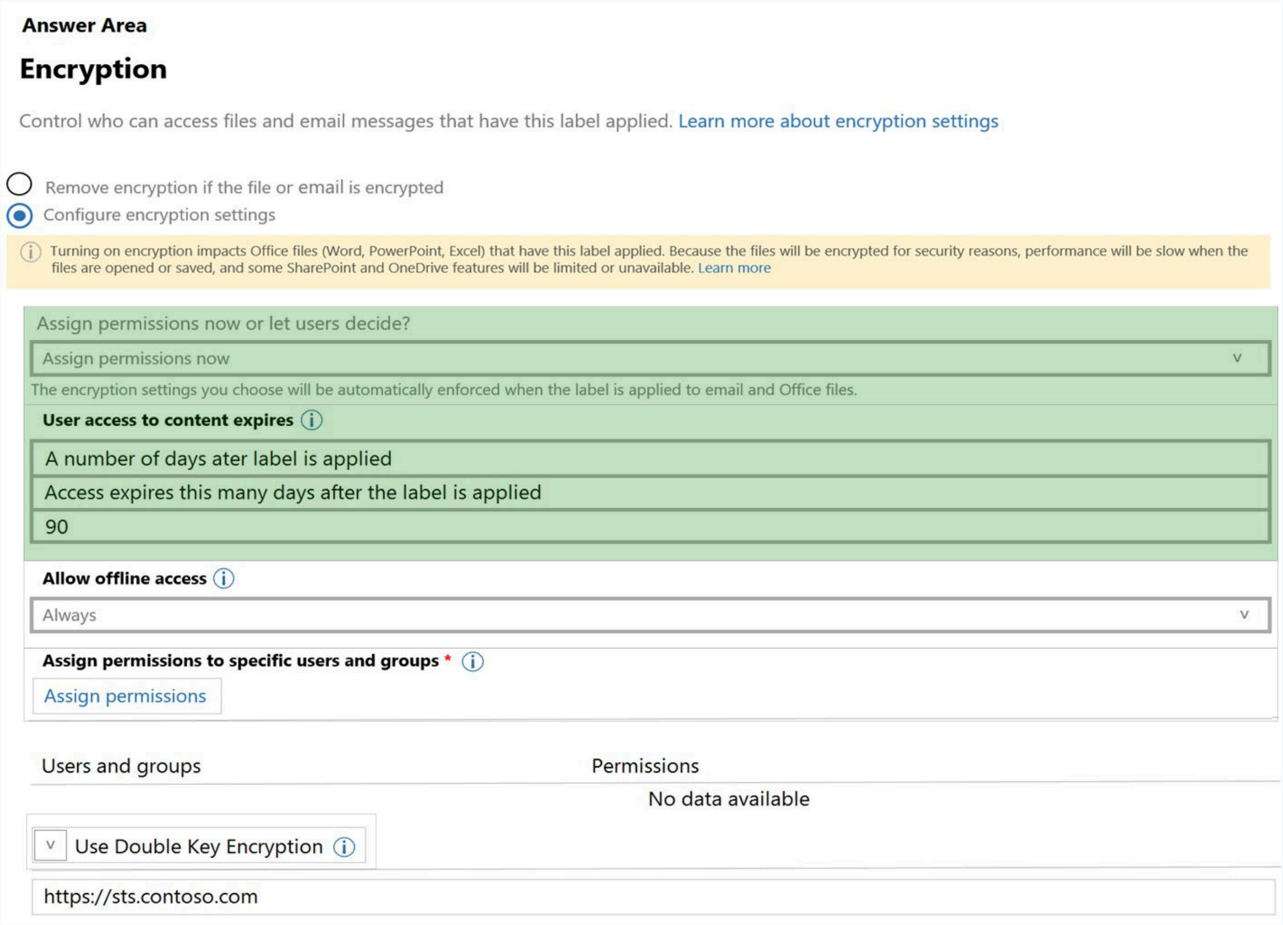
Assign permissions

Users and groups	Permissions
	No data available

∨ Use Double Key Encryption ⓘ

https://sts.contoso.com

Suggested 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 2 years, 9 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 8 times

⊟ **kiketxu** 2 years, 8 months 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

⊟ **narenbabu.chintu** Most Recent 11 months, 3 weeks ago

1. Selecting Double encryption does not cause any issue with co-authoring files.

2. Other options like "Assign permissions now" , "Assign Permissions to specific users and groups" are already selected.

3. Use access to content expires - does not effect co-authoring files.

Then the steps that are left:

Select "Assign Permissions to specific users and groups" --> Assign Permissions
Then
Select User or groups to select users to whom co-authoring can be provided

These are the two steps that have to be performed.
There are no multiple choices here.
upvoted 2 times

IndigoRabbit 10 months, 3 weeks ago
You are right! However, in this question, it shows the current configuration has double encryption enabled and 'user access to content expires' is set to anything but 'Never'. According to MS, Co-authoring and AutoSave aren't supported for Office documents that use the label encryption configuration User access to content expires when it's set to a value other than Never, or Double Key Encryption is configured.
https://learn.microsoft.com/en-us/purview/sensitivity-labels-coauthoring?view=o365-worldwide#limitations
upvoted 2 times

IndigoRabbit 10 months, 3 weeks ago
So, correct answers are
1. Disable double encryption
2. Set 'User access to content expires' to 'Never'
upvoted 1 times

Softeng 1 year, 4 months ago
Link to exact line of Microsoft Docs with the answer:

https://learn.microsoft.com/en-us/purview/sensitivity-labels-coauthoring?view=o365-worldwide#:~:text=Co%2Dauthoring%20and%20AutoSave%20aren%27t%20supported%20for%20Office%20documents%20that%20use%20the%20label%20enc
upvoted 2 times

phony 1 year, 8 months 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 3 times

Jonclark 2 years, 3 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 3 times

Question #36 Topic 1

HOTSPOT

-

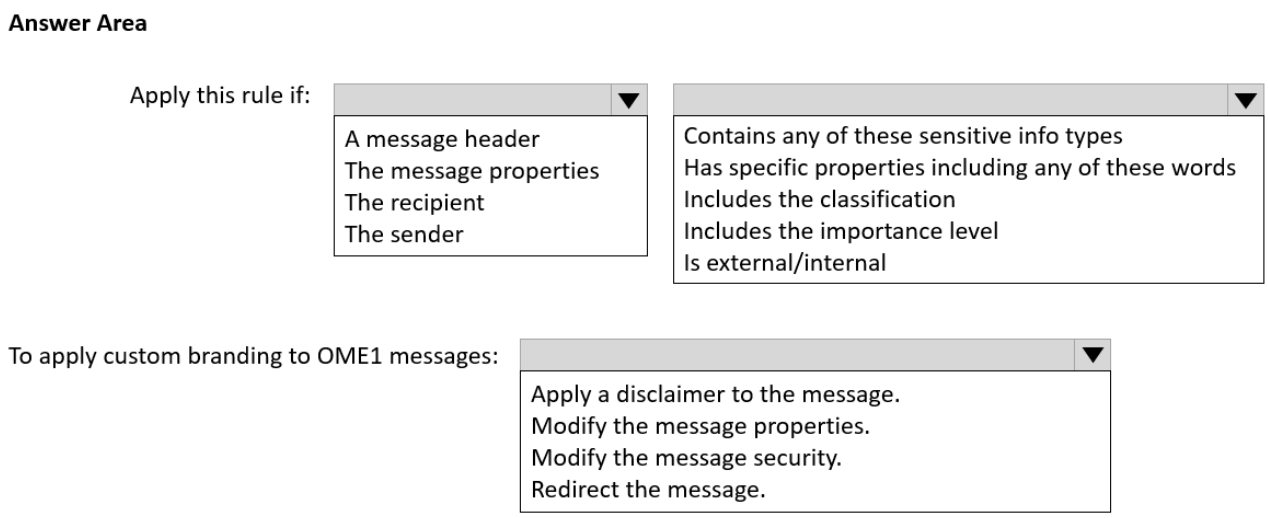
You have a Microsoft 365 E5 subscription.

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:

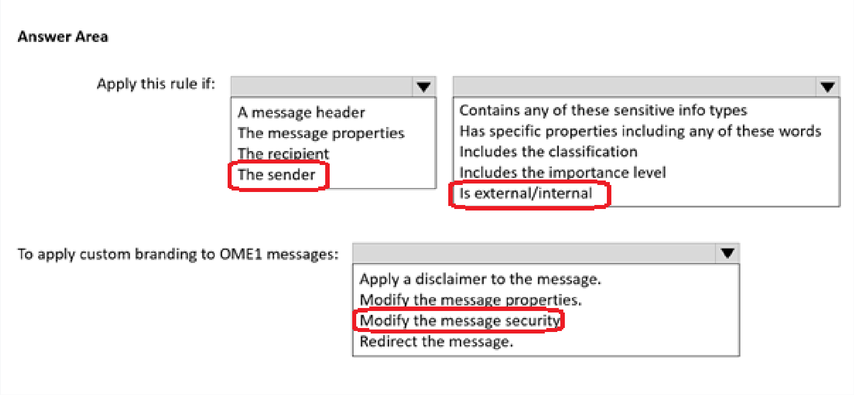
- A message header
- The message properties
- The recipient
- The sender

- 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.

Suggested 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.

Domza Highly Voted 1 year, 5 months ago

Looks correct~

Found it here: Steps 6-8

https://learn.microsoft.com/en-us/purview/add-your-organization-brand-to-encrypted-messages#create-an-exchange-mail-flow-rule-that-applies-your-custom-branding-to-encrypted-emails-sent-from-your-online-organization-to-external-recipients

with love-

upvoted 8 times

Co123 1 year, 5 months ago

txs for recent updatee

upvoted 3 times

⊟ **Mr_Big** Most Recent 5 months ago

I do not understand why the first option is the sender. If you wish to protect the message with OME, the mailflow rule should apply to the recpient. Not one wish to apply OME to internal mailboxes.

upvoted 1 times

⊟ **rupeshngp** 12 months ago

Correct. Both the options are correct.

If you've already defined a mail flow rule to apply encryption, skip this step. Otherwise, to configure the mail flow rule to apply encryption, from Do the following, select Modify the message security, and then select Apply Office 365 Message Encryption and rights protection. Select a Rights Management Service (RMS) template from the list and then select add action.

From Do the following, select Modify the message security > Apply custom branding to OME messages. Next, from the drop-down, select a branding template.

upvoted 1 times

⊟ **horseboxIRL** 1 year, 6 months ago

Just making you all aware, this question IS complete. It was on my exam today (20/12/2023) and was this exact question.

upvoted 4 times

⊟ **phony** 1 year, 8 months 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 2 times

⊟ **217f3c9** 2 years, 1 month 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** 2 years, 2 months 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 2 times

⊟ **luissaro** 2 years, 2 months ago

I guess something is missing in this question...

upvoted 1 times

⊟ **See_Es** 2 years, 5 months 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.

Suggested Answer: *C*

wooyourdaddy Highly Voted 10 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 7 times

See_Es Most Recent 11 months, 1 week ago

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

upvoted 3 times

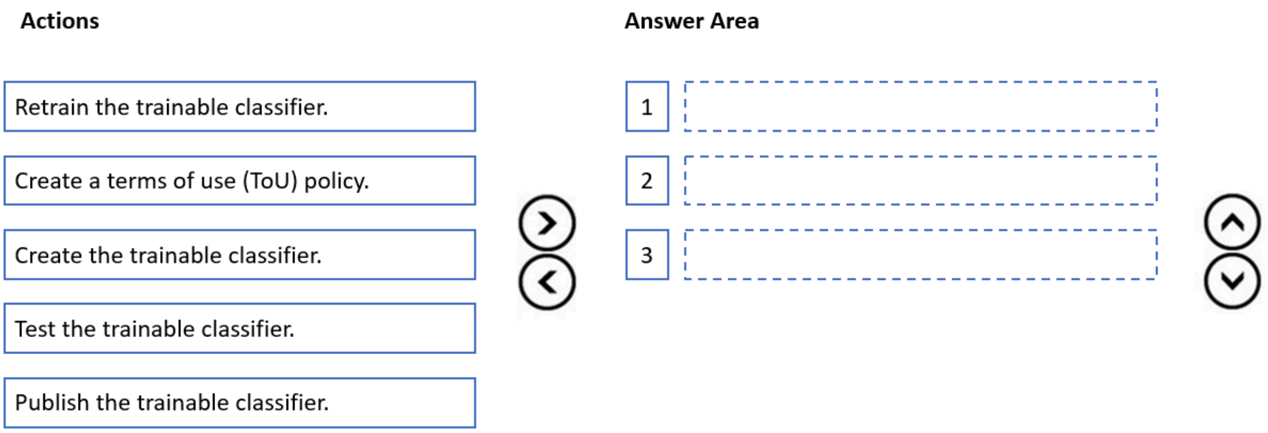
Question #38 Topic 1

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.



Actions

- Retrain the trainable classifier.
- Create a terms of use (ToU) policy.
- Create the trainable classifier.
- Test the trainable classifier.
- Publish the trainable classifier.

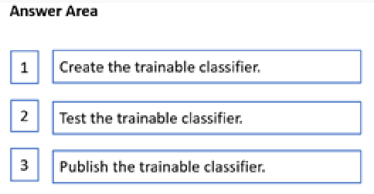
Answer Area

1

2

3

Suggested Answer:



Answer Area

1 Create the trainable classifier.

2 Test the trainable classifier.

3 Publish the trainable classifier.

wooyourdaddy 10 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 4 times

Chris7910 10 months, 3 weeks ago

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

upvoted 1 times

[Removed] 10 months, 2 weeks ago

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

upvoted 3 times

Jonclark 9 months, 3 weeks 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

Suggested Answer: *C*

Community vote distribution

C (100%)

⊟ **jinxie** Highly Voted 1 year, 11 months 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

⊟ **jimmyjose** Most Recent 9 months, 3 weeks ago

Correct answer - C

A. a trainable classifier - used to train the system by feeding it with bulk data; not correct
B. a sensitivity label - used for data classification; not correct
C. a sensitive info type - the only choice
D. a retention policy - used for retaining data; not correct

upvoted 2 times

⊟ **Domza** 1 year, 1 month ago

looks good~

upvoted 1 times

⊟ **xswe** 1 year, 8 months ago

Keyword dictionaries = Sensitive info type

upvoted 1 times

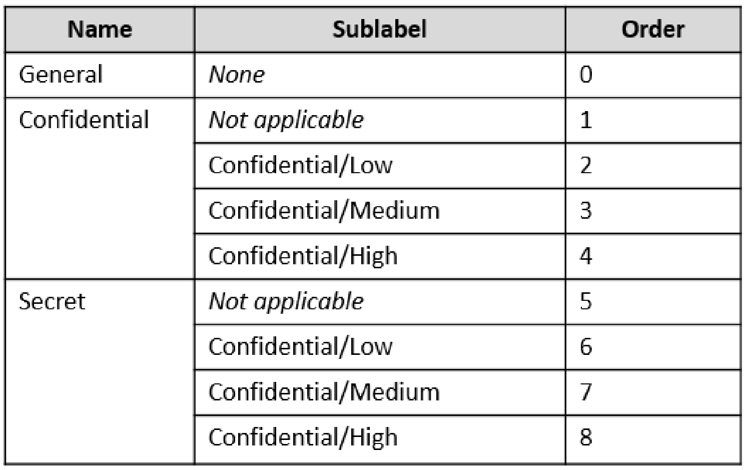
Question #40 *Topic 1*

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

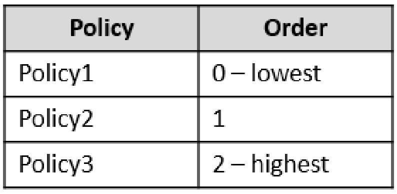
For Policy2, the default label for documents is Secret/Low.

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.

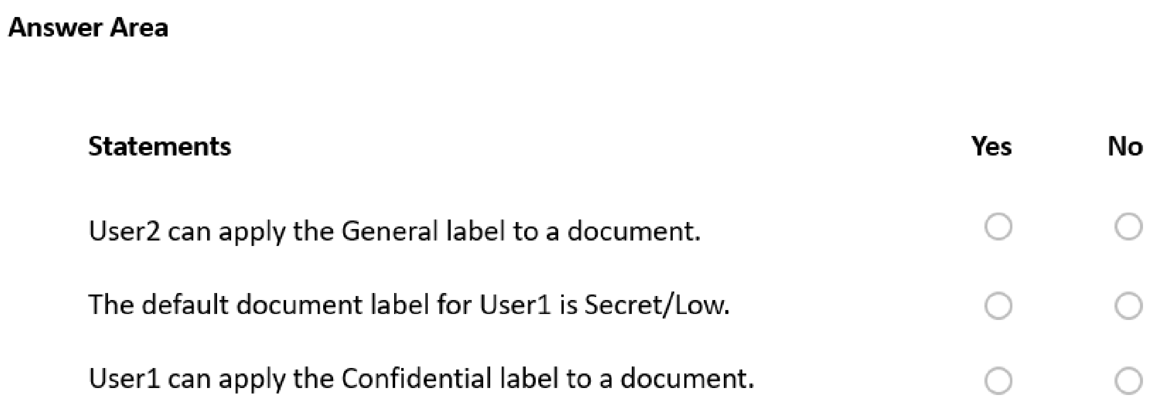
The order of the policies is shown in the following table.



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.

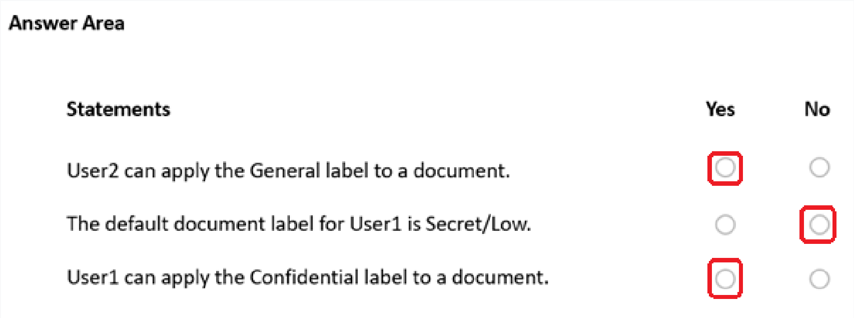
NOTE: Each correct selection is worth one point.



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.	○	○

Suggested 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 2 years, 5 months ago

Should be Y/N/N. The Confidential label is a parent label and cannot be selected as a document label

upvoted 19 times

⊟ **Jonclark** 2 years, 3 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 3 times

⊟ **narenbabu.chintu** Most Recent 11 months, 3 weeks ago

Agree, Y, N, N

1. User2 can apply the General Label to a document - Yes, User2 is part of Policy 3 as well as Policy 1, but Policy 3 has highest priority. The Labels that are part of Policy 3 include General. Hence User2 can assign General Label to Documents
2. The default document label for User1 is Secret/Low - No, User1 is part of Policy 3 as well as Policy1 , The Highest prioritized policy is Policy 3. The default label of Policy 3 is Secret / Medium. Hence the default label for the document created by User 1 is Secret/Medium.
3. User1 can apply the confidential label to a document - No, It is not possible to apply parent label as a default label.

upvoted 4 times

⊟ **Domza** 1 year, 5 months ago

YNN looks good~

upvoted 1 times

⊟ **trojansrj** 1 year, 9 months 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 2 times

⊟ **dmoorthy** 2 years, 2 months ago

Answers is Y/N/N

upvoted 1 times

⊟ **xswe** 2 years, 2 months 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** 1 year, 11 months 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

Suggested Answer: *A*

Community vote distribution

A (100%)

heshmat2022 8 months, 2 weeks ago

IT WAS ON EXAM OCTOBER 18 2023

upvoted 3 times

Gesbie 10 months, 3 weeks ago

was on Exam August 9, 2023

upvoted 3 times

xswe 1 year, 2 months ago

Always custom branding templates for this, you can use the following cmdlet

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

upvoted 3 times

jinxie 1 year, 5 months 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 1 year, 5 months 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 4 times

Jonclark 1 year, 3 months ago

In case the test question asks you about the PowerShell cmdlet, it looks something like this:

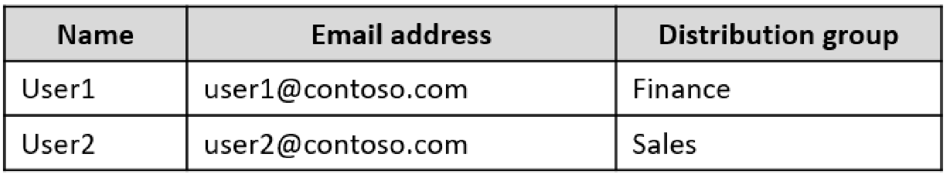
Set-OMEconfiguration -Identity My_OME_Template -ExternalMailExpiryInDays 7

upvoted 2 times

HOTSPOT

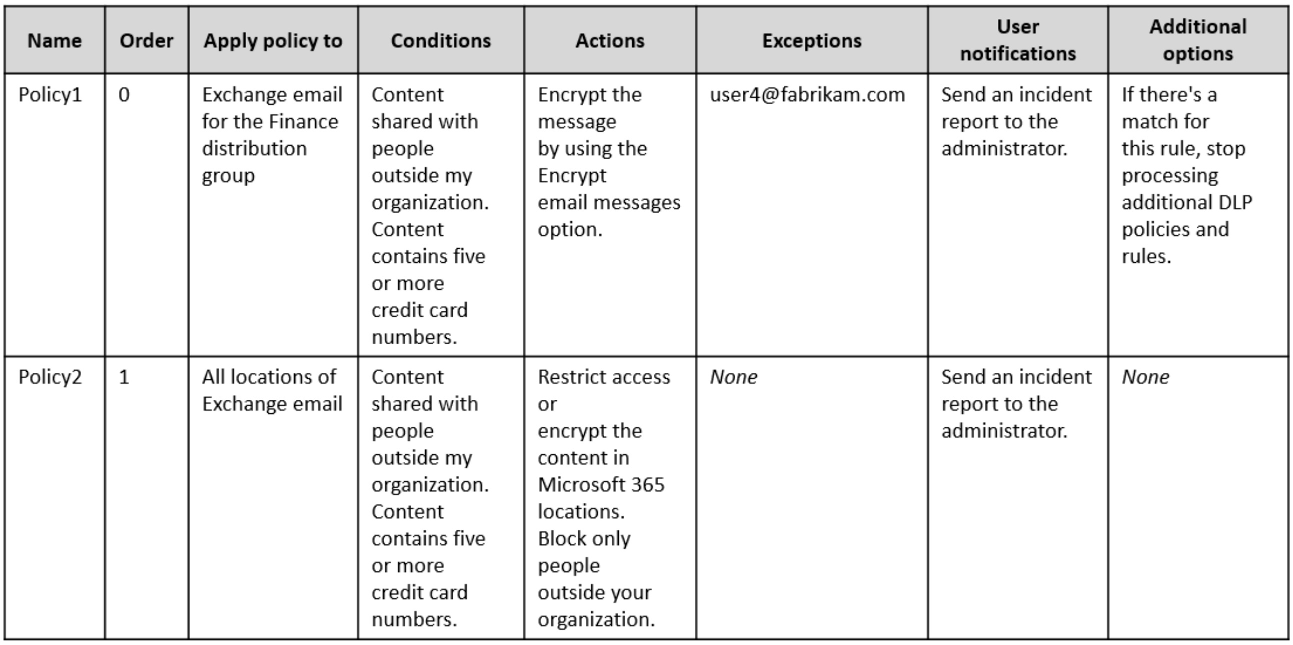
-

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

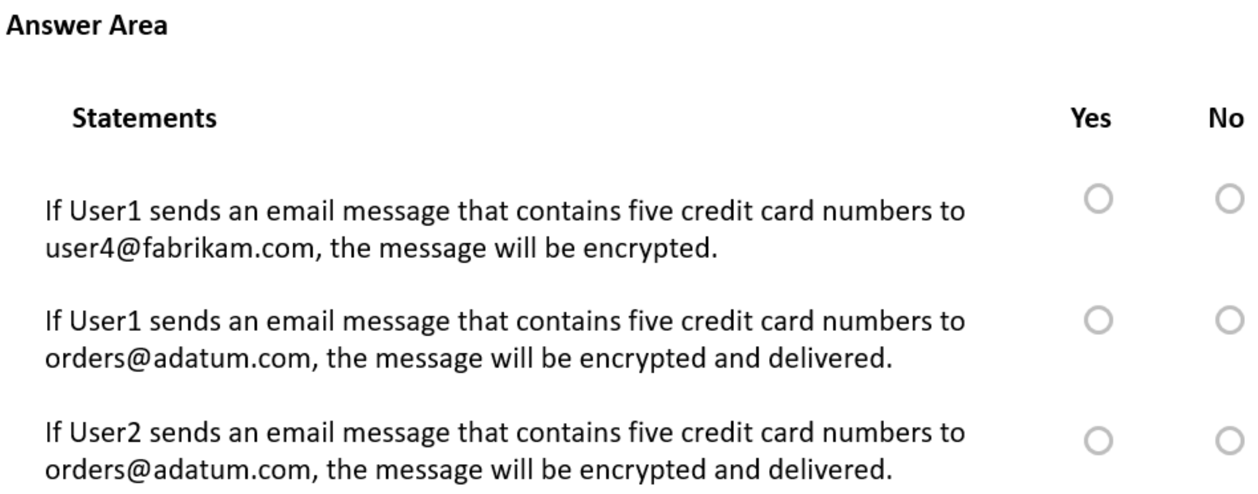
You create the data loss prevention (DLP) policies shown in the following table.



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.

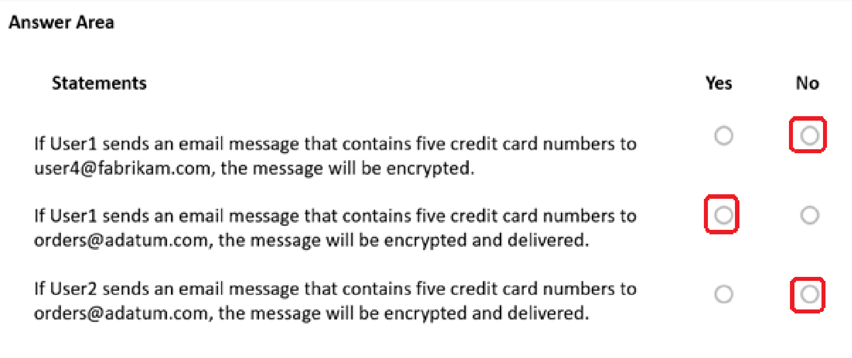
NOTE: Each correct selection is worth one point.



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.	○	○

Suggested Answer:



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.	○	[✓ ○]

See_Es Highly Voted 2 years, 5 months 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 10 times

xswe Highly Voted 2 years, 2 months 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 5 times

husamshahin Most Recent 11 months, 1 week ago

on Exam 28-7-2024

upvoted 3 times

XylosSW 1 year ago

NNN

1) It think it is No because user1 sends to user4@fabrikam.com which is on the exceptions list. So it won't be encrypted.

2) it is user1 but policy 2 will apply (all location so also 'sales' is included) content is shared with @adatum.com so it will be blocked because it goes outside the organization. So it is encrypted but BLOCKED it cannot be send outside.

3) User 2 part of sales also Policy 2 will apply so also outside is also blocked

upvoted 2 times

IndigoRabbit 10 months, 3 weeks ago

Answer of the 2nd part would be Yes cause even though both policies are published to user1, policy 1 has higher priority(priority 0), hence, policy 1 will trigger

upvoted 2 times

Domza 1 year, 5 months ago

Looks good~

upvoted 1 times

heshmat2022 1 year, 8 months ago

IT WAS ON EXAM OCTOBER 18 2023

upvoted 3 times

luissaro 2 years, 2 months 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

Wildz 1 year, 3 months ago

Wrong it says at the end block only out of org, adatum is out of org therefore blocked

upvoted 3 times

Question #43 *Topic 1*

HOTSPOT

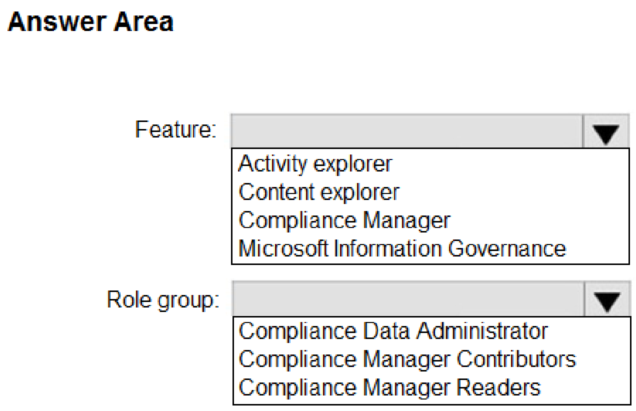
-

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.

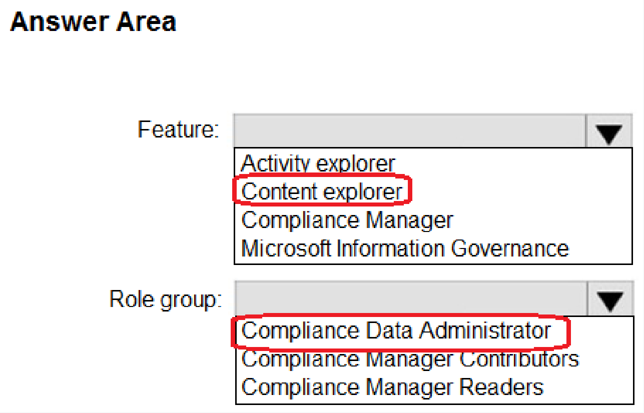


Answer Area

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

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

Suggested 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 2 years, 2 months 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 10 times

⊟ **belyo** Most Recent 8 months, 3 weeks ago

another obsolete, but seems correct during its time

https://learn.microsoft.com/en-us/purview/trainable-classifiers-learn-about?source=recommendations&view=o365-worldwide#retraining-classifiers

upvoted 1 times

⊟ **Domza** 1 year, 5 months ago

Looks good~

Thanks all

upvoted 2 times

⊟ **heshmat2022** 1 year, 8 months ago

IT WAS ON EXAM OCTOBER 18 2023

upvoted 2 times

⊟ **Gesbie** 1 year, 10 months ago

was on Exam August 9, 2023

upvoted 1 times

⊟ **shuffler** 2 years, 3 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 3 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.

Suggested Answer: *B*

xswe Highly Voted 👍 2 years, 2 months 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

Domza 1 year, 6 months ago

I reject your opinion~ PLEASE add supporting facts if you want to participate.

upvoted 1 times

husamshahin Most Recent 11 months, 1 week ago

on Exam 28-7-2024

upvoted 1 times

mimguy 1 year, 5 months ago

Answer B is correct. Of course, you can do this in a DLP Policy in the compliance portal but the key here is "Using the Exchange admin center". This definitely lends to B being the correct choice.

upvoted 2 times

jpcapone 1 year, 5 months ago

Can't you use a DLP policy to alert if a file is shared externally?

upvoted 1 times

Domza 1 year, 6 months ago

Correct~

Please see question 47 LOL

upvoted 1 times

heshmat2022 1 year, 8 months ago

IT WAS ON EXAM OCTOBER 18 2023

upvoted 2 times

mstfcskn 1 year, 11 months 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 4 times

Question #45 *Topic 1*

HOTSPOT

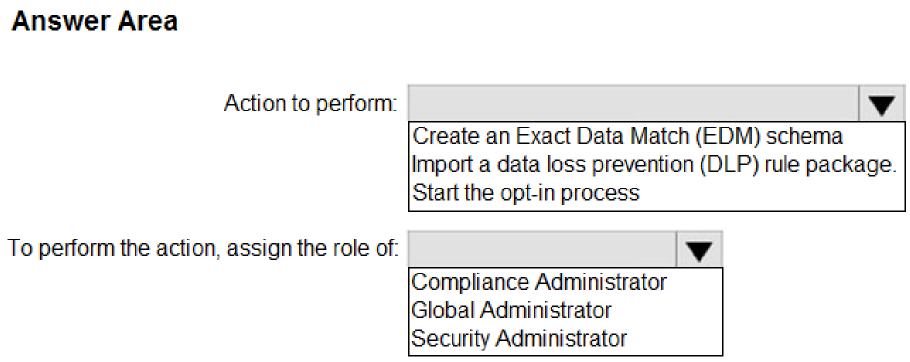
-

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.

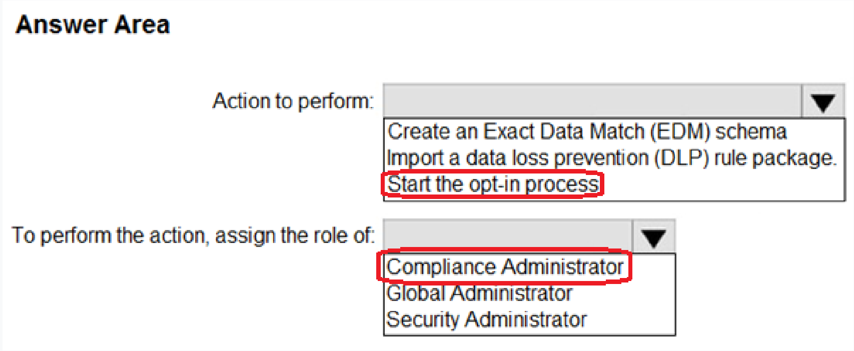


Answer Area

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

Suggested 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 2 years, 3 months 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 17 times

⊟ **EM1234** 1 year ago

this page does not say those words anymore

upvoted 1 times

⊟ **VishalMs** 1 year ago

Hey EM1234, does the exam have any labs to complete?

upvoted 1 times

⊟ **EM1234** 1 year ago

I have not taken the exam yet. I am still studying. I was just pointing out that I think this question is likely outdated since the link in the docs does not include the opt in process anymore. I bet it is opted-in by default now as Microsoft does after a feature been GA for a while. That is only my guess though.

upvoted 1 times

⊟ **reastman66** Highly Voted 2 years, 2 months ago

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

upvoted 5 times

dashadowman00 Most Recent 8 months, 1 week ago

I think the answer should be:

* Create an Exact Data Match (EDM) schema

* Compliance Administrator

upvoted 4 times

Mnguyen0503 7 months ago

No where in the question do they mention using EDM. EDM if also only applicable if there is a database to match the data with. For trainable classifier, opt-in is required before you can start using it.

upvoted 1 times

belyo 8 months, 3 weeks ago

can a custom trainable classifier be made from EDM ?

there are 3 types classifiers: 1 trainable 2 SIT 3 EDM

so the question ask to make a trainable classifier not and EDM classifier

maybe its the opt-in here but not sure whether should GA or CA

nowhere is said GA can opt-in

upvoted 1 times

EsamiTopici 1 year, 2 months ago

Why not create exact data match schema?

upvoted 1 times

emartiy 1 year, 4 months ago

In order to create a custom classifier, Global Admins ensure opt-in. So, correct answer is Start opt-in with global admin role.

upvoted 2 times

Domza 1 year, 5 months ago

Looks good!

upvoted 1 times

Futfuyfyjfj 1 year, 4 months ago

No it doesn't. See Shuffler:

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 1 times

willowvine 1 year, 8 months 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 year, 8 months ago

IT WAS ON EXAM OCTOBER 18 2023

upvoted 1 times

ikidreamz 1 year, 11 months ago

looks like Opt-in and Global admin)(TO CREATE not train) my bad I thought least privilege earlier

upvoted 1 times

ikidreamz 1 year, 11 months 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 1 year, 11 months ago

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

upvoted 1 times

⊟ **ikidreamz** 1 year, 11 months ago

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

upvoted 1 times

⊟ **GeoffLule** 2 years, 2 months ago

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

upvoted 1 times

⊟ **dmoorthy** 2 years, 2 months ago

Start the Opt-in process and Global Admin

upvoted 3 times

⊟ **xswe** 2 years, 2 months 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

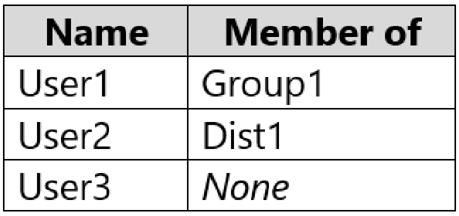
upvoted 4 times

Question #46 *Topic 1*

HOTSPOT

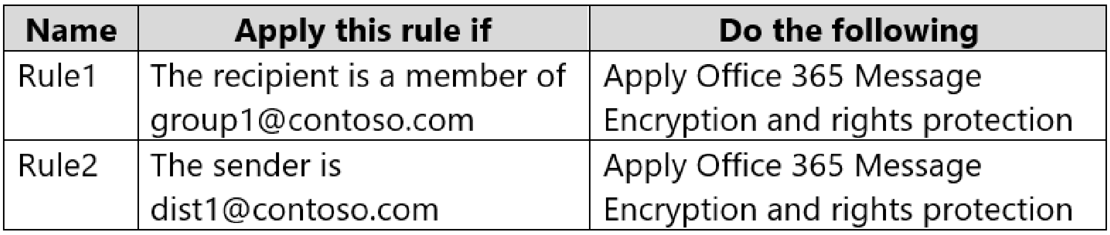
-

The subscription contains the users shown in the following table.



Name	Member of
User1	Group1
User2	Dist1
User3	*None*

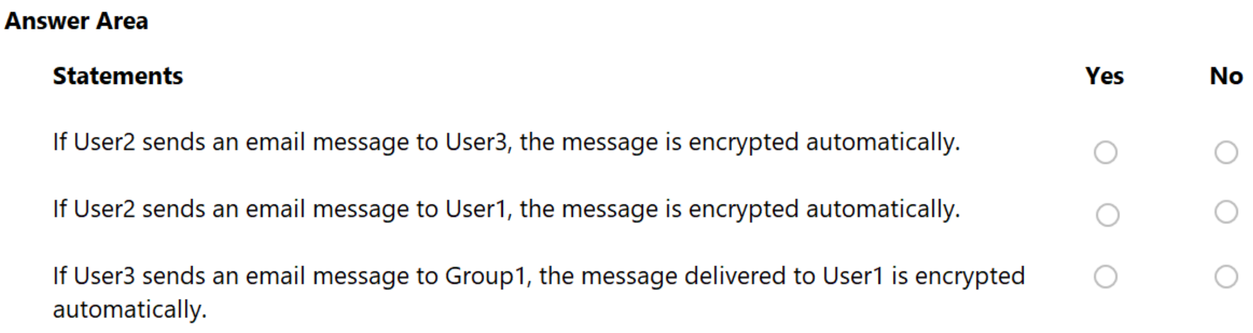
You create the mail flow rules shown in the following table.



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.

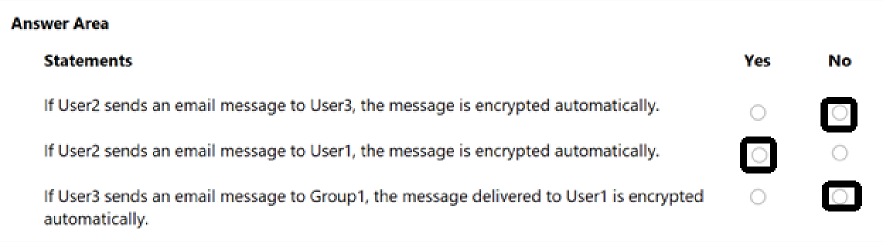
NOTE: Each correct selection is worth one point.



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.	○	○

Suggested 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.	○	[✓ ○]

⊟ **martutene** Highly Voted 1 year, 8 months 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 13 times

⊟ **Kuteron** 7 months ago

tested in my lab environment statement 3. Only the first member of the mail enabled security group get the mail encrypted. All other members (2,3,4,5) does not get the mail encrypted. In this szenario we only have one member in one group. so last statement is yes:

N - Y - Y

upvoted 2 times

⊟ **Ruslan23** 1 year, 3 months ago

3. Should be NO because the message is encrypted automatically when is sent from User3 to Group1, next the message will be delivered to User1 already encrypted.

The statement declare that the message is automatically encrypted in the second step Group1 > User1 but is NOT true.

upvoted 1 times

⊟ **Futfuyfyjfj** 1 year, 5 months ago

3. The question is whether the e-mail was encrypted automatically

upvoted 2 times

⊟ **HeirrBourne** Most Recent 5 months, 1 week ago

NYYIf the group has encryption (through Office 365 Message Encryption (OME)) and rights protection settings (like Azure Rights Management (Azure RMS)), these settings apply to any message sent to the group.

2. How Encryption Works for Group Emails:

When a user sends an email to the group, and the group has encryption settings applied (e.g., Office 365 Message Encryption (OME) or Azure Rights Management), the message is encrypted when it leaves the sender's mailbox.

If the email contains sensitive information, Microsoft 365 compliance policies like Information Protection can enforce rights management (such as restricting forwarding, printing, or copying).

3. What Happens to Each Member:

Each recipient who is a member of the group will receive the email, but the content will be encrypted, and rights protection will apply.

upvoted 1 times

⊟ **belyo** 8 months, 3 weeks ago

NO the sender is user2 not dist1@contoso.com - mail flow rules not applied

YES Rule 1 matched as U1 is the recipient of group1

YES Rule 1 matched as U1 is the recipient of group1

upvoted 1 times

⊟ **husamshahin** 11 months, 1 week ago

on Exam 28-7-2024

upvoted 3 times

⊟ **Amin4799** 1 year, 1 month ago

valid till 20/5/2024

Pass with good grade

upvoted 2 times

⊟ **Franc_Coetzee** 1 year, 7 months 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 4 times

⊟ **asdilhfnas** 1 year, 7 months 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 3 times

⊟ **asdilhfnas** 1 year, 7 months ago

3. Yes

upvoted 2 times

⊟ **Futfuyfyjfj** 1 year, 4 months ago

No where in question 3 User 1 is mentioned, so should be no

upvoted 2 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

Suggested Answer: *B*

Community vote distribution

B (100%)

tlgrittz 8 months, 2 weeks ago

Correct

https://learn.microsoft.com/en-us/defender-cloud-apps/data-protection-policies

upvoted 2 times

emartiy 10 months, 1 week ago

Selected Answer: B

Correct +

upvoted 1 times

Domza 1 year ago

Correct~

Please see Question 44 LOL

upvoted 3 times

martutene 1 year, 1 month ago

Selected Answer: B

Correct

upvoted 2 times

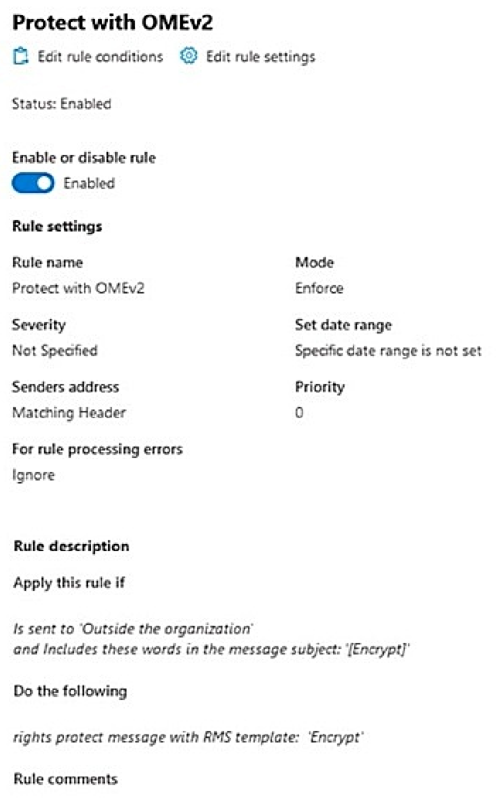
Question #48 *Topic 1*

HOTSPOT

-

You have a Microsoft 365 subscription.

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



Protect with OMEv2

Edit rule conditions Edit rule settings

Status: Enabled

Enable or disable rule

Enabled

Rule settings

Rule name Protect with OMEv2	Mode Enforce
Severity Not Specified	Set date range Specific date range is not set
Senders address Matching Header	Priority 0
For rule processing errors Ignore	

Rule description

Apply this rule if

Is sent to 'Outside the organization'
and Includes these words in the message subject: '[Encrypt]'

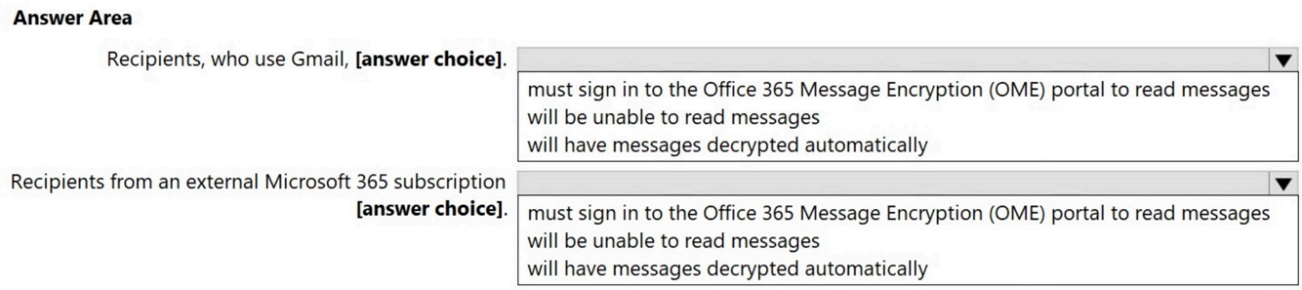
Do the following

rights protect message with RMS template: 'Encrypt'

Rule comments

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.

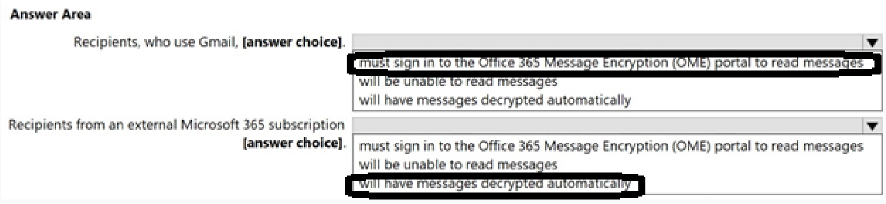


Answer Area

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

Suggested 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 Highly Voted 1 year, 1 month 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 5 times

Domza Most Recent 12 months ago

Looks good~

upvoted 2 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

Suggested Answer: *B*

Community vote distribution

B (100%)

Domza 11 months, 2 weeks ago

Selected Answer: B

Looks good~

upvoted 2 times

JacoH 1 year, 1 month ago

Answer is correct

https://learn.microsoft.com/en-us/purview/apply-sensitivity-label-automatically

upvoted 3 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

Suggested Answer: *A*

Community vote distribution

A (100%)

iamjay2020 6 months, 2 weeks ago

Selected Answer: B

Correct is B. The question is: identify resumes that are stored in the subscription by using a built-in trainable classifier

upvoted 1 times

Athena94 8 months, 3 weeks ago

Is "A" correct because in the Autolabeling policy we can use the condition of content contains - trainable classifer and then select a label?

upvoted 2 times

Domza 11 months, 2 weeks ago

Selected Answer: A

Correct!~

upvoted 2 times

JacoH 1 year, 1 month ago

Answer is correct

https://learn.microsoft.com/en-us/purview/apply-sensitivity-label-automatically

upvoted 3 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

Suggested Answer: *B*

ca7859c 1 month, 3 weeks ago

Selected Answer: A

Yes
DLP or Sensitivity labels can take SITs & Trainable classifiers
upvoted 1 times

Doinitza 8 months, 2 weeks ago

Tricky question, you can receive alerts every time a resume (built-in trainable classifier) is detected by using a DLP Policy, but it's a very uncomfortable way of working.
upvoted 1 times

blokechettri 9 months, 2 weeks ago

Yes. I was able to select built in Trianable SIT
upvoted 1 times

PsiCzar 11 months, 1 week ago

Answer is correct. There is no option to select a trainable classifier in the DLP policy wizard.
upvoted 2 times

brats_harsh 1 year ago

Yes is the answer - DLP supports trainable classifier

https://learn.microsoft.com/en-us/purview/trainable-classifiers-learn-about
upvoted 1 times

Domza 1 year, 7 months ago

It says"identify resumes that are stored" - sensitivity labels do that
upvoted 2 times

JacoH 1 year, 7 months ago

Answer is correct.
You can't use trainable classifiers in a (custom) DLP policy
upvoted 1 times

> **BJack** 1 year, 7 months 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

Suggested Answer: *A*

dillon123456789 3 months, 1 week ago

Selected Answer: A

on exam

upvoted 1 times

Domza 11 months, 3 weeks ago

Same as question 41

upvoted 1 times

kingAzure 1 year, 1 month 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

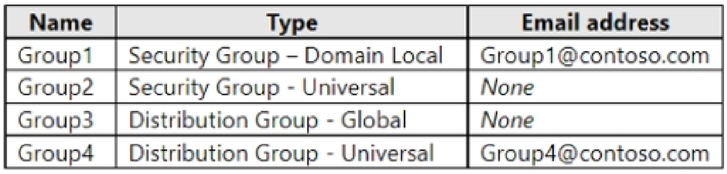
upvoted 3 times

Question #53 *Topic 1*

HOTSPOT

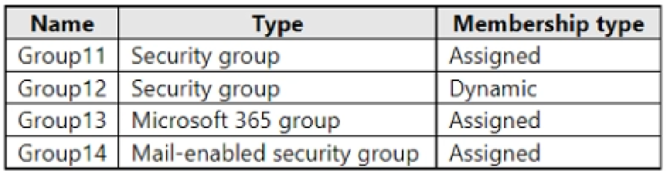
-

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.



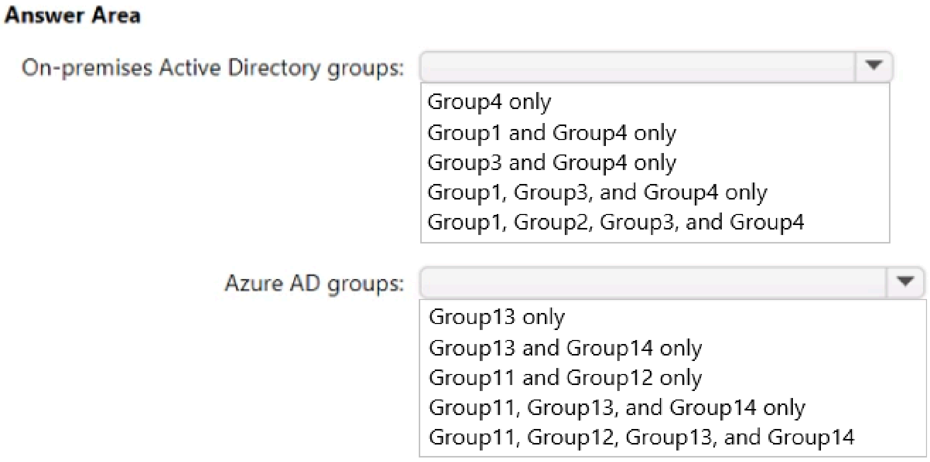
Name	Type	Membership type
Group11	Security group	Assigned
Group12	Security group	Dynamic
Group13	Microsoft 365 group	Assigned
Group14	Mail-enabled security group	Assigned

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

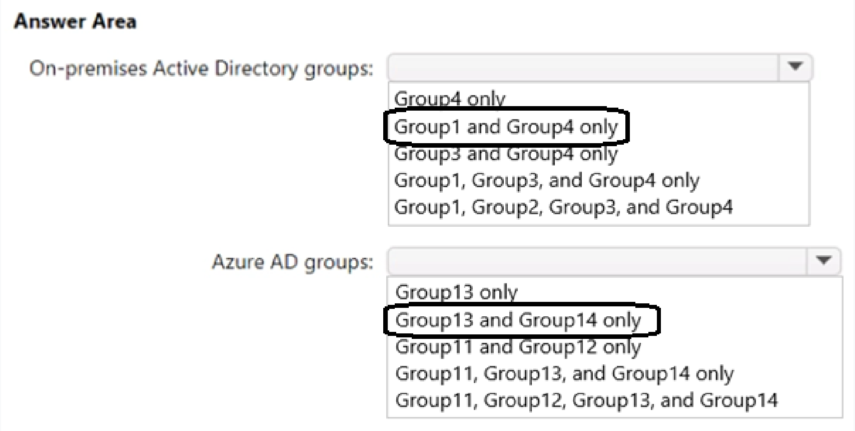
On-premises Active Directory groups:

- 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

Suggested 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

⊟ **Wixed** Highly Voted 👍 1 year, 6 months ago

Correct.

"Labels can be published to any specific user or email-enabled security group, distribution group, or Microsoft 365 group (which can have dynamic membership)"

Reference: https://learn.microsoft.com/en-us/purview/sensitivity-labels#what-label-policies-can-do

upvoted 8 times

⊟ **Domza** 1 year, 5 months ago

Thank you for the link ~

upvoted 4 times

⊟ **husamshahin** Most Recent 🕘 11 months, 1 week ago

on Exam 28-7-2024

upvoted 1 times

⊟ **emartiy** 1 year, 4 months ago

displayed answer is correct. For on-prem and azure ad focus on that these groups have email address.. For on prem Group 2-3 do not have email address, they are not included. for Azure Ad, Group 11-12 only security group, 13-14 also has emails based on their properties.. So, you can publish labels users or groups (has email address defined).

upvoted 1 times

Question #54 *Topic 1*

HOTSPOT

-

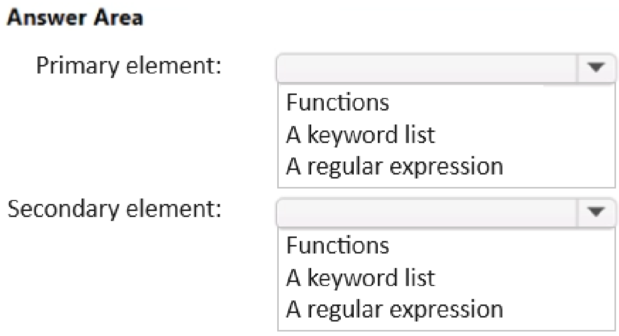
You have a Microsoft 365 tenant.

You need to create a new sensitive info type for items that contain the following:

• An employee ID number that consists of the hire date of the employee followed by a three digit number
• The words “Employee”, “ID”, or “Identification” within 300 characters of the employee ID number

What should you use for the primary and secondary elements? To answer, select the appropriate options in the answer area.

NOTE: Each correct selection is worth one point.

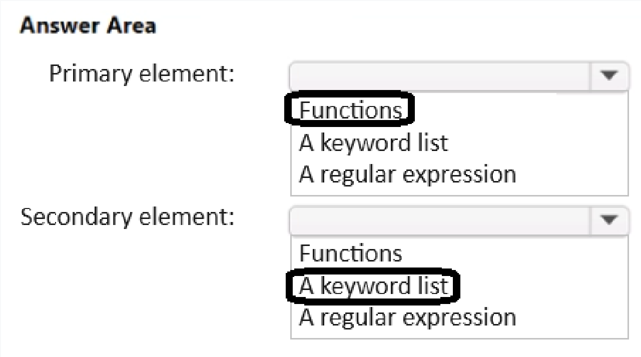


Answer Area

Primary element:
- Functions
- A keyword list
- A regular expression

Secondary element:
- Functions
- A keyword list
- A regular expression

Suggested Answer:



Answer Area

Primary element:
- [✓ Functions]
- A keyword list
- A regular expression

Secondary element:
- Functions
- [✓ A keyword list]
- A regular expression

Futfuyfyjfj Highly Voted 1 year, 4 months ago

I would say a regular expression for the first one. Couldn’t find a function while creating a SIT that could fulfill this.

upvoted 7 times

Tzu_Hsien 1 year, 4 months ago

yes agree with you ! I can't find the corresponding function type in doc: https://learn.microsoft.com/en-us/purview/sit-functions

upvoted 3 times

Rand0mConsultant Most Recent 9 months, 1 week ago

I would also have use Regex for the first one

upvoted 2 times

blokechettri 9 months, 1 week ago

I agree. The first can only be fulfilled by the REGEX expression

upvoted 1 times

brats_harsh 1 year ago

Primary Element: Regex

As - "An employee ID number that consists of the hire date of the employee followed by a three digit number" hiredate + followed by 3 digit number and only in regex you can create a pattern to detect 3 digit number after date

upvoted 2 times

⊟ **fahrulnizam** 1 year, 1 month ago

For the primary element, a regular expression is suitable because it allows you to define a pattern that matches the format of the employee ID number (hire date followed by a three-digit number).

upvoted 1 times

⊟ **Ehernandez** 1 year, 2 months ago

The Activity explorer provides a historical view of activities on your labeled content, collected from the Microsoft 365 unified audit logs. It's used to monitor what's being done with your labeled content, such as when a label is applied, changed, or removed.
On the other hand, the Content explorer gives you visibility into what content has been discovered and labeled, and where that content is located. It specifically allows you to see the actual content of scanned files that match your DLP policies.
This is why Content explorer is the appropriate tool for reviewing DLP policy matches, as it directly shows the content that triggered the DLP policy. Activity explorer is more about the actions taken on the content, rather than the content itself.
https://microsoft.github.io/ComplianceCxE/playbooks/teamsdlp/#introduction

upvoted 1 times

⊟ **mb0812** 1 year, 3 months ago

Regex,keyword list

upvoted 2 times

⊟ **JPByteK** 1 year, 4 months ago

Func_us_date
Func_us_date looks for dates in common U.S. formats. The common formats are "month/day/year", "month-day-year", and "month day year ". The names or abbreviations of months aren't case-sensitive.

upvoted 1 times

⊟ **CharlieGolf** 1 year, 4 months ago

Func_us_date doesn't look for numerical only formats of dates that would likely be used for an employee ID (ex: 20240224). For this reason, I think Regex would be the better tool since it can filter for the numerical date format that the company uses in their employee IDs.

upvoted 3 times

Question #55 *Topic 1*

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

You need to review DLP policy matches for the tenant.

What should you use?

A. Content explorer

B. Activity explorer

C. Compliance Manager

D. records management events

Suggested Answer: *B*

Community vote distribution

B (71%) A (29%)

TC1Labs 8 months, 3 weeks ago

Activity Explorer is the right answer

upvoted 2 times

SDiwan 1 year, 3 months ago

Selected Answer: B

Activity Explorer is the right answer. Content Explorer is Data Classification feature and not DLP feature.

upvoted 2 times

emartiy 1 year, 4 months ago

Selected Answer: B

Correct- B-

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

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

Fouces to words between (** **)

upvoted 4 times

Ruslan23 1 year, 4 months ago

Selected Answer: A

To review DLP policy matches for the tenant, you should use the Content Explorer (Option A). The Content Explorer in the Microsoft 365 compliance center allows you to view and manage sensitive information that matches your Data Loss Prevention (DLP) policies. It provides insights into where sensitive information resides in your organization and helps you manage risks associated with this data. Please note that appropriate permissions are required to access the Content Explorer.

- Copilot -

upvoted 2 times

Ruslan23 1 year, 3 months ago

Copilot shows you a link of a Microsoft doc, if you search in the page Content Explorer no results are found but Activity Explorer is mentioned, so don't trust Copilot for this question.

upvoted 3 times

Ehernandez 1 year, 2 months ago

The Activity explorer provides a historical view of activities on your labeled content, collected from the Microsoft 365 unified audit logs. It’s used to monitor what’s being done with your labeled content, such as when a label is applied, changed, or removed.

On the other hand, the Content explorer gives you visibility into what content has been discovered and labeled, and where that content is located. It specifically allows you to see the actual content of scanned files that match your DLP policies.

This is why Content explorer is the appropriate tool for reviewing DLP policy matches, as it directly shows the content that triggered the DLP policy. Activity explorer is more about the actions taken on the content, rather than the content itself.
https://microsoft.github.io/ComplianceCxE/playbooks/teamsdlp/#introduction
upvoted 1 times

⊟ **Ruslan23** 1 year, 2 months ago
https://learn.microsoft.com/en-us/training/modules/manage-data-loss-prevention-polices/4-use-data-loss-prevention-reports
The Activity explorer tab on the DLP page has multiple filters you can use to view DLP events. Use this tool to "review activity" related to content that contains sensitive info or has labels applied, such as what labels were changed, files were modified, and matched a rule.
upvoted 1 times

⊟ **Kodoi** 1 year, 4 months ago
Selected Answer: B
In addition, using Endpoint data loss prevention (DLP), Activity explorer gathers DLP policy matches events from Exchange, SharePoint, OneDrive, Teams Chat and Channel, on-premises SharePoint folders and libraries, on-premises file shares, and devices running Windows 10, Windows 11, and any of the three most recent major macOS versions.

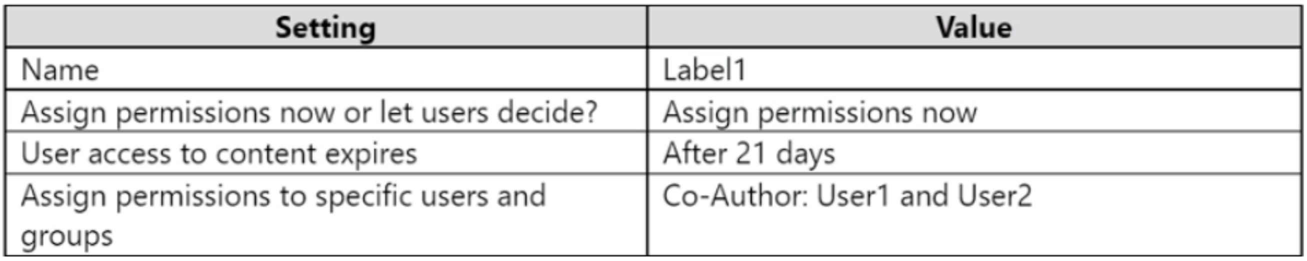
https://learn.microsoft.com/en-us/purview/data-classification-activity-explorer
upvoted 1 times

⊟ **Tzu_Hsien** 1 year, 4 months ago
I think it is (A)content explorer which can Investigating incidents related to data loss, security, or compliance.
upvoted 1 times

Question #56 *Topic 1*

You have a Microsoft 365 E5 subscription that contains two users named User1 and User2.

On January 1, you create the sensitivity label shown in the following table.



Setting	Value
Name	Label1
Assign permissions now or let users decide?	Assign permissions now
User access to content expires	After 21 days
Assign permissions to specific users and groups	Co-Author: User1 and User2

On January 2, you publish Label1 to User1.

On January 3, User1 creates a Microsoft Word document named Doc and applies Label to the document.

On January 4, User2 edits Doc1.

On January 15, you increase the content expiry period for Label1 to 28 days.

When will access to Doc1 expire for User2?

A. January 23

B. January 24

C. January 25

D. January 31

Suggested Answer: *D*

Community vote distribution

D (100%)

MrParfumeDeluxe 6 months, 1 week ago

Selected Answer: B

Correct answer is B. In Microsoft's official sensitivity label documentation, it's stated that "label settings are embedded at the time of labeling" and that updates to the label do not retroactively affect already labeled content.

upvoted 4 times

itsadel 6 months, 2 weeks ago

Selected Answer: B

Initial Expiry Period:

The sensitivity label "Label1" specifies that user access to content expires after 21 days.
User1 created Doc1 on January 3, which means the 21-day expiry period is calculated as:
January 3 + 21 days = January 24.
Change to Expiry Period on January 15:

On January 15, the expiry period is updated to 28 days.
However, changes to the sensitivity label do not retroactively affect content that already has the label applied.
Since Doc1 already had Label1 applied on January 3 with the original 21-day expiry, it will still follow the original expiry rule.
Conclusion:

For User2, access to Doc1 expires on January 24, as the original expiry setting remains in effect.

upvoted 3 times

Athena94 8 months, 3 weeks ago

Label-1 was never published to User2, isn't this question incorrect?

upvoted 1 times

emartiy 10 months, 1 week ago

Selected Answer: D

Item was created on 3th Jan. so updating label 21 to 28 days will make document accessible until 31 of Jan.. Created at 3th + 28 days from label = 31.

upvoted 2 times

Domza 11 months ago

Selected Answer: D

Looks good~

Adding extra 7 days to access Doc 1

upvoted 1 times

Question #57 *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 retention policy.

Does this meet the goal?

A. Yes

B. No

Suggested Answer: *B*

Community vote distribution

B (100%)

emartiy 10 months, 1 week ago

Selected Answer: B

Solution to create retention policy isn't used to identify such files stored in organization. That kind of policies are used for retain (keep item) based on settings defined in it.

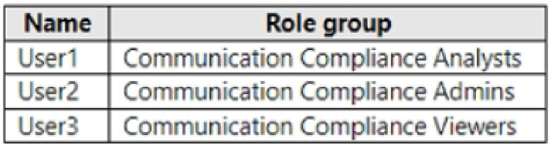
upvoted 2 times

Question #58 Topic 1

HOTSPOT

-

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



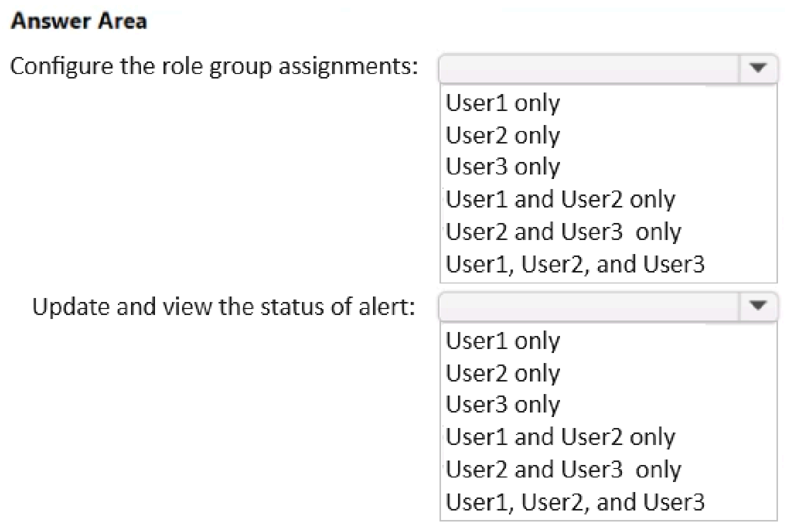
Name	Role group
User1	Communication Compliance Analysts
User2	Communication Compliance Admins
User3	Communication Compliance Viewers

You need to delegate the following tasks:

- Configure role group assignments for communication compliance.
- Update and view the status of communication compliance alerts.

Which users can perform each task? To answer, select the appropriate options in the answer area.

NOTE: Each correct selection is worth one point.



Answer Area

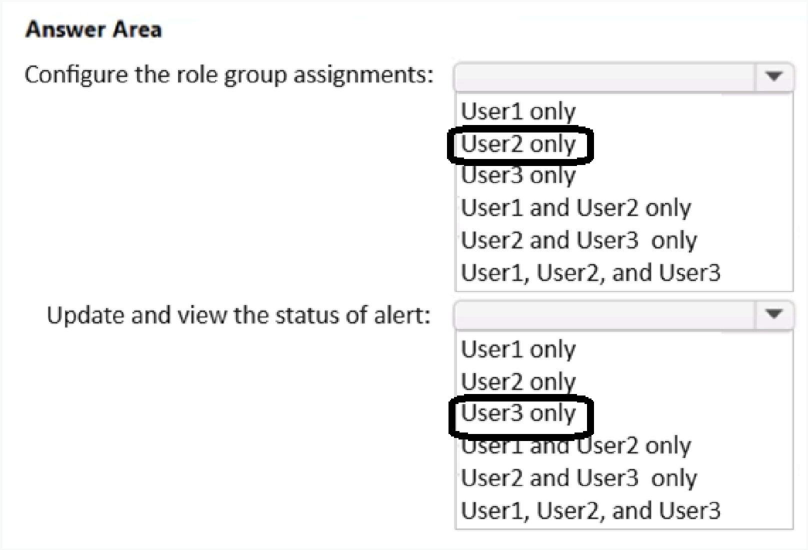
Configure the role group assignments:

- User1 only
- User2 only
- User3 only
- User1 and User2 only
- User2 and User3 only
- User1, User2, and User3

Update and view the status of alert:

- User1 only
- User2 only
- User3 only
- User1 and User2 only
- User2 and User3 only
- User1, User2, and User3

Suggested Answer:



Answer Area

Configure the role group assignments:

- User1 only
- [✓ User2 only]
- User3 only
- User1 and User2 only
- User2 and User3 only
- User1, User2, and User3

Update and view the status of alert:

- User1 only
- User2 only
- [✓ User3 only]
- User1 and User2 only
- User2 and User3 only
- User1, User2, and User3

emartiy Highly Voted 1 year, 4 months ago

I have searched for this and reached some learn links.

Based on what I read, selections should be like following;

To configure role group assignment the Selection: User 2 Only (based on the given 3 user).
Update and view status of alert : User 1 only

Ref: https://learn.microsoft.com/en-us/purview/communication-compliance-investigate-remediate#:~:text=After%20you%27ve%20configured,and%20remediate%20issues.

User 3 (Communictaion Compliance Viewers can "View and export policy updates"
https://learn.microsoft.com/en-us/purview/communication-compliance-configure#:~:text=View%20and%20export%20policy%20updates
upvoted 6 times

⊟ **JimboJones99** 11 months, 1 week ago
For the second one the user needs to be able to UPDATE and view. The Viewer wouldn't be able to update so I think it's Analyst for the second one.
upvoted 1 times

⊟ **EsamiTopici** Highly Voted 10 months ago
Why the second is not 1-2?
upvoted 5 times

⊟ **roelski** 7 months ago
For the 2nd item Update and view the status of alert:
Answer should be User1 and User2. Since this 2 can update and view the status alert.
User3 can view only and cannot update.
It's a little bit tricky
upvoted 2 times

⊟ **Kuteron** 6 months, 4 weeks ago
wrong. User2 does not have access to investigate alerts. See here:
https://learn.microsoft.com/en-us/purview/communication-compliance-configure#step-1-required-enable-permissions-for-communication-compliance
upvoted 3 times

⊟ **ca7859c** Most Recent 1 month, 3 weeks ago
1. User2 Only (Global Admin

"Access to all administrative features in all Microsoft 365 services. Only global administrators can assign other administrator roles. For more information, see Global Administrator / Company Administrator."
https://learn.microsoft.com/en-us/purview/purview-permissions
upvoted 1 times

⊟ **ca7859c** 2 months, 1 week ago
Configure role group: Admin

There are six role:
Microsoft Entra ID Global Administrator role
Microsoft Entra ID Compliance Administrator role
Microsoft Purview portal Organization Management role group
Microsoft Purview portal Compliance Administrator role group
Communication Compliance role group
Communication Compliance Admins role group

https://learn.microsoft.com/en-us/purview/communication-compliance-configure#step-1-required-enable-permissions-for-communication-compliance

Update & View: Analyst or Investigator
After you've configured your communication compliance policies, you'll begin receiving alerts for message issues that match your policy conditions.
To view and act on alerts, users must be assigned to the following permissions:

"The Communication Compliance Analysts or the Communication Compliance Investigators role group
Reviewer in the policy that is associated with the alert"

https://learn.microsoft.com/en-us/purview/communication-compliance-investigate-remediate
upvoted 1 times

⊟ **Kodoi** 1 year, 4 months ago
In the question, only the analyst has access to the alerts.

https://learn.microsoft.com/ja-jp/purview/communication-compliance-configure#step-1-required-enable-permissions-for-communication-compliance
upvoted 3 times

⊟ **Domza** 1 year, 5 months ago
Agreed,
User 2 and User 1
upvoted 4 times

⊟ **Domza** 1 year, 5 months ago
Link: https://learn.microsoft.com/en-us/purview/communication-compliance-configure#step-1-required-enable-permissions-for-communication-compliance
upvoted 1 times

⊟ **Futfuyfyjfj** 1 year, 5 months ago
Based on below link I would say the second question is only the Analyst

https://learn.microsoft.com/en-us/purview/communication-compliance-configure#step-1-required-enable-permissions-for-communication-compliance
upvoted 2 times

⊟ **louisaok** 1 year, 5 months ago
Yes, Viewer can't do much.
#2 should be ANalyst
upvoted 2 times

⊟ **JPByteK** 1 year, 4 months ago
https://learn.microsoft.com/en-us/purview/communication-compliance-investigate-remediate

After you've configured your communication compliance policies, you'll begin receiving alerts for message issues that match your policy conditions. To view and act on alerts, users must be assigned to the following permissions:

The Communication Compliance Analysts or the Communication Compliance Investigators role group
Reviewer in the policy that is associated with the alert
upvoted 1 times

Question #59 *Topic 1*

You have a Microsoft 365 E5 tenant that contains a user named User1. User1 is assigned the Compliance Administrator role.

User1 cannot view the regular expression in the IP Address sensitive info type.

You need to ensure that User1 can view the regular expression.

What should you do?

A. Assign User1 the Global Reader role.

B. Assign User1 to the Reviewer role group.

C. Instruct User to use the Test function on the sensitive info type.

D. Create a copy of the IP Address sensitive info type and instruct User1 to edit the copy.

Suggested Answer: *A*

Community vote distribution

D (100%)

SDiwan 1 year, 3 months ago

Selected Answer: D

Correct answer is D. Test in lab now. You can only see the regex in edit screen. since this is a in-built SIT, only option is to make a copy and then go to edit screen of that copied SIT.

upvoted 3 times

emartiy 1 year, 4 months ago

https://learn.microsoft.com/en-us/purview/sit-customize-a-built-in-sensitive-information-type

upvoted 1 times

emartiy 1 year, 4 months ago

Selected Answer: D

What Ruslan23 shared seems correct. Correct selection should be D based on the description.

upvoted 2 times

SDiwan 1 year, 3 months ago

But the question does not say that user1 wants to edit the regular expression. It just says the user1 wants to View.

upvoted 1 times

Ruslan23 1 year, 3 months ago

SDiwan check this link and go to the purple Note: https://learn.microsoft.com/en-us/entra/identity/role-based-access-control/permissions-reference#global-reader

As you can see: Microsoft Purview doesn't support the Global Reader role

For the Reviewer role you can only access review sets in eDiscovery (Premium) cases: eDiscovery > Advanced.

This is the link: https://learn.microsoft.com/en-us/microsoft-365/security/office-365-security/scc-permissions?view=o365-worldwide

upvoted 2 times

EM1234 1 year ago

I agree is it D (to me). I just wanted to comment that in that same link in the paragraph above it says:

"Global Reader works with Microsoft 365 admin center, Exchange admin center, SharePoint admin center, Teams admin center, Microsoft 365 Defender portal, Microsoft Purview compliance portal, Azure portal, and Device Management admin center."

So be careful, Global Reader DOES work with "Microsoft Purview compliance portal", even if it is stated below in purple that it does not work with "Microsoft Purview". My guess is the purple section is referring to what used to be called "Azure Purview".

upvoted 1 times

Ruslan23 1 year, 4 months ago

Selected Answer: D

To ensure that User1 can view the regular expression in the IP Address sensitive info type, you should create a copy of the IP Address sensitive info type and instruct User1 to edit the copy (Option D).

Here's why: The built-in sensitive info types, such as the IP Address type, are predefined by Microsoft and cannot be edited1. However, you can create a copy of a built-in sensitive info type, and then modify the copy2. In the copied sensitive info type, User1 will be able to view and edit the regular expression2.

Please note that the Compliance Administrator role does not grant the ability to view or edit the regular expressions of built-in sensitive info types1. The Global Reader role (Option A) and the Reviewer role group (Option B) also do not provide these permissions1. The Test function (Option C) is used to test the effectiveness of a sensitive info type, but it does not allow a user to view or edit the regular expression1.

- Copilot -
upvoted 2 times

Question #60 *Topic 1*

You have a Microsoft 365 E5 subscription.

You need to ensure that any message or document containing a credit card number is deleted automatically 12 months after it was created. The solution must minimize administrative effort.

Which two components should you create? Each correct answer presents part of the solution.

NOTE: Each correct selection is worth one point.

A. a sensitivity label

B. an auto-labeling policy for a sensitivity label

C. a retention label

D. an auto-labeling policy for a retention label

E. a sensitive information type (SIT)

Suggested Answer: *CE*

Community vote distribution

CD (100%)

ChrisBaird 6 months, 3 weeks ago

Selected Answer: CD

There is a built-in SIT for credit card information. The question says least admin effort. No need to build a new SIT. This needs a retention label and a retention label policy.

upvoted 1 times

Ruslan23 9 months ago

Selected Answer: CD

C: A retention label allow you to set the retention period for the data, so 12 months but you could do it manually.

D: An auto-labeling policy allow you to automatically apply the retention label to "any message or document" as mentioned in the question that has the credit card number match.

upvoted 2 times

CheMetto 9 months, 3 weeks ago

Selected Answer: CD

CD for me too. You already own a SIT for that info, so you don't need to create a new one. So you create an auto-labeling policy, you apply based on sit Credit card number, and you autoapply the retention label previously created.

upvoted 2 times

emartiy 10 months, 1 week ago

Selected Answer: CD

I think we need a retention label to specify how long an email or item needs to be retained based on creation time. And then apply this label automatically to the emails and files based on the SIT which check if content match credit card.

upvoted 4 times

Question #61 *Topic 1*

You have a Microsoft 365 subscription.

You create a new trainable classifier.

You need to train the classifier.

Which source can you use to train the classifier?

A. a Microsoft SharePoint Online site

B. an on-premises Microsoft SharePoint Server site

C. an NFS file share

D. an Azure Files share

Suggested Answer: *A*

Community vote distribution

A (100%)

emartiy 10 months, 1 week ago

Selected Answer: A

Correct. You need to upload seed files there to be used.

upvoted 1 times

Futfuyfyjfj 11 months, 1 week ago

Is correct

https://learn.microsoft.com/en-us/purview/classifier-get-started-with#how-to-create-a-trainable-classifier

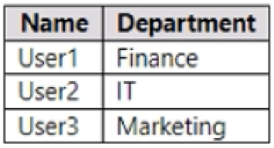
upvoted 2 times

Question #62 Topic 1

HOTSPOT

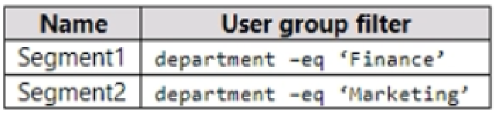
-

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



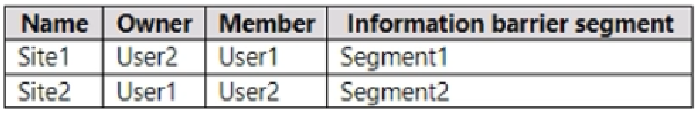
Name	Department
User1	Finance
User2	IT
User3	Marketing

The subscription contains the information barrier segments shown in the following table.



Name	User group filter
Segment1	`department -eq 'Finance'`
Segment2	`department -eq 'Marketing'`

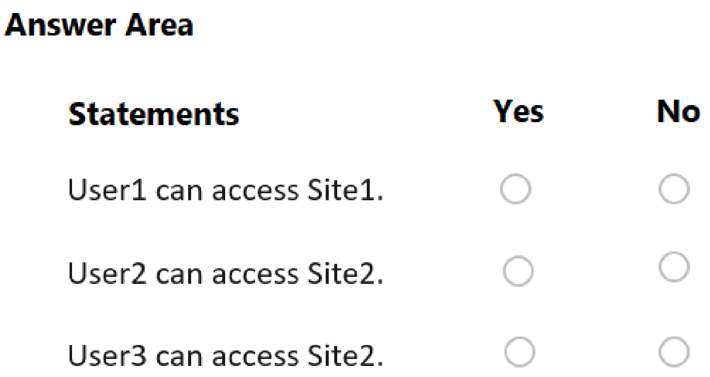
The subscription contains the Microsoft SharePoint Online sites shown in the following table.



Name	Owner	Member	Information barrier segment
Site1	User2	User1	Segment1
Site2	User1	User2	Segment2

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

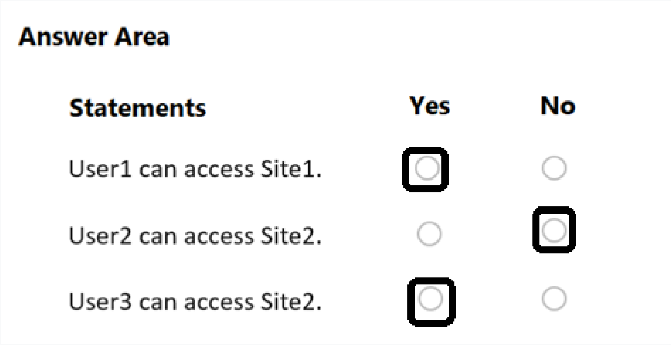
NOTE: Each correct selection is worth one point.



Answer Area

Statements	Yes	No
User1 can access Site1.	○	○
User2 can access Site2.	○	○
User3 can access Site2.	○	○

Suggested Answer:



Answer Area

Statements	Yes	No
User1 can access Site1.	[✓ ○]	○
User2 can access Site2.	○	[✓ ○]
User3 can access Site2.	[✓ ○]	○

Ruslan23 Highly Voted 10 months, 2 weeks ago

Y: User1 is a member of the site also in Finance department (Segment1)

N: User2 is a member of the site but not in Marketing department (Segment2)

N: User3 is not a member of the site and it is in Marketing department (Segment2). If a user is not a member of a SharePoint site, they will not be able to access the site, even if they match the information barrier segment associated with the site12.

upvoted 13 times

⊟ **jimmyjose** Highly Voted 11 months ago

User3 is not a member anywhere, so it should not be able to access Site2.

upvoted 10 times

⊟ **ca7859c** Most Recent 1 month, 3 weeks ago

Answer is correct

YNY

upvoted 1 times

⊟ **mb0812** 9 months, 2 weeks ago

Y..N..N

upvoted 4 times

⊟ **emartiy** 10 months, 1 week ago

Y - N - Y

For confisution about User 3: User's department "Marketing" Site2 's segment is also for "Marketing" if site2's owner or member share file with User3, he can access.. Isn't it?

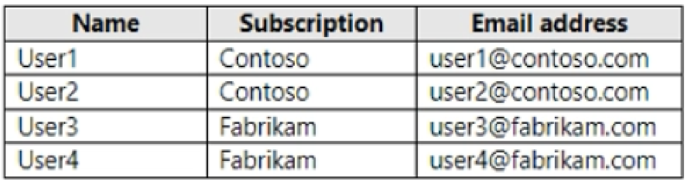
upvoted 1 times

Question #63 *Topic 1*

HOTSPOT

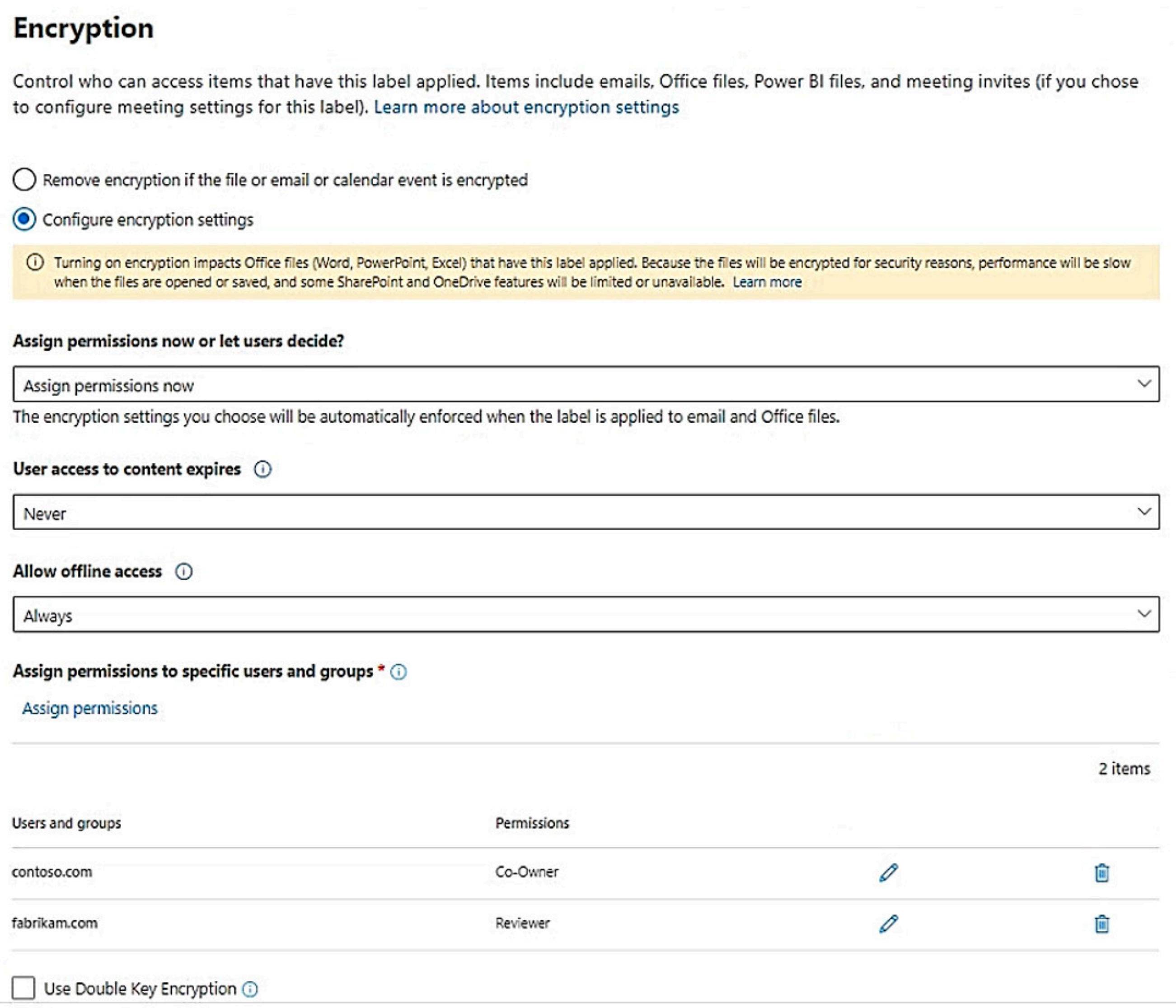
-

You have two Microsoft 365 subscriptions named Contoso and Fabrikam. The subscriptions contain the users shown in the following table.



Name	Subscription	Email address
User1	Contoso	user1@contoso.com
User2	Contoso	user2@contoso.com
User3	Fabrikam	user3@fabrikam.com
User4	Fabrikam	user4@fabrikam.com

You have a sensitivity label named Sensitiviy1 as shown in the exhibit. (Click the Exhibit tab.)



Encryption

Control who can access items that have this label applied. Items include emails, Office files, Power BI files, and meeting invites (if you chose to configure meeting settings for this label). Learn more about encryption settings

○ Remove encryption if the file or email or calendar event 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 ⓘ

Never

Allow offline access ⓘ

Always

Assign permissions to specific users and groups * ⓘ

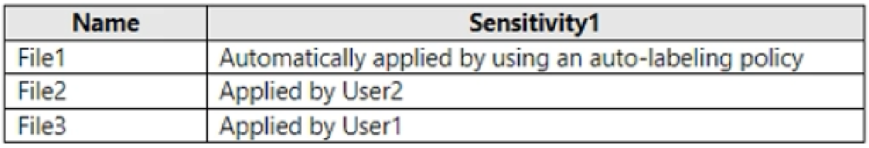
Assign permissions

2 items

Users and groups	Permissions
contoso.com	Co-Owner
fabrikam.com	Reviewer

□ Use Double Key Encryption ⓘ

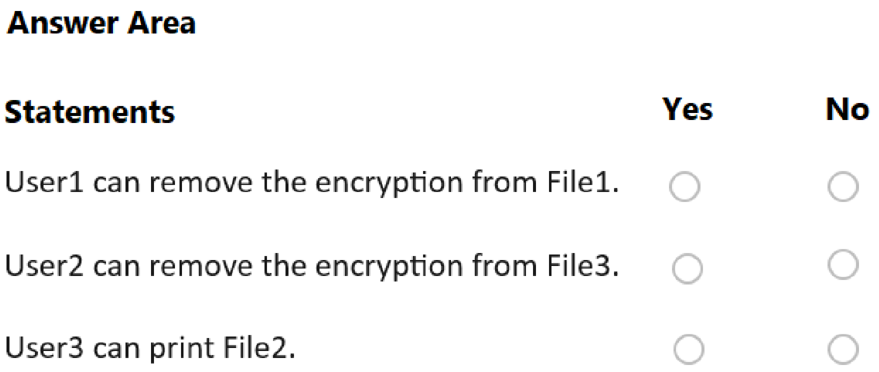
You have the files shown in the following table.



Name	Sensitivity1
File1	Automatically applied by using an auto-labeling policy
File2	Applied by User2
File3	Applied by User1

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

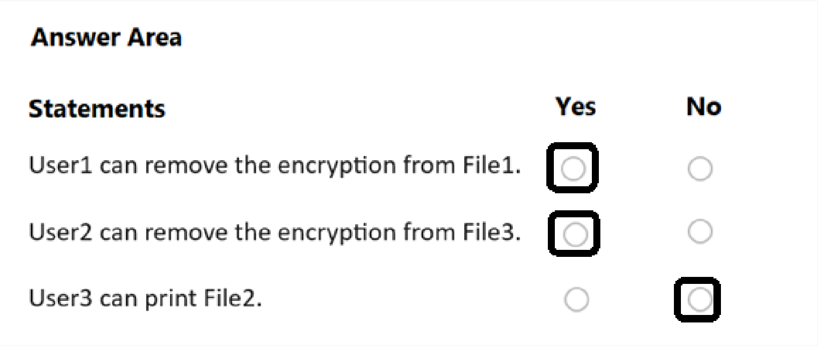
NOTE: Each correct selection is worth one point.



Answer Area

Statements	Yes	No
User1 can remove the encryption from File1.	○	○
User2 can remove the encryption from File3.	○	○
User3 can print File2.	○	○

Suggested Answer:



Answer Area

Statements	Yes	No
User1 can remove the encryption from File1.	[✓ ○]	○
User2 can remove the encryption from File3.	[✓ ○]	○
User3 can print File2.	○	[✓ ○]

emartiy Highly Voted 1 year, 4 months ago

YES - YES - NO

For two option, it is easy to say YES, for the thrid one, User 3 has Reviewer permission for User2's labeled document based on his organization. Reviewers do not have print permission.

https://learn.microsoft.com/en-us/azure/information-protection/configure-usage-rights#rights-included-in-permissions-levels:~:text=Permissions%20level,Export%3B%20Print%3B%20Reply%20%5B3%5D%3B%20Reply

upvoted 10 times

RAJRYB Most Recent 12 months ago

I would rather go with NO-YES-NO, because auto-labeled file will be encrypted still

upvoted 2 times

Ruslan23 1 year, 2 months ago

I think the first statement is NO, User1 technically is able to remove the Sensitivity1 label BUT File1 is auto-labeling and it's just a temporary solution. Other given answer are correct, so: NO - YES - NO

upvoted 2 times

HarryDefender 1 year, 4 months ago

No-Yes-Yes

upvoted 2 times

Question #64 Topic 1

DRAG DROP
-

You have a Microsoft 365 E5 subscription.

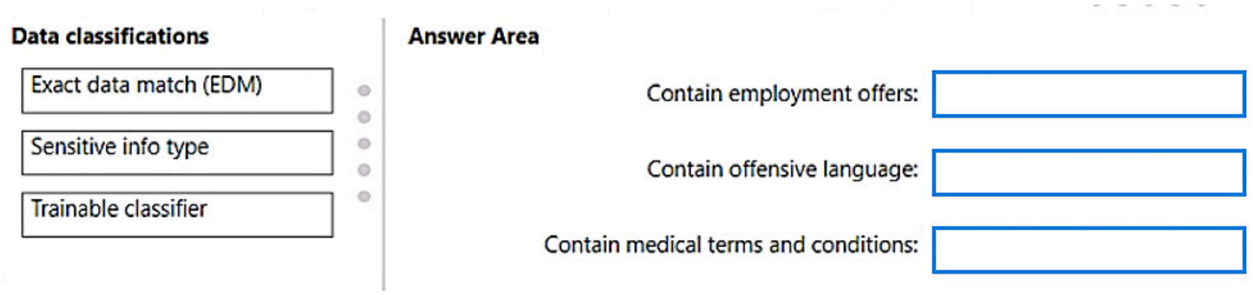
You need to label Microsoft Exchange Online emails that match the following conditions:

• Contain employment offers
• Contain offensive language
• Contain medical terms and conditions

The solution must minimize administrative effort.

Which type of data classification should you use for each condition? To answer, drag the appropriate data classification types to the correct conditions. Each data classification type 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.



Data classifications

Exact data match (EDM)

Sensitive info type

Trainable classifier

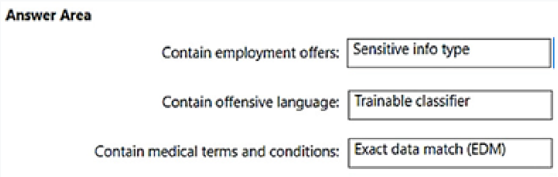
Answer Area

Contain employment offers:

Contain offensive language:

Contain medical terms and conditions:

Suggested Answer:



Answer Area

Contain employment offers: Sensitive info type

Contain offensive language: Trainable classifier

Contain medical terms and conditions: Exact data match (EDM)

⊟ **Chairborne33** Highly Voted 1 year, 4 months ago

This is incorrect. Should be
Trainable Classifier as there is a pre-configured one for employment agreement and profanity (offensive language),

The medical terms and conditions is covered by a SIT

upvoted 9 times

⊟ **Boeroe** 1 year ago

Agree, but I also believe the employment offers could be a trainable classifier. The TA Employment Agreement contains information which would match:

"Classifies employment agreement which is a contract made between an employer and an employee. It details the starting date, salary, compensation, duties of employment. In addition, there are detailed terms and conditions that state the obligations and responsibilities of the employer and the employee"

upvoted 1 times

⊟ **Ruslan23** Highly Voted 1 year, 2 months ago

Employment offers: Trainable classifier
Offensive language: Sensitive info type - you can use keyword dictionaries and you must minimize administrative effort
Medical terms and conditions: Sensitive info type

upvoted 7 times

EM1234 1 year ago

I think for the offensive language this would be least effort, however, I think it is kind of a bad question since trainable classifier could be easier if you had the source material and if you needed to do it in non-native languages. I am going with this answer. Thanks Rus

upvoted 1 times

ca7859c Most Recent 1 month, 3 weeks ago

Offensive Language: Trainable Classifier
\
https://learn.microsoft.com/en-us/purview/trainable-classifiers-definitions#profanity

Medical Terms: SIT
\
https://learn.microsoft.com/en-us/purview/sit-defn-all-medical-terms-conditions

upvoted 1 times

ca7859c 1 month, 3 weeks ago

Employment Agreement: SIT
\
https://learn.microsoft.com/en-us/purview/trainable-classifiers-definitions#employment-agreement

upvoted 1 times

ca7859c 1 month, 3 weeks ago

I am sorry: Employment Agreement: Trainable Classifier

upvoted 1 times

dashadowman00 8 months ago

Contain employment offers: Trainable classifier
https://learn.microsoft.com/en-us/purview/trainable-classifiers-definitions

Contain offensive language: Trainable classifier
https://learn.microsoft.com/en-us/purview/communication-compliance-policies?tabs=purview-portal

Contain medical terms and conditions: Sensitive info type
https://learn.microsoft.com/en-us/purview/sit-defn-all-medical-terms-conditions

upvoted 3 times

ExamStudy68 10 months ago

They are all sensitive information types

upvoted 1 times

narenbabu.chintu 11 months, 4 weeks ago

Contain Employement offers: Trainable Classifiers
Contain Offensive Language : EDM (use EDM to provide exact terms of offensive lanaguages)
Contain Medical terms and conditions: Sensitive Info Type (Use built in "All Medical terms and conditions"

upvoted 2 times

brats_harsh 1 year ago

Trainable classifier
Trainable classifier
SIT

upvoted 5 times

CheMetto 1 year, 3 months ago

Contain employment offers: There is employment agreement as trainable classifiers. Maybe this one is better?

Offensive Language: As already said, there is trainable classifiers with profanity, i'll go for this one.

For the medical terms and conditions there is the sit "all medical terms and conditions".

upvoted 4 times

Question #65 *Topic 1*

HOTSPOT

-

You have a Microsoft 365 E5 subscription that contains two users named User1 and User2.

You create a sensitivity label that has the following settings:

- Name: Sensitivity1
- Define the scope for this label: Items
- Choose protection settings for files and emails: Mark the content of files
- Add custom headers, footers, and watermarks to files and emails that have this label applied

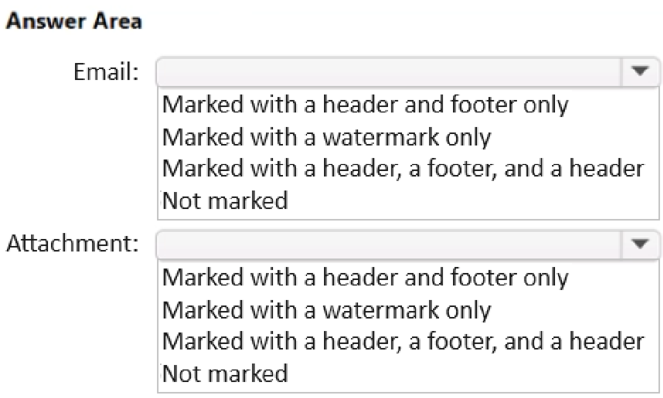
You make Sensitivity available to User1.

User1 performs the following actions:

- Creates a new email
- Adds a file named File1.docx as an attachment to the email
- Applies Sensitivity1 to the email
- Sends the email to User2

How will the email and the attachment be marked? To answer, select the appropriate options in the answer area.

NOTE: Each correct selection is worth one point.

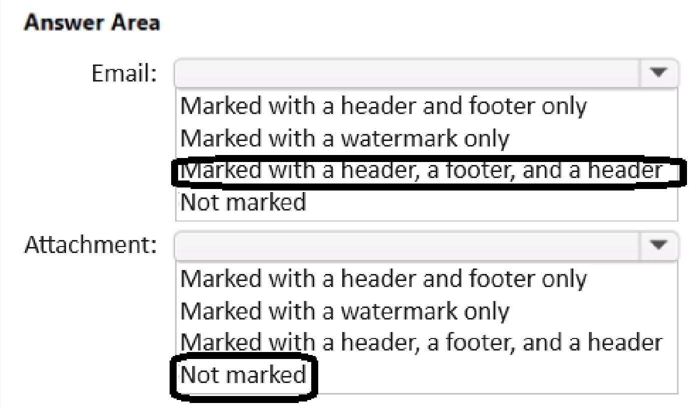


Answer Area

Email:
- Marked with a header and footer only
- Marked with a watermark only
- Marked with a header, a footer, and a header
- Not marked

Attachment:
- Marked with a header and footer only
- Marked with a watermark only
- Marked with a header, a footer, and a header
- Not marked

Suggested Answer:



Answer Area

Email:
- Marked with a header and footer only
- Marked with a watermark only
- [✓ Marked with a header, a footer, and a header]
- Not marked

Attachment:
- Marked with a header and footer only
- Marked with a watermark only
- Marked with a header, a footer, and a header
- [✓ Not marked]

⊟ **Ruslan23** Highly Voted 9 months ago

Email: Header + Footer

You cannot apply watermarks to emails and meeting invites.

Attachment: Not marked

As described in User's actions performed "Applies Sensitivity1 to email", if you want to apply the Sensitivity1 to attachment you need to apply it directly from Word, so it would be marked with Header, Footer and Watermark

upvoted 10 times

leeevvv 5 months, 2 weeks ago

he scope is items it doesnt say emails so there shouldn't be any header of footer on the email. since labels arent applied to attachment there wont be any watermarks or headers or footers on the document either?

upvoted 1 times

dillon123456789 Most Recent 3 months, 1 week ago

for Q1, is it header and footer only or header, a footer, and a header?

upvoted 1 times

mb0812 9 months, 2 weeks ago

Email: marked with header and footer

Attachments- not marked

upvoted 3 times

emartiy 10 months, 1 week ago

Email = Header + Footer

Attachment = Header + Footer + Watermark since all was chosen based on question description.

upvoted 3 times

Alcpt 5 months, 3 weeks ago

Not correct.

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

https://learn.microsoft.com/en-us/purview/sensitivity-labels#what-sensitivity-labels-can-do

upvoted 1 times

jimmyjose 11 months ago

Email will be marked by a header, a footer, and a watermark.

upvoted 2 times

Futfuyfyjfj 10 months, 4 weeks ago

You are wrong as per Microsoft documentation:

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

upvoted 7 times

itsadel 6 months, 1 week ago

email: header + footer

attachment : watermark only?

upvoted 1 times

Futfuyfyjfj 10 months, 4 weeks ago

https://learn.microsoft.com/en-us/purview/sensitivity-labels#what-sensitivity-labels-can-do

upvoted 2 times

Question #66 *Topic 1*

You have a Microsoft 365 subscription that contains 100 users and a Microsoft 365 group named Group1.

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

A sensitivity label named Label1 is published as the default label for Group1.

You add two sublabels named Sublabel1 and Sublabel2 to Label1.

You need to ensure that the settings in Sublabel1 are applied by default to Group1.

What should you do?

A. Change the order of Sublabel1.

B. Modify the policy of Label1.

C. Delete the policy of Label1 and publish Sublabel1.

D. Duplicate all the settings from Sublabel1 to Label1.

Suggested Answer: *B*

Community vote distribution

B (100%)

SSL2 9 months, 4 weeks ago

Selected Answer: B

To ensure that the settings in Sublabel1 are applied by default to Group1, you should:

B. Modify the policy of Label1.

When you publish sensitivity labels and want to set a specific label as default for a group, you adjust the label policy that applies to that group. You do not need to delete the existing policy or change the settings of the parent label; instead, you can modify the existing policy to set Sublabel1 as the default label within the policy settings for Group1.

upvoted 4 times

emartiy 10 months, 1 week ago

Selected Answer: B

Other than B options not gives us solution to make SubLabel1 as default.

upvoted 1 times

Domza 11 months ago

Selected Answer: B

Agreed~

upvoted 2 times

Futfuyfyjfj 11 months, 1 week ago

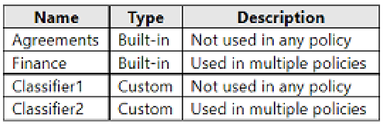
Seems correct:

https://office365itpros.com/2022/06/22/default-sensitivity-labels-spo/

upvoted 1 times

Question #67 Topic 1

You have a Microsoft 365 E5 subscription that has the trainable classifiers shown in the following table.



Name	Type	Description
Agreements	Built-in	Not used in any policy
Finance	Built-in	Used in multiple policies
Classifier1	Custom	Not used in any policy
Classifier2	Custom	Used in multiple policies

Which trainable classifiers can you retrain?

A. Classifier1 only

B. Agreements and Classifier1 only

C. Classifier1 and Classifier2 only

D. Agreements, Finance, Classifier1, and Classifier2

Suggested Answer: *C*

Community vote distribution

A (83%) C (17%)

Domza Highly Voted 1 year, 5 months ago

Note: Pre-trained classifiers cannot be re-trained

upvoted 7 times

JimboJones99 Most Recent 11 months, 1 week ago

Selected Answer: A

A - reasoning is same as NICKTON81 and techpam

upvoted 1 times

NICKTON81 1 year ago

Selected Answer: A

A is correct:

Retraining classifiers

Retraining published custom classifiers is no longer supported. If you need to improve the accuracy of a trainable classifier you've published, remove the classifier and start over with larger sample sets.

To improve the accuracy of an unpublished classifier, review the test results, update the data set with additional data, and restart the training.

https://learn.microsoft.com/en-us/purview/trainable-classifiers-learn-about#retraining-classifiers

upvoted 4 times

techpam 1 year, 1 month ago

Retraining published custom classifiers is no longer supported. If you need to improve the accuracy of a trainable classifier you've published, remove the classifier and start over with larger sample sets.

https://learn.microsoft.com/en-us/purview/trainable-classifiers-learn-about#retraining-classifiers

upvoted 4 times

emartiy 1 year, 4 months ago

Selected Answer: C

Based on I understand from below link, a Custom Trainable Classifier does not need be used in any policy, only publishing is enough to retrain it. So C is seem

https://learn.microsoft.com/en-us/purview/trainable-classifiers-learn-about#:~:text=When%20you%20publish%20the%20classifier%2C%20it%20sorts%20through%20items%20in%20locations%20like%20SharePoint%20Online%2

upvoted 2 times

Futfuyfyjfj 1 year, 5 months ago

I agree based on the answer options, however besides the option I would say only classifier 2 can be retrained:

https://learn.microsoft.com/en-us/purview/classifier-how-to-retrain-content-explorer

‘A classifier must already be published and in use before it can be retrained.’
upvoted 3 times

⊟ **Softeng** 1 year, 4 months ago
Agree with you:

https://learn.microsoft.com/en-us/purview/classifier-how-to-retrain-content-explorer#:~:text=A%20classifier%20must%20already%20be%20published%20and%20in%20use%20before%20it%20can%20be%20retrained.
upvoted 1 times

⊟ **EsamiTopici** 12 months ago
Retraining published custom classifiers is no longer supported. If you need to improve the accuracy of a trainable classifier you've published, remove the classifier and start over with larger sample sets.

Only classifier 1
upvoted 1 times

Question #68 *Topic 1*

HOTSPOT

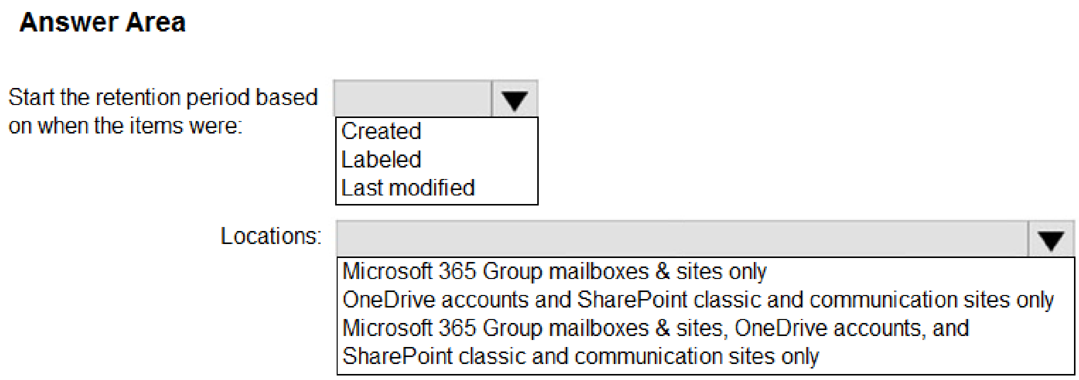
-

You have a Microsoft 365 E5 subscription that uses Microsoft Exchange Online and Teams.

You need to ensure that when a user sends a message containing a cloud attachment, a retention label is applied to the cloud attachment by using auto-labeling policy.

How should you configure the retention label to start the retention period, and to which locations should you apply the auto-labeling policy? To answer, select the appropriate options in the answer area.

NOTE: Each correct selection is worth one point.

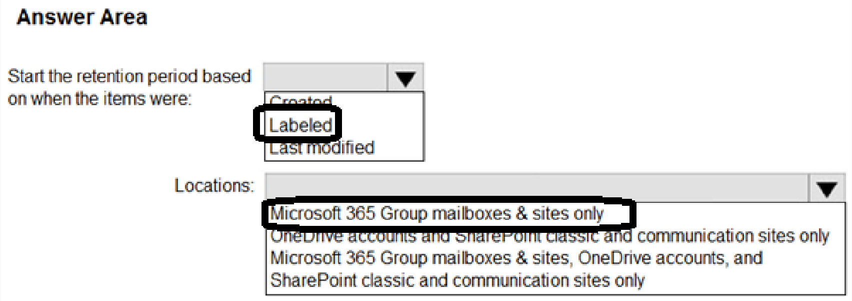


Answer Area

Start the retention period based on when the items were:
- Created
- Labeled
- Last modified

Locations:
- Microsoft 365 Group mailboxes & sites only
- OneDrive accounts and SharePoint classic and communication sites only
- Microsoft 365 Group mailboxes & sites, OneDrive accounts, and SharePoint classic and communication sites only

Suggested Answer:



Answer Area

Start the retention period based on when the items were:
- Created
- [✓ Labeled]
- Last modified

Locations:
- [✓ Microsoft 365 Group mailboxes & sites only]
- OneDrive accounts and SharePoint classic and communication sites only
- Microsoft 365 Group mailboxes & sites, OneDrive accounts, and SharePoint classic and communication sites only

Ruslan23 Highly Voted 9 months ago

- Start the retention period based on when the items were: Labeled
This is the best option because you need to ensure that when a users sends items a retention label is applied using auto-labeling policy, the other two options didn't match with the answer.
Look the "Service-side labeling labeling" method:
https://learn.microsoft.com/en-us/purview/apply-sensitivity-label-automatically

- Locations: Microsoft 365 Group mailboxes & sites, OneDrive accounts and SharePoint classic and communication sites only.
As mentioned your subscription uses both Microsoft Exchange Online and Teams.
Teams' files are stored in SharePoint and Teams chat's files are stored in OneDrive so you need to include them:
https://support.microsoft.com/en-us/office/file-storage-in-microsoft-teams-df5cc0a5-d1bb-414c-8870-46c6eb76686a

upvoted 13 times

Question #69 Topic 1

HOTSPOT

-

You have a Microsoft 365 E5 subscription.

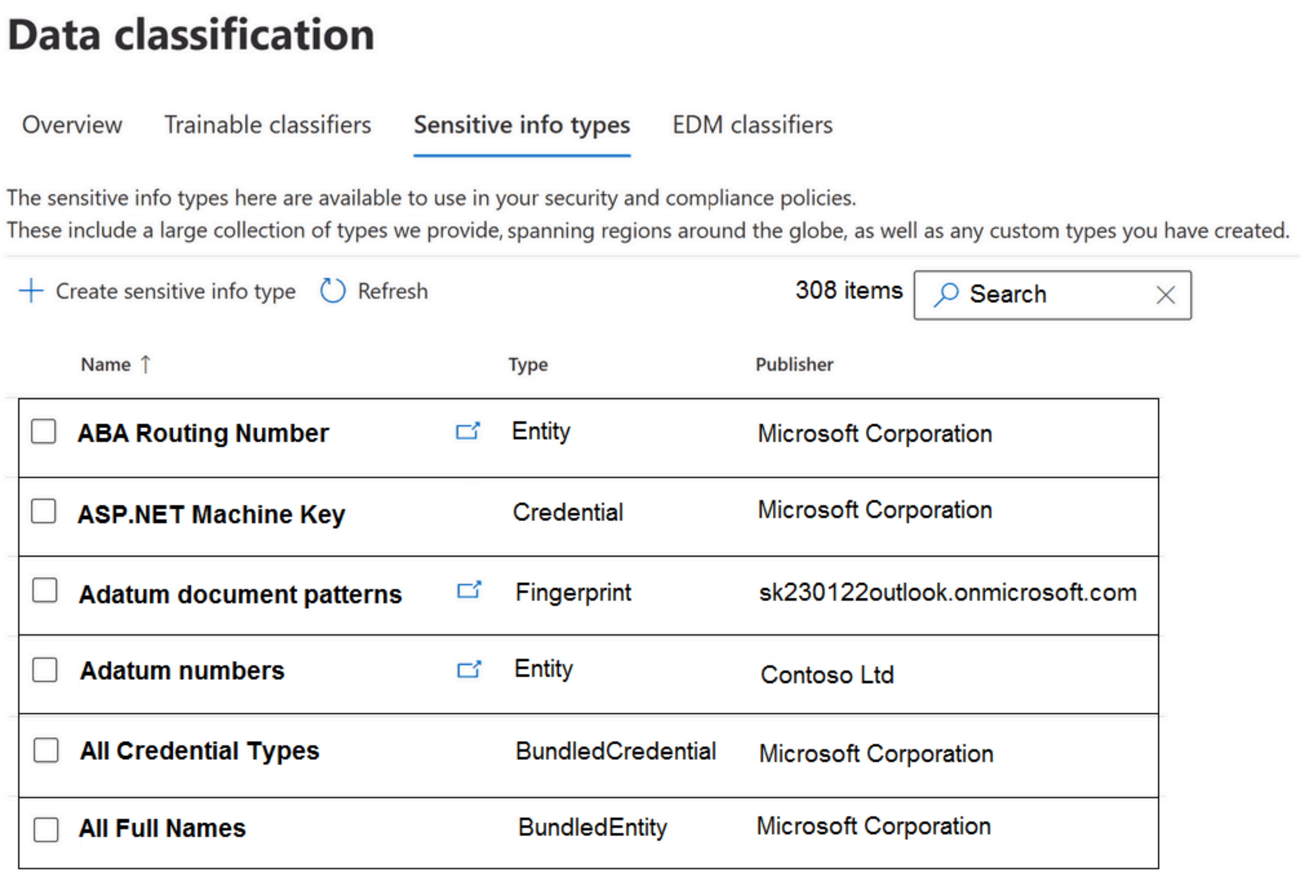
You plan to create a new sensitive information type (SIT) by using the Microsoft Purview compliance portal.

You need to copy and modify an existing SIT from which to create the new SIT.

What are two SITs that you can copy and modify? To answer, select the appropriate SITs in the answer area.

NOTE: Each selection is worth one point.

Answer Area

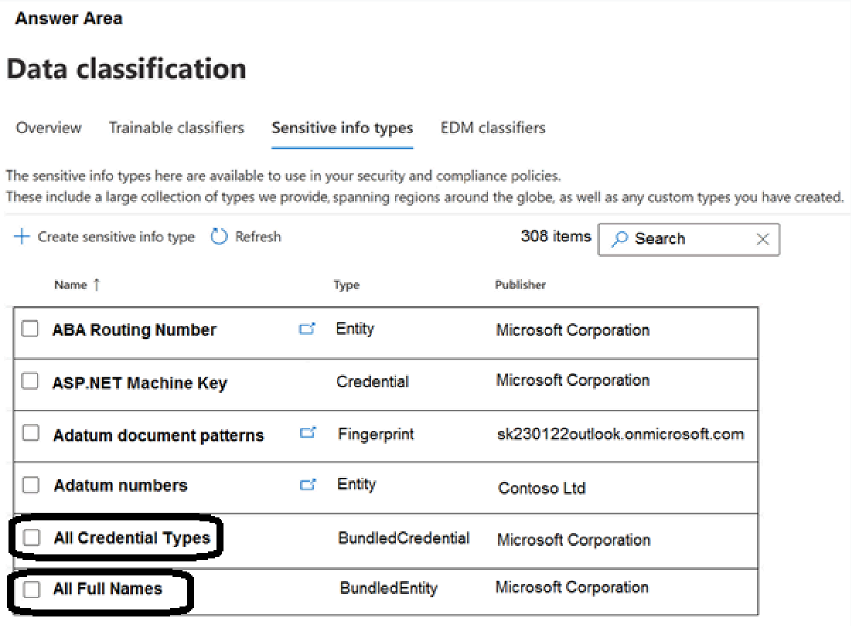


Data classification

The sensitive info types here are available to use in your security and compliance policies.
These include a large collection of types we provide, spanning regions around the globe, as well as any custom types you have created.

	Name ↑	Type	Publisher
□	**ABA Routing Number**	Entity	Microsoft Corporation
□	**ASP.NET Machine Key**	Credential	Microsoft Corporation
□	**Adatum document patterns**	Fingerprint	sk230122outlook.onmicrosoft.com
□	**Adatum numbers**	Entity	Contoso Ltd
□	**All Credential Types**	BundledCredential	Microsoft Corporation
□	**All Full Names**	BundledEntity	Microsoft Corporation

Suggested Answer:



Answer Area

Data classification

Overview | Trainable classifiers | Sensitive info types | EDM classifiers

The sensitive info types here are available to use in your security and compliance policies.
These include a large collection of types we provide, spanning regions around the globe, as well as any custom types you have created.

+ Create sensitive info type | Refresh | 308 items | Search

Name ↑	Type	Publisher
☐ ABA Routing Number	Entity	Microsoft Corporation
☐ ASP.NET Machine Key	Credential	Microsoft Corporation
☐ Adatum document patterns	Fingerprint	sk230122outlook.onmicrosoft.com
☐ Adatum numbers	Entity	Contoso Ltd
☐ All Credential Types	BundledCredential	Microsoft Corporation
☐ All Full Names	BundledEntity	Microsoft Corporation

SDiwan Highly Voted 1 year, 3 months ago

The answer is wrong. Basically copy option is only available for those SITs where you can see the open button blue color logo next to the name. So in this questions, ABA Routing Number, Adatum number and Adatum document patterns can be copied and modified.

upvoted 9 times

Ruslan23 1 year, 3 months ago

No, both the given answer and the your answer are wrong.
You can copy all the existing SITs but you can't modify built-in SITs:
https://learn.microsoft.com/en-us/purview/sit-sensitive-information-type-learn-about#built-in-sensitive-information-types

The blue button "Open in new window" option is not available for all SITs due to the way there are configured or their specific properties.

The correct answer is: Adatum document patterns + Adatum numbers

upvoted 3 times

Ruslan23 1 year, 2 months ago

I read the question again and I'm not sure about my last given answer.
Custom SITs might have been customized for specific use cases in their respective organizations, therefore, they might not be as broadly applicable as the SITs provided by Microsoft Corporation, such as the "ABA Routing Number" and "ASP.NET Machine Key".

upvoted 1 times

mb0812 1 year, 3 months ago

100% right

upvoted 1 times

bleysen Highly Voted 10 months, 1 week ago

I did test this and from what I could figure out you can only copy "ABA routing numbers" and "Adatum numbers". That is the correct answer according to me.

upvoted 8 times

dashadowman00 Most Recent 8 months ago

https://learn.microsoft.com/en-us/purview/sit-create-a-custom-sensitive-information-type?tabs=purview#copy-and-modify-an-existing-sit

These SITs can't be copied in note doesn't match the list in the question!

upvoted 1 times

ross9876986 10 months ago

Entity types in Microsoft Purview are predefined sensitive information types that identify specific data patterns (like numbers or text strings) that you might want to protect or monitor within your organization. Since both the ABA Routing Number and Adatum numbers are standard types provided by Microsoft or other organizations (like Contoso Ltd), they can be copied and modified according to your specific compliance requirements.

upvoted 3 times

PsiCzar 10 months, 2 weeks ago

Confirmed in my own tenant, I can copy/edit the ABA Routing Number and custom SITs that I have created. I can't for the All Credentials, All Full Names, or any bundledentity SITs, the copy option is greyed out.

So the answer should be ABA Routing Number and Adatum numbers.

upvoted 4 times

samuelmj2002 1 year, 1 month ago

Only Entity Type SITs can be copied and modified. The Copy Option is disabled for Credential, Fingerprint, BundledCredential, and BundledEntity. The Correct answer is "ABA Routing Number and Adetum Numbers. Please test in your environment.

upvoted 6 times

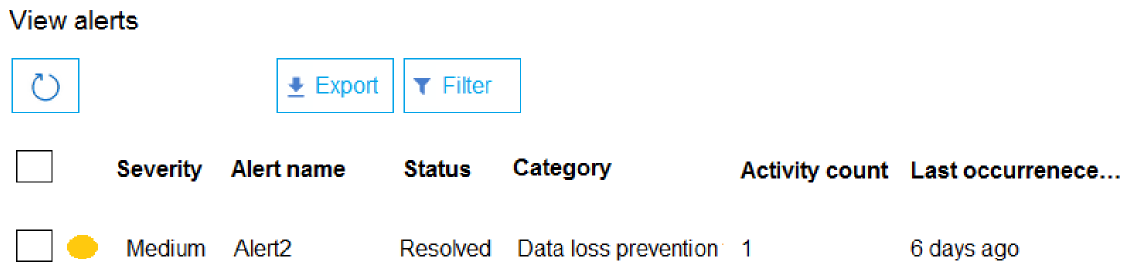
nubemi 1 year, 1 month ago

everything that is Entity can be copied and modified but Credential and BoundledCredential are not copyable.

upvoted 3 times

Question #70 *Topic 1*

You have a Microsoft 365 alert named Alert2 as shown in the following exhibit.



View alerts

□		Severity	Alert name	Status	Category	Activity count	Last occurrenece...
□	●	Medium	Alert2	Resolved	Data loss prevention	1	6 days ago

You need to manage the status of Alert2.

To which status can you change Alert2?

A. The status cannot be changed.

B. Dismissed only

C. Investigating only

D. Active or Investigating only

E. Investigating, Active, or Dismissed.

Suggested Answer: *E*

Community vote distribution

E (50%) A (50%)

JimboJones99 Highly Voted 11 months, 2 weeks ago

Selected Answer: E

I think the given answer is correct - E

https://learn.microsoft.com/en-us/purview/alert-policies#manage-alerts

upvoted 6 times

ca7859c Most Recent 2 months, 1 week ago

Selected Answer: E

Same thing goes with Defender Alerts, not just Purview

upvoted 1 times

Athena94 1 year, 2 months ago

Answer is correct, I tested it.

upvoted 2 times

Ruslan23 1 year, 3 months ago

Selected Answer: A

No change status option on resolved alerts, I have the global administrator role assigned.

upvoted 4 times

SharePat 1 year, 3 months ago

I don't see a way to change the status once it has been resolved so A

upvoted 2 times

Jo696 1 year, 3 months ago

https://learn.microsoft.com/en-us/purview/alert-policies

Assign a status to alerts: You can assign one of the following statuses to alerts: Active (the default value), Investigating, Resolved, or Dismissed. Then, you can filter on this setting to display alerts with the same status setting. This status setting can help track the process of managing alerts.

upvoted 1 times

⊟ **[Removed]** 1 year, 2 months ago

Important

Changing the status of a Defender for Cloud Apps alert in the Microsoft Purview portal won't update the resolution status for the same alert in the Defender for Cloud Apps portal. For example, if you mark the status of the alert as Resolved in the Microsoft Purview portal, the status of the alert in the Defender for Cloud Apps portal is unchanged. To resolve or dismiss a Defender for Cloud Apps alert, manage the alert in the Defender for Cloud Apps portal.

upvoted 1 times

Question #71 *Topic 1*

You have a Microsoft SharePoint Online site named Site1 that contains a document library. The library contains more than 1,000 documents. Some of the documents are job applicant resumes. All the documents are in the English language.

You plan to apply a sensitivity label automatically to any document identified as a resume. Only documents that contain work experience, education, and accomplishments must be labeled automatically.

You need to identify and categorize the resumes. The solution must minimize administrative effort.

What should you include in the solution?

A. a trainable classifier

B. an exact data match (EDM) classifier

C. a function

D. a keyword dictionary

Suggested Answer: *A*

Community vote distribution

A (100%)

fiksarion 6 months, 3 weeks ago

Selected Answer: A

To automatically apply a sensitivity label to documents identified as resumes that contain work experience, education, and accomplishments, the best option is:

A. a trainable classifier

upvoted 1 times

mb0812 1 year, 3 months ago

Selected Answer: A

It has to be Trainable classifier

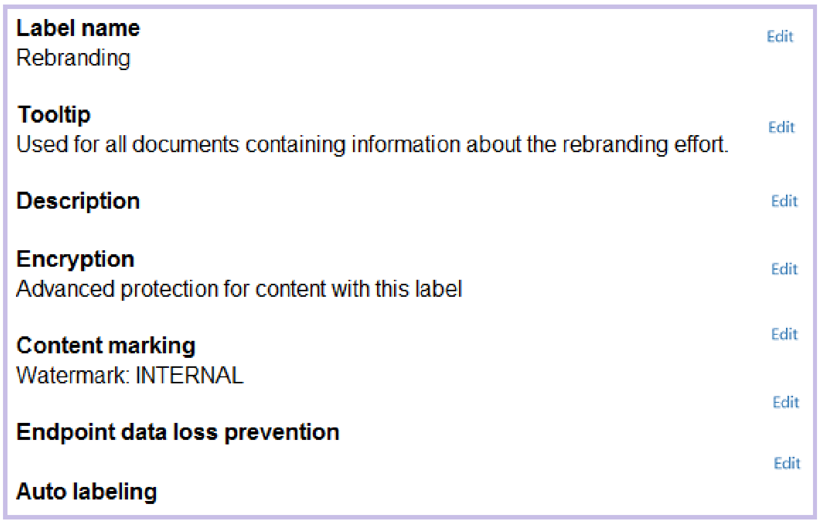
upvoted 3 times

Question #72 *Topic 1*

HOTSPOT

-

You have a Microsoft 365 sensitivity label that is published to all the users in your Microsoft Entra tenant as shown in the following exhibit.



Label name
Rebranding

Tooltip
Used for all documents containing information about the rebranding effort.

Description

Encryption
Advanced protection for content with this label

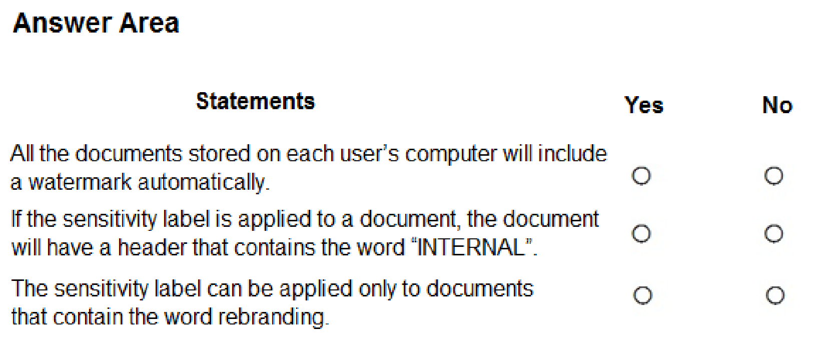
Content marking
Watermark: INTERNAL

Endpoint data loss prevention

Auto labeling

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

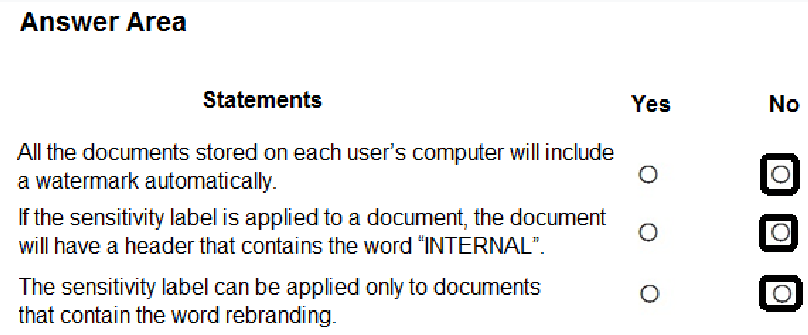
NOTE: Each correct selection is worth one point.



Answer Area

Statements	Yes	No
All the documents stored on each user's computer will include a watermark automatically.	○	○
If the sensitivity label is applied to a document, the document will have a header that contains the word "INTERNAL".	○	○
The sensitivity label can be applied only to documents that contain the word rebranding.	○	○

Suggested Answer:



Answer Area

Statements	Yes	No
All the documents stored on each user's computer will include a watermark automatically.	○	[✓ ○]
If the sensitivity label is applied to a document, the document will have a header that contains the word "INTERNAL".	○	[✓ ○]
The sensitivity label can be applied only to documents that contain the word rebranding.	○	[✓ ○]

Ruslan23 Highly Voted 9 months ago

Given answer is correct:

- NO, there is no auto-labeling policy.
- NO, only the watermark option is selected in Content marking.
- NO, there is no filtered keywords selected.

upvoted 6 times

BewiseExams Most Recent 9 months, 1 week ago

Correct

upvoted 2 times

Question #73 *Topic 1*

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

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

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

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

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

NOTE: Each correct selection is worth one point.

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

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

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

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

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

Suggested Answer: *AC*

Community vote distribution

CD (58%) AC (17%) AD (17%) 8%

SDiwan Highly Voted 1 year, 3 months ago

Selected Answer: CD

I feel option A is wrong. As we dont have any condition based on which label must be applied, rather all users if they are part of group 1 must apply this label. So, in option C, we modify the label1 policy to ensure that users must apply label and group 1 in the policy. Then option D, AIP scanner, as there can be documents which are on users laptop and not directly stored to SP online.

upvoted 6 times

IndigoRabbit Most Recent 10 months, 2 weeks ago

The question here is asking "You need to ensure that the users in Group MUST apply Label1 to their email and documents." D would 't be the answer, as this is satisfy the MUST requirement. So, I will go with A and C and here is why

A - This will automatically apply the sensitivity label to the specified types of documents without requiring user intervention (Data at rest)

B - This involves configuring the Label1 policy to ensure it is set as the default label and applied appropriately to the content used by Group1.

upvoted 1 times

NICKTON81 1 year ago

Selected Answer: CD

https://learn.microsoft.com/en-us/purview/sensitivity-labels#what-label-policies-can-do

upvoted 1 times

ChrisBaird 1 year ago

Selected Answer: CE

C and E.

C - modify the label policy to include mandatory labeling, and modify the label to include client-side auto-labeling if required.

E - Dynamic groups are not supported for sensitivity labels. Set the group type to Assigned.

upvoted 1 times

Boeroe 9 months, 3 weeks ago

No appearantly dynamic groups are possible: https://learn.microsoft.com/en-us/answers/questions/1701631/applying-sensitivity-labels-to-groups-best-practic

upvoted 1 times

Amin4799 1 year, 1 month ago

Selected Answer: AC

AC more accurate IMO

upvoted 1 times

⊟ **Toxik** 1 year, 1 month ago

Selected Answer: AC

AIP ul client is not any more used for labeling

upvoted 3 times

⊟ **Ruslan23** 1 year, 3 months ago

Selected Answer: AD

A: Auto-labeling policies can help ensure that sensitivity labels are applied automatically to emails and documents, this can be particularly useful in a dynamic group where membership might change frequently.

D: The Azure Information Protection unified labeling client provides the necessary labeling and protection capabilities for Office apps on Windows 10 devices

upvoted 2 times

⊟ **Ruslan23** 1 year, 2 months ago

I was wrong, C instead of A.

There is a setting "Require users to apply a label" also known as mandatory labeling, these options ensure a label must be applied before users can save documents and send emails or meeting invites, create new groups or sites, and when they use unlabeled content for Power BI.

https://learn.microsoft.com/en-us/purview/sensitivity-labels#what-label-policies-can-do

upvoted 2 times

⊟ **Jo696** 1 year, 3 months ago

Agree with SDiwan, D was my first go to and wasn't quite sure about the second but C makes sense

upvoted 1 times

Question #74 *Topic 1*

SIMULATION

-

Use the following login credentials as needed:

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

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

Microsoft 365 Username: admin@123456789.onmicrosoft.com
Microsoft 365 Password: **********

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

The following information is for technical support purposes only:

Lab Instance: 12345678

-

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

- The users must be able to apply a classification of Product1 to the files.
- Any authenticated user must be able to open files classified as Product1.
- Files classified as Product1 must be encrypted.

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

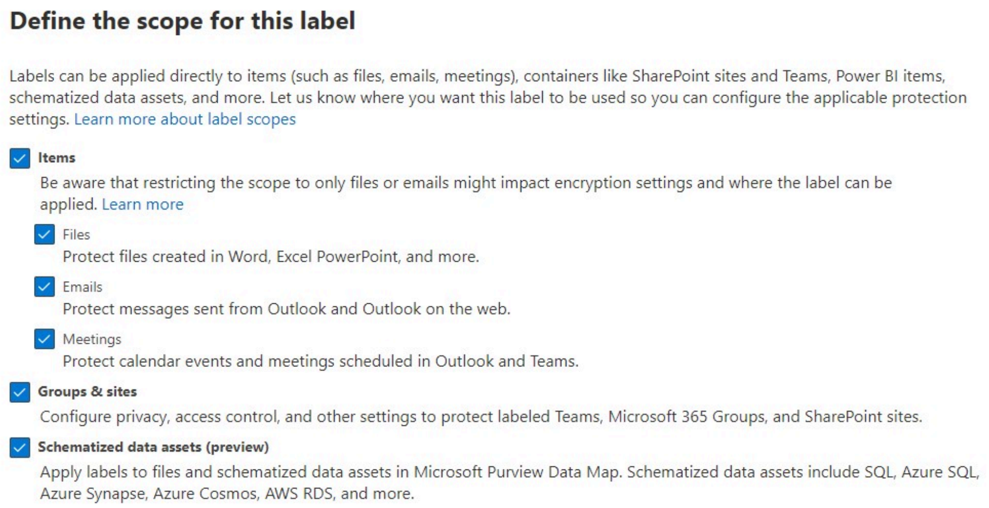
Suggested Answer:

Restrict access to content by using sensitivity labels to apply encryption
When you create a sensitivity label, you can restrict access to content that the label will be applied to. For example, with the encryption settings for a sensitivity label, you can protect content so that:
* Only users within your organization can open a confidential document or email.
* Etc.

How to configure a label for encryption
Step 1: From the Microsoft Purview compliance portal, select Solutions > Information protection > Labels

Step 2: Locate and select label Product1.

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



Define the scope for this label

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

☑ **Items**
Be aware that restricting the scope to only files or emails might impact encryption settings and where the label can be applied. Learn more

☑ Files
Protect files created in Word, Excel PowerPoint, and more.

☑ Emails
Protect messages sent from Outlook and Outlook on the web.

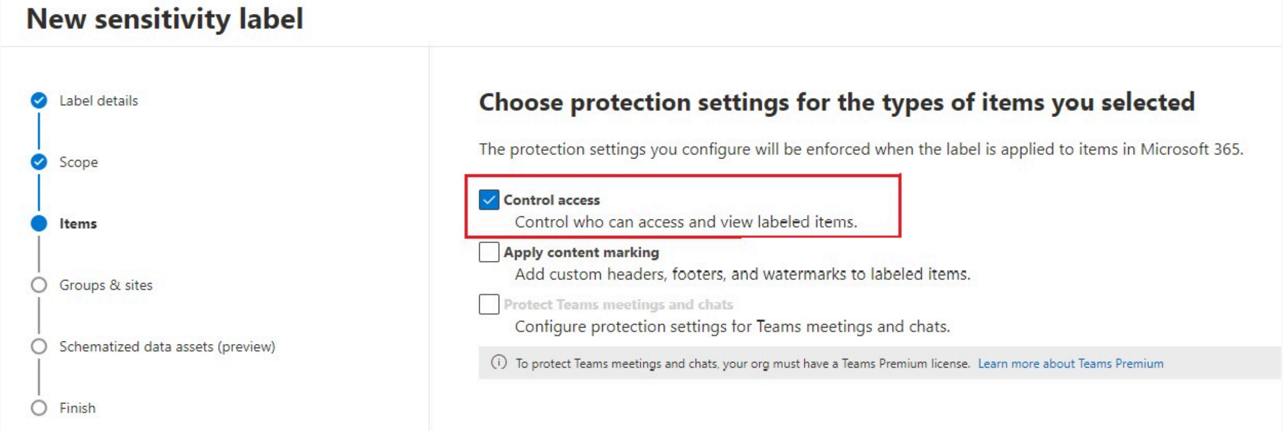
☑ Meetings
Protect calendar events and meetings scheduled in Outlook and Teams.

☑ **Groups & sites**
Configure privacy, access control, and other settings to protect labeled Teams, Microsoft 365 Groups, and SharePoint sites.

☑ **Schematized data assets (preview)**
Apply labels to files and schematized data assets in Microsoft Purview Data Map. Schematized data assets include SQL, Azure SQL, Azure Synapse, Azure Cosmos, AWS RDS, and more.

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

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



New sensitivity label

Choose protection settings for the types of items you selected

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

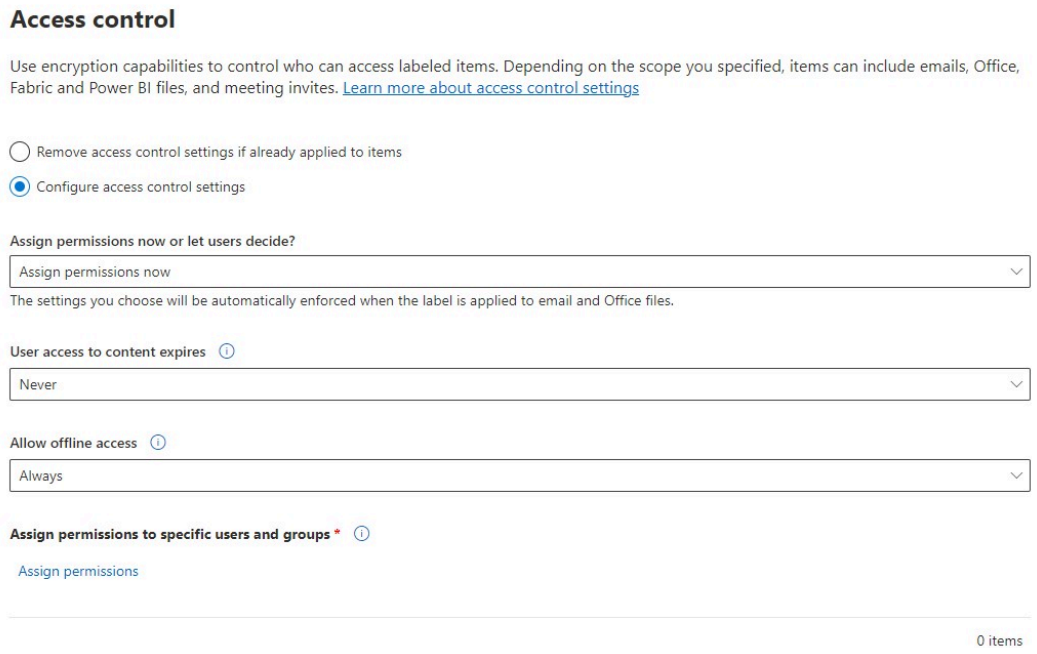
☑ **Control access**
Control who can access and view labeled items.

☐ **Apply content marking**
Add custom headers, footers, and watermarks to labeled items.

☐ Protect Teams meetings and chats
Configure protection settings for Teams meetings and chats.

ⓘ To protect Teams meetings and chats, your org must have a Teams Premium license. Learn more about Teams Premium

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



Access control

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

○ Remove access control settings if already applied to items
● Configure access control settings

Assign permissions now or let users decide?
Assign permissions now
The settings you choose will be automatically enforced when the label is applied to email and Office files.

User access to content expires ⓘ
Never

Allow offline access ⓘ
Always

Assign permissions to specific users and groups * ⓘ
Assign permissions

0 items

Users and groups	Permissions	Edit	Delete

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

Step 7a: For users: Any authenticated users.

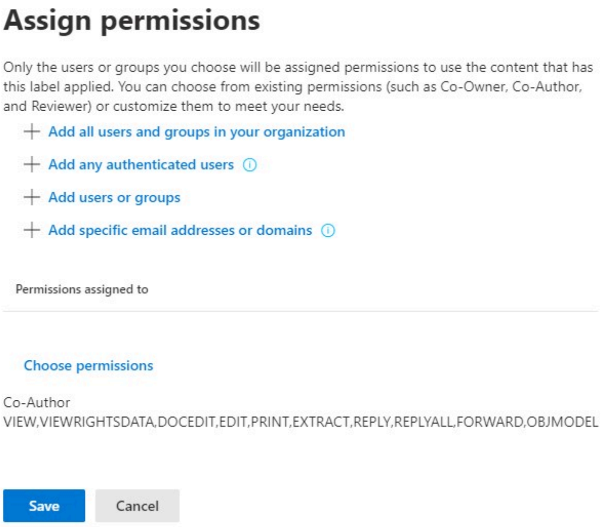
Step 7b: Permissions: Select View

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

1. First, add users or groups that will be assigned permissions to the labeled content.

2. Then, choose which permissions those users should have for the labeled content.

Assigning permissions:



Assign permissions

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

+ Add all users and groups in your organization

+ Add any authenticated users ⓘ

+ Add users or groups

+ Add specific email addresses or domains ⓘ

Permissions assigned to

Choose permissions

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

Step 8: Click Save

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

⊟ **6ae7225** 7 months, 2 weeks ago

Step 7b - Why is it "View2?

So it's select custom -> View? But why?

upvoted 3 times

⊟ **ca7859c** 2 months ago

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

--For least privilege, set the permission to view so users can only read, but not edit

upvoted 1 times

Question #75 *Topic 1*

SIMULATION

-

Use the following login credentials as needed:

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

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

Microsoft 365 Username: admin@123456789.onmicrosoft.com
Microsoft 365 Password: **********

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

The following information is for technical support purposes only:

Lab Instance: 12345678

-

You discover that all users can apply the Confidential - Finance label.

You need to ensure that the Confidential - Finance label is available only to the members of the Finance Team group.

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

Suggested Answer:

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

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

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

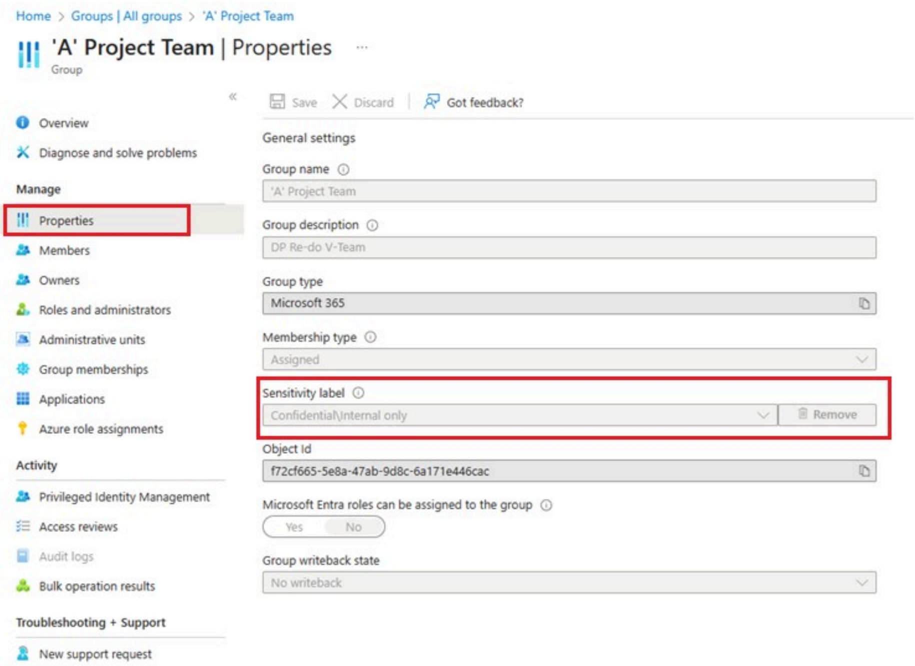
Step 2: Select Microsoft Entra ID.

Step 3: Select Groups

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

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

Select the Confidential - Finance label



General settings

Group name: 'A' Project Team

Group description: DP Re-do V-Team

Group type: Microsoft 365

Membership type: Assigned

Sensitivity label: Confidential\Internal only

Object Id: f72cf665-5e8a-47ab-9d8c-6a171e446cac

Microsoft Entra roles can be assigned to the group: Yes No

Group writeback state: No writeback

Step 6: Select Save to save your changes.

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

Stevecammi Highly Voted 1 year, 1 month ago

I think the answer is wrong. Instead, you need to edit the label policy that publishes the Finance Confidence Label and remove all users by adding only the Finance Team group

upvoted 14 times

ca7859c 2 months ago

Agreed

upvoted 1 times

dashadowman00 Most Recent 8 months ago

The question about specific group not administrative units, I think the answer is correct

upvoted 1 times

MKnight25 8 months, 2 weeks ago

The answer is completely wrong, see the following links with explanations
https://learn.microsoft.com/en-us/purview/create-sensitivity-labels#publish-sensitivity-labels-by-creating-a-label-policy
https://learn.microsoft.com/en-us/entra/identity/users/groups-assign-sensitivity-labels?tabs=microsoft
https://learn.microsoft.com/en-us/purview/sensitivity-labels-teams-groups-sites#how-to-configure-groups-and-site-settings

upvoted 2 times

Question #76 *Topic 1*

SIMULATION

-

Use the following login credentials as needed:

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

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

Microsoft 365 Username: admin@123456789.onmicrosoft.com
Microsoft 365 Password: **********

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

The following information is for technical support purposes only:

Lab Instance: 12345678

-

You plan to automatically apply a watermark to the documents of a project named Falcon.

You need to create a label that will add a watermark of “Project Falcon” in red, size-12 font diagonally across the documents.

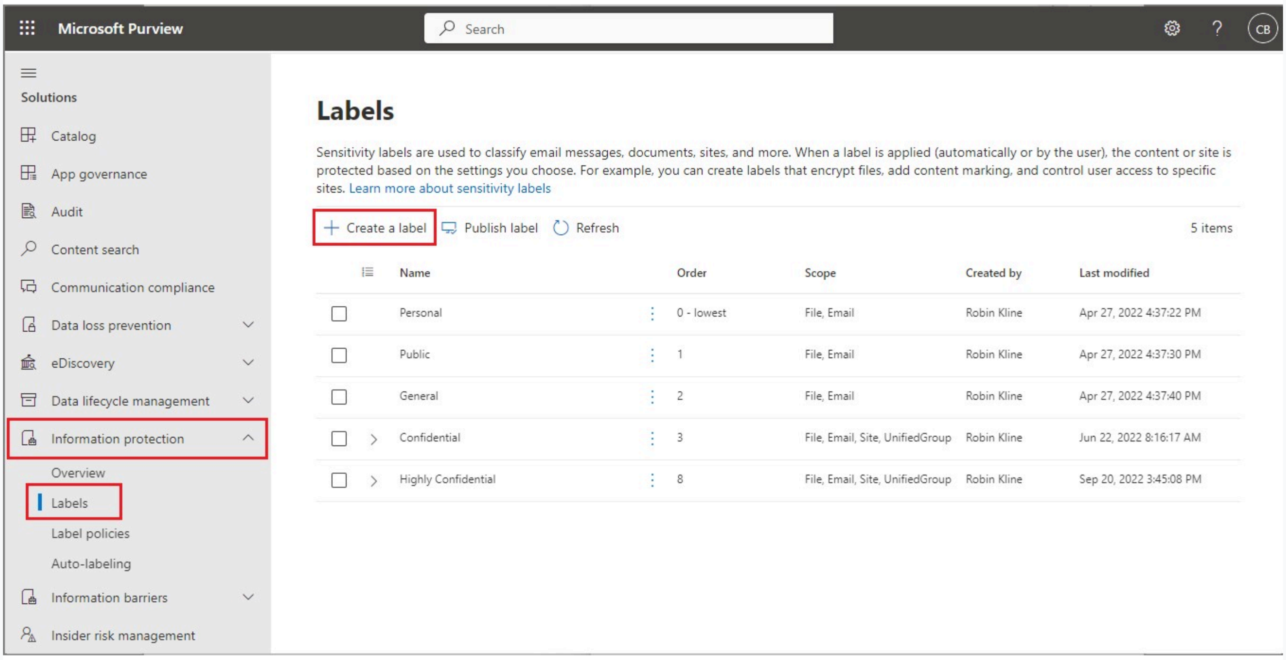
To complete this task, sign in to the appropriate admin center.

Suggested Answer:

Create and configure sensitivity labels

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

Step 2: On the Labels page, select + Create a label to start the new sensitivity label configuration:



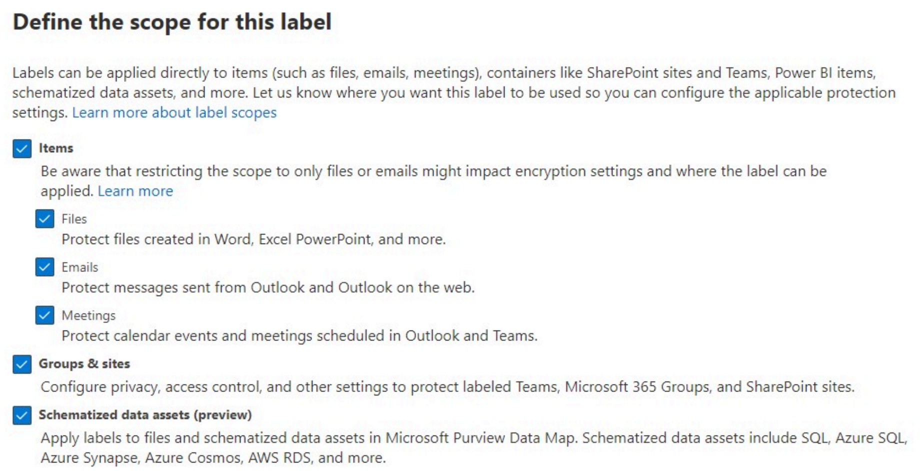
Labels

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. Learn more about sensitivity labels

+ Create a label | Publish label | Refresh — 5 items

Name	Order	Scope	Created by	Last modified
Personal	0 - lowest	File, Email	Robin Kline	Apr 27, 2022 4:37:22 PM
Public	1	File, Email	Robin Kline	Apr 27, 2022 4:37:30 PM
General	2	File, Email	Robin Kline	Apr 27, 2022 4:37:40 PM
Confidential	3	File, Email, Site, UnifiedGroup	Robin Kline	Jun 22, 2022 8:16:17 AM
Highly Confidential	8	File, Email, Site, UnifiedGroup	Robin Kline	Sep 20, 2022 3:45:08 PM

Step 3: On the Define the scope for this label page, the options selected determine the label's scope for the settings that you can configure and where they'll be visible when they're published. In our case select: Items, Files, and select Word documents.



Define the scope for this label

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

☑ **Items**
Be aware that restricting the scope to only files or emails might impact encryption settings and where the label can be applied. Learn more

- ☑ Files
  Protect files created in Word, Excel PowerPoint, and more.
- ☑ Emails
  Protect messages sent from Outlook and Outlook on the web.
- ☑ Meetings
  Protect calendar events and meetings scheduled in Outlook and Teams.

☑ **Groups & sites**
Configure privacy, access control, and other settings to protect labeled Teams, Microsoft 365 Groups, and SharePoint sites.

☑ **Schematized data assets (preview)**
Apply labels to files and schematized data assets in Microsoft Purview Data Map. Schematized data assets include SQL, Azure SQL, Azure Synapse, Azure Cosmos, AWS RDS, and more.

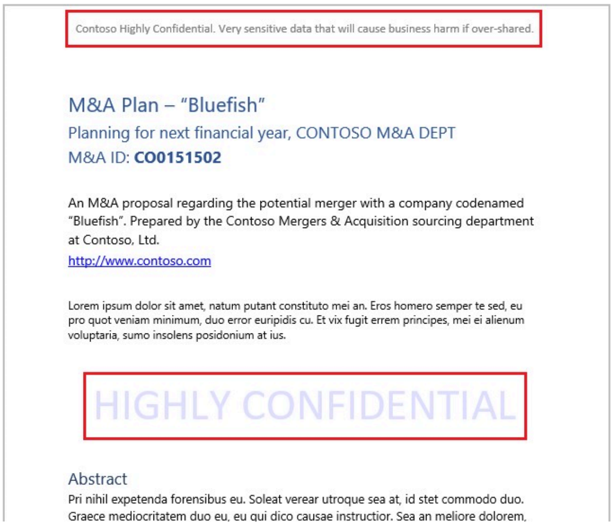
Note: If Items is selected, you can configure settings that apply to apps that support sensitivity labels, such as Office Word and Outlook. Optionally, you can extend these labels to include meetings from Teams and Outlook, and to protecting Teams meetings themselves by enforcing settings for Teams meetings and related chat.

Step 4: Follow the configuration prompts for the label settings. Use the help in the UI for individual settings.

Step 5: In the UI add a watermark of “Project Falcon” in red, size-12 font diagonally across the document.

Note: What sensitivity labels can do
After a sensitivity label is applied to an email, meeting invite, or document, any configured protection settings for that label are enforced on the content. You can configure a sensitivity label to:

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



Contoso Highly Confidential. Very sensitive data that will cause business harm if over-shared.

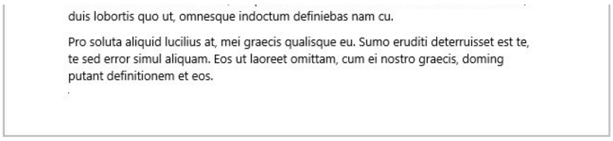
M&A Plan – “Bluefish”
Planning for next financial year, CONTOSO M&A DEPT
M&A ID: **CO0151502**

An M&A proposal regarding the potential merger with a company codenamed “Bluefish”. Prepared by the Contoso Mergers & Acquisition sourcing department at Contoso, Ltd.
http://www.contoso.com

Lorem ipsum dolor sit amet, natum putant constituto mei an. Eros homero semper te sed, eu pro quot veniam minimum, duo error euripidis cu. Et vix fugit errem principes, mei ei alienum voluptaria, sumo insolens posidonium at ius.

HIGHLY CONFIDENTIAL

Abstract
Pri nihil expetenda forensibus eu. Soleat verear utroque sea at, id stet commodo duo. Graece mediocritatem duo eu, eu qui dico causae instructior. Sea an meliore dolorem,



duis lobortis quo ut, omnesque indoctum definiebas nam cu.

Pro soluta aliquid lucilius at, mei graecis qualisque eu. Sumo eruditi deterruisset est te, te sed error simul aliquam. Eos ut laoreet omittam, cum ei nostro graecis, doming putant definitionem et eos.

Step 6: Finish the Wizard

Reference:
https://learn.microsoft.com/en-us/purview/create-sensitivity-labels
https://answers.microsoft.com/en-us/msteams/forum/all/how-to-automatically-apply-sensitivity-labels-to/2482d1b2-1fe6-4a80-af4a-2b93b9c670de

IndigoRabbit 10 months, 2 weeks ago

After the label is created, it needs to be published to the members of Project Falcon. If the project members are unknown, a custom sensitive info type should be created with keywords such as "Falcon," "Project Falcon," and "Falcon Project." Following this, an auto-labeling policy should be created with conditions set to identify and label documents related to Project Falcon.

upvoted 2 times

MKnight25 8 months, 2 weeks ago

I would go the following way

1. Create a sensitive info type with keywords related to Falcon, Project Falcon etc
2. Create a label with the required setting, incl. Auto-label for Files based on the custome SIT
3. Publish the label via Label Policy

upvoted 2 times

Question #77 *Topic 1*

SIMULATION

-

Use the following login credentials as needed:

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

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

Microsoft 365 Username: [email protected]
Microsoft 365 Password: **********

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

The following information is for technical support purposes only:

Lab Instance: 12345678

-

You plan to create a data loss prevention (DIP) policy that will apply to content containing the following keywords:

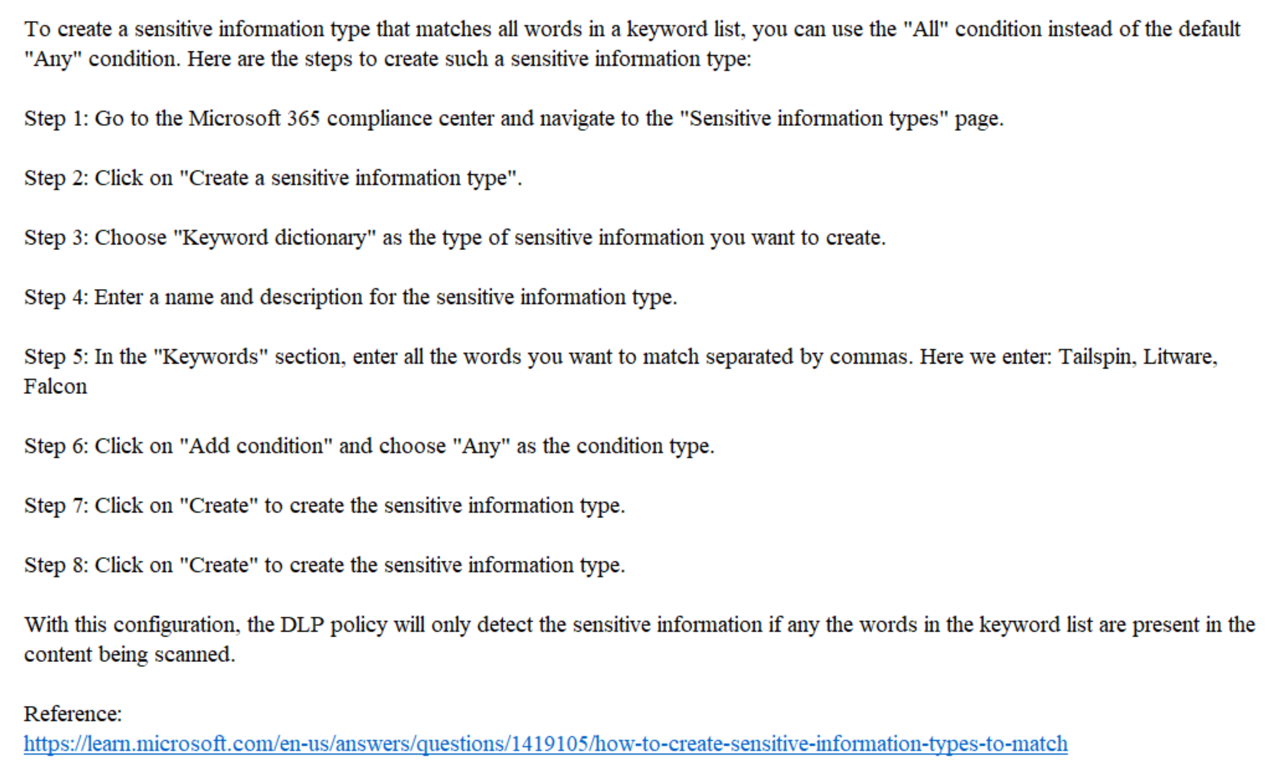
- Tailspin
- Litware
- Falcon

You need to create a keyword list that can be used in the DLP policy.

You do NOT need to create the DLP policy at this time.

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

Correct Answer:



To create a sensitive information type that matches all words in a keyword list, you can use the "All" condition instead of the default "Any" condition. Here are the steps to create such a sensitive information type:

Step 1: Go to the Microsoft 365 compliance center and navigate to the "Sensitive information types" page.

Step 2: Click on "Create a sensitive information type".

Step 3: Choose "Keyword dictionary" as the type of sensitive information you want to create.

Step 4: Enter a name and description for the sensitive information type.

Step 5: In the "Keywords" section, enter all the words you want to match separated by commas. Here we enter: Tailspin, Litware, Falcon

Step 6: Click on "Add condition" and choose "Any" as the condition type.

Step 7: Click on "Create" to create the sensitive information type.

Step 8: Click on "Create" to create the sensitive information type.

With this configuration, the DLP policy will only detect the sensitive information if any the words in the keyword list are present in the content being scanned.

Reference:
https://learn.microsoft.com/en-us/answers/questions/1419105/how-to-create-sensitive-information-types-to-match

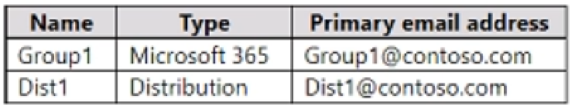
Currently there are no comments in this discussion, be the first to comment!

Question #78 Topic 1

HOTSPOT

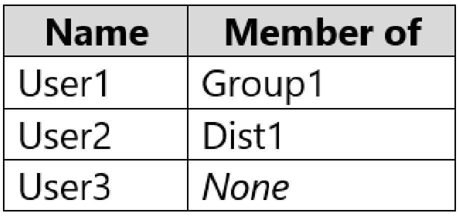
-

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



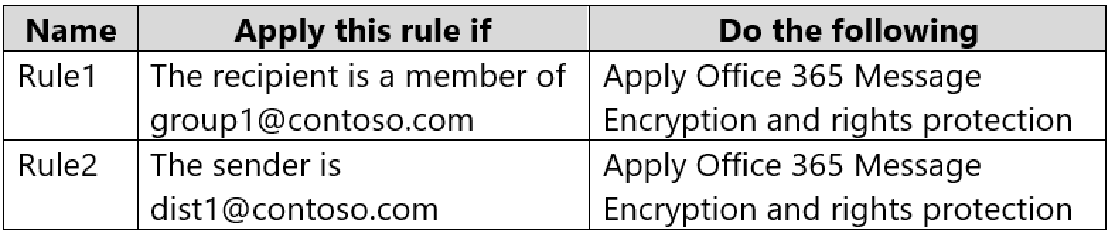
Name	Type	Primary email address
Group1	Microsoft 365	Group1@contoso.com
Dist1	Distribution	Dist1@contoso.com

The subscription contains the users shown in the following table.



Name	Member of
User1	Group1
User2	Dist1
User3	*None*

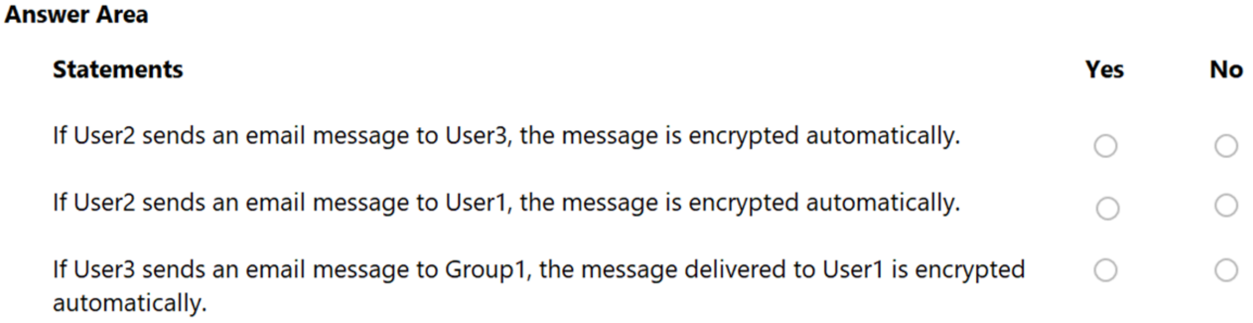
You create the mail flow rules shown in the following table.



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.

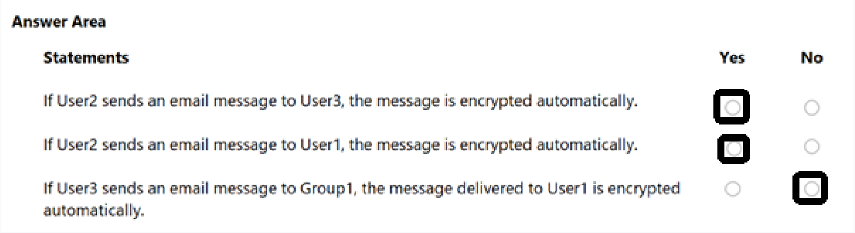
NOTE: Each correct selection is worth one point.



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.	○	○

Suggested 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.	○	[✓ ○]

Ruslan23 Highly Voted 1 year, 2 months ago

N - Y - N

Same statement of Question #46

upvoted 15 times

itsadel 6 months, 2 weeks ago

but right answer NYY

upvoted 5 times

ca7859c Most Recent 2 months ago

Ruslan is right

N (user3 isn't a member of any group)

Y (user1 is recipient "member" of group1)

N (the rule applies to recipient "members of group1, and not group1 itself)

upvoted 1 times

ca7859c 2 months ago

Correction:

N (Rule2 applies only if sender is dist1@contoso, NOT when sender is a member of it

Y (Rule1 applies if the recipient is a member of group1@contoso)

N (Rule1 applies to members of group1@contoso AND group1@contoso itself)

upvoted 1 times

husamshahin 11 months, 1 week ago

on Exam 28-7-2024

upvoted 2 times

Stevecammi 1 year, 1 month ago

I agree with you

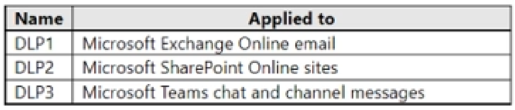
upvoted 1 times

Question #79 Topic 1

HOTSPOT

-

You have a Microsoft 365 E5 subscription that contains the data loss prevention (DLP) policies shown in the following table.



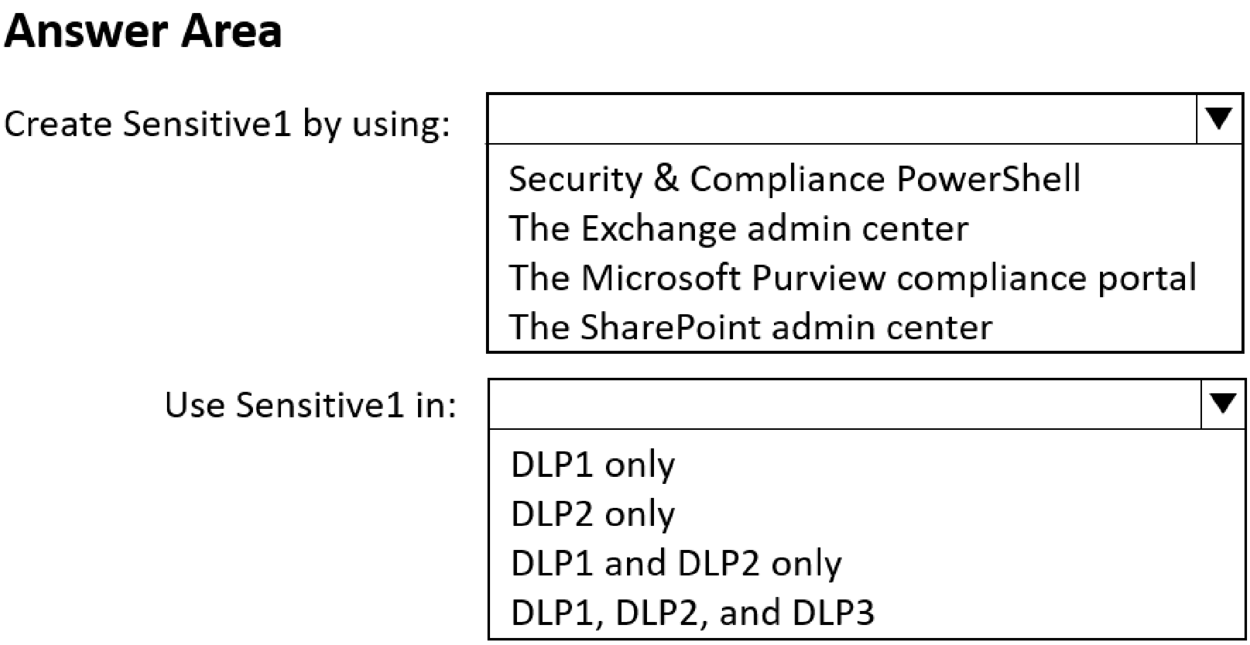
Name	Applied to
DLP1	Microsoft Exchange Online email
DLP2	Microsoft SharePoint Online sites
DLP3	Microsoft Teams chat and channel messages

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

You plan to create a sensitive info type named Sensitive1 that will use the document fingerprint from Template1.docx.

What should you use to create Sensitive1, and in which DLP policies can you use Sensitive1? To answer, select the appropriate options in the answer area.

NOTE: Each correct selection is worth one point.



Answer Area

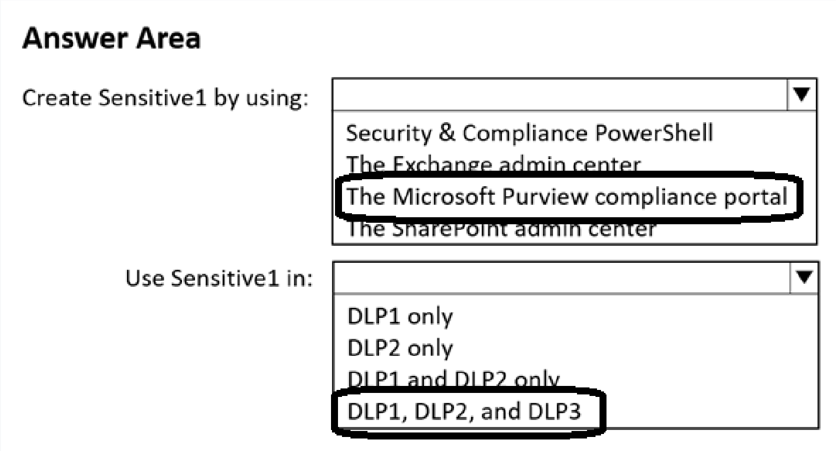
Create Sensitive1 by using: ▼

- Security & Compliance PowerShell
- The Exchange admin center
- The Microsoft Purview compliance portal
- The SharePoint admin center

Use Sensitive1 in: ▼

- DLP1 only
- DLP2 only
- DLP1 and DLP2 only
- DLP1, DLP2, and DLP3

Suggested Answer:



Answer Area

Create Sensitive1 by using: ▼

- Security & Compliance PowerShell
- The Exchange admin center
- [✓ The Microsoft Purview compliance portal]
- The SharePoint admin center

Use Sensitive1 in: ▼

- DLP1 only
- DLP2 only
- DLP1 and DLP2 only
- [✓ DLP1, DLP2, and DLP3]

Ruslan23 Highly Voted 1 year, 2 months ago

Create Sensitive1 by using: Security & Compliance PowerShell (New-DlpSensitiveInformationType)

https://learn.microsoft.com/en-us/purview/sit-document-fingerprinting#create-a-custom-sensitive-information-type-based-on-document-fingerprinting-using-powershell

Use Sensitive1 in: DLP1, DLP2, DLP3

upvoted 7 times

⊟ **I3eza** 5 months, 3 weeks ago

Currently, you can create a document fingerprint only in Security & Compliance PowerShell.

Use Sensitive1 in: DLP1, DLP2, DLP3

upvoted 1 times

⊟ **MrParfumeDeluxe** 6 months, 1 week ago

Disagree. For this scenario (creating Sensitive1 with document fingerprinting), the Microsoft Purview compliance portal is the only correct option. PowerShell is not suitable because it lacks the necessary functionality to handle document templates or fingerprinting.

upvoted 1 times

⊟ **EM1234** 1 year ago

The link clearly explains it can currently only be made in the sec and compliance powershell.

upvoted 1 times

⊟ **e6f184d** 11 months, 2 weeks ago

There is a button in the Sensitive Info Types blade of the Purview portal to create a Fingerprint-based SIT. So you can use either Powershell or the Purview portal.

upvoted 2 times

⊟ **Jo696** Highly Voted 1 year, 2 months ago

I am pretty sure this should be DLP1 and 2 only

upvoted 5 times

⊟ **narenbabu.chintu** Most Recent 11 months, 4 weeks ago

The answer is correct:

Create sensitive 1 by using: Security & Compliance Power

and User Sensitive 1 in DLP1, DLP2 and DLP3.

It can be included in Teams location as well, when Finger print SIT is called in the conditions of the DLP policy, and saved, then a message can be seen:

Conditions

Content contains any of these sensitive info types: Sample_Fingerprint_SIT

Evaluate predicate for Message or attachment

Actions

Send alerts to Administrator

So incase of messages, it will evaluate predicate of messages.

upvoted 1 times

⊟ **nubemi** 1 year, 1 month ago

If we talk about DLP for Teams it means chat message not documents? So you cant apply sensitivity labels to teams messages.

upvoted 2 times

⊟ **e6f184d** 11 months, 2 weeks ago

DLP for Teams policies will include documents shared in a chat or a channel, the policy just needs to also have Sharepoint and OneDrive included - https://learn.microsoft.com/en-us/purview/dlp-microsoft-teams?tabs=purview

upvoted 2 times

⊟ **MKnight25** 8 months, 2 weeks ago

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 enforced.

upvoted 1 times

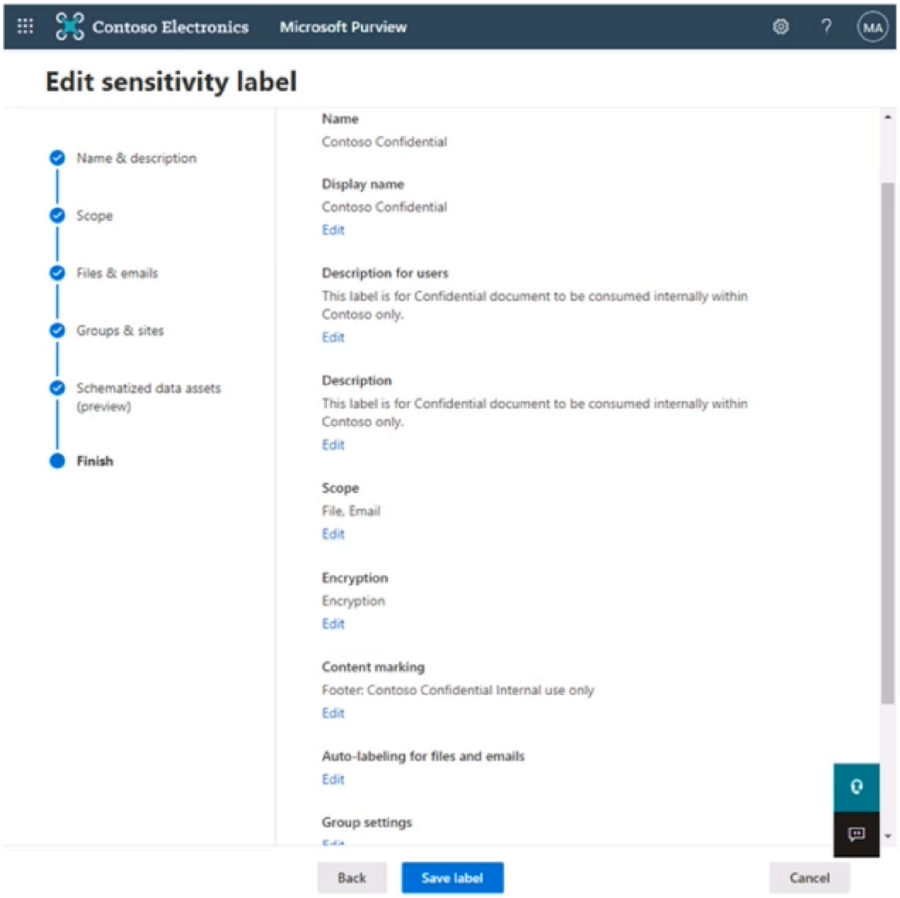
HOTSPOT

-

You have a Microsoft 365 subscription that contains a sensitivity label named Contoso Confidential.

You publish Contoso Confidential to all users.

Contoso Confidential is configured as shown in the Configuration exhibit. (Click the Configuration tab.)



Edit sensitivity label

- Name & description
- Scope
- Files & emails
- Groups & sites
- Schematized data assets (preview)
- Finish

Name
Contoso Confidential

Display name
Contoso Confidential
Edit

Description for users
This label is for Confidential document to be consumed internally within Contoso only.
Edit

Description
This label is for Confidential document to be consumed internally within Contoso only.
Edit

Scope
File, Email
Edit

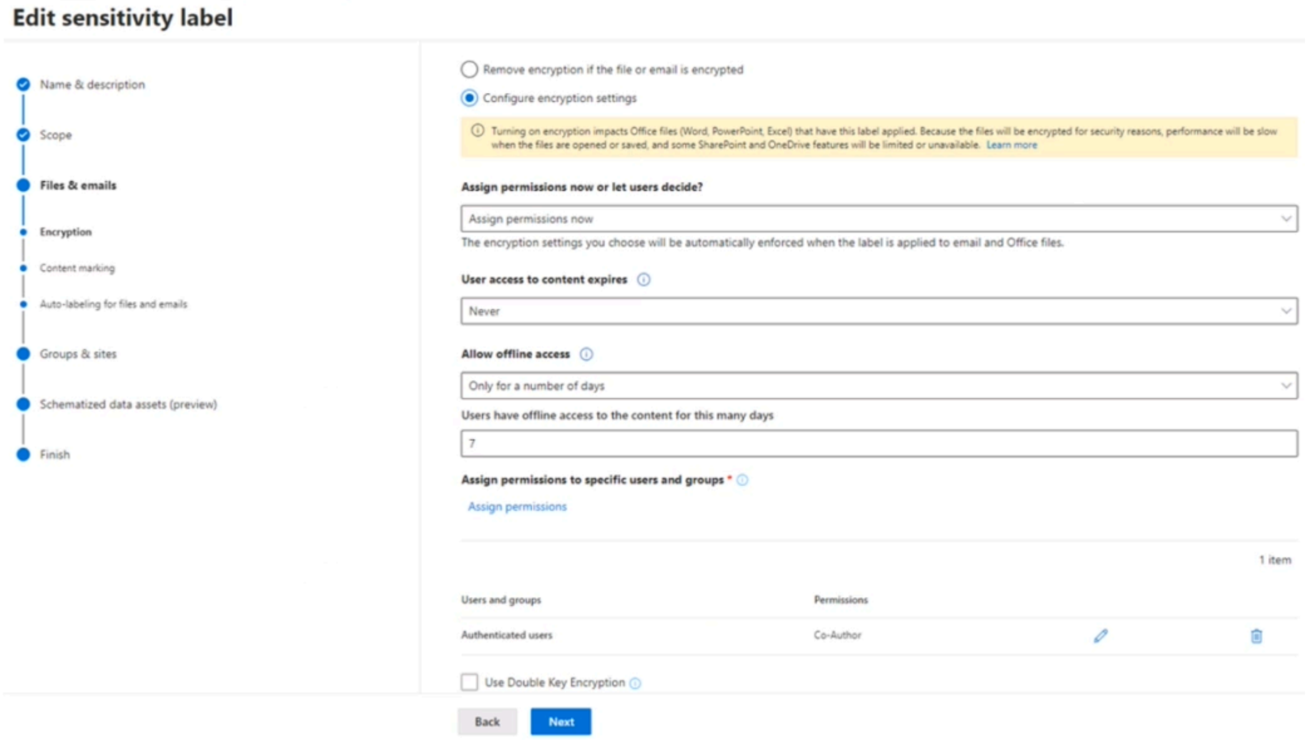
Encryption
Encryption
Edit

Content marking
Footer: Contoso Confidential Internal use only
Edit

Auto-labeling for files and emails
Edit

Group settings
Edit

The Encryption settings of Contoso Confidential are configured as shown in the Encryption exhibit. (Click the Encryption tab.)



Edit sensitivity label

○ 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 ⓘ

Never

Allow offline access ⓘ

Only for a number of days

Users have offline access to the content for this many days

7

Assign permissions to specific users and groups * ⓘ

Assign permissions

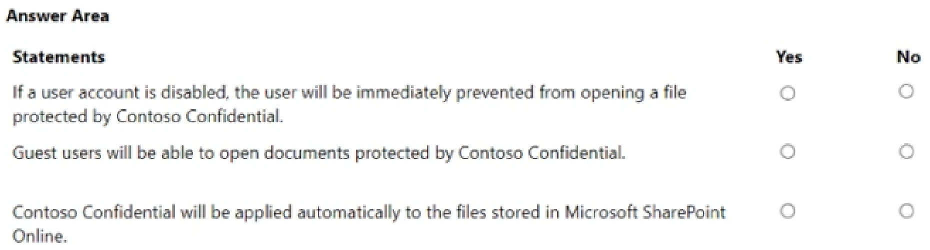
1 item

Users and groups	Permissions
Authenticated users	Co-Author

□ Use Double Key Encryption ⓘ

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

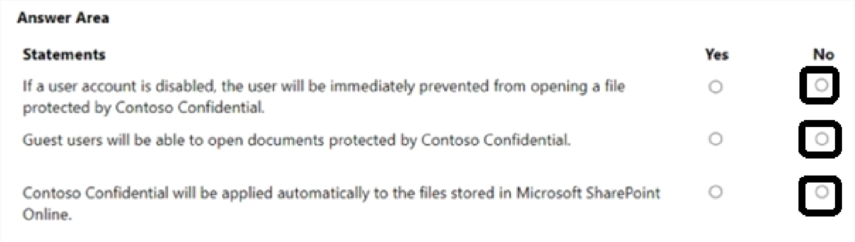
NOTE: Each correct selection is worth one point.



Answer Area

Statements	Yes	No
If a user account is disabled, the user will be immediately prevented from opening a file protected by Contoso Confidential.	○	○
Guest users will be able to open documents protected by Contoso Confidential.	○	○
Contoso Confidential will be applied automatically to the files stored in Microsoft SharePoint Online.	○	○

Suggested Answer:



Answer Area

Statements	Yes	No
If a user account is disabled, the user will be immediately prevented from opening a file protected by Contoso Confidential.	○	[✓ ○]
Guest users will be able to open documents protected by Contoso Confidential.	○	[✓ ○]
Contoso Confidential will be applied automatically to the files stored in Microsoft SharePoint Online.	○	[✓ ○]

⊟ **Ruslan23** Highly Voted 1 year, 2 months ago

NO: The user will be prevented from opening a file after 7 days.

YES: Guest users are considered authenticated users.

NO: No auto-labeling policy was configured.

upvoted 11 times

⊟ **ca7859c** 2 months ago

N (offline access is 7 days, so user will continue to stop having access after 7 days)

Y (guests users authenticate to the Entra tenant)

N (Auto-labeling in the first picture is blank (which is why it has no Words indicating a setting review above the word "Edit"

upvoted 1 times

⊟ **a056e5f** 1 year, 2 months ago

NO

NO: The description says internal use only and members must be contoso. It is assuming guest users are from out side the org

NO

upvoted 6 times

⊟ **Phil_79** 4 months, 3 weeks ago

Description is a free text field, you can write whatever you want. If you apply protection to Authenticated Users, then guests and B2B members can access the file.

upvoted 3 times

⊟ **jakke91** Most Recent 7 months, 3 weeks ago

Has someone else an idea, because I'm lost on this one.

upvoted 1 times

⊟ **[Removed]** 8 months ago

When you assign permissions, you can choose:

Everyone in your organization (all tenant members). This setting excludes guest accounts.

Any authenticated users. Make sure you understand the requirements and limitations of this setting before selecting it.

https://learn.microsoft.com/en-us/purview/encryption-sensitivity-labels

upvoted 1 times

⊟ **narenbabu.chintu** 11 months, 4 weeks ago

Explanation for YES, YES, NO

If a user account is disabled, the user will be immediately prevented from opening a file protected by Contoso Confidential - YES, Look at the definition provided in the purview about "Allow Offline Access", it says : "

If you specify that labeled content is never available offline or that it's available offline only for a number of days, when that threshold is reached, users must be reauthenticated and their access is logged. When this happens, if their credentials aren't cached, users are prompted to sign into Microsoft 365 before they can open the document or email. "

Based on this, when a user is even disabled, if the user credentials are cached in the system where this document is available, the user can still access the file with these creds.

But, here is user account is disabled. that means, he is disabled at AD level. that means he cannot access the SharePoint, teams or exchange.

upvoted 3 times

⊟ **Mnguyen0503** 7 months, 1 week ago

If the computer has a copied of the file and stays offline after the termination, the user can still open the offline copy. Doesn't matter if the account is disabled or not. Your login is also cached for a number of day before it's prompted again.

upvoted 2 times

⊟ **narenbabu.chintu** 11 months, 4 weeks ago

YES, YES, NO

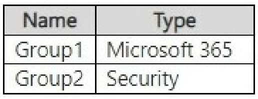
upvoted 3 times

Question #81 Topic 1

HOTSPOT

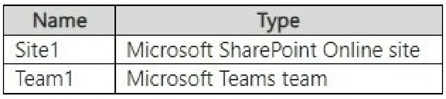
-

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



Name	Type
Group1	Microsoft 365
Group2	Security

The subscription contains the resources shown in the following table.



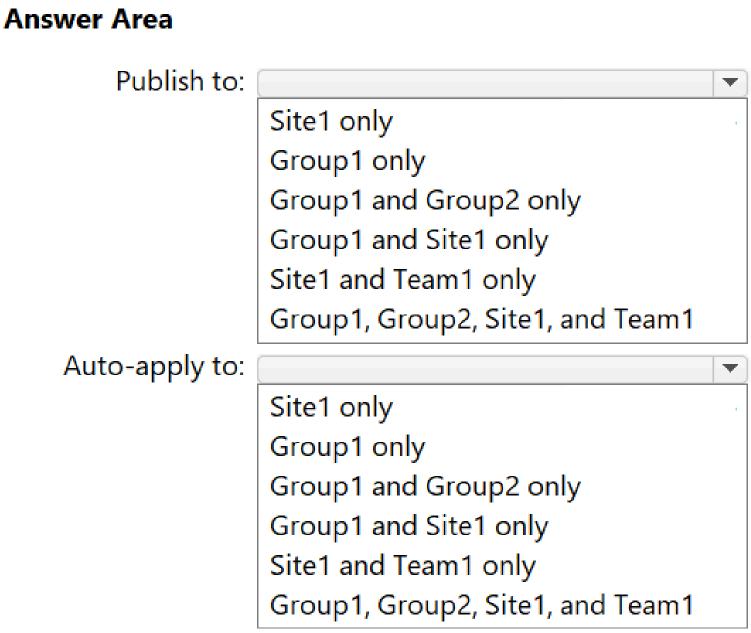
Name	Type
Site1	Microsoft SharePoint Online site
Team1	Microsoft Teams team

You create a sensitivity label named Label 1.

You need to publish Label1 and have the label apply automatically.

To what can you publish Label1, and to what can Label1 be auto-applied? To answer, select the appropriate options in the answer area.

NOTE: Each correct selection is worth one point.



Answer Area

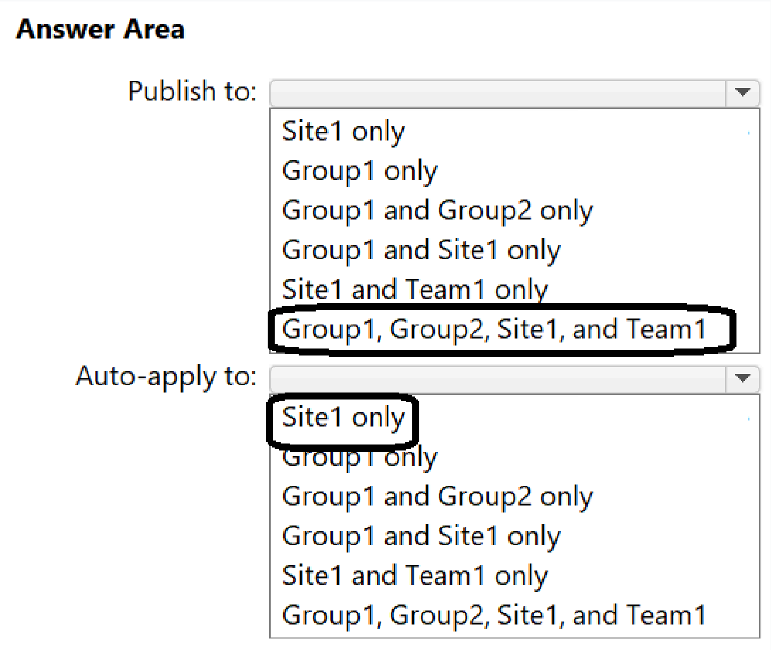
Publish to:

Site1 only
Group1 only
Group1 and Group2 only
Group1 and Site1 only
Site1 and Team1 only
Group1, Group2, Site1, and Team1

Auto-apply to:

Site1 only
Group1 only
Group1 and Group2 only
Group1 and Site1 only
Site1 and Team1 only
Group1, Group2, Site1, and Team1

Suggested Answer:



Answer Area

Publish to:

- Site1 only
- Group1 only
- Group1 and Group2 only
- Group1 and Site1 only
- Site1 and Team1 only
- [✓ Group1, Group2, Site1, and Team1]

Auto-apply to:

- [✓ Site1 only]
- Group1 only
- Group1 and Group2 only
- Group1 and Site1 only
- Site1 and Team1 only
- Group1, Group2, Site1, and Team1

[Removed] 8 months ago

Answer: Group 1 only (There is no mention if the security group is mail enabled) & Site 1 only

There are two different methods for automatically applying a sensitivity label to content in Microsoft 365

1. Client-side labeling when users edit documents or compose (also reply or forward) emails
2.Service-side labeling when content is already saved (in SharePoint or OneDrive) or emailed (processed by Exchange Online).

This indicates that MS Teams team is not supported

upvoted 3 times

Kuteron 6 months, 4 weeks ago

correct. See it the same.

upvoted 1 times

MKnight25 8 months, 2 weeks ago

I would select
Group1 Only (because: Labels can be published to any specific user or email-enabled security group, distribution group, or Microsoft 365 group (which can have dynamic membership) in Microsoft Entra ID. --> it's not clear if the Security Group is mail enabled

Auto-Apply to: Site1 only thats correct

upvoted 2 times

Question #82 *Topic 1*

You have a Microsoft 365 tenant that is opt-in for trainable classifiers.

You need to ensure that a user named User1 can create custom trainable classifiers. The solution must use the principle of least privilege.

Which role should you assign to User1?

A. Global Administrator

B. Security Operator

C. Security Administrator

D. Compliance Administrator

Suggested Answer: *D*

BloodRaideN 1 month, 2 weeks ago

Selected Answer: D

D: Tenant is already opt-in. Least privilege = Compliance Administrator

upvoted 1 times

ca7859c 1 month, 3 weeks ago

Selected Answer: D

D. Compliance Administrator

(The tenant is already opt-in. No need for Global admin in this case)

upvoted 2 times

JambonBlanc 2 months, 1 week ago

Selected Answer: D

Because the tenant is already opt-in for trainable classifiers (requires Global Admin role), the least privilege role to train classifiers is COMPLIANCE ADMINISTRATOR. This role ensure the necessary permissions to manage compliance related settings, including creating and training classifiers.

upvoted 3 times

itsadel 6 months, 2 weeks ago

Selected Answer: A

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."

upvoted 4 times

HardeWerker433 5 months ago

But boss, read the first sentence, it states that the Tenant is already opt-in. Wouldn't that mean that compliance administrator is the right answer?

upvoted 5 times

Jideakin 3 months, 3 weeks ago

Thank you! That was first thing I thought. the opt-in is already done. Compliance Administrator is correct answer

upvoted 2 times

[Removed] 8 months ago

Answer given seems correct.

To use classifiers in the following scenarios, you need the following permissions:

Scenario = Sensitivity label policy

Required Role/Permission

Security Administrator

Compliance Administrator

Compliance Data Administrator

https://learn.microsoft.com/en-us/purview/trainable-classifiers-get-started-with

upvoted 1 times

Question #83 *Topic 1*

HOTSPOT

-

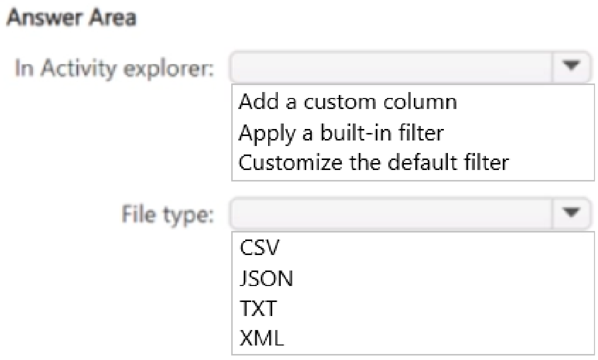
You have a Microsoft 365 E5 subscription that has data loss prevention (DLP) implemented.

You plan to export DLP activity by using Activity explorer.

The exported file needs to display the sensitive info type detected for each DLP rule match.

What should you do in Activity explorer before exporting the data, and in which file format is the file exported? To answer, select the appropriate options in the answer area.

NOTE: Each correct selection is worth one point.



Answer Area

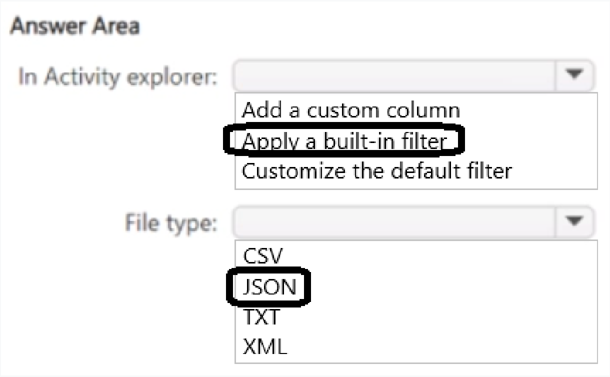
In Activity explorer: ▼

Add a custom column
Apply a built-in filter
Customize the default filter

File type: ▼

CSV
JSON
TXT
XML

Suggested Answer:



Answer Area

In Activity explorer: ▼

Add a custom column
[✓ Apply a built-in filter]
Customize the default filter

File type: ▼

CSV
[✓ JSON]
TXT
XML

JambonBlanc 2 months, 1 week ago

In Activity explorer: "Add a custom column"
Please note that "the exported file needs to display the SENSITIVITY INFO TYPE detected for each DLP rule match". Therefore, you must "Add a custom column", applying a filter will not add the column to the exported file.

File Type: CSV
I've tested on my tenant.
upvoted 1 times

Phil_79 4 months, 3 weeks ago

Tricky question... you have to apply a default filter to select only DLP activities, but you also have to customize the columns to diplay the sensitive info type... here they talk about add a custom column that is different from "customize colums" (that means "change the displayed colums)... so I'd go with default filter first... in any case, the export is in CSV format
upvoted 1 times

marpengar1 7 months ago

The solution is to add a custom column. The download is done in CSV. With built-in filter the requested sensitivity label information is not added.
upvoted 2 times

⊟ **MKnight25** 8 months, 2 weeks ago

The file format is csv and not json

upvoted 2 times

⊟ **[Removed]** 8 months ago

Agreed. Tested in lab. The export downloads as csv file (no option to choose file format).

You also need to 'Apply a built-in filter'

upvoted 4 times

Question #84 Topic 1

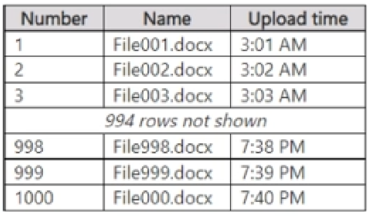
HOTSPOT

-

You have a Microsoft 365 E5 subscription.

You plan to create a custom trainable classifier by uploading 1,000 machine-generated files as seed content.

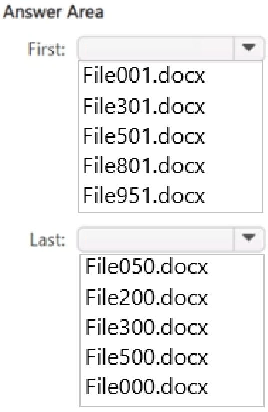
The files have sequential names and are uploaded in one-minute intervals as shown in the following table.



Number	Name	Upload time
1	File001.docx	3:01 AM
2	File002.docx	3:02 AM
3	File003.docx	3:03 AM
994 rows not shown		
998	File998.docx	7:38 PM
999	File999.docx	7:39 PM
1000	File000.docx	7:40 PM

Which files were processed first and last when you created the custom trainable classifier? To answer, select the appropriate options in the answer area.

NOTE: Each correct selection is worth one point.

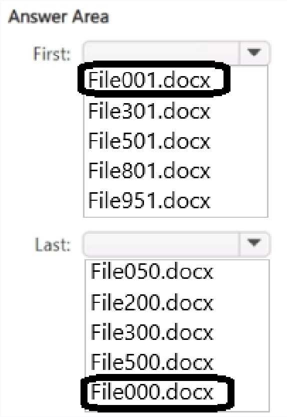


Answer Area

First:
- File001.docx
- File301.docx
- File501.docx
- File801.docx
- File951.docx

Last:
- File050.docx
- File200.docx
- File300.docx
- File500.docx
- File000.docx

Suggested Answer:



Answer Area

First:
- [✓ File001.docx]
- File301.docx
- File501.docx
- File801.docx
- File951.docx

Last:
- File050.docx
- File200.docx
- File300.docx
- File500.docx
- [✓ File000.docx]

JambonBlanc 2 months, 1 week ago

The answer is correct:

First = File001
Last = File000

At least 50 positive samples (up to 500) and at least 150 negative samples (up to 1500) are required to train a classifier. The more samples you provide, the more accurate the predictions the classifier makes will be. The trainable classifier processes up to the 2000 most recently created samples (by file created date/time stamp).

Source:
https://learn.microsoft.com/en-us/purview/trainable-classifiers-get-started-with#seed-content
upvoted 2 times

⊟ **ca7859c** 2 months ago

Agreed. The 2000 samples are a mix of positive and negative samples

upvoted 1 times

⊟ **marpengar1** 7 months ago

The question is poorly formulated. If it is positive content it is up to 500 files, if it is negative content you can upload up to 1500. The type of content is not specified. https://learn.microsoft.com/es-es/purview/trainable-classifiers-get-started-with

upvoted 2 times

⊟ **Dools** 7 months, 1 week ago

I think the answer is as follows.

First = File001
Last = File500

Creating a trainable classifier requires between 50 and 500 seed sample files. If there are more than 500 files uploaded to a Microsoft SharePoint Online site, only the first 500 files are processed based on the time stamp.

upvoted 1 times

⊟ **Kuteron** 6 months, 4 weeks ago

no, you are wrong. 500 files only for positive content. But the question and don't split into positive and negative content.
500 files for positive content and 1500 for negative content results into 2000

upvoted 1 times

⊟ **DCarma** 3 months, 4 weeks ago

Negative seed content has to be contained in a separate SharePoint folder, so this is clearly only the positive seed content.

So I agree with Dools:

First = File001
Last = File500

upvoted 1 times

⊟ **[Removed]** 8 months ago

The trainable classifier processes up to the 2000 most recently created samples (by file created date/time stamp).

https://learn.microsoft.com/en-us/purview/trainable-classifiers-get-started-with

upvoted 2 times

Question #85 Topic 1

DRAG DROP

-

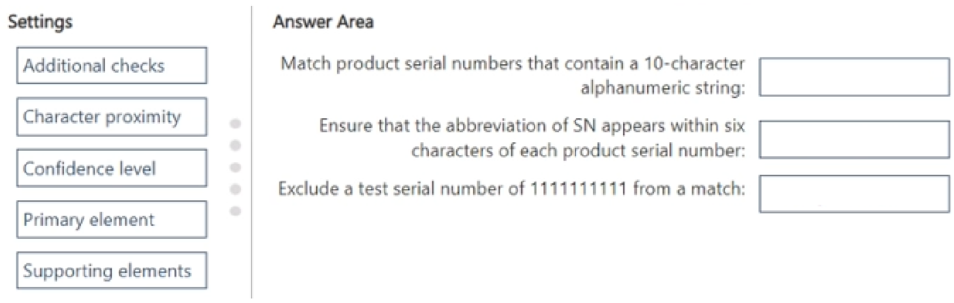
You have a Microsoft 365 E5 subscription that has data loss prevention (DLP) implemented.

You need to create a custom sensitive info type. The solution must meet the following requirements:

• Match product serial numbers that contain a 10-character alphanumeric string.
• Ensure that the abbreviation of SN appears within six characters of each product serial number.
• Exclude a test serial number of 1111111111 from a match.

Which pattern settings should you configure for each requirement? To answer, drag the appropriate settings to the correct requirements. Each setting 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.



Settings

Additional checks

Character proximity

Confidence level

Primary element

Supporting elements

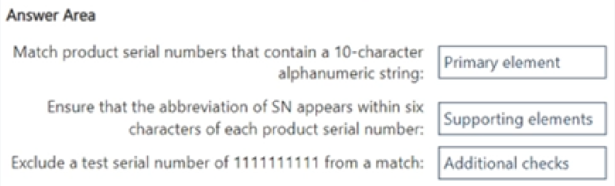
Answer Area

Match product serial numbers that contain a 10-character alphanumeric string:

Ensure that the abbreviation of SN appears within six characters of each product serial number:

Exclude a test serial number of 1111111111 from a match:

Suggested Answer:



Answer Area

Match product serial numbers that contain a 10-character alphanumeric string: Primary element

Ensure that the abbreviation of SN appears within six characters of each product serial number: Supporting elements

Exclude a test serial number of 1111111111 from a match: Additional checks

JambonBlanc 2 months, 1 week ago

The correct answer is:

1. PRIMARY ELEMENT: match product serial numbers that contain a 10-character alphanumeric string.

2. CHARACTER PROXIMITY: ensure that the abbreviation of SN appears within 6 characters of each product serial number. "Supporting Elements" cannot replace "Character proximity" for this specific requirement. While "Supporting Elements" are used to validate the presence of secondary indicators (like keywords or patterns) near the primary element, they do not enforce a specific distance or proximity between elements. To ensure that the abbreviation "SN" appears within six characters of the product serial number, you must use the Character proximity setting. This setting explicitly defines the distance between the primary element (serial number) and the supporting keyword ("SN").

3. ADDITIONAL CHECKS: exclude a test serial number of 1111111111 from a match. This allows you to define exclusions or exceptions, such as ignoring the test serial number.

upvoted 1 times

Dools 7 months, 1 week ago

This is a tricky one because you could combine all these checks into a single regex within the primary element or you could split it into primary and supporting elements.

upvoted 1 times

Phil_79 4 months, 3 weeks ago

You're right, but put in this format the answer is correct base on the test I did in my lab

upvoted 1 times

jakke91 7 months, 3 weeks ago

To me 'Ensure that the abbreviation of SN appears within six characters of each product serial number.' should be character proximirty

upvoted 1 times

Question #86 *Topic 1*

HOTSPOT

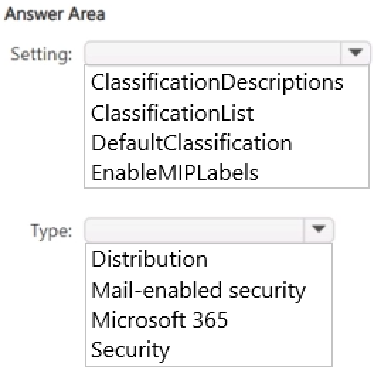
-

You have a Microsoft 365 E5 tenant that contains a published sensitivity label named Sensitivity1.

You plan to create a Microsoft Entra group named Group1 and assign Sensitivity1 to Group1.

How should you configure Group1? To answer, select the appropriate options in the answer area.

NOTE: Each correct selection is worth one point.

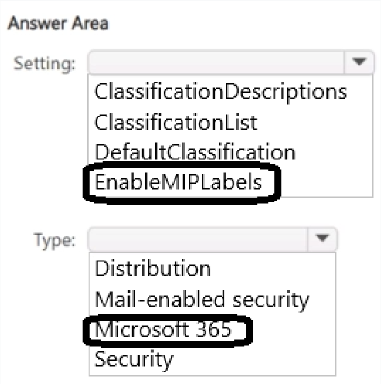


Answer Area

Setting:
- ClassificationDescriptions
- ClassificationList
- DefaultClassification
- EnableMIPLabels

Type:
- Distribution
- Mail-enabled security
- Microsoft 365
- Security

Correct Answer:



Answer Area

Setting:
- ClassificationDescriptions
- ClassificationList
- DefaultClassification
- [✓ EnableMIPLabels]

Type:
- Distribution
- Mail-enabled security
- [✓ Microsoft 365]
- Security

JambonBlanc 2 months, 1 week ago

The answer is correct:

Settings:
EnableMIPLabels: This setting must be enabled to allow sensitivity labels to be assigned to Microsoft Entra groups. It ensures that the label functionality is active for the group.

Group Type:
Microsoft 365 Group: Sensitivity labels are designed to work with Microsoft 365 Groups, Teams sites, and SharePoint Online sites. Other group types like Distribution, Mail-enabled security, or Security groups are not compatible with sensitivity labels.

upvoted 1 times

Question #87 *Topic 1*

HOTSPOT

-

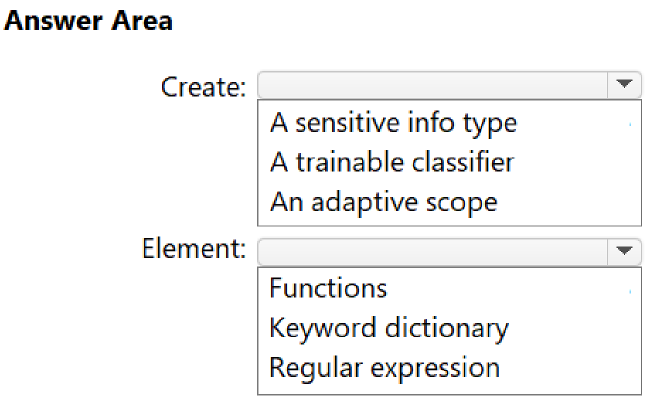
You have a Microsoft 365 E5 subscription.

You have a file named Customer.csv that contains a list of 1,000 customer names.

You plan to use Customer.csv to classify documents stored in a Microsoft SharePoint Online library.

What should you create in the Microsoft Purview compliance portal, and which type of element should you select? To answer, select the appropriate options in the answer area.

NOTE: Each correct selection is worth one point.

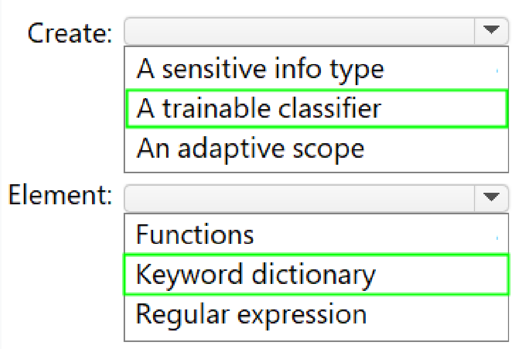


Answer Area

Create:
- A sensitive info type
- A trainable classifier
- An adaptive scope

Element:
- Functions
- Keyword dictionary
- Regular expression

Correct Answer:



Create:
- A sensitive info type
- [✓ A trainable classifier]
- An adaptive scope

Element:
- Functions
- [✓ Keyword dictionary]
- Regular expression

TC1Labs 1 month ago

Exact Data Match (EDM) + Keyword list. We need to label documents on the base of csv file.

upvoted 1 times

ca7859c 2 months ago

sensitive info type + keyword list (trainable classifiers are used to detect patterns in documents and not add a keyword list)

upvoted 2 times

JambonBlanc 2 months, 1 week ago

The answer is correct:

Create: A TRAINABLE CLASSIFIER

This is the best choice for classifying documents based on the content in the file. Trainable classifiers are designed to identify patterns and classify content based on examples, such as the customer names in the file.Trainable classifiers are better suited for identifying content that doesn't follow a specific pattern, such as free-text documents or emails (unstructured data).

A Sensitive Information Type (SIT) can be used instead of a Trainable Classifier in certain scenarios. SITs are ideal for detecting specific patterns, such as credit card number, Social Security numbers, or other structured data (pattern-based detection).

Element: KEYWORD DICTIONARY: Use this to create a list of customer names from the Customer.csv file. The keyword dictionary will act as a reference to match and classify documents containing those names.

upvoted 1 times

⊟ **Mattia8** 3 months, 3 weeks ago

SIT + Keyword

upvoted 3 times

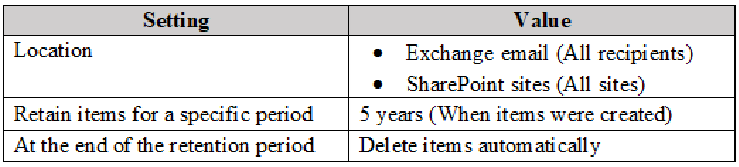
⊟ **Jideakin** 3 months, 3 weeks ago

The correct answer is Sensitive Info Type and Keyword Dictionary.

upvoted 3 times

Question #88 Topic 1

You have a Microsoft 365 E5 subscription that contains a retention policy named RP1 as shown in the following table.



Setting	Value
Location	• Exchange email (All recipients) • SharePoint sites (All sites)
Retain items for a specific period	5 years (When items were created)
At the end of the retention period	Delete items automatically

You place a preservation lock on RP1.

You need to modify RP1.

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

NOTE: Each correct selection is worth one point.

A. Decrease the retention period of the policy.

B. Delete the policy.

C. Increase the retention period of the policy.

D. Disable the policy.

E. Remove locations from the policy.

F. Add locations to the policy.

Suggested Answer: *CF*

Community vote distribution

BE (100%)

ca7859c 2 months ago

Selected Answer: CF

CF is correct.
Only "Additive" actions are allowed

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

https://learn.microsoft.com/en-us/purview/retention-preservation-lock
upvoted 2 times

JambonBlanc 2 months, 1 week ago

Selected Answer: CF

The correct answers are:

C. Increase the retention period of the policy
A preservation lock ensures that retention settings cannot be reduced, but extending the retention period is still allowed.

F. Add locations to the policy
You can add locations to the retention policy even after a preservation lock is in place, but you cannot remove existing ones.
upvoted 3 times

DCarma 3 months, 4 weeks ago

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

https://learn.microsoft.com/en-us/purview/retention-preservation-lock

upvoted 2 times

⊟ **Phil_79** 4 months, 3 weeks ago

Selected Answer: CF

on a locked policy you cannot perform actions that reduces the policy retention scope: https://learn.microsoft.com/en-us/purview/retention-preservation-lock

upvoted 4 times

⊟ **mokkosu** 5 months, 1 week ago

Selected Answer: BE

AI□□□□□□BE□□□□□□□□□□□□□□□□□□□□

upvoted 1 times

Question #89 *Topic 1*

You have a Microsoft 365 E5 subscription.

You have a Microsoft Entra tenant named contoso.com.

Your company collaborates with a partner company that has a Microsoft Entra tenant named fabrikam.com.

You need to ensure that email sent to fabrikam.com always uses TLS and is sent only if the email server certificate of fabrikam.com is validated.

What should you do?

A. From the Exchange admin center, create a connector.

B. From the Microsoft Purview compliance portal, create a communication compliance policy.

C. From the Microsoft Purview compliance portal, create a sensitivity label policy.

D. From the Exchange admin center, create a remote domain.

E. From the Microsoft Defender portal, enable DomainKeys Identified Mail (DKIM).

Correct Answer: *A*

JambonBlanc 2 months, 1 week ago

Selected Answer: A

The answer is correct.
A. From the Exchange admin center, create a connector.

A connector in the Exchange admin center allows you to enforce TLS for email communication with specific domains. It also ensures that the certificate of the destination domain, in this case, fabrikam.com, is validated before email delivery.

upvoted 3 times

Question #90 *Topic 1*

You have a Microsoft 365 subscription that contains two Microsoft SharePoint Online sites named Site1 and Site2.

You plan to use policies to meet the following requirements:

- Add a watermark of Confidential to a document if the document contains the words Project1 or Project2.
- Retain a document for seven years if the document contains credit card information.
- Add a watermark of Internal Use Only to all the documents stored on Site2.
- Add a watermark of Confidential to all the documents stored on Site1.

You need to recommend the minimum number of sensitive info types required.

How many sensitive info types should you recommend?

A. 1

B. 2

C. 3

D. 4

Suggested Answer: *C*

Community vote distribution

B (100%)

ca7859c 2 months ago

Selected Answer: B

2 SITs

1 for keyword list "Project1" & "Project2"

2 for the credit card info (using the built-in credit card info type)

upvoted 1 times

JambonBlanc 2 months, 1 week ago

Selected Answer: C

To meet the requirements outlined in the question, the minimum number of sensitive information types required is 3.

Sensitive Info Type 1: Matches documents containing the keywords "Project1" or "Project2" and applies the watermark "Confidential."

Sensitive Info Type 2: Detects documents containing credit card information to retain them for seven years.

Sensitive Info Type 3: Identifies all documents stored on Site2 to apply the "Internal Use Only" watermark.

upvoted 1 times

Jideakin 3 months, 3 weeks ago

Selected Answer: B

You need 2 SIT. The built-in one for Credit card and a custom one with keyword ist contain both Project1 and Project2. Others don't require SITs, just setting default label for those sites

upvoted 2 times

Phil_79 4 months, 3 weeks ago

Selected Answer: B

you need a custom SIT for Project1 and Project2 and the built-in SIT for credit card information. The other actions do not require SITs, just auto-labeling since are base on location and not on content

upvoted 3 times

Question #91 Topic 1

DRAG DROP

-

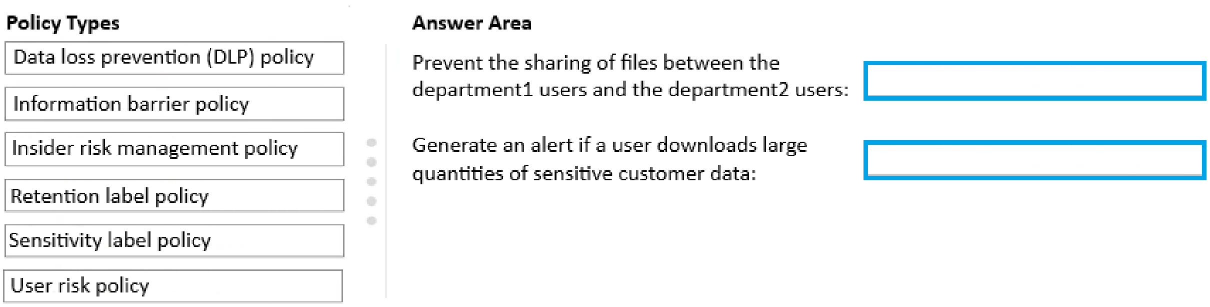
You have a Microsoft 365 E5 subscription.

You need to meet the following requirements:

• Prevent the sharing of files between the users in a department named department and the users in a department named department2.
• Generate an alert if a user downloads large quantities of sensitive customer data.

Which type of policy should you use for each requirement? To answer, drag the appropriate policy types to the correct requirements. Each policy type 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.



Policy Types

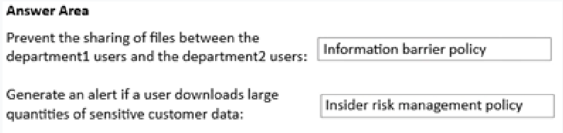
- Data loss prevention (DLP) policy
- Information barrier policy
- Insider risk management policy
- Retention label policy
- Sensitivity label policy
- User risk policy

Answer Area

Prevent the sharing of files between the department1 users and the department2 users:

Generate an alert if a user downloads large quantities of sensitive customer data:

Suggested Answer:



Answer Area

Prevent the sharing of files between the department1 users and the department2 users: Information barrier policy

Generate an alert if a user downloads large quantities of sensitive customer data: Insider risk management policy

naveenbio Highly Voted 5 months, 1 week ago

Information Barrier Policy

Explanation: Information Barrier policies are specifically designed to restrict communication and data sharing between different groups or individuals within an organization. You can define rules that prevent users in department1 from sharing files with users in department2 and vice versa.

Insider Risk Management Policy

Explanation: Insider Risk Management policies are used to detect and respond to anomalous user behavior that may indicate insider threats or data breaches. You can configure the policy to monitor file download activities and generate alerts when a user downloads an unusually large volume of sensitive customer data. This can help identify potential data exfiltration attempts

upvoted 5 times

NiucsE Most Recent 5 months, 1 week ago

2nd should be DLP

upvoted 1 times

Question #92 *Topic 1*

HOTSPOT

-

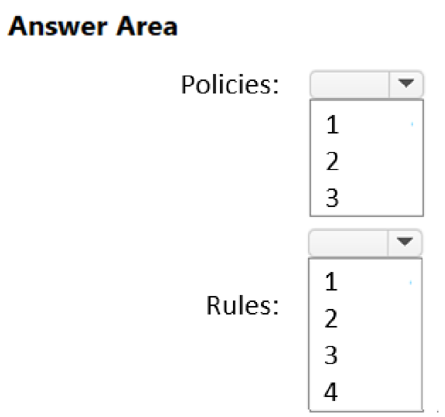
You have a Microsoft 365 subscription.

You identify the following data loss prevention (DLP) requirements:

• Send notifications to users if they attempt to send attachments that contain an EU Social Security Number (SSN) or Equivalent ID.
• Prevent any email messages that contain credit card numbers from being sent outside your organization.
• Block the external sharing of Microsoft OneDrive content that contains EU passport numbers.
• Send administrators email alerts if any rule matches occur.

What is the minimum number of DLP policies and rules you must create to meet the requirements? To answer, select the appropriate options in the answer area.

NOTE: Each correct selection is worth one point.

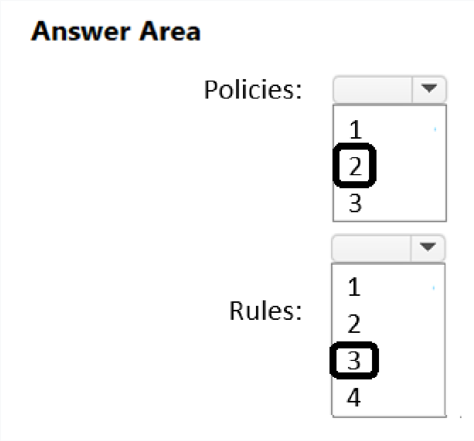


Answer Area

Policies:
1
2
3

Rules:
1
2
3
4

Suggested Answer:



Answer Area

Policies:
1
[✓ 2]
3

Rules:
1
2
[✓ 3]
4

Phil_79 4 months, 3 weeks ago

Actually, to meet the requirements, you need three DLP policies but a total of four rules within those policies:

Policy 1:
Rule to detect EU SSNs and Equivalent IDs and send notifications to users.
Policy 2:
Rule to detect credit card numbers and block emails from being sent outside the organization.
Policy 3:
Rule to detect EU passport numbers and block external sharing of OneDrive content.
finally:

Rule to send administrators email alerts if any rule matches occur (this can be configured within each policy).

So, the minimum number of DLP policies is three, and the minimum number of rules is four

upvoted 3 times

Jideakin 3 months, 3 weeks ago

I disagree. THe first 2 rule can be in the same policy, therefore the answer is correct. 2 policies and 3 rules.

upvoted 2 times

Question #93 Topic 1

HOTSPOT

-

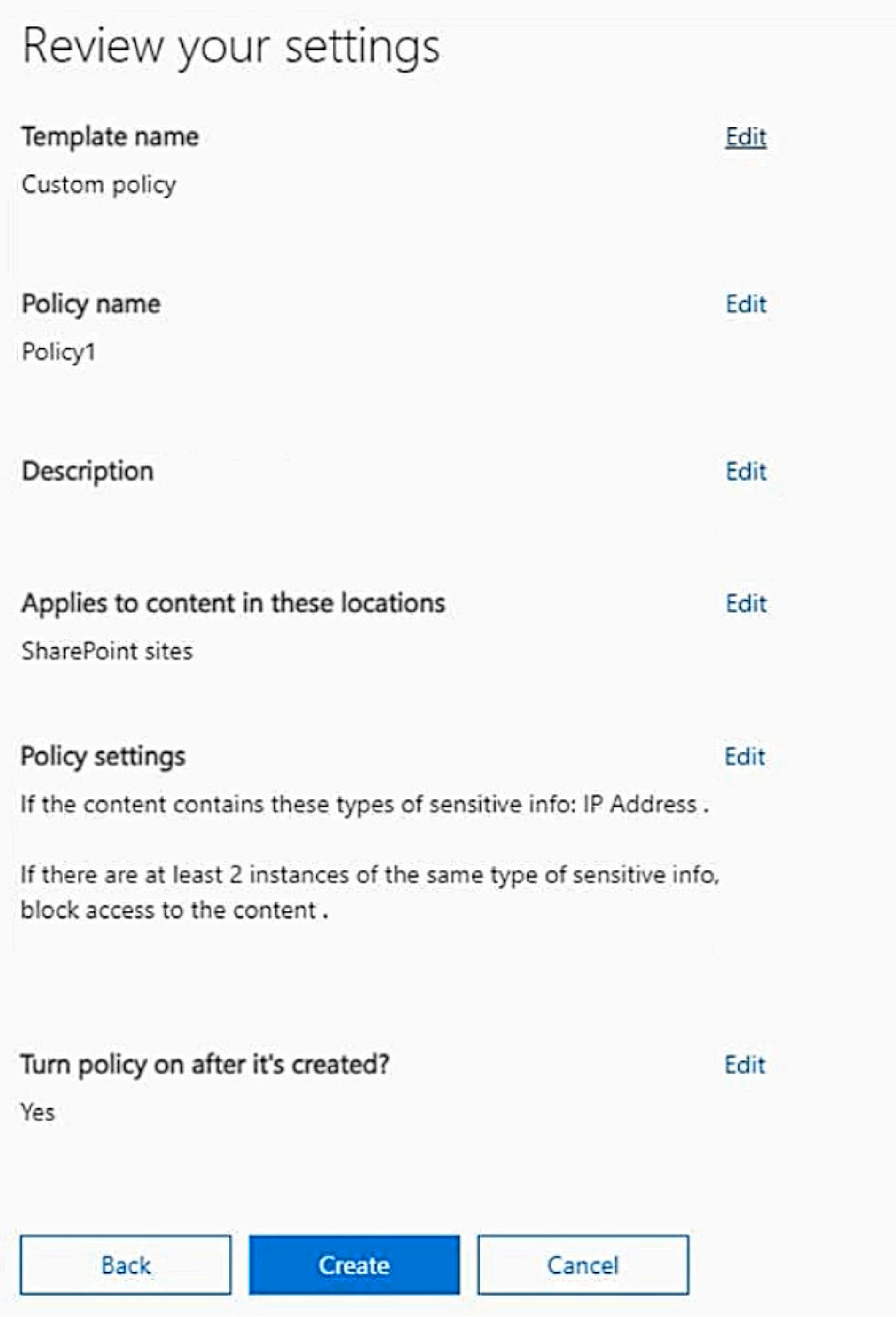
You have a Microsoft E5 subscription that contains two users named User1 and User2.

You have a Microsoft SharePoint site named Site1. Site1 stores files that contain IP addresses as shown in the following table.

Name	Number of IP addresses
File1.txt	3
File2.docx	1

User1 is assigned the SharePoint admin role for Site1. User2 is a member of Site1.

You create the data loss prevention (DLP) policy shown in the following exhibit.



Review your settings

Template name

Custom policy

Policy name

Policy1

Description

Applies to content in these locations

SharePoint sites

Policy settings

If the content contains these types of sensitive info: IP Address .

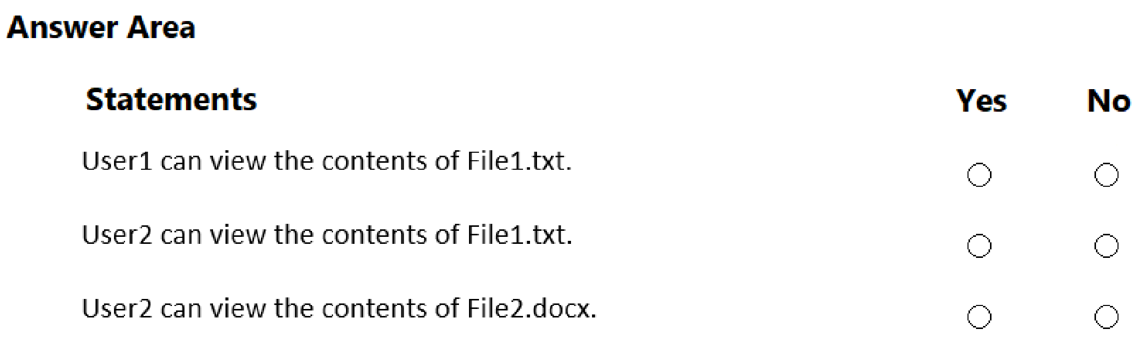
If there are at least 2 instances of the same type of sensitive info, block access to the content .

Turn policy on after it's created?

Yes

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

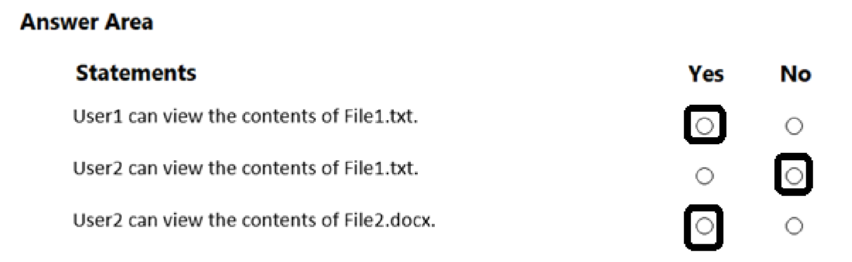
NOTE: Each correct selection is worth one point.



Answer Area

Statements	Yes	No
User1 can view the contents of File1.txt.	○	○
User2 can view the contents of File1.txt.	○	○
User2 can view the contents of File2.docx.	○	○

Suggested Answer:



Answer Area

Statements	Yes	No
User1 can view the contents of File1.txt.	[✓ ○]	○
User2 can view the contents of File1.txt.	○	[✓ ○]
User2 can view the contents of File2.docx.	[✓ ○]	○

JambonBlanc 2 months, 1 week ago

Answer is correct:

User1 can view the contents of File1.txt: YES
User1, being the SharePoint admin for Site1, has unrestricted access to all files on the site, regardless of the DLP policy configuration.

User2 can view the contents of File1.txt: NO
The DLP policy blocks access to content containing at least two instances of IP addresses. Since File1.txt contains three instances of IP addresses, User2 cannot access it due to the policy enforcement.

User2 can view the contents of File2.docx: YES
File2.docx contains only one instance of an IP address, which does not meet the DLP policy's threshold of at least two instances. Therefore, User2 can access File2.docx.

upvoted 3 times

ca7859c 2 months ago

Correct

upvoted 1 times

Phil_79 4 months, 3 weeks ago

No, No, Yes:
DLP policies applied to files applies even if the accessing user is a site admin, so User1 and User2 are both blocked while accessing File1.txt. File2 contains only 1 IP and does not trigger the rule

upvoted 2 times

Question #94 *Topic 1*

You have a Microsoft 365 E5 subscription that uses retention label policies.

You need to identify all the changes made to retention labels during the last 30 days.

What should you use in the Microsoft Purview compliance portal?

A. User data search

B. Reports

C. Content search

D. Activity explorer

Correct Answer: *D*

JambonBlanc 2 months, 1 week ago

Selected Answer: D

The answer is correct: D

Activity explorer is the tool in Microsoft Purview that tracks changes and activities related to various compliance features, including retention labels. It provides detailed logs and insights for auditing and monitoring purposes.

upvoted 1 times

Question #95 *Topic 1*

You have a Microsoft 365 E5 subscription.

You use the following services:

- Microsoft Teams
- Microsoft Entra ID
- Microsoft OneDrive
- Microsoft Exchange Online
- Microsoft SharePoint Online

Which two services can you monitor by using Microsoft Purview communication compliance? Each correct answer presents a complete solution.

NOTE: Each correct selection is worth one point.

A. SharePoint Online

B. Exchange Online

C. Microsoft Entra ID

D. OneDrive

E. Teams

Correct Answer: *BE*

ca7859c 1 month, 3 weeks ago

Selected Answer: BE

https://learn.microsoft.com/en-us/purview/communication-compliance#integration-with-microsoft-365-services
Exchange Online
Microsoft Teams
Viva Engage
Among others

upvoted 1 times

JambonBlanc 2 months, 1 week ago

Selected Answer: BE

Correct answer: BE

B. Exchange Online: Communication compliance monitors email communications for policy violations, ensuring compliance with regulations or organizational policies.

E. Teams: Microsoft Teams conversations and chats can also be monitored for compliance purposes, detecting sensitive or non-compliant communication.

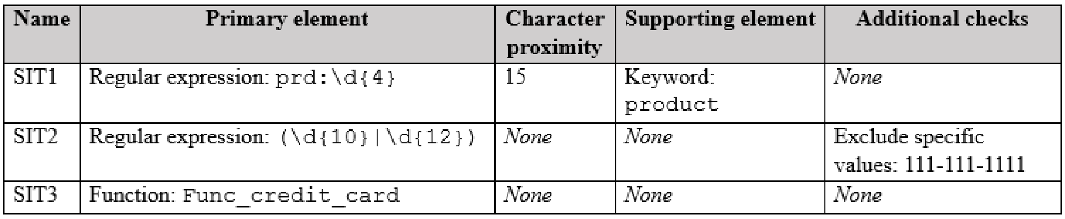
upvoted 1 times

Question #96 *Topic 1*

HOTSPOT

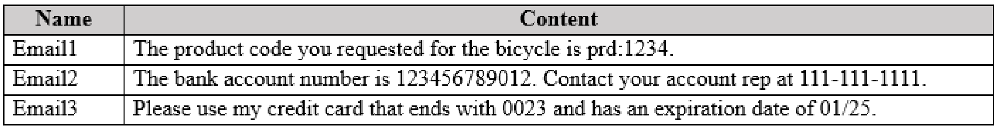
-

You have a Microsoft 365 E5 subscription that contains the sensitive information types (SITs) shown in the following table.



Name	Primary element	Character proximity	Supporting element	Additional checks
SIT1	Regular expression: `prd:\d{4}`	15	Keyword: `product`	*None*
SIT2	Regular expression: `(\d{10}|\d{12})`	*None*	*None*	Exclude specific values: 111-111-1111
SIT3	Function: `Func_credit_card`	*None*	*None*	*None*

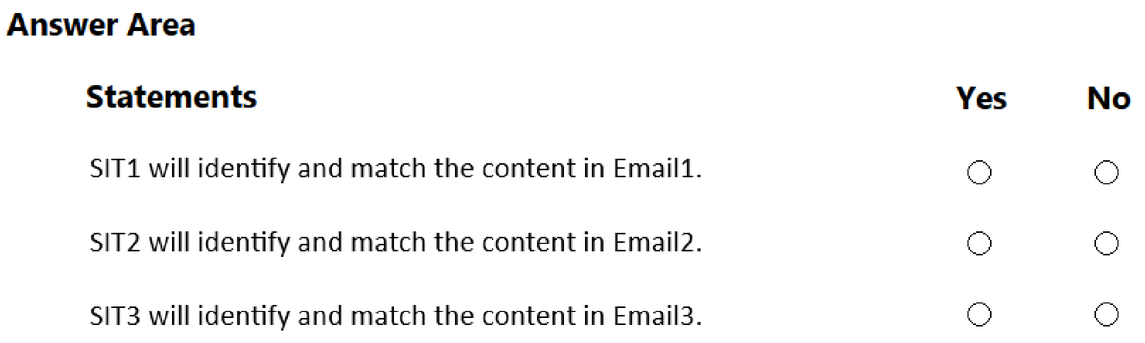
A user sends the email messages shown in the following table.



Name	Content
Email1	The product code you requested for the bicycle is prd:1234.
Email2	The bank account number is 123456789012. Contact your account rep at 111-111-1111.
Email3	Please use my credit card that ends with 0023 and has an expiration date of 01/25.

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

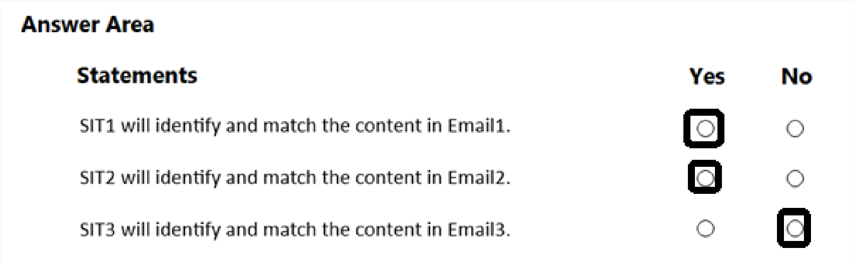
NOTE: Each correct selection is worth one point.



Answer Area

Statements	Yes	No
SIT1 will identify and match the content in Email1.	○	○
SIT2 will identify and match the content in Email2.	○	○
SIT3 will identify and match the content in Email3.	○	○

Suggested Answer:



Answer Area

Statements	Yes	No
SIT1 will identify and match the content in Email1.	[✓ ○]	○
SIT2 will identify and match the content in Email2.	[✓ ○]	○
SIT3 will identify and match the content in Email3.	○	[✓ ○]

ca7859c 2 months ago

Additional checks in sensitive info types are for testing and not actually excluding things.

So, SIT2 will identify 111-111-1111

upvoted 1 times

Phil_79 4 months, 1 week ago

I have a doubt about the first one: the supporting element is more than 15 character away from the primary element match... in this situation there shouldn't be a match... Any idea?

upvoted 2 times

Jideakin 3 months, 3 weeks ago

you're right. I tested it

upvoted 1 times

⊟ **ICTSBRD** 5 months, 2 weeks ago

Shouldn't SIT2 be 'No', since there is an exclude on 111-111-1111?

upvoted 1 times

⊟ **Jideakin** 3 months, 3 weeks ago

The exclude doesn't work like. What is means is that if you have for example 123456111-111-1111789012. It will ignore the 111-111-1111 and still see the number as 123456789012

upvoted 1 times

⊟ **Phil_79** 4 months, 3 weeks ago

Nope 'cause the regex matches the 123456789012 number, in this case the exclusion should not have effect

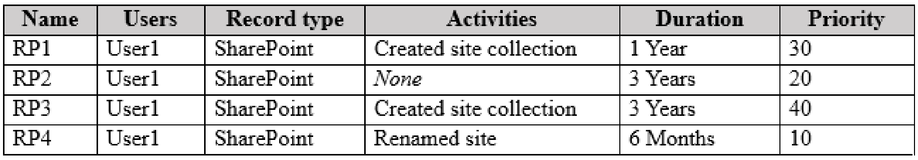
upvoted 1 times

HOTSPOT

-

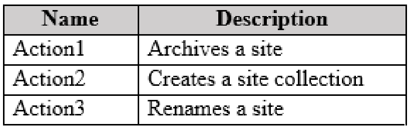
You have a Microsoft 365 E5 subscription that uses Microsoft Purview Audit (Premium) with the 10-Year Audit Log Retention add-on license.

The subscription contains the audit retention policies shown in the following table.



Name	Users	Record type	Activities	Duration	Priority
RP1	User1	SharePoint	Created site collection	1 Year	30
RP2	User1	SharePoint	*None*	3 Years	20
RP3	User1	SharePoint	Created site collection	3 Years	40
RP4	User1	SharePoint	Renamed site	6 Months	10

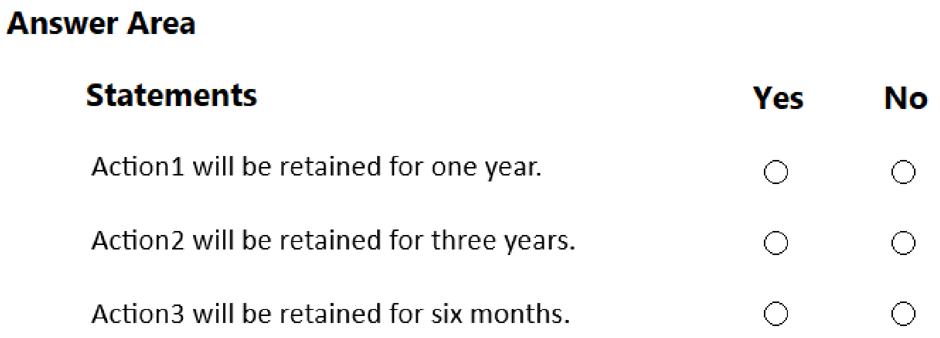
From the SharePoint Online admin center, User1 performs the actions shown in the following table.



Name	Description
Action1	Archives a site
Action2	Creates a site collection
Action3	Renames a site

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

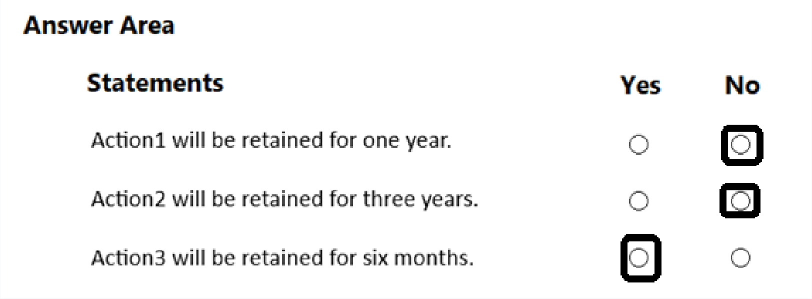
NOTE: Each correct selection is worth one point.



Answer Area

Statements	Yes	No
Action1 will be retained for one year.	○	○
Action2 will be retained for three years.	○	○
Action3 will be retained for six months.	○	○

Correct Answer:



Answer Area

Statements	Yes	No
Action1 will be retained for one year.	○	[✓ ○]
Action2 will be retained for three years.	○	[✓ ○]
Action3 will be retained for six months.	[✓ ○]	○

ca7859c 2 months ago

Retention labels with a longer retention period take precedence even if they have a lower priority (An effort by Microsoft to preserve data)

upvoted 1 times

ca7859c 1 month, 3 weeks ago

Answer: NYY

upvoted 1 times

JambonBlanc 2 months, 1 week ago

The correct answer is: NO, YES, YES

Action1: Archives a site

* None of the audit retention policies explicitly match the activity "Archives a site."

* Conclusion: Action1 will not be retained for one year. No.

Action2: Creates a site collection

* Policies RP1 and RP3 both apply to the activity "Creates a site collection." However:

- RP1 retains for 1 year with priority 30.

- RP3 retains for 3 years with priority 40 (higher priority than RP1).

* Conclusion: Action2 will be retained for 3 years. Yes.

Action3: Renames a site

* RP4 explicitly matches the activity "Renames a site" and retains it for 6 months.

* Conclusion: Action3 will be retained for 6 months. Yes.

upvoted 2 times

⊟ **Jideakin** 3 months, 3 weeks ago

I believe the answer is NYY

upvoted 1 times

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

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

Community vote distribution

A (71%) B (29%)

⊟ **olsi** Highly Voted 👍 3 years, 7 months ago
Correct
upvoted 9 times

⊟ **Eltooth** Highly Voted 👍 3 years, 5 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 5 times

⊟ **ChrisBaird** Most Recent ⏲ 6 months, 3 weeks ago
Selected Answer: A
Devices onboarded via Defender are automatically shown in the Purview portal.
upvoted 2 times

⊟ **Gesbie** 1 year, 4 months ago
was on Exam August 9, 2023
upvoted 1 times

⊟ **xswe** 1 year, 8 months ago
To be able to deploy Endpoint DLP you need to ensure that you devices are onboarded.
upvoted 1 times

⊟ **Abhishek1610** 2 years, 1 month ago
Selected Answer: A
Correct Answer A
upvoted 3 times

⊟ **aclondon** 2 years, 5 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 2 years, 8 months ago

The answer is A - Yes.

upvoted 1 times

JrGreen 2 years, 9 months ago

Selected Answer: A

A is right

upvoted 4 times

olsenOnS 2 years, 10 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 2 years, 10 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 2 years, 11 months ago

Selected Answer: B

MDE is not required for the DLP to manage.

upvoted 4 times

> **Jonclark** 1 year, 9 months 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 2 years, 11 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

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

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

Community vote distribution

B (82%) (18%)

ExamReviewerIZ Highly Voted 3 years, 2 months 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 8 times

ExamReviewerIZ 3 years, 2 months 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 13 times

Domza 1 year ago
dude, how did you come up with the name? LOL
upvoted 2 times

sergioandreslq 3 years 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 5 times

wooyourdaddy Highly Voted 2 years, 6 months ago
Selected Answer: B
I wrote the exam today, this question was on it, I choose B, scored 890!
upvoted 7 times

Domza 1 year ago
the Best!
upvoted 3 times

Ruslan23 Most Recent 8 months, 2 weeks ago
Selected Answer: B
use the DLP policy matches report
upvoted 2 times

emartiy 10 months, 1 week ago

Selected Answer: B

B is correct.

upvoted 1 times

Domza 1 year ago

Ladies and Gents,

Did you know can now manage your DLP alerts in the Microsoft Defender portal? Alerts are automatically combined into incidents, which provide a comprehensive view into potential policy violations and advanced tools for investigation and remediation.

Enjoy

upvoted 2 times

heshmat2022 1 year, 2 months ago

IT WAS ON EXAM OCTOBER 18 2023

upvoted 2 times

Gesbie 1 year, 4 months ago

was on Exam August 9, 2023

upvoted 2 times

heshmat2022 1 year, 4 months ago

YOU DID NOT MENTION WHAT WAS THE RIGHT ANSWER THOUGH.

upvoted 2 times

Domza 1 year ago

Haha LOL

upvoted 2 times

Ruslan23 8 months, 2 weeks ago

You didn't too LOL

upvoted 1 times

xswe 1 year, 8 months 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

LoNwUi2uprVHKCX9IlpE 2 years, 7 months ago

On exam 11/05/2022

upvoted 1 times

mT3 2 years, 8 months ago

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 1 year, 3 months ago

ok, thank you

upvoted 1 times

Holii 2 years, 8 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 2 years, 10 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 2 years, 11 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

Suggested 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 4 years 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 25 times

Eltooth Highly Voted 4 years, 1 month ago
You can use Power Automate to trigger an alert to send a message into a Teams channel.
upvoted 10 times

Eltooth 3 years, 12 months ago
Answer should be Yes
upvoted 8 times

trut_hz Most Recent 5 months, 1 week ago
Selected Answer: B
Configure the File Policy with Data Classification Service:

Set up a file policy in Microsoft Defender for Cloud Apps that uses the Data Classification Service to detect files containing credit card numbers.
Integrate with Microsoft Power Automate:

Create a flow in Power Automate that triggers when an alert is generated in Defender for Cloud Apps.
Within this flow, define actions to:
Send an email notification to the file owner.
Post a message to the specific Microsoft Teams channel associated with the affected department.
upvoted 2 times

husamshahin 11 months, 1 week ago
on Exam 28-7-2024
upvoted 1 times

emartiy 1 year, 4 months ago
Selected Answer: A
A - seems correct
upvoted 1 times

mbhasker 1 year, 7 months ago
ans: No
upvoted 1 times

mbhasker 1 year, 7 months ago

ans: B. No

upvoted 1 times

Gesbie 1 year, 10 months ago

was on Exam August 9, 2023

upvoted 2 times

xswe 2 years, 2 months ago

Microsoft Power Automate are needed to be able to get alerts sent to Microsoft Teams.

upvoted 4 times

NinjaSchoolProfessor 2 years, 6 months 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 2 years, 7 months ago

A should be the answer

upvoted 1 times

GGFiogos 2 years, 9 months ago

reference link is 404 for me

upvoted 1 times

> **NinjaSchoolProfessor** 2 years, 6 months ago
>
> There's a space between those two URLs, look again.
>
> upvoted 1 times

Lion007 2 years, 10 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

JamesM9 3 years, 2 months ago

The answer here is A - Yes.

upvoted 1 times

ayush0312 3 years, 3 months ago

Yes is the correct ans

upvoted 1 times

crista_ 3 years, 3 months ago

Yes is correct answer

upvoted 2 times

PrettyFlyWifi 3 years, 5 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

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

Suggested 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 👍 3 years 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 23 times

⊟ **luissaro** Highly Voted 👍 1 year, 2 months 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 18 times

⊟ **mbhasker** Most Recent ⊙ 7 months ago
ans: NO
upvoted 1 times

⊟ **heshmat2022** 8 months, 2 weeks ago
IT WAS ON EXAM OCTOBER 18 2023
upvoted 1 times

⊟ **dmoorthy** 1 year, 2 months ago
Answer is B.
upvoted 1 times

⊟ **xswe** 1 year, 2 months ago
Microsoft Power Automate are needed to be able to get alerts sent to Microsoft Teams.
upvoted 1 times

⊟ **wooyourdaddy** 1 year, 4 months 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 3 times

Rockalm 1 year, 5 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, 7 months ago

A (Yes) should be the answer.

upvoted 2 times

wooyourdaddy 2 years ago

Selected Answer: A

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

upvoted 3 times

JamesM9 2 years, 2 months ago

The answer here is A - Yes.

upvoted 1 times

Pravda 2 years, 5 months ago

On exam 1/20/2022

upvoted 1 times

CalST 2 years, 6 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** 2 years, 6 months ago
>
> My bad - you can indeed.
>
> upvoted 1 times

Zorolloo 2 years, 6 months ago

Question 4 and 26 are the same?

upvoted 1 times

Zorolloo 2 years, 6 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, 11 months ago
>
> english bitte
>
> upvoted 3 times

Eltooth 2 years, 12 months ago

Answer should be Yes

upvoted 8 times

Anker 3 years 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.

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

Community vote distribution
CD (68%) CE (32%)

⊟ **Azurefox79** Highly Voted 👍 2 years, 4 months 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 16 times

⊟ **mcas** Highly Voted 👍 2 years, 8 months 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 8 times

⊟ **fimbulvetrk** 2 years, 7 months ago
agreed, I'd go with C and E
upvoted 2 times

⊟ **Azurefox79** 2 years, 4 months 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** 2 years, 4 months 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

Domza 1 year, 7 months ago

"any cloud service" it means - OneDrive, SharePoint that kind of services :)

upvoted 1 times

Jideakin 3 months, 3 weeks ago

Yep! The focus of the question is on the browsers. You don't want the uploading with those browsers at all. The way to achieve that is to block those browsers. And to ensure that goes into effect for all users, you need to ensure that all devices are onboarded. CD

upvoted 1 times

Jideakin Most Recent 3 months, 3 weeks ago

Selected Answer: CD

The focus of the question is on the browsers. You don't want the uploading with those browsers at all. The way to achieve that is to block those browsers. And to ensure that goes into effect for all users, you need to ensure that all devices are onboarded. CD

upvoted 1 times

NICKTON81 1 year ago

Selected Answer: CD

C and D

upvoted 1 times

emartiy 1 year, 4 months ago

Selected Answer: CD

Since question says block "From Chrome and Firefox to any services". So, we need to block users to upload confidential items being uploaded via Chrome and Firefox with an onboarded device it can be granularly managed and blocked.

upvoted 2 times

Arloo 1 year, 6 months ago

It's B and C. We must assume devices have already been onboarded. Adding Chrome and Firefox as unallowed browsers in Endpoint DLP does nothing unless you then create a DLP policy targeted at devices and enforce the unauthorized browsers block. I just tested this in Purview Compliance Center. Without an associated DLP policy targeted at devices, marking unallowed browsers in Endpoint DLP does nothing.

upvoted 1 times

Futfuyfyjfj 1 year, 4 months ago

You shouldn't assume that. The question starts with you are using/implementing DLP. Nothing is said about ENDPOINT DLP...

upvoted 1 times

mbhasker 1 year, 7 months ago

ans: CD

upvoted 1 times

Domza 1 year, 7 months 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 year, 8 months 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 1 year, 9 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 1 year, 10 months 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 2 years 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 3 times

xswe 2 years, 2 months 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 3 times

UnDarisp 2 years, 4 months 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 2 years, 4 months ago

No. A has nothing to do with the question at all. CD is correct.

upvoted 1 times

Harry008 2 years, 7 months 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 2 years, 4 months 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 2 times

BTL_Happy 2 years, 7 months ago

I will go with C & E

upvoted 3 times

Question #6 Topic 2

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:

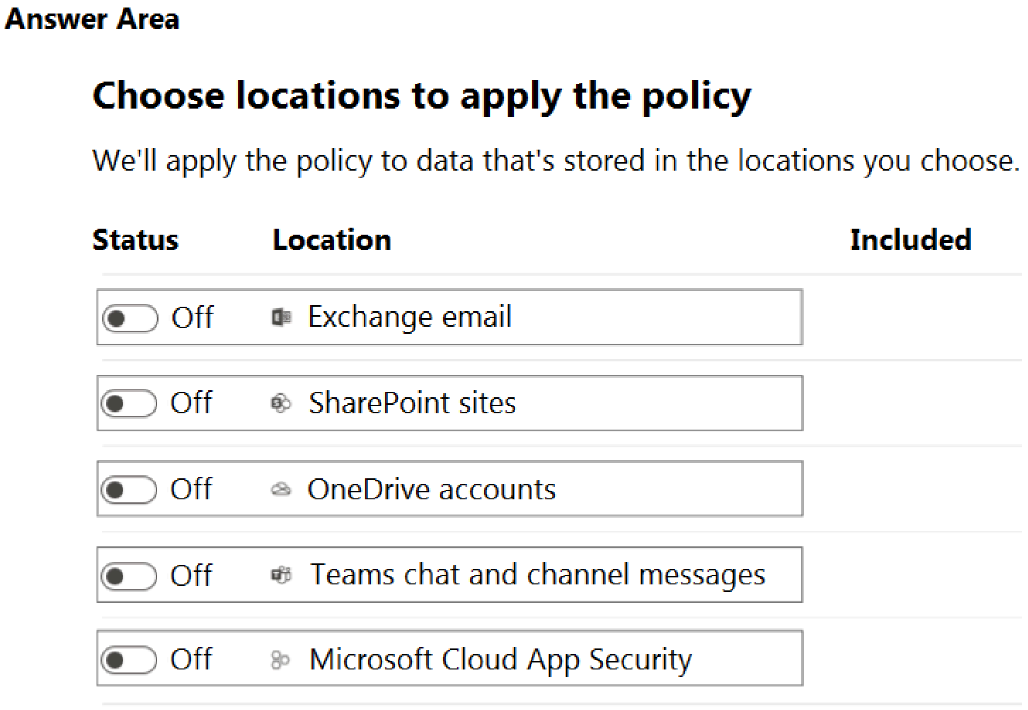
✑ Documents that contain sensitive information must not be shared inappropriately in Microsoft Teams.

✑ 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:



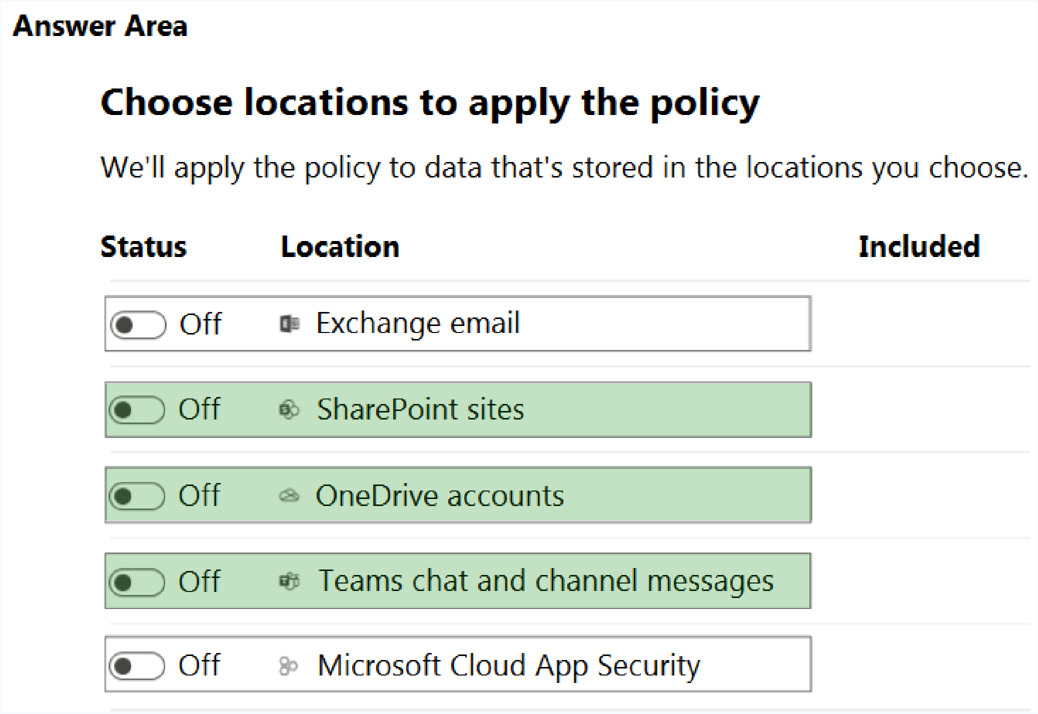
Answer Area

Choose locations to apply the policy

We'll apply the policy to data that's stored in the locations you choose.

Status	Location	Included
Off	Exchange email	
Off	SharePoint sites	
Off	OneDrive accounts	
Off	Teams chat and channel messages	
Off	Microsoft Cloud App Security	

Suggested Answer:



Answer Area

Choose locations to apply the policy

We'll apply the policy to data that's stored in the locations you choose.

Status	Location	Included
Off	Exchange email	
Off	[✓ SharePoint sites]	
Off	[✓ OneDrive accounts]	
Off	[✓ Teams chat and channel messages]	
Off	Microsoft Cloud App Security	

Reference:

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

Eltooth Highly Voted 3 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 17 times

JakubK64 Highly Voted 👍 3 years, 5 months ago

Looks correct. Teams use SharePoint and OneDrive to store files

upvoted 8 times

Domza Most Recent ⊙ 12 months ago

Looks good! Easy breezy~

upvoted 1 times

heshmat2022 1 year, 2 months ago

IT WAS ON EXAM OCTOBER 18 2023

upvoted 1 times

xswe 1 year, 8 months 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 2 years, 6 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 2 years, 11 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 2 years, 11 months ago

On exam 1/20/2022

upvoted 1 times

HardcodedCloud 3 years 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 3 years, 2 months ago

I think that we should include and MACS because only there is the option delete message available

upvoted 1 times

xofowi5140 3 years, 5 months ago

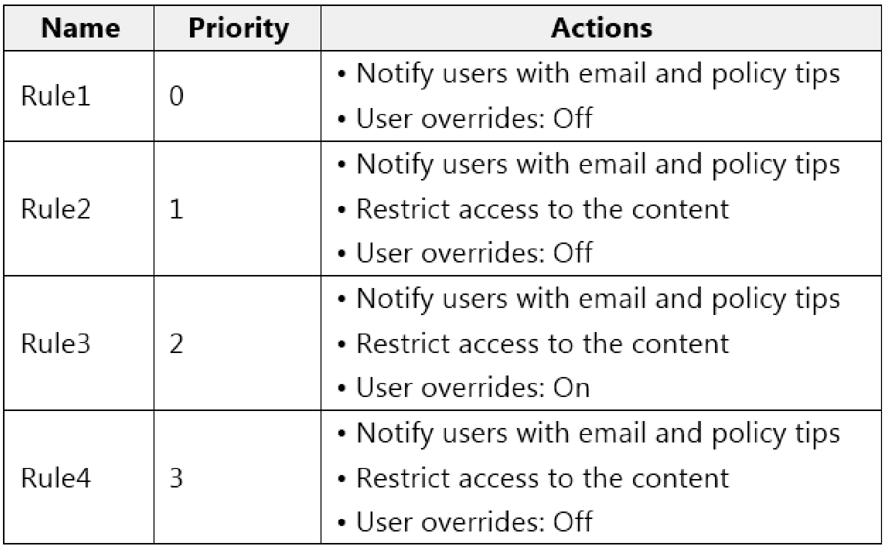
Why not Exchange email?

upvoted 1 times

Question #7 Topic 2

HOTSPOT -

You have a data loss prevention (DLP) policy that has the advanced DLP rules shown in the following table.



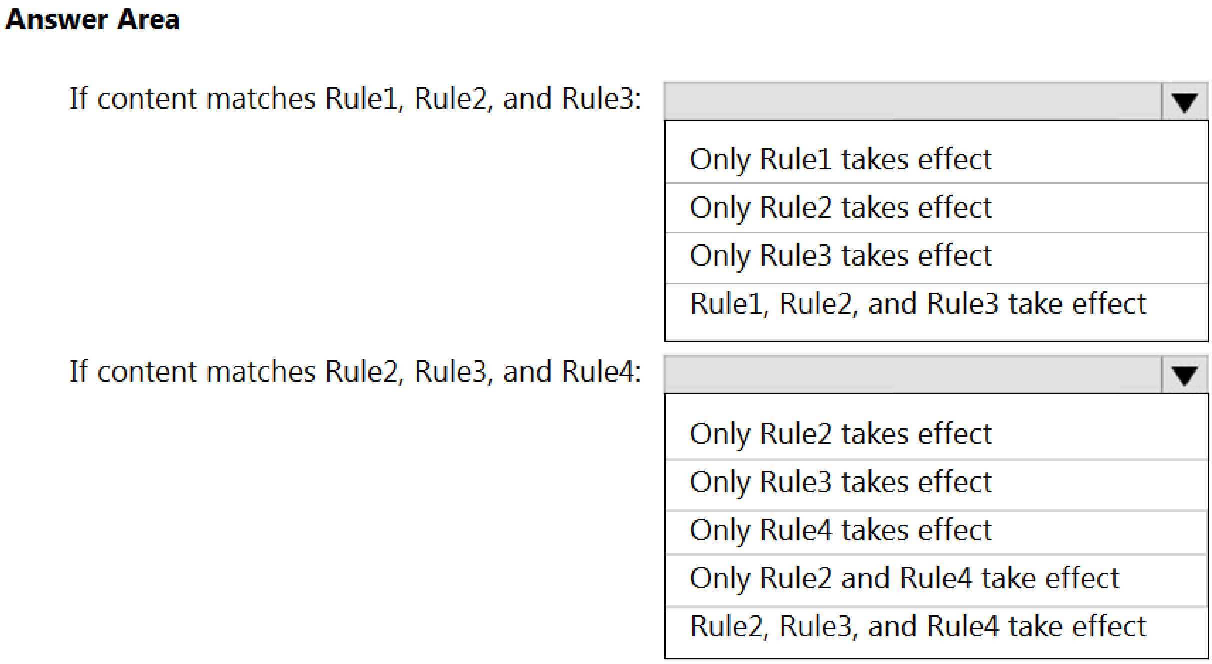
Name	Priority	Actions
Rule1	0	• Notify users with email and policy tips • User overrides: Off
Rule2	1	• Notify users with email and policy tips • Restrict access to the content • User overrides: Off
Rule3	2	• Notify users with email and policy tips • Restrict access to the content • User overrides: On
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

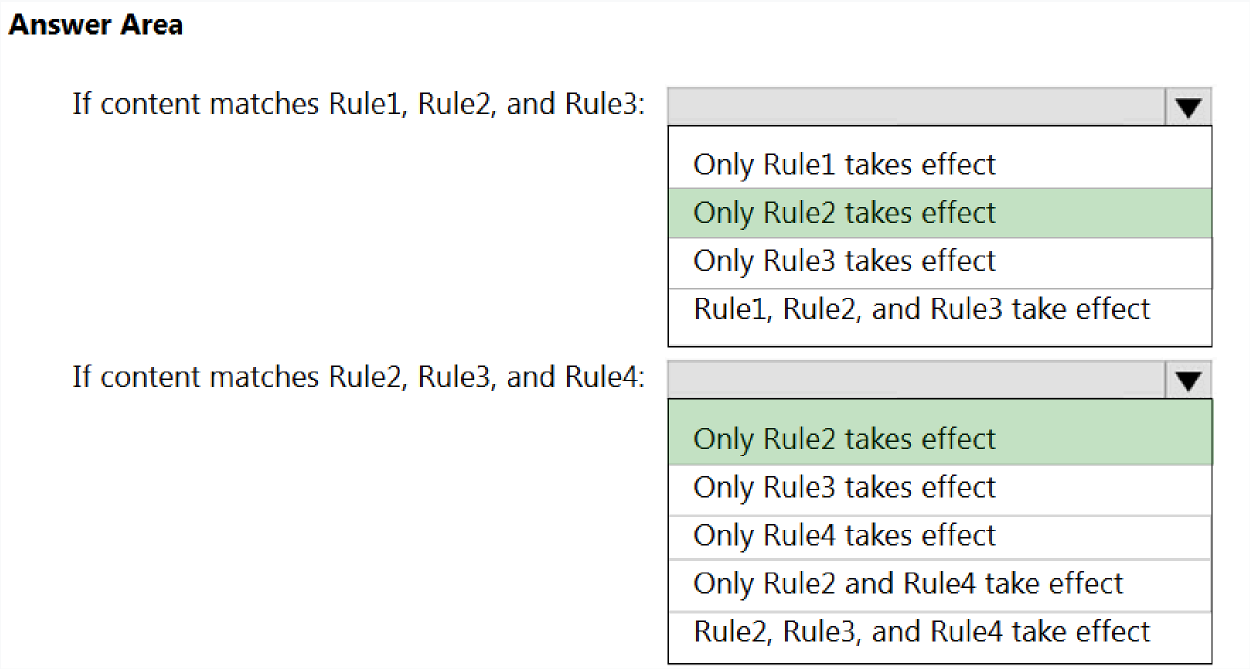
If content matches Rule1, Rule2, and Rule3: ▼

- 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

Suggested 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 3 years, 12 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 17 times

⊟ **sergioandreslq** 3 years, 6 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** 3 years, 6 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 2 times

⊟ **McAlec** Highly Voted 3 years, 8 months ago

Correct, but right reference is

https://docs.microsoft.com/en-us/microsoft-365/compliance/dlp-policy-reference?view=o365-worldwide

upvoted 5 times

⊟ **husamshahin** Most Recent 11 months, 1 week ago on Exam 28-7-2024

upvoted 1 times

⊟ **xswe** 2 years, 2 months 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** 3 years, 5 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

Suggested 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, 3 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 16 times

sergioandreslq 2 years 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, 5 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 7 times

bowlinbd 2 years, 4 months ago
Should be Yes. Deploying the package is what onboards the devices into the Compliance portal.
upvoted 13 times

kiketxu 1 year, 2 months 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 8 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** 1 year 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

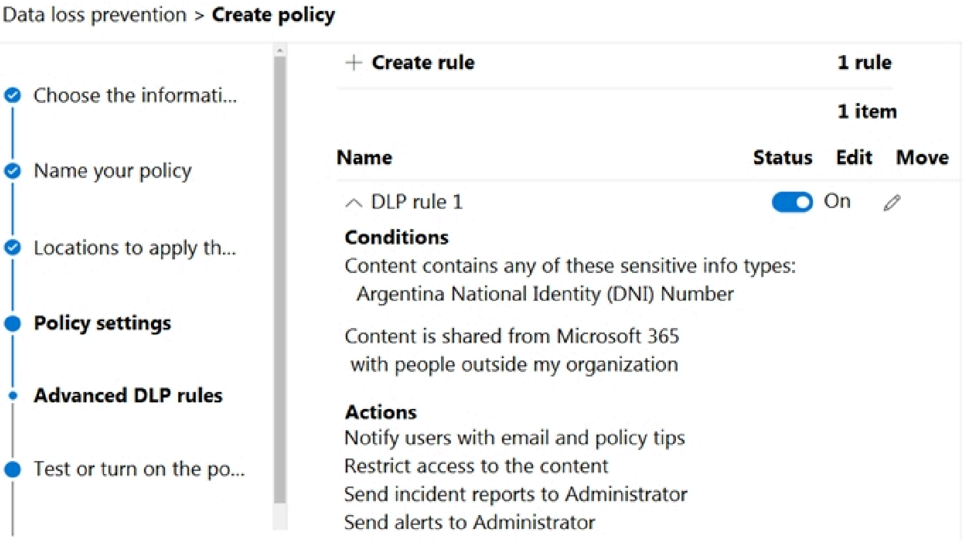
⊟ **PrettyFlyWifi** 1 year, 11 months ago

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

Question #9 *Topic 2*

You create a data loss prevention (DLP) policy. The Advanced DLP rules page is shown in the Rules exhibit.



Data loss prevention > **Create policy**

- Choose the informati...
- Name your policy
- Locations to apply th...
- **Policy settings**
- **Advanced DLP rules**
- Test or turn on the po...

+ **Create rule** **1 rule**

1 item

Name	**Status**	**Edit**	**Move**
^ DLP rule 1	On	✎	

Conditions

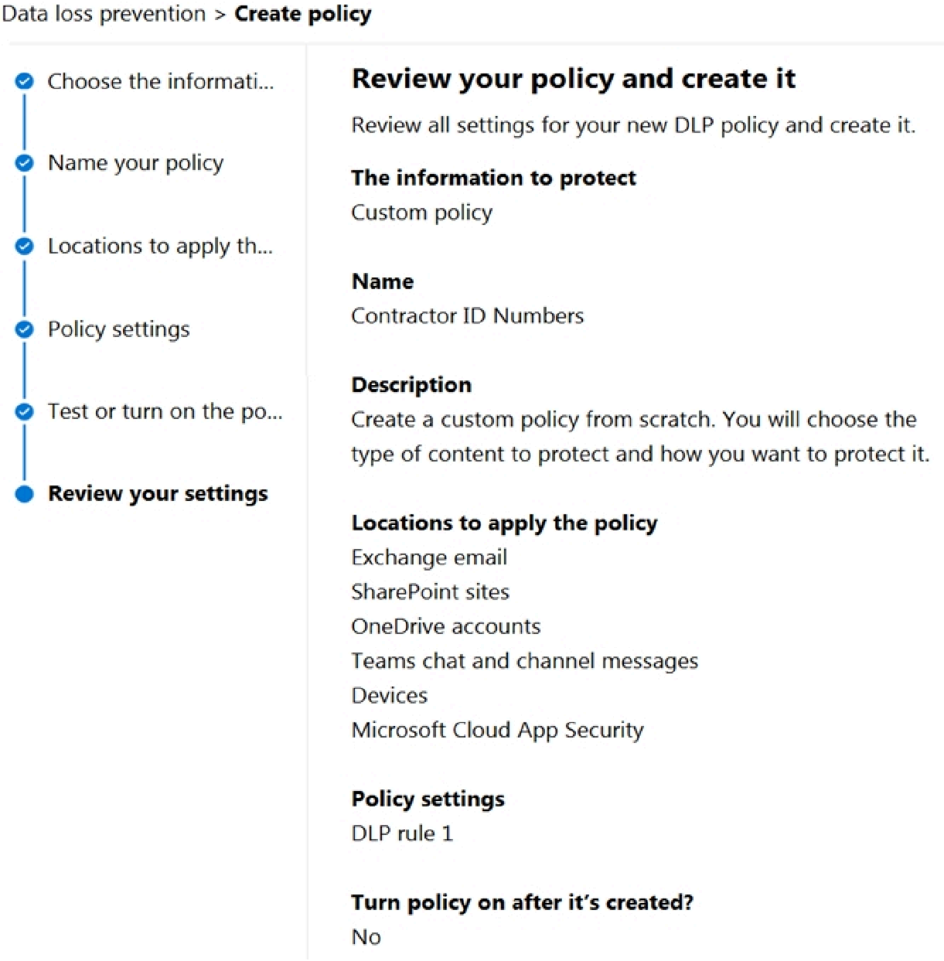
Content contains any of these sensitive info types:
Argentina National Identity (DNI) Number

Content is shared from Microsoft 365
with people outside my organization

Actions

Notify users with email and policy tips
Restrict access to the content
Send incident reports to Administrator
Send alerts to Administrator

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



Data loss prevention > **Create policy**

- Choose the informati...
- Name your policy
- Locations to apply th...
- Policy settings
- Test or turn on the po...
- **Review your settings**

Review your policy and create it

Review all settings for your new DLP policy and create it.

The information to protect
Custom policy

Name
Contractor ID Numbers

Description
Create a custom policy from scratch. You will choose the type of content to protect and how you want to protect it.

Locations to apply the policy
Exchange email
SharePoint sites
OneDrive accounts
Teams chat and channel messages
Devices
Microsoft Cloud App Security

Policy settings
DLP rule 1

Turn policy on after it's created?
No

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.

Suggested 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 2 years, 11 months ago

Selected Answer: D

d is right

upvoted 7 times

emartiy Most Recent 10 months, 1 week ago

Selected Answer: D

Of course - D Whitout impact, you need to test it with all actions selections.

upvoted 1 times

Domza 1 year, 1 month ago

Correct -D

upvoted 1 times

ServerBrain 1 year, 3 months ago

Selected Answer: D

do is the only option that is closer to audit mode

upvoted 1 times

xswe 1 year, 8 months 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 2 years ago

Answer [D] - https://learn.microsoft.com/en-us/microsoft-365/compliance/create-test-tune-dlp-policy

upvoted 1 times

Marzie 2 years, 1 month 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** 1 year, 1 month ago
>
> IF you remove the "Actions" nothing will happen lol
>
> upvoted 1 times

wooyourdaddy 2 years, 6 months ago

Selected Answer: D

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

upvoted 1 times

Eltooth 3 years, 5 months ago

Correct answer is D

upvoted 4 times

> **sergioandreslq** 3 years 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 3 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

Suggested Answer: *A*

Community vote distribution

A (100%)

PrettyFlyWifi Highly Voted 👍 3 years, 4 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 9 times

Kuteron 8 months, 1 week ago

i don't can find "contains any of these sensitive info types" under the messages so i guess you are wrong.

upvoted 1 times

andreane Most Recent 1 year, 5 months ago

In Purview - Create DLP rule - location Exchange - Content Contains : Sensitive Info type : Azure Storage Key

upvoted 1 times

andreane 1 year, 5 months ago

Seems outdated, here is the message in Exchange :
DLP policies and DLP-related conditions and actions in Mail flow rules are no longer supported and can no longer be created or edited in the Exchange Admin Center (EAC) or using Exchange Online PowerShell. We recommend migrating all DLP-related rules to Microsoft Purview DLP in the compliance center as soon as possible. Once you have migrated these rules please delete them here in the EAC or via PowerShell. Learn more: Migrate DLP policies | No DLP-conditions or actions
https://compliance.microsoft.com/datalossprevention?viewid=policies&redirectedFromEAC=true

upvoted 3 times

luissaro 2 years, 2 months ago

shouldn't you first set the ome config?

upvoted 1 times

xswe 2 years, 2 months 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 3 years, 5 months ago

On exam 1/20/2022

upvoted 2 times

digitallycan 3 years, 8 months 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 3 years, 6 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** 3 years, 6 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** 3 years, 11 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** 3 years, 11 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

Suggested Answer: *B*

Community vote distribution

B (63%) A (38%)

Eltooth Highly Voted 3 years, 11 months ago

Correct - no. Mail flow rules are needed.

upvoted 8 times

ExamReviewerIZ 3 years, 8 months 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 15 times

Jideakin 3 months, 3 weeks ago

Both of you are partially correct. You can do it from DLP without a mail flow rule, but when you select all location, the action relating to sending encrypted email will not be available because it doesn't relate to all locations. Therefore the correct answer is No.

upvoted 2 times

Sam12 3 years, 5 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 3 years, 3 months ago

But not if you have "all locations" selected.

upvoted 8 times

Lion007 2 years, 10 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 7 times

PrettyFlyWifi Highly Voted 3 years, 5 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 6 times

narenbabu.chintu Most Recent 11 months, 3 weeks ago

DLP is needed, but not all locations have to be selected.

upvoted 1 times

ChrisBaird 1 year ago

Selected Answer: A

A DLP policy only requires the "Content Contains" condition, which is available for all locations. Add the SIT to the condition, et voila! The answer is A.

upvoted 1 times

ServerBrain 1 year, 9 months ago

Selected Answer: B

selecting all locations will not suffice

upvoted 1 times

xswe 2 years, 2 months 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 2 times

music_man 2 years, 9 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 3 times

Lion007 2 years, 10 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

nupagazi 3 years, 5 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

Pravda 3 years, 5 months ago

On exam 1/20/2022

upvoted 2 times

Sam12 3 years, 5 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 3 years, 5 months ago

I don't find the action encrypt message in DLP polic

upvoted 1 times

RAMmulator 3 years, 6 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 3 years, 6 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 3 years, 8 months 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

Suggested Answer: *B*

Community vote distribution

A (64%) B (36%)

Jideakin 3 months, 3 weeks ago

Selected Answer: A

Because Exchange is the only location selected, DLP policy will be sufficient for this.

upvoted 1 times

emartiy 1 year, 4 months ago

Selected Answer: B

The solution presented in the question is not sufficient to meet the stated goal of ensuring that Azure Storage keys are encrypted when emailed.

The solution involves creating a data loss prevention (DLP) policy that has only the Exchange email location selected. This would mean that the DLP policy only applies to emails sent from Exchange, but it does not ensure that the content of the email, including Azure Storage keys, is encrypted.

To ensure that Azure Storage keys are encrypted when emailed, a more comprehensive solution is required. One possible solution would be to configure Azure Information Protection (AIP) to automatically classify and protect sensitive data, including Azure Storage keys.

upvoted 4 times

bgurny 1 year, 9 months 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 3 times

Emmuyah 11 months ago

Yes! You can set up mail flow rules in Exchange Online or by using DLP in the Microsoft Purview compliance portal.

upvoted 2 times

dmoorthy 2 years, 2 months ago

Answer is A- Yes.

upvoted 3 times

xswe 2 years, 2 months 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 2 years, 4 months ago

Selected Answer: A

Since Exchange is the only location selected, it is possible to meet the goal with a DLP policy.

upvoted 3 times

kingAzure 1 year, 7 months ago

I thought there could only be one "yes" on these series of questions?

upvoted 1 times

Ruslan23 1 year, 2 months ago

"Some question sets might have more than one correct solution"

upvoted 1 times

biff791 2 years, 5 months ago

Selected Answer: A

works if only exchange location is selected

upvoted 2 times

Harry008 2 years, 7 months 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 2 years, 7 months ago

A should be the answer, only on exchange location is selected.

upvoted 1 times

kiketxu 2 years, 8 months 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

fimbulvetrk 2 years, 7 months ago

you may have a sensitive info type based in a keyword list which may have contain all the storage keys

upvoted 1 times

Reinto 2 years, 4 months 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 2 years, 4 months ago

Never mind: Document does not equal attachment and this rule option is not relevant, I suspect.

upvoted 1 times

chrissempai 2 years, 9 months ago

Selected Answer: A

The answer is A

you have only exchange selected

upvoted 1 times

Lion007 2 years, 10 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

Lion007 2 years, 10 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

cwilson91 2 years, 10 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

UWSFish 3 years, 4 months ago

Just set it up in DLP in my tenant. 100% yes

upvoted 4 times

PrettyFlyWifi 3 years, 4 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 3 years, 5 months ago

On exam 1/20/2022

upvoted 1 times

RAMmulator 3 years, 6 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 3 years, 6 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

Holii 3 years, 2 months ago

DLP Policy provides an "Encrypt email messages (applies only to content in Exchange)" [not blocked]

upvoted 1 times

ServerBrain 1 year, 9 months ago

if you say so.
but Mail Flow Rule is more specific

upvoted 1 times

digitallycan 3 years, 8 months 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 #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

Suggested Answer: *AB*

Community vote distribution

AB (100%)

Val_0 Highly Voted 3 years, 11 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 15 times

nupagazi 3 years, 5 months ago

totally agree

upvoted 2 times

PrettyFlyWifi 3 years, 4 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 2 times

pheb 3 years, 10 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

Boeroe Most Recent 9 months, 1 week ago

Selected Answer: AB

Tested: If all locations are selected you will only have the option "Content contains". Once you deselect On-Premise and Devices you also receive the option "Content is shared from Microsoft 365"

upvoted 1 times

emartiy 1 year, 4 months ago

Selected Answer: AB

Definitely correct.

upvoted 1 times

ServerBrain 1 year, 9 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 2 years, 2 months 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 4 times

fimbulvetrk 2 years, 7 months 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 2 years, 9 months ago

Selected Answer: AB

A and B

tested in test environnement

upvoted 3 times

PrettyFlyWifi 3 years, 4 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 3 years, 6 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 3 years, 10 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 3 years, 12 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

Suggested 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 3 years 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

Eltooth Highly Voted 3 years, 5 months ago
Correct - security reader is least privilege role that can read DLP reports.
upvoted 5 times

emartiy Most Recent 10 months, 1 week ago
Selected Answer: D
Correct.
upvoted 1 times

xswe 1 year, 8 months ago
The least privileged role that can be used for reports in general are Security reader
upvoted 3 times

wooyourdaddy 2 years, 6 months ago
Selected Answer: D
I wrote the exam today, this question was on it, I choose D, scored 890!
upvoted 1 times

PrettyFlyWifi 2 years, 11 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** 3 years 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

⊟ **JakubK64** 3 years, 5 months ago

Correct

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.

Suggested 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, 9 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 11 times

heshmat2022 Most Recent 8 months, 2 weeks ago
IT WAS ON EXAM OCTOBER 18 2023
upvoted 1 times

xswe 1 year, 2 months 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, 7 months 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

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

Community vote distribution
D (52%) B (48%)

Browniez Highly Voted 3 years, 8 months ago
D is correct, as others are not solutions,
upvoted 16 times

Abhishek1610 Highly Voted 2 years, 7 months ago
Selected Answer: D
D is correct, as others are not solutions
upvoted 6 times

fimbulvetrk 2 years, 7 months 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 3 times

Kuteron 8 months, 1 week ago
sensitivity labels are encrypting the document but not checking if SIT's are used. The only way is DLP Rule which block's external out of indicators of the SIT's
upvoted 1 times

Flacky_Penguin32 Most Recent 3 months, 1 week ago
Selected Answer: B
A sensitivity label can:

Encrypt the document

Restrict access to internal users only

Automatically apply based on sensitive information types like credit card numbers (when configured with auto-labeling)
upvoted 1 times

Test90 3 months, 3 weeks ago
Selected Answer: B
B. a sensitivity label, on that label, you can allow permission "to all users in the org" and it will be encrypted to others.
upvoted 1 times

Jideakin 3 months, 3 weeks ago
Selected Answer: B
prevent ... from being opened by users outside your company. If it had said prevent from being shared with external users, I would have picked DLP. This question is focused on the function of each technology. Sensitivity Label is what you use to prevent external users from opening files

irrespective of how they got the file.

upvoted 1 times

HardeWerker433 5 months ago

Selected Answer: B

Correct Answer: B. A sensitivity label

Reasoning:

Sensitivity labels can encrypt documents, control access, and ensure that only internal users are authorized to open sensitive files, such as those containing credit card numbers. This directly addresses the requirement to prevent external users from opening the documents while allowing internal users to do so.

upvoted 1 times

SneakyBD 8 months, 2 weeks ago

Selected Answer: D

Only D makes Sense

upvoted 1 times

Boeroe 8 months, 3 weeks ago

Selected Answer: B

Using a sensitivity label you can assign access only for internal users and groups using the built-in SIT for creditcard

upvoted 3 times

IndigoRabbit 10 months, 2 weeks ago

Here the question has mention "You need to protect documents that contain credit card numbers "FROM BEING OPENED" by users outside your company." So, it is not asking to restrict sharing, hence, DLP can't be the answer. This can only be done using a Sensitive label > Add CCN as SIT > Include All users in your org. So, wherever the file resides, or travels, only internal users can access the document. And that's the reason organization applies encryption and access control. So, answer is B.

upvoted 2 times

RAJRYB 12 months ago

Selected Answer: B

I would rather go with Sensitivity label, because of opening the file by outsiders. But it requires Auto-labeling and the sensitivity label needs to encrypt the file

upvoted 2 times

ChrisBaird 1 year ago

Selected Answer: B

The questions says you need to "protect documents that contain credit card numbers from being opened by users outside your company". It does not say that you need to "prevent documents that contain credit card numbers from shared with users outside your company".

Prevention is done with DLP.

Protection is done with sensitivity labels.

The answer is B.

upvoted 3 times

Amin4799 1 year, 1 month ago

DLP for sure- allows you to define rules that detect sensitive information like credit card numbers and then restrict access or actions based on those rules

upvoted 1 times

BewiseExams 1 year, 3 months ago

Selected Answer: D

D is correct, just tested it, you can secure credit card numbers by using a PICE Data Security Standard template. Everything in 1 single policy.

upvoted 1 times

Davidf 1 year, 10 months ago

Selected Answer: B

A DLP policy will detect content, but a sensitivty label applies protection to the document

upvoted 2 times

T3st3r 2 years, 1 month ago

perhaps B ?

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

upvoted 1 times

⊟ **xswe** 2 years, 2 months ago

To protect documents from being opened by user outisde the organization you need a DLP policy.

upvoted 2 times

⊟ **fimbulvetrk** 2 years, 7 months 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** 2 years, 2 months ago

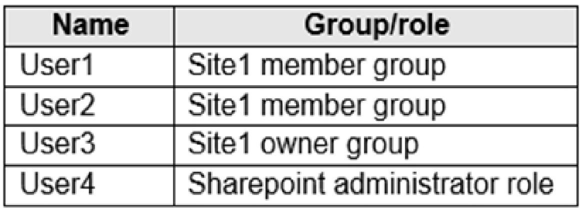
I guess the reason is that sensitivity label nee to be published by a policy otherwise they do not work

upvoted 2 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

Suggested 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

E (53%) D (47%)

DeeJayU Highly Voted 3 years 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 35 times

Mdwro 2 years, 12 months ago

You are right

upvoted 3 times

Mdwro 2 years, 11 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 16 times

klosedotorg83 Highly Voted 3 years, 2 months 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 12 times

Jideakin Most Recent 3 months, 3 weeks ago

Selected Answer: D

Notify user who shared or last modified is the default setting

upvoted 1 times

ChrisBaird 6 months, 3 weeks ago

Selected Answer: D

It said default settings. The default is "Notify the user who sent, shared, or last modified the content"

upvoted 4 times

Lukas2100 7 months, 2 weeks ago

Selected Answer: E

Just created the DLP Policy Rule in a new Tenant (CDX - Compliance package Data).

The default settings for "Customize policy tips and email notifications" are:

Notify these people:

- The person who sent, shared, or modified the content
- Owner of the SharePoint site or OneDrive account
- Owner of the SharePoint or OneDrive conent

So Answer should be : E

P.s. Does Microsoft review older exams questions and may change the answer ?

upvoted 1 times

> **ChrisBaird** 6 months, 3 weeks ago
>
> Why did you customize the policy tips? It said default settings. The default is "Notify the user who sent, shared, or last modified the content"
>
> upvoted 1 times

fayeb 8 months, 1 week ago

D:

https://learn.microsoft.com/en-us/purview/dlp-use-notifications-and-policy-tips#default-text-for-policy-tips-on-sites

upvoted 2 times

BewiseExams 9 months, 1 week ago

Selected Answer: E

Just tested it

Default notify users in office 365 service with a policy tip:

notify these people:

the person who sent, shared, or modified the content

owner of the sp site or od account

owner of the sp or od content

upvoted 1 times

Domza 1 year, 1 month ago

Its under "email notification" in DLP

D is correct

Enjoy

upvoted 1 times

heshmat2022 1 year, 2 months ago

IT WAS ON EXAM OCTOBER 18 2023

upvoted 1 times

ServerBrain 1 year, 3 months ago

Selected Answer: D

notifications to other users are irrelevant

upvoted 1 times

dmoorthy 1 year, 8 months ago

E is the Answer

upvoted 1 times

xswe 1 year, 8 months 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 2 years 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** 2 years ago

Selected Answer: D

D is correct.

upvoted 1 times

⊟ **RamenIsDelicious** 2 years, 4 months ago

Selected Answer: E

Tested 8/11/22 its E with default notification settings on.

upvoted 2 times

⊟ **Bear4** 2 years, 7 months ago

There are Site owners but there is no site owner group. I am right?

upvoted 1 times

⊟ **JamesM9** 2 years, 8 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

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

Suggested 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, 8 months 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** 2 years, 6 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

⊟ **wooyourdaddy** Highly Voted 2 years ago

Selected Answer: D

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

upvoted 5 times

⊟ **Domza** Most Recent 7 months, 3 weeks ago

Correct~

upvoted 1 times

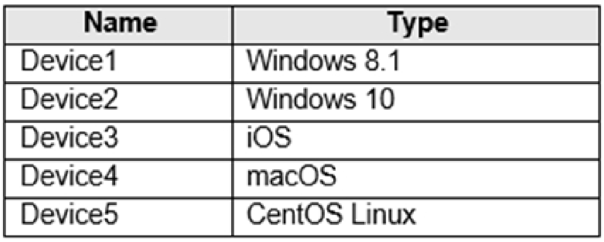
⊟ **xswe** 1 year, 2 months ago

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

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

Suggested 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 3 years, 7 months 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 27 times

gursimran_s 3 years, 2 months ago

That is not an option here. Maybe the question is outdated!

upvoted 5 times

xswe Highly Voted 2 years, 2 months ago

Outdated question, windows 10,11 and MacOS are supported for Endpoint DLP

upvoted 9 times

emartiy Most Recent 1 year, 4 months ago

Selected Answer: B

Since there is no option Device 2 and Device 4, based on the given selection, correct answer is B.

upvoted 2 times

MKnight25 8 months, 2 weeks ago

you're write usually Win10 and macOS is supported

https://learn.microsoft.com/en-us/purview/endpoint-dlp-learn-about

upvoted 1 times

fimbulvetrk 2 years, 7 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 3 years, 8 months 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

Suggested Answer: *B*

Reference:

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

Community vote distribution

B (100%)

wooyourdaddy Highly Voted 👍 2 years, 6 months ago

Selected Answer: B

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

upvoted 6 times

emartiy Most Recent 2 years... 10 months, 1 week ago

Selected Answer: B

B is correct option.

upvoted 2 times

Domza 1 year ago

B is correct ~

Rule matched- will stop the process - File copied to clipboard - action.

Simply open detail tab/Event of impacted entries

With love~

upvoted 1 times

xswe 1 year, 8 months 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

BTAB 2 years, 7 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] 2 years, 10 months ago

Why is this policy matches when the incidents report shows matches at a rule level?

upvoted 1 times

[Removed] 2 years, 10 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 2 years, 11 months ago

On exam 1/20/2022

upvoted 1 times

⊟ **Ras1364** 3 years, 1 month ago

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

upvoted 2 times

⊟ **klosedotorg83** 3 years, 2 months ago

Correct

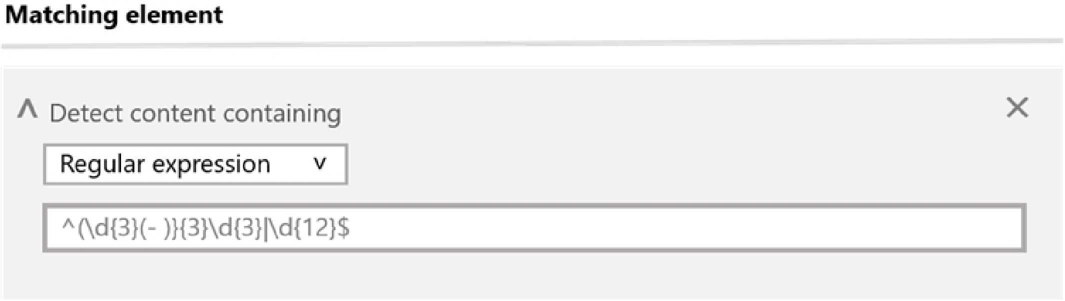
upvoted 4 times

Question #21 *Topic 2*

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.



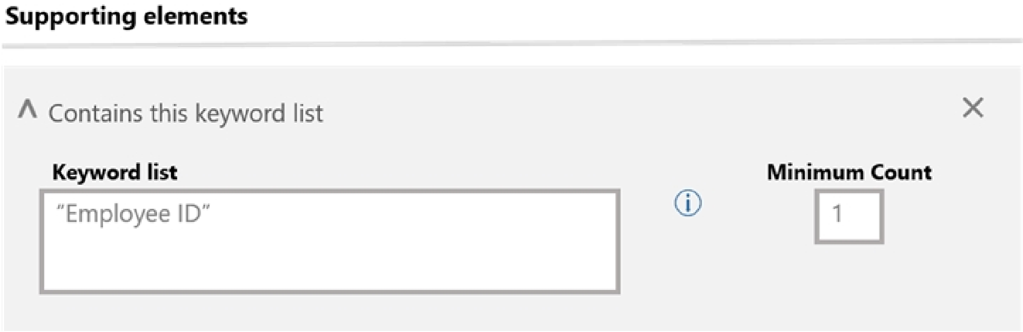
Matching element

Λ Detect content containing ✕

Regular expression ∨

^(\d{3}(-)){3}\d{3}|\d{12}$

The supporting elements are configured as shown in the following exhibit.

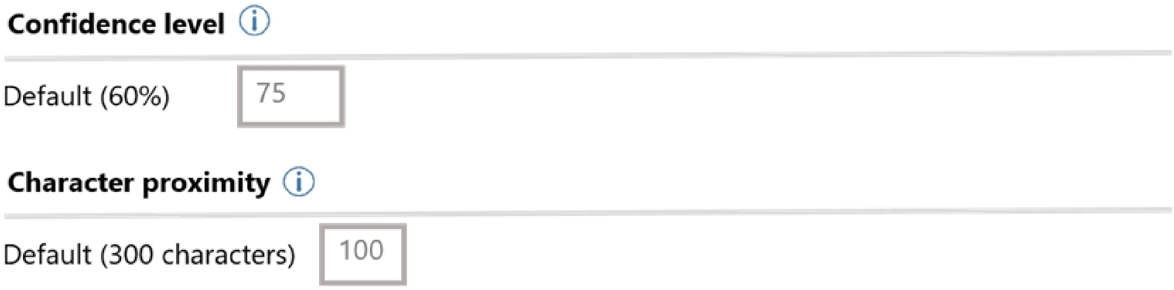


Supporting elements

Λ Contains this keyword list ✕

Keyword list	Minimum Count
"Employee ID"	1

The confidence level and character proximity are configured as shown in the following exhibit.



Confidence level ⓘ

Default (60%) 75

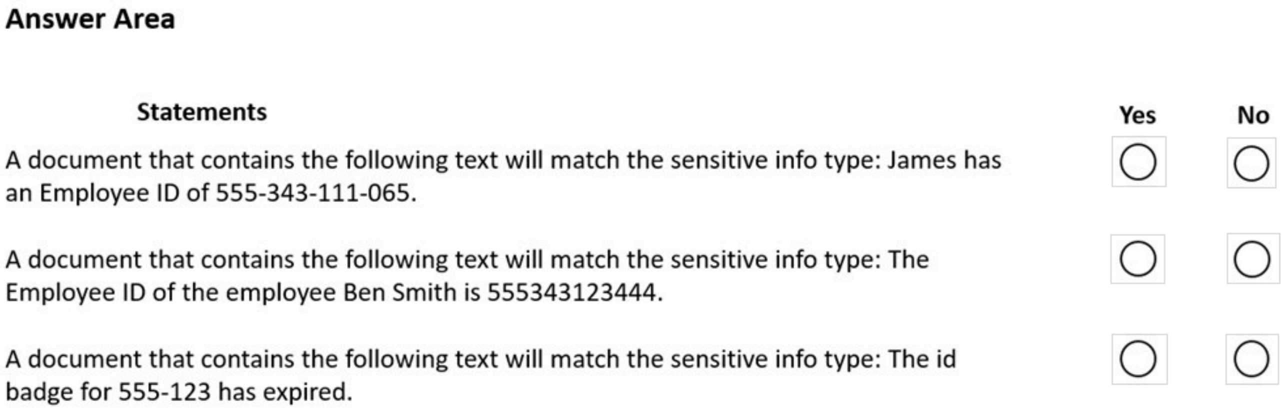
Character proximity ⓘ

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.

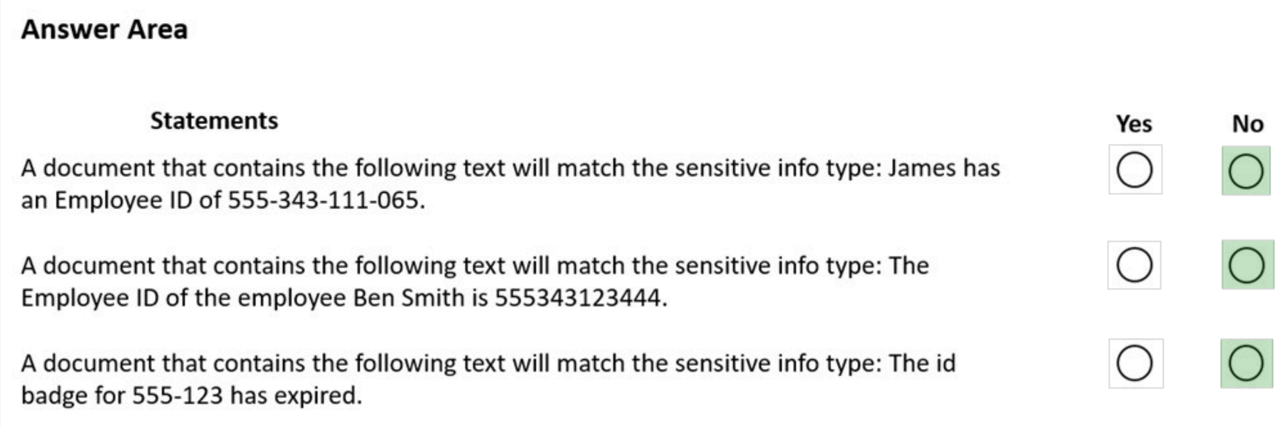
Hot Area:



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.	○	○

Suggested 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 3 years, 6 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 17 times

PsiCzar Most Recent 10 months, 3 weeks ago

No for all.

Regex is invalid, 3rd "}" doesn't have a matching "{", validated it with regex101.com

upvoted 1 times

Sam12 3 years, 5 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 3 years, 3 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 3 years, 5 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 3 times

xlws 3 years, 6 months ago

that is 3 numbers - 3 numbers - 3 numbers - 3 numbers or 12 numbers, I vote for yes,no,no.

upvoted 3 times

sergioandreslq 3 years, 6 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 5 times

⊟ **Boeroe** 9 months, 2 weeks ago
Agree, the ^ is the reason the regex wont work. Microsoft article: https://learn.microsoft.com/en-us/purview/dlp-policy-learn-about-regex-use#example-of-using-a-regex-in-a-dlp-policy-rule
upvoted 1 times

⊟ **klosedotorg83** 3 years, 8 months 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** 3 years, 8 months ago
option 2nd, 9 digit number matches regular expression... so is 2nd TRUE? not sure
upvoted 1 times

⊟ **Sam12** 3 years, 5 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** 3 years, 3 months ago
The dot is not part of the text. Microsoft allways ends the answers with a dot
upvoted 2 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

Suggested 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%)

emartiy 10 months, 1 week ago

Selected Answer: B

Correct.

upvoted 1 times

NinjaSchoolProfessor 2 years 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 3 times

wooyourdaddy 2 years, 6 months ago

Selected Answer: B

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

upvoted 2 times

McAlec 3 years, 1 month 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

Suggested 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 8 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 7 months, 1 week 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 5 times

hpl1908 11 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 11 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 2 times

hpl1908 11 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 4 times

NinjaSchoolProfessor 1 year 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, 6 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

Suggested 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 3 years, 4 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

trut_hz Most Recent 5 months, 1 week ago

Selected Answer: B

Are you sure "You need to block Tailspin_scanner.exe from accessing sensitive documents without preventing the application from accessing other documents." without preventing the app from accessing other docs. It still needs to work and function. Making unallowed will stop it completely, am I the only one that sees that?

upvoted 1 times

trut_hz 5 months, 1 week ago

Never mind apparently unallowed doesn't make the app stop completely, only limits the ability to interact with sensitive documents.

upvoted 1 times

Domza 1 year, 4 months ago

Selected Answer: A

Looks good~

upvoted 1 times

xswe 2 years, 2 months 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 3 times

NinjaSchoolProfessor 2 years, 6 months 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 2 years, 11 months ago

Correct answer A

upvoted 1 times

wooyourdaddy 3 years ago

Selected Answer: A

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

upvoted 2 times

jakke91 7 months ago

go away!

upvoted 2 times

Question #25 *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 as email.
Does this meet the goal?

A. Yes

B. No

Suggested 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, 8 months 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 👍 2 years, 5 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 7 months ago
Ans: YES
upvoted 1 times

NinjaSchoolProfessor 1 year, 6 months 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

Pravda 2 years, 5 months ago
On exam 1/20/2022
upvoted 1 times

klosedotorg83 2 years, 8 months 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

Suggested 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 (50%) B (50%)

Artgum Highly Voted 1 year, 4 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 10 times

trut_hz Most Recent 5 months, 1 week ago
Selected Answer: B
Sending alerts to power automate is not enough to ensure every file owner and the respective dept's team site receive notifications\
upvoted 1 times

Domza 1 year, 1 month ago
Quest 4 and Quest 26 the same
upvoted 2 times

Gesbie 1 year, 4 months ago
was on Exam August 9, 2023
upvoted 1 times

dmoorthy 1 year, 8 months ago
Answer is B
upvoted 2 times

RamenIsDelicious 2 years, 4 months ago
Selected Answer: A
Tested 8/15/22 should be a=YES
upvoted 4 times

IAGirl 2 years, 10 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 2 years, 10 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 2 years, 10 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 4 times

⊟ **PrettyFlyWifi** 2 years, 10 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

⊟ **emartiy** 10 months ago

you can send notification to data/file owner or admin thanks to dlp action sections. however, there is no option to send email notification to the affected department teams.. You need a function to perform this, so including Power Automate make this question's answer "YES"

upvoted 1 times

⊟ **Pravda** 2 years, 11 months ago

On exam 1/20/2022

upvoted 1 times

⊟ **DeeJayU** 3 years 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** 3 years ago

Question 4 and 26 are the same? Why?

upvoted 2 times

⊟ **casti** 3 years, 2 months 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

Suggested 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 10 months, 1 week ago

Selected Answer: B

To send messages to teams we need power automate

upvoted 7 times

⊟ **ChaBum** Highly Voted 11 months, 2 weeks 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 9 months, 3 weeks 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** 7 months, 1 week 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

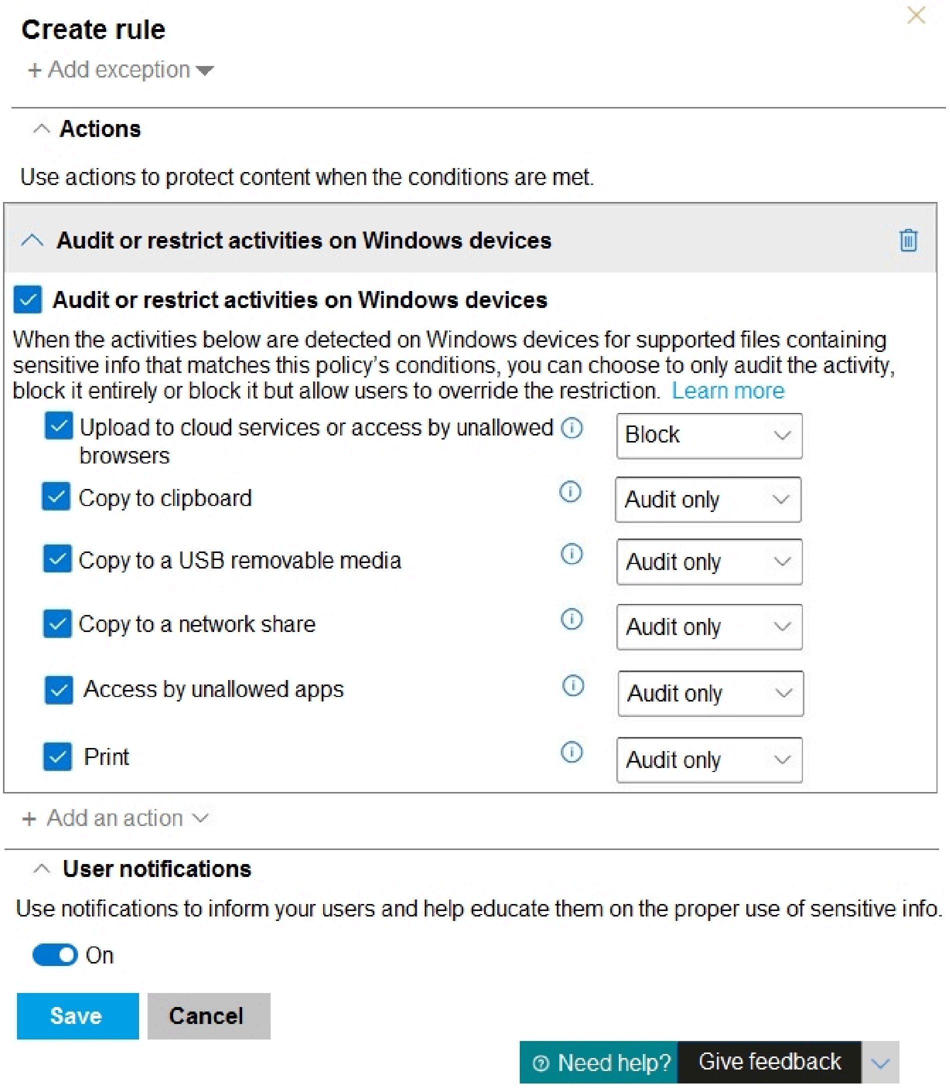
⊟ **Pravda** 11 months, 2 weeks ago

On exam 1/20/2022

upvoted 2 times

Question #28 Topic 2

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



Create rule

+ Add exception

Actions

Use actions to protect content when the conditions are met.

Audit or restrict activities on Windows devices

☑ **Audit or restrict activities on Windows devices**

When the activities below are detected on Windows devices for supported files containing sensitive info that matches this policy's conditions, you can choose to only audit the activity, block it entirely or block it but allow users to override the restriction. Learn more

☑ Upload to cloud services or access by unallowed browsers	Block
☑ Copy to clipboard	Audit only
☑ Copy to a USB removable media	Audit only
☑ Copy to a network share	Audit only
☑ Access by unallowed apps	Audit only
☑ Print	Audit only

+ Add an action

User notifications

Use notifications to inform your users and help educate them on the proper use of sensitive info.

On

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.

Suggested Answer: *CD*

Community vote distribution

CE (70%) AE (19%) 11%

IAGirl Highly Voted 2 years, 10 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 9 times

PrettyFlyWifi Highly Voted 2 years, 10 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 6 times

Domza 1 year ago

Correct~ A and E - the rest is out) read and read!

upvoted 1 times

Kodoi Most Recent 10 months, 1 week ago

Selected Answer: CE

A is incorrect. If Computer 1 is not onboarded, the DLP policy does not apply. In other words, the user will not fail to upload.

B is False. Auditing does not inhibit uploading.

C is correct. Uploads are normally blocked, but can be uploaded if the file exists in an excluded path.

D is incorrect. Auditing does not inhibit uploading.

E is correct. For example, uploads from a browser are allowed, while uploads from Explorer are blocked.

The point of this question is that uploads can succeed or fail depending on the user scenario.

upvoted 2 times

heshmat2022 1 year, 2 months ago

IT WAS ON EXAM OCTOBER 18 2023

upvoted 1 times

Tommytong 1 year, 2 months 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 1 year, 4 months ago

was on Exam August 9, 2023

upvoted 1 times

xswe 1 year, 8 months 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 1 year, 7 months 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 1 year, 10 months ago

Selected Answer: CE

The only logical choices

upvoted 1 times

⊟ **Rockalm** 1 year, 12 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** 2 years, 2 months 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** 2 years, 8 months ago

The answer here is C & E.

upvoted 4 times

⊟ **UWSFish** 2 years, 11 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** 2 years, 10 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** 2 years, 11 months ago

On exam 1/20/2022

upvoted 1 times

⊟ **Sam12** 2 years, 11 months ago

Selected Answer: CE

CE for me!

upvoted 4 times

⊟ **ChaBum** 2 years, 12 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** 1 year, 6 months ago

totally agree

upvoted 1 times

⊟ **Pereiraman** 2 years, 11 months ago

agree, the only ones that can cause unstable and related with DLP.

upvoted 1 times

⊟ **solfis737** 3 years 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** 3 years ago

AE looks more valid.

upvoted 1 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

Suggested Answer: *A*

Community vote distribution

A (58%) B (42%)

ExamReviewerIZ Highly Voted 👍 3 years, 8 months 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 16 times

TC1Labs Most Recent ⊙ 1 month ago

Selected Answer: C

1 policy + 2 rules.

upvoted 1 times

GebAn 7 months, 2 weeks ago

Selected Answer: A

Its A,

One Policy for Block (including all Users and exlude Group1 with action Block)

One Policy for Audit (including only Group1 with action Audit)

If you would only create one Policy with exclude Group1 and Block only the Blocked ones would be audited not the successfully copyed one from Group1

upvoted 1 times

GebAn 7 months, 2 weeks ago

Its A,

One Policy for Block (including all Users and exlude Group1 with action Block)

One Policy for Audit (including only Group1 with action Audit)

If you would only create one Policy with exclude Group1 and Block only the Blocked ones would be audited not the successfully copyed one from Group1

upvoted 1 times

Jo696 1 year, 3 months ago

Selected Answer: A

If it wasn't for the Audit requirement this would be just one policy with a block and exclude group 1, however with the audit requirement it would be t DLP policies

upvoted 1 times

Kodoi 1 year, 4 months ago

Selected Answer: A

A is the correct answer.

The first DLP policy sets up a block for all users. Group 1 is excluded.

The second policy sets up recording in the audit log for group 1.

upvoted 1 times

xswe 2 years, 2 months ago

You should go for two DLP policies and one DLP rule to achieve this

upvoted 1 times

Azurefox79 2 years, 4 months 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 2 years, 6 months 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 3 times

mcas 2 years, 8 months 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 3 times

chrissempai 2 years, 9 months ago

Selected Answer: A

A is the only way

upvoted 1 times

Lion007 2 years, 10 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 3 times

wyindualizer 2 years, 10 months ago

And what about audit?

upvoted 5 times

Pravda 3 years, 5 months ago

On exam 1/20/2022

upvoted 1 times

nupagazi 3 years, 5 months ago

I think 1 policy, 1 rule using exlusion group or user

upvoted 3 times

PrettyFlyWifi 3 years, 4 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.

Suggested 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 3 years, 7 months ago
Selected Answer: D
Answer is D.
We can configure an alert in MCAS by creating a file policy
upvoted 15 times

⊟ **sergioandreslq** 3 years, 6 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 8 times

⊟ **digitallycan** Highly Voted 3 years, 8 months 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

⊟ **MKnight25** Most Recent 8 months, 2 weeks ago
Selected Answer: C
I see only option C as possible, because the requirement is "To every user outside the company" that is not possible with a file policy.
upvoted 1 times

⊟ **fayeb** 1 year, 2 months ago
D: https://security.microsoft.com/cloudapps/policy/file/create
upvoted 1 times

⊟ **heshmat2022** 1 year, 8 months ago

IT WAS ON EXAM OCTOBER 18 2023

upvoted 2 times

xswe 2 years, 2 months ago

DLP Policy in Purview or File Policy should be used to achieve this

upvoted 1 times

xswe 2 years, 2 months ago

File policy in MCA and DLP policy in Purview should be used to achieve this.

upvoted 1 times

mcas 2 years, 8 months ago

Selected Answer: C

this is also possible with insider risk policy

upvoted 2 times

chrissempai 2 years, 9 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 2 years, 2 months ago

you do not create in EAC a DLP policy related to onedrive, either the topic is exchange or onedrive

upvoted 1 times

MahmoudEldeep 3 years, 2 months ago

Selected Answer: D

Answer is D

upvoted 1 times

JamesM9 3 years, 2 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 3 years, 3 months ago

I actually think this can be done with an insider risk policy

upvoted 2 times

daavidsc400 3 years, 3 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 3 years, 4 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 3 years, 4 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 3 years, 4 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 3 years, 4 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** 2 years, 9 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 3 years, 5 months ago

On exam 1/20/2022

upvoted 1 times

Sam12 3 years, 5 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

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.

Suggested 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 2 years, 6 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 9 times

xswe Highly Voted 1 year, 2 months 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 5 times

yoshizutakahiro Most Recent 1 year ago
Selected Answer: D
D□□□□□□
upvoted 2 times

nicekoda 1 year, 5 months 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 1 year, 5 months ago
pls disregard. Confused dotx with docx
upvoted 2 times

chrissempai 1 year, 9 months ago
Selected Answer: D
Was on exam the 9/9/22
upvoted 1 times

music_man 1 year, 10 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 2 years, 4 months ago

Selected Answer: D

Because the question states "The solution must minimize effort."

upvoted 1 times

Pravda 2 years, 5 months ago

On exam 1/20/2022

upvoted 1 times

Pravda 2 years, 5 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 2 years, 5 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 2 years, 5 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 2 years, 6 months ago

on second thoughts I will stick with A as must be administratively simpler

upvoted 3 times

bingomutant 2 years, 6 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 7 months, 3 weeks 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

Suggested Answer: *A*
Reference:
https://docs.microsoft.com/en-us/microsoft-365/compliance/dlp-policy-reference?view=o365-worldwide

Community vote distribution
C (43%) D (37%) A (19%)

⊟ **xlws** Highly Voted 3 years, 6 months ago
The answer is C, https://docs.microsoft.com/en-us/defender-cloud-apps/data-protection-policies, sharing with external domain.
upvoted 15 times

⊟ **sivis** Highly Voted 3 years, 7 months 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 13 times

⊟ **Phil_79** Most Recent 4 months, 1 week ago
Selected Answer: D
Sorry for the "C" party, but data protection policies are for filed "shared" not for file "sent" with email... so in this case a file policy won't fire (see point 7 of this link to look at a the file policy target: https://learn.microsoft.com/en-us/defender-cloud-apps/data-protection-policies#create-a-new-file-policy).
upvoted 1 times

⊟ **JimboJones99** 11 months, 1 week ago
Selected Answer: C
https://learn.microsoft.com/en-us/defender-cloud-apps/data-protection-policies#policies
upvoted 1 times

⊟ **JimboJones99** 11 months, 2 weeks ago
Selected Answer: C
https://docs.microsoft.com/en-us/defender-cloud-apps/data-protection-policies
upvoted 1 times

⊟ **RAJRYB** 12 months ago
Selected Answer: C
I will go with C. there is the word "documents", so it will be the file policy
upvoted 1 times

⊟ **EM1234** 1 year ago
Selected Answer: C
I am going with C for the reasons kodoi said.

But I am not sure as I do not see what a person who recently scored an 890 would have picked. /s
upvoted 5 times

⊟ **EsamiTopici** 1 year ago
ahahahha
upvoted 1 times

SDiwan 1 year, 3 months ago

Selected Answer: C

Documentation from Microsoft Defender for Cloud apps (old name MCAS) .
"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."
So, correct answer is C
https://learn.microsoft.com/en-us/defender-cloud-apps/data-protection-policies

upvoted 2 times

Kodoi 1 year, 4 months ago

Selected Answer: C

A is incorrect. Privacy categories detect and protect the type of privacy information; DLP policies restrict the transmission of information to outside parties, but privacy categories are ineligible.

B is incorrect. An activity policy cannot specify a domain. It detects multiple failed sign-ins and sign-ins from unfamiliar locations.

C is correct. File policy allows you to receive alerts about files shared with accounts owned by a specific external domain.

D is incorrect. The alerts displayed on the dashboard are just extracted by specific criteria and displayed in an easy-to-read manner.

https://learn.microsoft.com/en-us/defender-cloud-apps/data-protection-policies

upvoted 4 times

Softeng 1 year, 4 months ago

Selected Answer: A

It's A:

https://learn.microsoft.com/en-us/defender-cloud-apps/data-protection-policies#:~:text=Sharing%20with%20external%20domains%20%2D%20Receive%20an%20alert%20about%20any%20file%20shared%20with%20accounts%20o

upvoted 3 times

Elangamban 1 year, 6 months ago

answer is A

upvoted 1 times

samrith 1 year, 8 months ago

Community vote D(50%). A(19%) why suggest answer A

upvoted 1 times

TomasValtor 1 year, 9 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 3 times

TomasValtor 1 year, 9 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 3 times

TomasValtor 1 year, 9 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 4 times

Davidf 1 year, 10 months 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 2 years 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 3 times

doori88 2 years 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 2 years, 1 month ago

Why not C?

upvoted 1 times

Question #33 *Topic 2*

HOTSPOT -

You create a data loss prevention (DLP) policy that meets the following requirements:

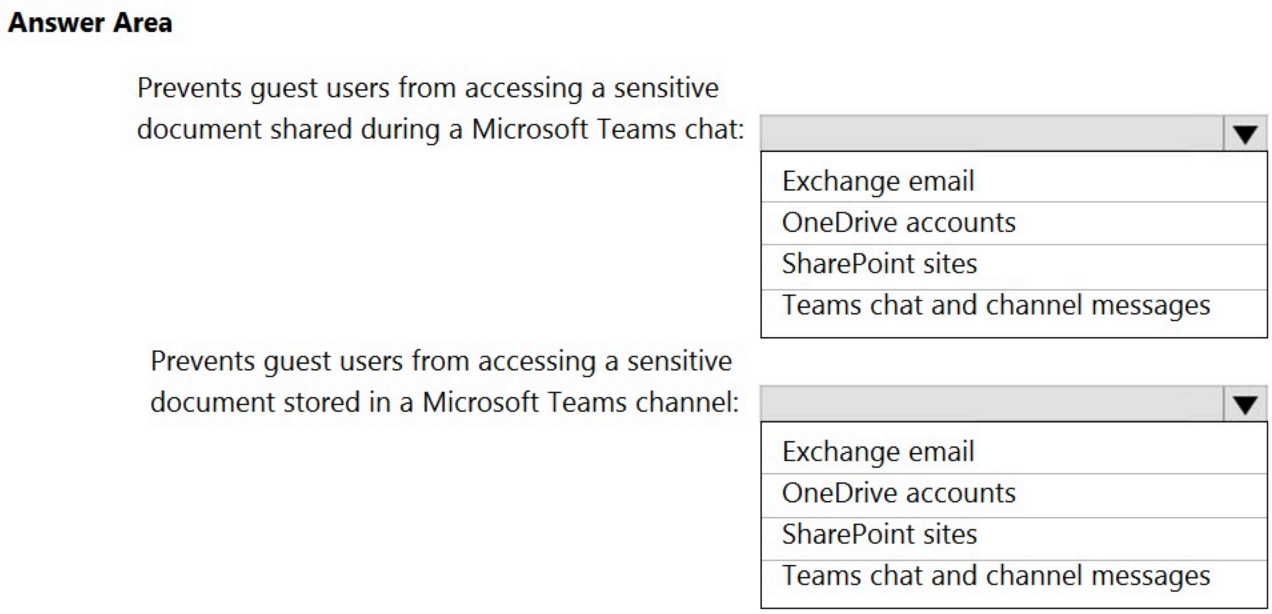
✑ Prevents guest users from accessing a sensitive document shared during a Microsoft Teams chat

✑ 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

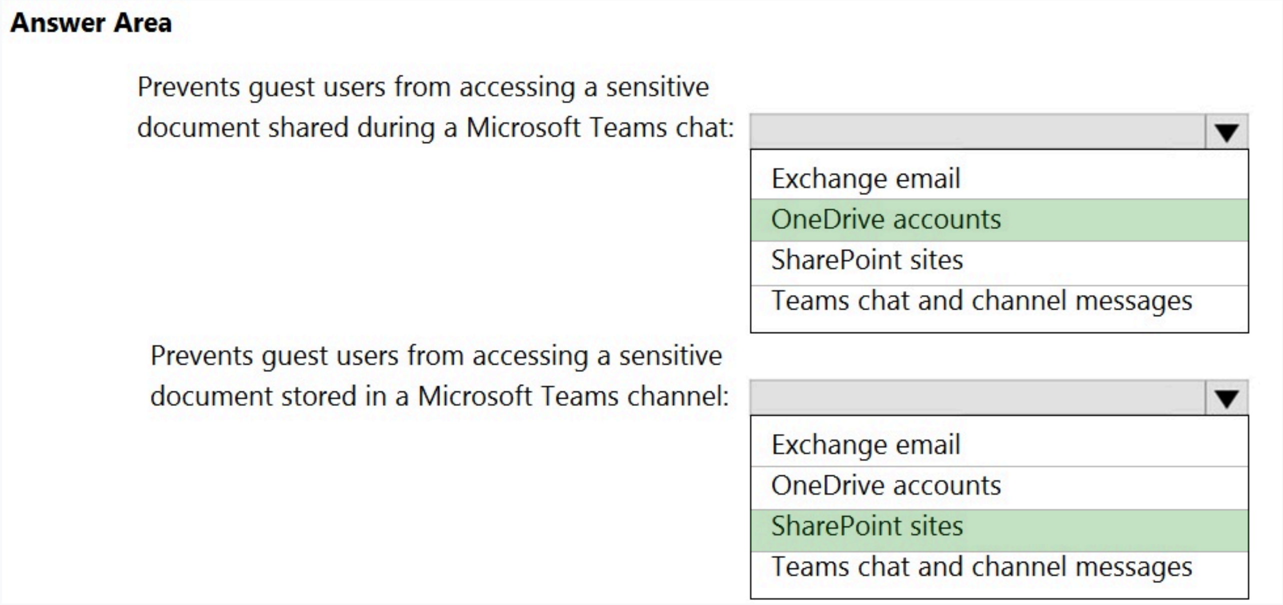
Prevents guest users from accessing a sensitive document shared during a Microsoft Teams chat:

- 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

Suggested 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 3 years, 7 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 23 times

⊟ **xswe** Most Recent 1 year, 8 months ago

DLP policy that will protect documents shared in Teams chat = Onedrive

Teams channels = Sharepoint

upvoted 2 times

⊟ **wooyourdaddy** 2 years, 6 months ago

I wrote the exam today, this question was on it, I choose Box1: OneDrive accounts, Box2: SharePoint sites, scored 890!

upvoted 3 times

⊟ **mb0812** 9 months, 2 weeks ago

fake user

upvoted 2 times

⊟ **Jahoor69** 2 years, 9 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** 2 years, 11 months ago

On exam 1/20/2022

upvoted 1 times

⊟ **Cmora** 3 years 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]** 3 years, 1 month 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** 3 years, 6 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** 3 years, 6 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** 3 years, 7 months ago

It must be sharePoint + Onedrive + Teams chat and channel messages

upvoted 1 times

⊟ **dasha_an** 3 years, 7 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

Suggested Answer: *D*
Reference:
https://docs.microsoft.com/en-us/microsoft-365/compliance/endpoint-dlp-using?view=o365-worldwide

Community vote distribution

B (72%) A (28%)

⊟ **liozuf** Highly Voted 👍 3 years, 7 months ago

B. an action is a better answer

upvoted 33 times

⊟ **Eltooth** Highly Voted 👍 3 years, 7 months ago

B. An action would prevent a data copy function.

upvoted 14 times

⊟ **dillon123456789** Most Recent 🕘 3 months ago

Selected Answer: B

on exam 2025

upvoted 1 times

⊟ **Lukas2100** 7 months, 2 weeks ago

Selected Answer: B

In my test Tenant (Microsoft CDX Tenant) is a pre-configured DLP Policy named "Default Policy for devices". When I edit this policy an go on to the "Advanced DLP Rules" and also edit the rule in this sector then I'm able to configure "an action" which is called "File activities for all apps" -> "Aply restrictions to specific activity" -> "Copy to Clipboard". There you can "block" this kind of action.

Therefore I choose "B"

upvoted 2 times

⊟ **mbhasker** 1 year, 1 month ago

D. user overrides

upvoted 1 times

⊟ **TomasValtor** 1 year, 3 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 2 times

⊟ **TomasValtor** 1 year, 3 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 2 times

dmoorthy 1 year, 8 months ago

B is the right Answer.

upvoted 1 times

GeoffLule 1 year, 8 months ago

Scenario 3: Modify the existing policy, block the action with allow override

upvoted 1 times

xswe 1 year, 8 months ago

An action, test it out in purview to find this out by yourself!

upvoted 2 times

Katea 1 year, 9 months ago

Selected Answer: B

B. an action is a better answer

upvoted 1 times

Katea 1 year, 9 months 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 2 years, 3 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 2 times

Lotanna_ 2 years, 5 months ago

B for me

upvoted 1 times

wooyourdaddy 2 years, 6 months ago

Selected Answer: B

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

upvoted 3 times

MahmoudEldeep 2 years, 8 months ago

Selected Answer: B

Correct answer is B

upvoted 1 times

Solozero 2 years, 10 months ago

Selected Answer: B

B. an action

upvoted 2 times

Pravda 2 years, 11 months ago

On exam 1/20/2022

upvoted 1 times

Mdwro 2 years, 11 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 6 times

Question #35 Topic 2

HOTSPOT -

You have a Microsoft 365 E5 tenant.

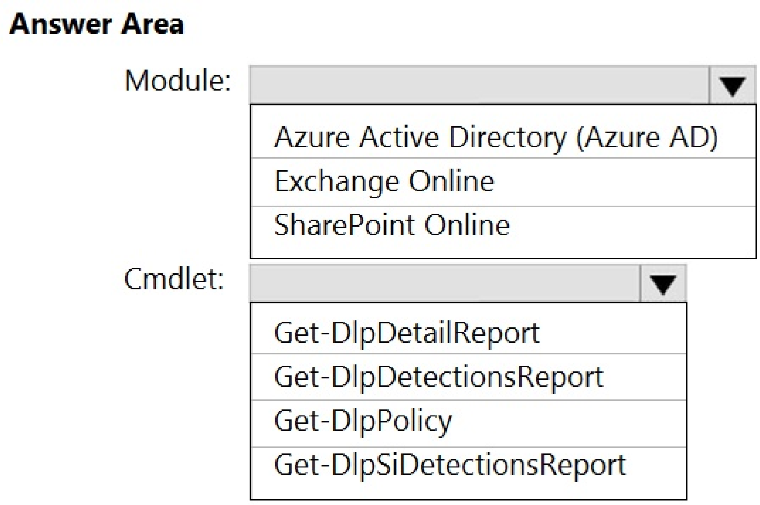
Data loss prevention (DLP) policies are applied to Exchange email, SharePoint sites, and OneDrive accounts locations.

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:

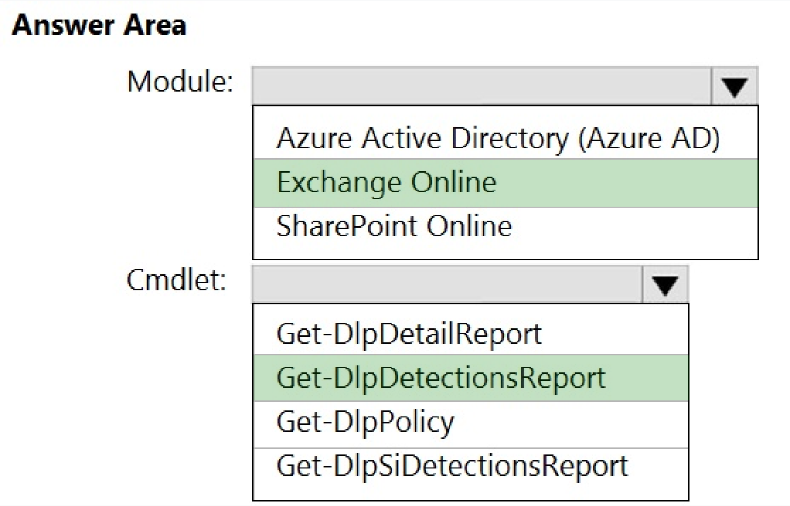


Answer Area

Module:
- Azure Active Directory (Azure AD)
- Exchange Online
- SharePoint Online

Cmdlet:
- Get-DlpDetailReport
- Get-DlpDetectionsReport
- Get-DlpPolicy
- Get-DlpSiDetectionsReport

Suggested 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 3 years 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 18 times

Gesbie Most Recent 10 months, 3 weeks ago

was on Exam August 9, 2023

upvoted 1 times

xswe 1 year, 2 months ago

Exchange Online

Get-DLPDetectionsReport cmdlet will show a summary of the DLP rule matches in Exchange, Sharepoint and Onedrive

upvoted 3 times

wooyourdaddy 2 years 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** 2 years, 4 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** 2 years, 5 months ago

On exam 1/20/2022

upvoted 2 times

⊟ **shanti0091** 2 years, 11 months ago

correct Answer

upvoted 4 times

Question #36 *Topic 2*

HOTSPOT -

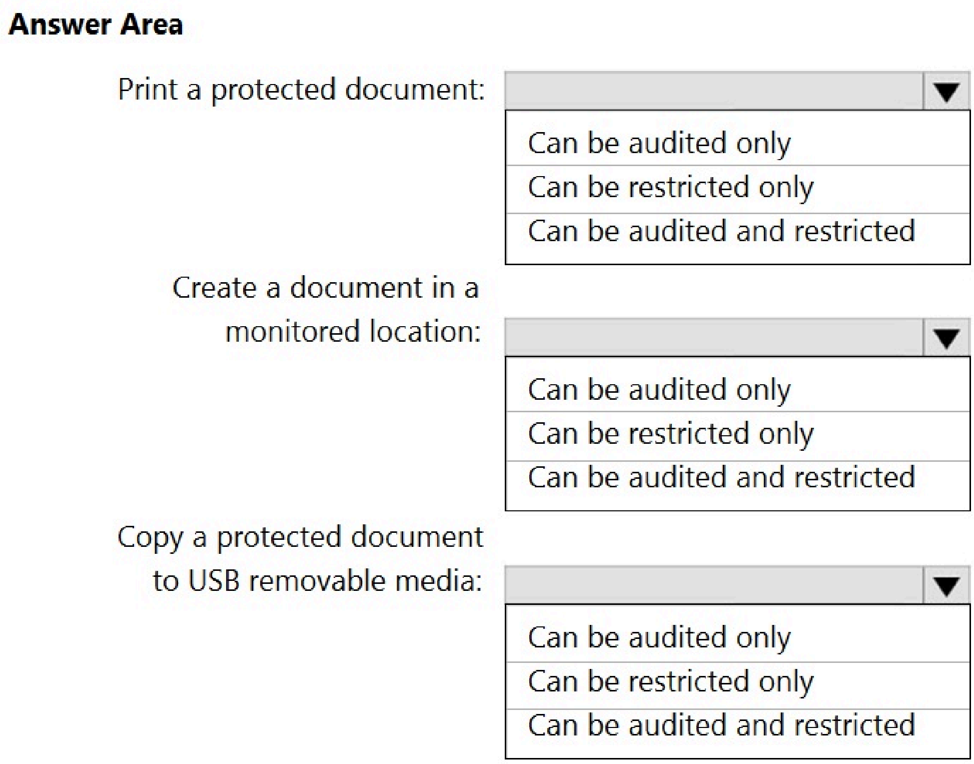
You plan to implement Microsoft 365 Endpoint data loss prevention (Endpoint DLP).

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:



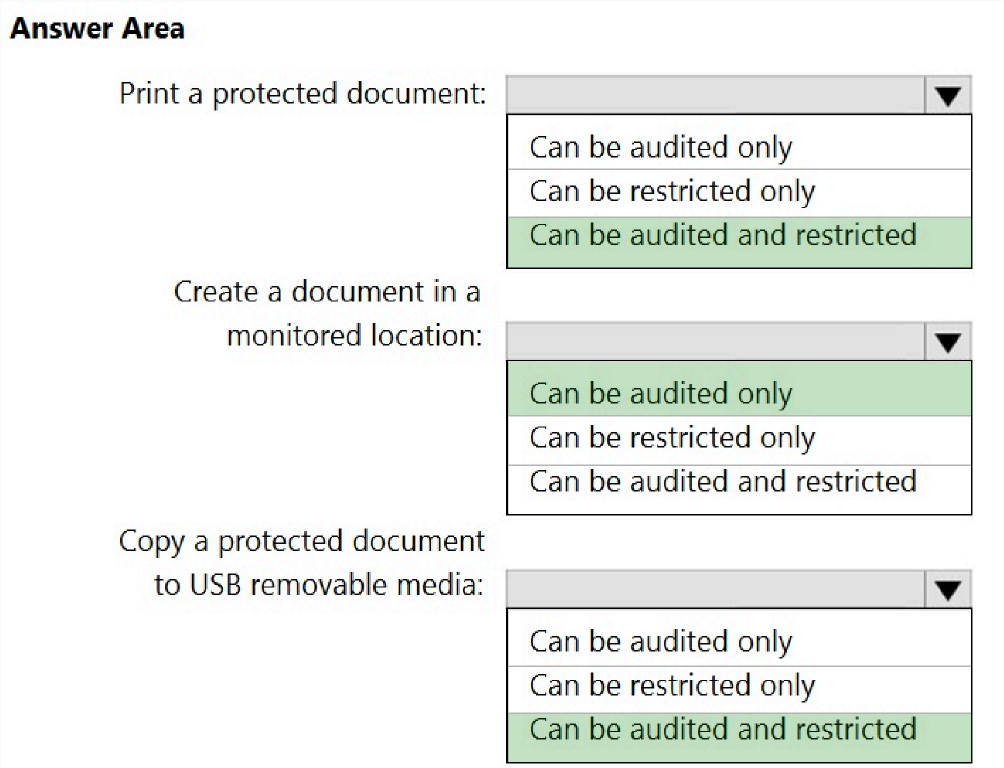
Answer Area

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

Suggested Answer:



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]

Reference:

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

Banzaaai Highly Voted 2 years, 7 months ago

Print: audited and restricted
Creation: audited only
USB: audited and restricted

checked, all are corrected
upvoted 26 times

⊟ **xswe** Highly Voted 8 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 8 times

⊟ **Pravda** Most Recent 1 year, 11 months ago

On exam 1/20/2022
upvoted 3 times

⊟ **Eltooth** 2 years, 6 months ago

Looks correct.
upvoted 4 times

⊟ **Che1** 2 years, 6 months ago

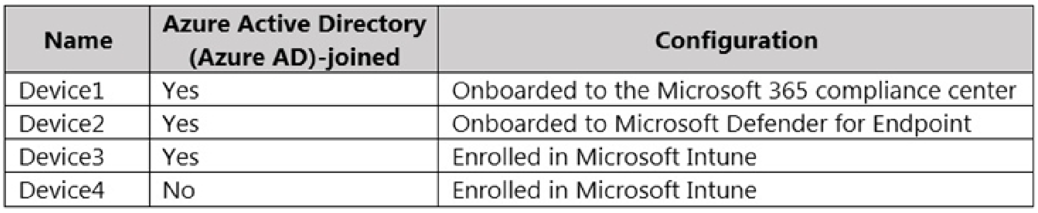
All correct
upvoted 4 times

⊟ **k4d4v4r** 2 years, 7 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

Suggested 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 3 years, 6 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

HardcodedCloud Highly Voted 3 years 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 5 times

emartiy Most Recent 10 months, 1 week ago

Selected Answer: C

Correct -

https://learn.microsoft.com/en-us/purview/endpoint-dlp-getting-started#:~:text=Microsoft%20Endpoint%20DLP,might%20compromise%20them.

upvoted 1 times

Gesbie 1 year, 4 months ago

was on Exam August 9, 2023

upvoted 2 times

xswe 1 year, 8 months ago

If you want to use endpoint DLP you have to onboard the devices

upvoted 1 times

prabhjot 2 years, 3 months ago

seems correct

upvoted 1 times

wooyourdaddy 2 years, 6 months ago

Selected Answer: C

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

upvoted 2 times

Pravda 2 years, 11 months ago

On exam 1/20/2022

upvoted 1 times

⊟ **Eltooth** 3 years, 6 months ago

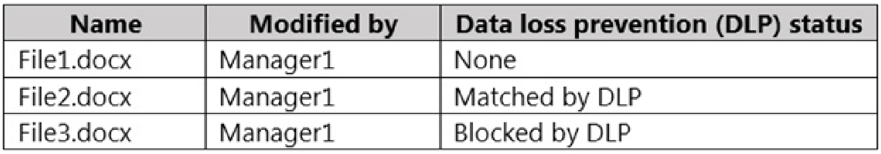
Correct.

upvoted 4 times

Question #38 Topic 2

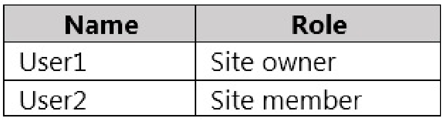
HOTSPOT -

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.

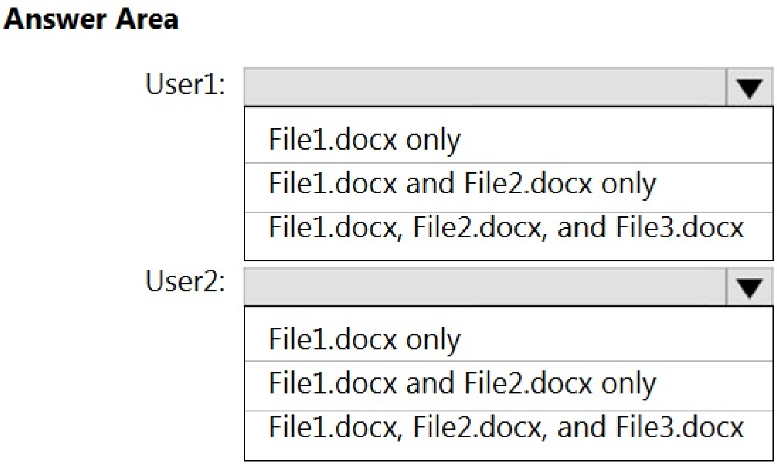


Name	Role
User1	Site owner
User2	Site member

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

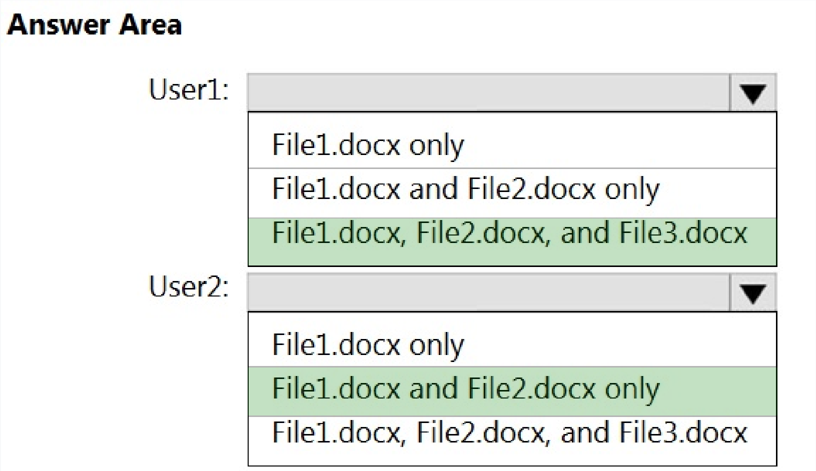
User1: ▼

- 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

Suggested 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 2 years, 6 months ago

Tested & verified

upvoted 11 times

Discuss4certi Highly Voted 2 years, 10 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 2 years, 5 months ago

except owner, last modifier and site owner.. "For use only by"

upvoted 1 times

izgi43 Most Recent 7 months, 2 weeks ago

on exam thu nov 9

upvoted 1 times

daavidsc400 2 years, 3 months ago

What does "matched by dlp" actually mean in terms of access?

upvoted 5 times

> **Rockalm** 1 year, 5 months ago
>
> Matched by another DLP rulethat doesn't block.
>
> upvoted 3 times

Pravda 2 years, 5 months ago

On exam 1/20/2022

upvoted 1 times

Eltooth 2 years, 11 months ago

Correct.

upvoted 1 times

shanti0091 2 years, 11 months ago

correct

upvoted 1 times

Goseu 3 years 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

Suggested 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 1 year, 4 months ago
was on Exam August 9, 2023
upvoted 1 times

Gesbie 1 year, 4 months ago
was on Exam August 9, 2023
upvoted 1 times

IAGirl 2 years, 10 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 4 times

remy75 3 years 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 2 times

> **Futfuyfyjfj** 11 months ago
> Wrong, enrolling in Intune doesn't automatically mean onboarding in Defender for Endpoint automatically. MDfE is even licensed separately.
> upvoted 2 times

girikedar 3 years ago
I think Enrolling the Device into intune & onboarding the device might work
upvoted 4 times

> **Dreamhaxx** 2 years, 11 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 5 times

bingomutant 3 years ago
I dont know why Intune does not satisfy this
upvoted 3 times

> **sergioandreslq** 3 years 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** 3 years, 5 months ago

Correct - No.

upvoted 1 times

⊟ **olsi** 3 years, 7 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

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

Gesbie 10 months, 3 weeks ago
was on Exam August 9, 2023
upvoted 1 times

Gesbie 10 months, 3 weeks ago
was on Exam August 9, 2023
upvoted 1 times

NinjaSchoolProfessor 1 year, 6 months 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, 11 months ago
Correct - no.
upvoted 2 times

JoeRoxy007 3 years 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 3 years, 1 month 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

Suggested Answer: *B*
Reference:
https://docs.microsoft.com/en-us/microsoft-365/compliance/endpoint-dlp-using?view=o365-worldwide

FronsterRoo 7 months, 3 weeks 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 4 times

ca7859c 2 months ago
in Defender for Cloud Apps or MCAS
"Unsanctioning" an App blocks
"Monitoring" an App Monitors app without blocking
upvoted 1 times

arlia 10 months, 2 weeks 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

Suggested 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, 5 months ago
Answer is correct, you can use mail flow rule to match text pattern but storage account key is binary value
upvoted 9 times

[Removed] Highly Voted 1 year, 7 months 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 7 times

kiketxu 8 months, 1 week 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, 5 months ago
On exam 1/20/2022
upvoted 1 times

ExamReviewerIZ 1 year, 8 months ago
I believe this could be achieved using Mailflow Rules, as you can use regex for Azure Storage Keys.

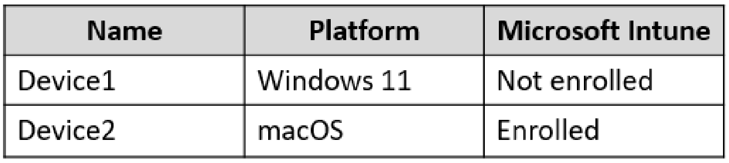
Someone could confirm if is possible to represent an Azure Storage Key using regular expressions.
upvoted 2 times

Question #43 Topic 2

HOTSPOT

-

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

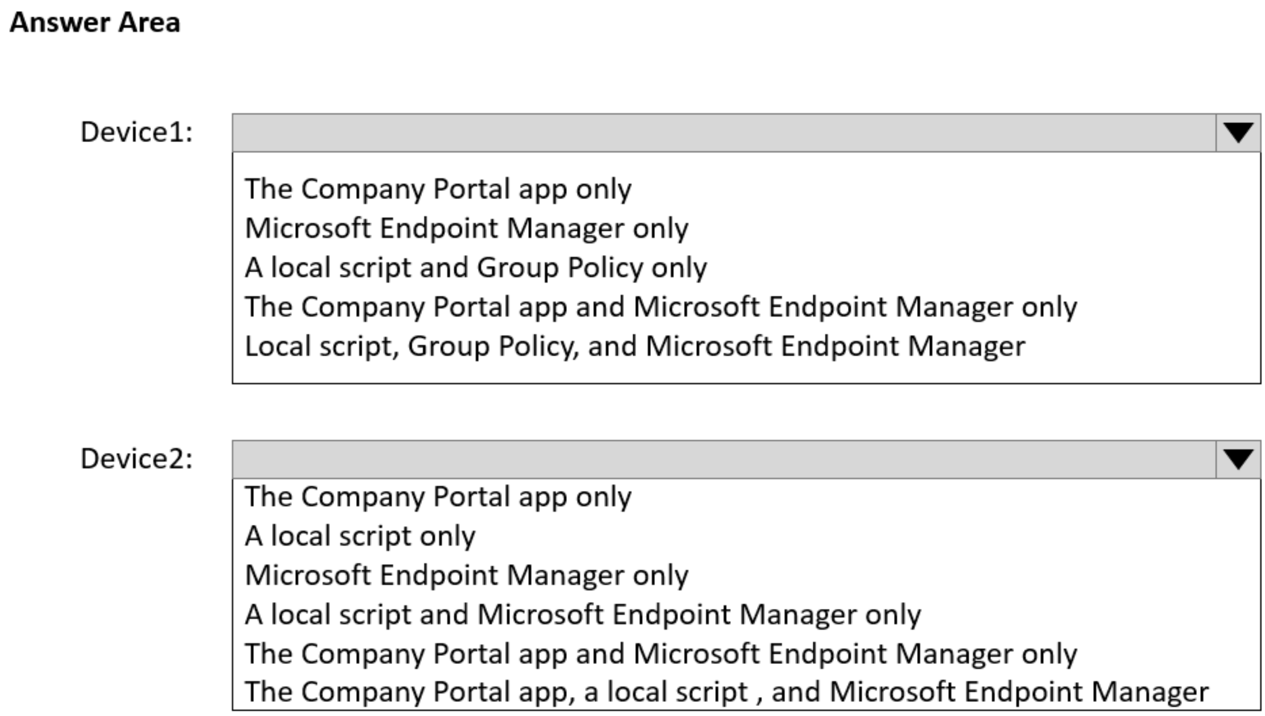


Name	Platform	Microsoft Intune
Device1	Windows 11	Not enrolled
Device2	macOS	Enrolled

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

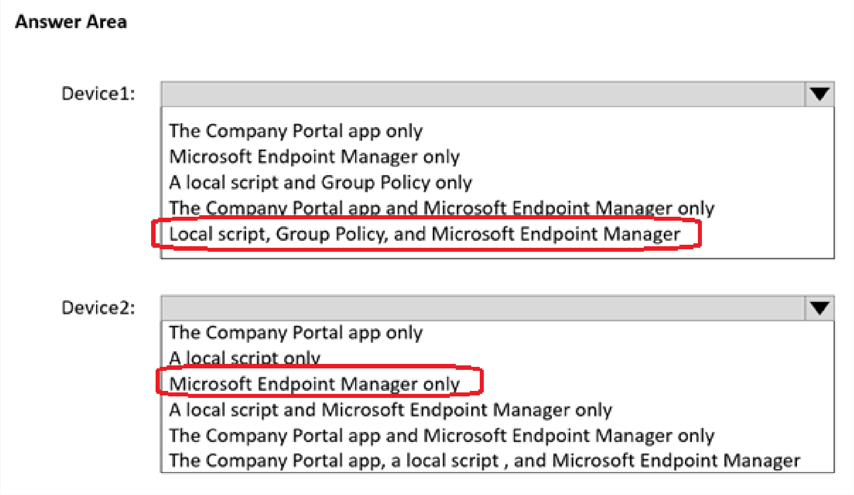
Device1:

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

Suggested 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 1 year, 11 months 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 8 times

itsadel 6 months, 2 weeks ago

Device1 (Windows 11, Not Enrolled in Intune):

A local script and Group Policy only
Explanation:

As you pointed out, the Company Portal app is primarily used for Intune enrollment and management. Since Device1 is not enrolled, it cannot utilize the Company Portal app for onboarding.
For unenrolled devices, you would need to rely on alternative methods like:
Local scripts: To install necessary agents or components for Endpoint DLP.
Group Policy: To enforce security settings and configurations related to data protection.
Device2 (macOS, Enrolled in Intune):

Microsoft Endpoint Manager only
upvoted 1 times

See_Es 1 year, 11 months 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 11 times

JambonBlanc Most Recent 2 months ago

Device1 (Windows 11, Not Enrolled in Intune): Local Script and Group Policy only
To onboard this device to Microsoft Purview and apply Endpoint DLP policies, you can use a local script and Group Policy only. Since the device is not enrolled in Intune, options involving Intune or Microsoft Endpoint Manager are not applicable.

Device2 (macOS, Enrolled in Intune): Microsoft Endpoint Manager only
For this device, the onboarding method would be Microsoft Endpoint Manager only, as it is already enrolled in Intune, allowing seamless management through Endpoint Manager.
upvoted 1 times

Sango 1 year, 4 months ago

macOS is now both Local Script and Intune.
upvoted 4 times

Ruslan23 8 months, 1 week ago

Where did you found this information? Take a look of the Microsoft Doc, you can only use Intune or JAMF:
https://learn.microsoft.com/en-us/purview/device-onboarding-macos-overview#next-steps
upvoted 1 times

cris_exam 1 year, 6 months 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** 1 year, 9 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 2 times

⊟ **formazionehs** 1 year, 10 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 4 times

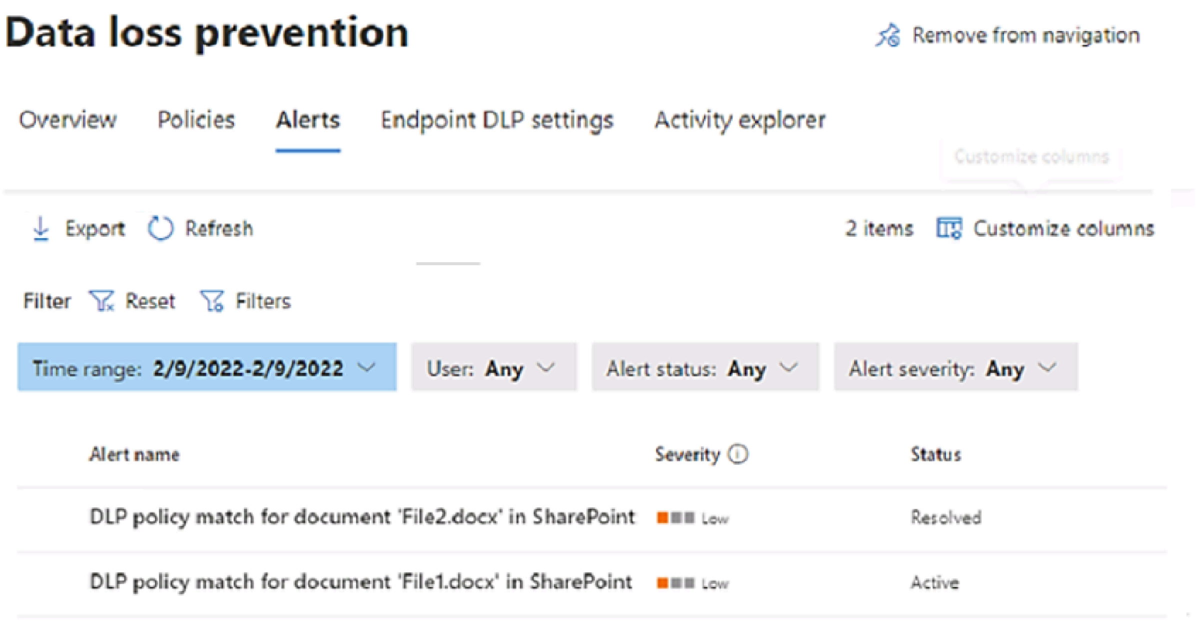
Question #44 *Topic 2*

HOTSPOT

-

You have a Microsoft 365 E5 subscription.

You have the alerts shown in the following exhibit.



Data loss prevention

2 items

Time range: **2/9/2022-2/9/2022** | User: **Any** | Alert status: **Any** | Alert severity: **Any**

Alert name	Severity	Status
DLP policy match for document 'File2.docx' in SharePoint	Low	Resolved
DLP policy match for document 'File1.docx' in SharePoint	Low	Active

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

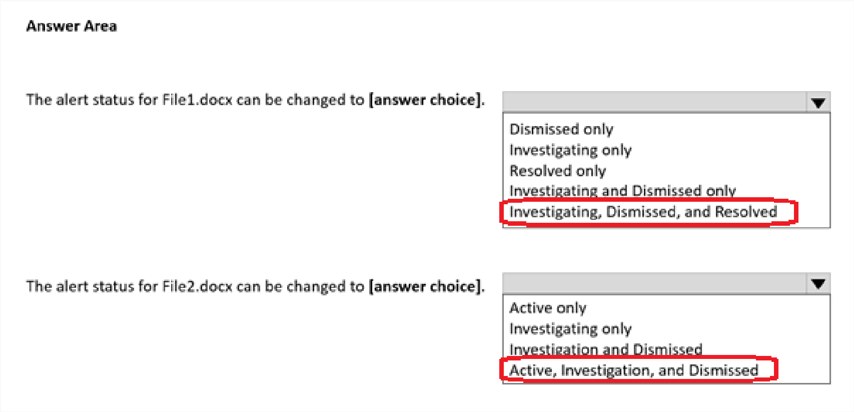
The alert status for File1.docx can be changed to **[answer choice]**.

▼
- 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

Suggested 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 2 years, 3 months 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 6 times

ExamStudy68 Most Recent 10 months ago

Disregard last - I didn't pay close enough attention to the file itself in question.

upvoted 1 times

ExamStudy68 10 months ago

I was confused by this as if it is already resolved how can you change it to resolved and if it is already active how can you change it to active.

upvoted 1 times

Domza 1 year, 5 months ago

Haha, this is funny! they flip the Files 2 and 1 - look closely :)

Its magical ~Q~

Answer is correct!~

upvoted 2 times

phony 1 year, 6 months ago

Watch it: in the picture, file2 (resolved) and file1 (active) reversed compared to the answer area file1 and file2. the given answer is correct.

upvoted 3 times

ServerBrain 1 year, 9 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 4 times

JimboJones99 11 months, 1 week ago

I thought this too, but they have flipped the answer boxes for the files.

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

Suggested Answer: *C*

Community vote distribution

C (91%) 9%

⊟ **See_Es** **Highly Voted 👍** 1 year, 11 months ago

Selected Answer: C

Correct. Tested in my tenant. With all locations selected the sensitive info type is the only option left.

upvoted 12 times

⊟ **Domza** 1 year, 1 month ago

Thank you

upvoted 2 times

⊟ **Amin4799** **Most Recent 🕘** 7 months, 2 weeks ago

Selected Answer: B

Content search query (B) allows for complex pattern matching and searching within the data content. This is ideal for scenarios where you need to define specific criteria for identifying sensitive information beyond pre-defined categories or keywords.

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

Suggested Answer: *D*

Community vote distribution

D (50%) B (50%)

⊟ **Domza** Highly Voted 👍 1 year, 6 months ago

Built-in Trainable classifiers

Microsoft 365 comes with five classifiers already trained and ready to use.

- Résumés
- Source Code
- Harassment
- Profanity
- Threat

Enjoy,
with love

upvoted 7 times

⊟ **[Removed]** Most Recent ⏲ 8 months ago

Selected Answer: D

Trainable classifier

upvoted 1 times

⊟ **Boeroe** 9 months, 1 week ago

Selected Answer: D

Just tested: Trainable classifier > Source code

upvoted 1 times

⊟ **Amin4799** 1 year, 1 month ago

Selected Answer: D

Trainable classifier

upvoted 1 times

⊟ **Ruslan23** 1 year, 2 months ago

Selected Answer: D

Trainable classifier is a better choise.

upvoted 1 times

⊟ **jax84** 1 year, 3 months ago

The sensitive info types specify which specific type, neither of them say "source code sensitive info type", so neither listed would work.

upvoted 1 times

⊟ **emartiy** 1 year, 4 months ago

Selected Answer: D

It says "The solution must minimize administrative effort." So Option D is minimize administrative effort. If you use SIT for source code, wouldn't you perform more effort?

upvoted 1 times

Elangamban 1 year, 6 months ago

Option C

upvoted 1 times

Vashill 1 year, 8 months ago

Selected Answer: B

It should be B

upvoted 1 times

jamspurple 1 year, 8 months ago

Selected Answer: B

There is already a Sensitive Info Type for source code. So it should not be trainable classifier

upvoted 4 times

Davidf 1 year, 10 months ago

Selected Answer: D

There is a source code trainable classifier

upvoted 2 times

217f3c9 2 years, 1 month 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 2 years, 1 month 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 2 years, 2 months ago

Just use the trainable classifier that have been configured and trained already to look for source code

upvoted 1 times

Chris7910 2 years, 4 months ago

Isn't it an administrative effort creating a trainable classifier here?

upvoted 1 times

> **wooyourdaddy** 2 years, 4 months 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.

Suggested Answer: *C*

Community vote distribution

C (100%)

EM1234 1 year ago

Selected Answer: C

I am kind of surprised that there were not any people who chose B.

When you read:
https://learn.microsoft.com/en-us/purview/dlp-alerts-get-started?view=o365-worldwide#aggregate-event-alert-configuration

You see that one way (maybe the most important?) to configure the "threshold" is to increase the instances required for alert.

I am going with C, since it is the more general answer but having B as an option makes it less clear.

upvoted 1 times

emartiy 1 year, 4 months ago

Selected Answer: C

Accepted

upvoted 1 times

Domza 1 year, 7 months ago

Correct ~

upvoted 1 times

Gesbie 1 year, 10 months ago

was on Exam August 9, 2023

upvoted 1 times

xswe 2 years, 2 months ago

Changing the alert threshold will create less alerts but not effect the policy

upvoted 4 times

See_Es 2 years, 5 months ago

Selected Answer: C

Correct. Tested in my tenant

upvoted 4 times

wooyourdaddy 2 years, 4 months 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.

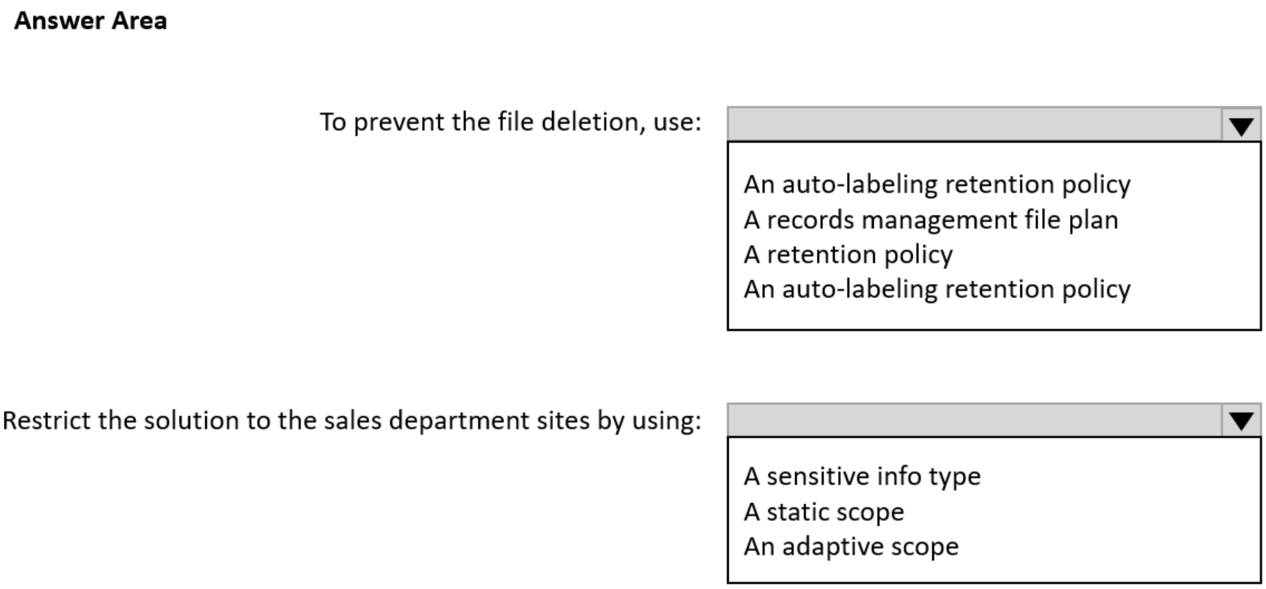
You create SharePoint sites for each department and country. The sites are named by using a naming convention of [Department]-[Country], for example, Sales-France.

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

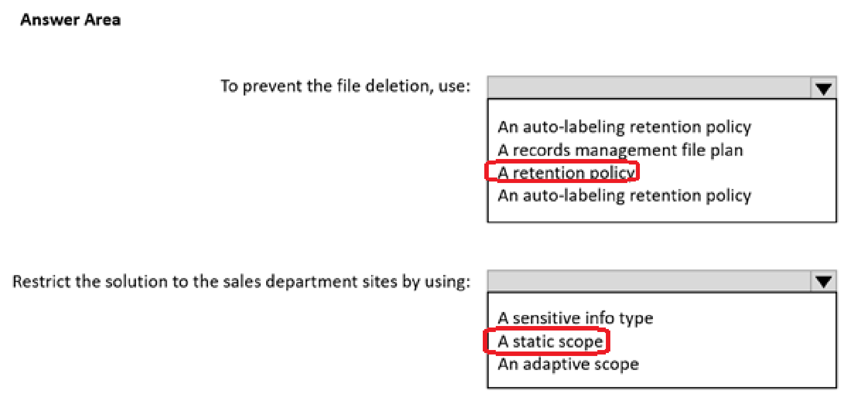
To prevent the file deletion, use: ▼

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

Suggested 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 2 years, 3 months 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 7 times

See_Es Highly Voted 👍 2 years, 5 months 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 2 years, 1 month ago

You forgot "Minimize administrative effort.". Retention policy with static scope (required SharePoint site) will be enough.

upvoted 1 times

ImparaLeon 1 year, 8 months 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

1fea064 Most Recent 11 months ago

They talk about 30 countries, so i belive in their minds doubling the time to make adaptive scope is easier than 30*time to go through all and set static ones

upvoted 1 times

SDiwan 1 year, 3 months ago

Answer should be Retention Policy + Adaptive Scope. In adaptive scope we can mention query that site is "Sales-<whattever>. So, it is less admin overhead than static scope

upvoted 1 times

217f3c9 2 years 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

xswe 2 years, 2 months 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

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

Suggested Answer: *C*

Community vote distribution

A (82%) C (18%)

tarroka Highly Voted 1 year, 11 months ago

Correct Answer is A OneDrive as it refers to document in the question

upvoted 14 times

See_Es 1 year, 11 months 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

SDiwan Most Recent 9 months, 2 weeks ago

Selected Answer: A

Files in Teams chat are stored in OneDrive

upvoted 2 times

emartiy 10 months, 1 week ago

Selected Answer: C

For 1:1 chat yes documents stores on OneDrive Account but question is about Team Chat sessions, it maybe a Team chat etc. If you share document in Team chat not a private 1:1 chat, files are stored at SharePoint, so For all Chat sessions, displayed answer seems correct.

upvoted 2 times

emartiy 10 months, 1 week ago

https://learn.microsoft.com/en-us/purview/dlp-microsoft-teams#add-microsoft-teams-as-a-location-to-existing-dlp-policies

upvoted 1 times

EM1234 6 months, 3 weeks ago

Did you read the page you shared?

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 enforced.

upvoted 1 times

xswe 1 year, 8 months 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 1 year, 9 months 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 3 times

FireOzzie 1 year, 9 months 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 1 year, 10 months ago

yes agreed

upvoted 1 times

formazionehs 1 year, 10 months 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

Suggested Answer: *D*

Community vote distribution

C (100%)

CharlieGolf Highly Voted 2 years, 3 months 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 14 times

JimboJones99 Most Recent 11 months, 2 weeks ago

Selected Answer: C

https://learn.microsoft.com/en-us/purview/trainable-classifiers-definitions#harassment

Does not apply to XLSX files.

upvoted 1 times

predator8149 1 year, 1 month ago

The ask is about retention label, not trainable classifier. Answer D is correct and retention label gets assigned to a site and not to files.

upvoted 1 times

emartiy 1 year, 4 months ago

Selected Answer: C

https://learn.microsoft.com/en-us/purview/trainable-classifiers-definitions#harassment

upvoted 1 times

SFine 1 year, 6 months ago

Any confirmation on this? MS tests like to be tricky... They said it can be applied, not if it will detect. It can be applied to .xlsx but just won't detect anything.

upvoted 1 times

naren49 1 year, 7 months 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 1 year, 10 months 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 2 times

xswe 2 years, 2 months 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 2 years, 2 months 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

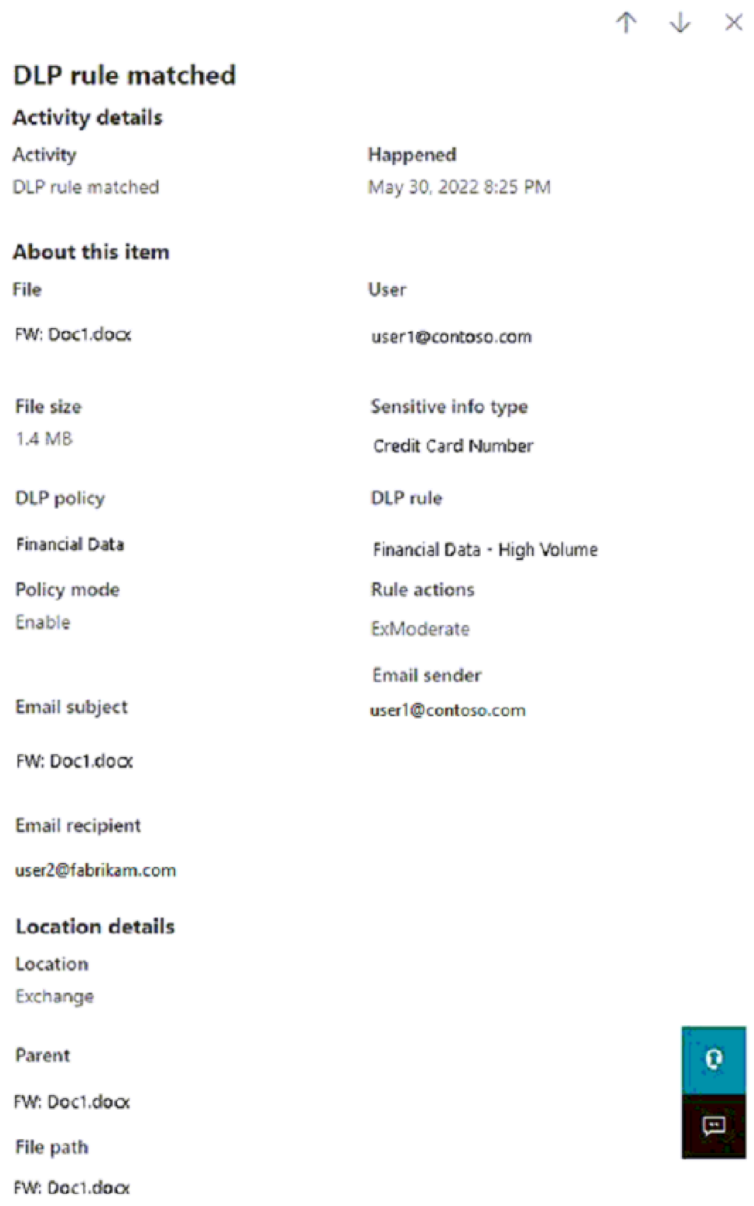
Question #51 *Topic 2*

HOTSPOT

-

You have a Microsoft 365 E5 subscription.

You have the data loss prevention (DLP) rule match shown in the following exhibit.



DLP rule matched

Activity details

Activity	Happened
DLP rule matched	May 30, 2022 8:25 PM

About this item

File	User
FW: Doc1.docx	user1@contoso.com
File size	Sensitive info type
1.4 MB	Credit Card Number
DLP policy	DLP rule
Financial Data	Financial Data - High Volume
Policy mode	Rule actions
Enable	ExModerate
	Email sender
Email subject	user1@contoso.com
FW: Doc1.docx	
Email recipient	
user2@fabrikam.com	

Location details

Location

Exchange

Parent

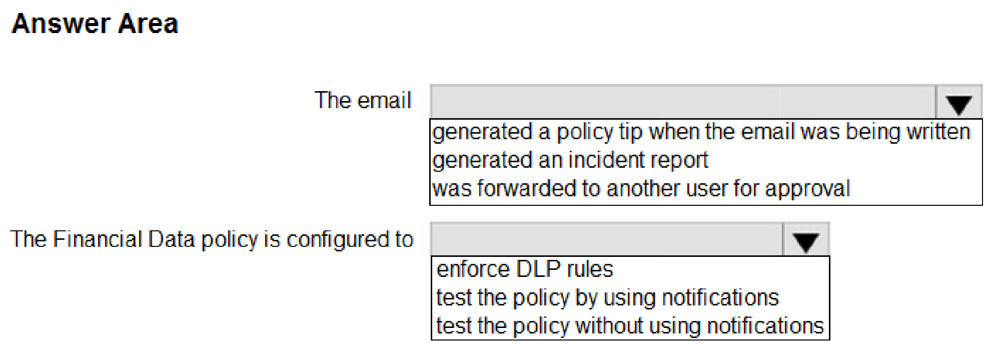
FW: Doc1.docx

File path

FW: Doc1.docx

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.

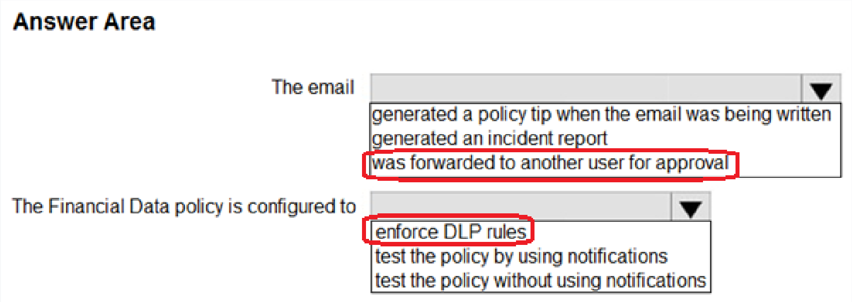


Answer Area

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

Suggested Answer:



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

⊟ **xswe** Highly Voted 2 years, 2 months ago

The email... was forwarded to another user for approval, user2

Enforce DLP rules, since "Policy mode: Enable"

upvoted 7 times

⊟ **luissaro** 2 years, 2 months ago

how can approver be of another domain?

upvoted 1 times

⊟ **217f3c9** 2 years, 1 month ago

afaik the approver is not listed here.

upvoted 1 times

⊟ **Futfuyfyjfj** 1 year, 5 months ago

You can have multiple custom domains added to your M365 tenant, right? Another domain doesn't mean a user with another home tenant perse.

upvoted 1 times

⊟ **JimboJones99** Most Recent 11 months, 2 weeks ago

"ExModerate" means to send to someone for approval

upvoted 4 times

⊟ **hsinchang** 1 year, 10 months ago

Moderate -> Forward the message for approval

Policy mode: Enable -> Enforce DLP rules

upvoted 2 times

⊟ **cris_exam** 2 years 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 2 times

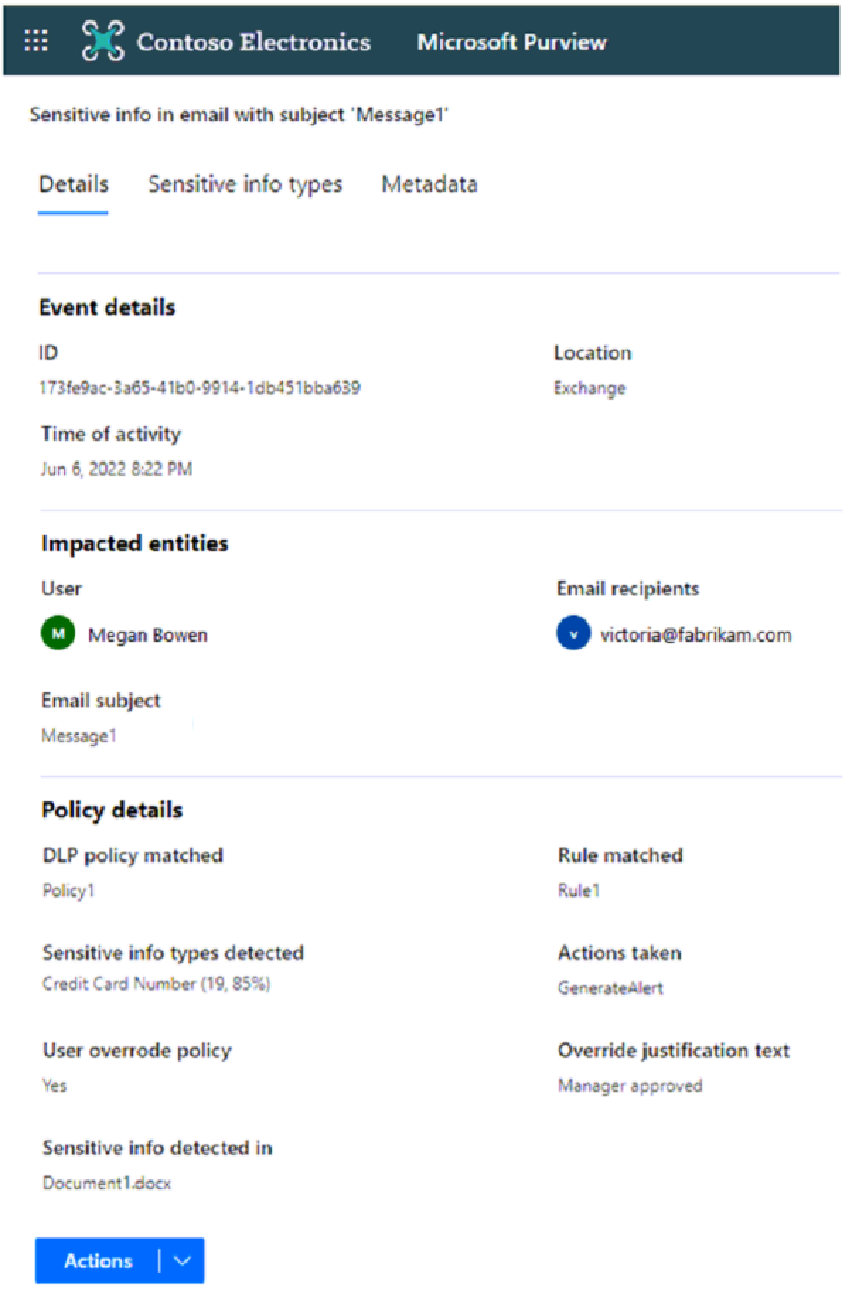
Question #52 *Topic 2*

HOTSPOT

-

You have a Microsoft 365 E5 subscription.

You receive the data loss prevention (DLP) alert shown in the following exhibit.



Sensitive info in email with subject 'Message1'

Event details

ID
173fe9ac-3a65-41b0-9914-1db451bba639

Location
Exchange

Time of activity
Jun 6, 2022 8:22 PM

Impacted entities

User
Megan Bowen

Email recipients
victoria@fabrikam.com

Email subject
Message1

Policy details

DLP policy matched
Policy1

Rule matched
Rule1

Sensitive info types detected
Credit Card Number (19, 85%)

Actions taken
GenerateAlert

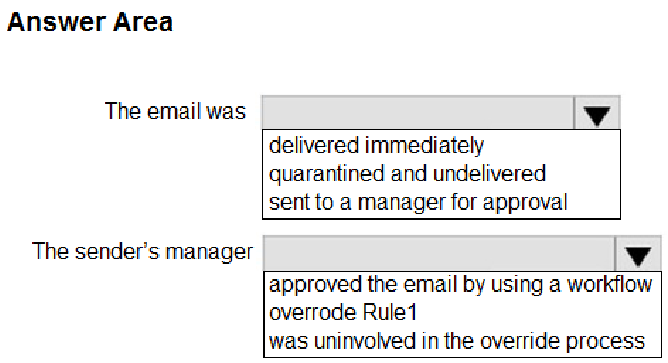
User overrode policy
Yes

Override justification text
Manager approved

Sensitive info detected in
Document1.docx

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.

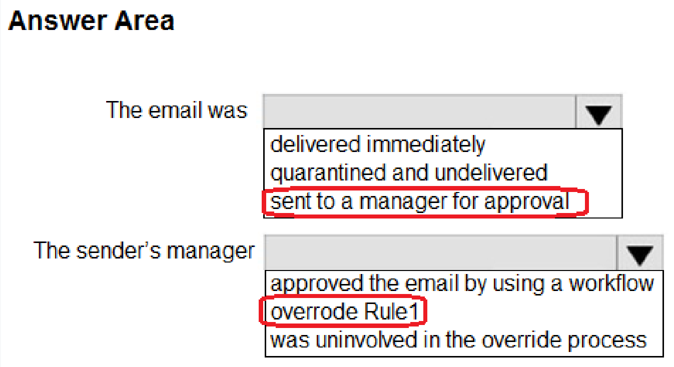


Answer Area

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

Suggested 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 2 years, 2 months 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 23 times

⊟ **Boeroe** 9 months, 1 week ago

Agree, the User overrode the policy using a justification text. The manager had no involvement in this proces

upvoted 5 times

⊟ **cris_exam** Highly Voted 2 years 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 6 times

⊟ **Futfuyfyjfj** 1 year, 4 months ago

2-> not correct it's just plain text filled by the user himself, manager was not involved in the override action from a technical perspective.

upvoted 2 times

⊟ **Domza** Most Recent 1 year, 5 months ago

Why would you send email it for approval, if or generate an alert and override Rule?

upvoted 1 times

⊟ **xswe** 2 years, 2 months ago

Sent to manager for approval, since "Manager approved"
Overrode Rule1 since "User overrode policy = Yes"

upvoted 3 times

⊟ **217f3c9** 2 years ago

Its only the text the user put in while overriding the policy.

upvoted 4 times

⊟ **Futfuyfyjfj** 1 year, 4 months ago

Exactly!

upvoted 1 times

⊟ **CharlieGolf** 2 years, 3 months 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

⊟ **EM1234** 1 year ago

I agree with this logic. The user overided and then chose "Manager Approved.. etc". The user was the only one who did anything here and the email was sent immediately

upvoted 1 times

⊟ **bsongwk** 2 years, 2 months 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 5 times

⊟ **pokus00132** 2 years, 2 months ago

I agree that the first part is also wrong, it should be "delivered immediately"

upvoted 4 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

Suggested Answer: *D*

Domza 7 months, 3 weeks ago

Looks good~

upvoted 1 times

heshmat2022 8 months, 1 week 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 10 months, 3 weeks ago

was on Exam August 9, 2023

upvoted 1 times

xswe 1 year, 2 months ago

File policy in MCA is used for DLP policies

upvoted 1 times

CharlieGolf 1 year, 3 months 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

Suggested Answer: *A*

Community vote distribution

A (70%) C (30%)

CharlieGolf Highly Voted 1 year, 9 months 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 12 times

Domza 1 year, 1 month ago

Thank you for the link

upvoted 2 times

EM1234 6 months, 3 weeks ago

The answer looks right to me according to your link and having read the chart.

upvoted 2 times

Amin4799 Most Recent 7 months, 2 weeks ago

Selected Answer: C

The correct answer is: C. 1:1/n chats, general channels, and private channels

Here's why:

By default, DLP policies applied to the Teams chat and channel messages location encompass all message types within Teams. This includes:
1:1 chats: Direct messages between two users.
n:1 chats: Group chats involving multiple users.
General channels: Public channels accessible by all members of a team.
Private channels: Restricted channels accessible only to authorized team members.
Since the DLP policy is applied to the overall "Teams chat and channel messages" location for both User1 and User2, it will provide protection across all these Teams entities.

There are no inherent limitations in the scenario that would restrict DLP to specific channel types. The policy applies to the entirety of chat and channel messages within Teams for the designated users.

upvoted 4 times

Jideakin 3 months, 3 weeks ago

Read this: https://learn.microsoft.com/en-us/microsoft-365/compliance/dlp-microsoft-teams?view=o365-worldwide#scope-of-dlp-protection

upvoted 1 times

Amin4799 7 months, 2 weeks ago

Selected Answer: C

In Microsoft Teams, there are three main types of communication channels:

1:1/n chats: These are private conversations between two users or small group chats.

General channels: These are channels within a team where all team members can participate in discussions and share files.

Private channels: These are channels within a team that are visible and accessible only to specific members.

When you apply a data loss prevention (DLP) policy to the Teams chat and channel messages location for User1 and User2, it means that any communication happening in these channels by User1 and User2 will have DLP protection.

So, the correct answer is:

C. 1:1/n chats, general channels, and private channels
upvoted 1 times

⊟ **Jideakin** 3 months, 3 weeks ago
Read this: https://learn.microsoft.com/en-us/microsoft-365/compliance/dlp-microsoft-teams?view=o365-worldwide#scope-of-dlp-protection
upvoted 1 times

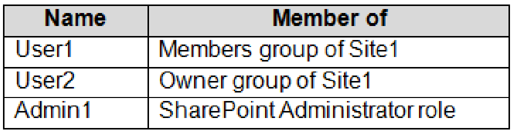
⊟ **xswe** 1 year, 8 months ago
Tested out, its correct
upvoted 1 times

Question #55 Topic 2

HOTSPOT

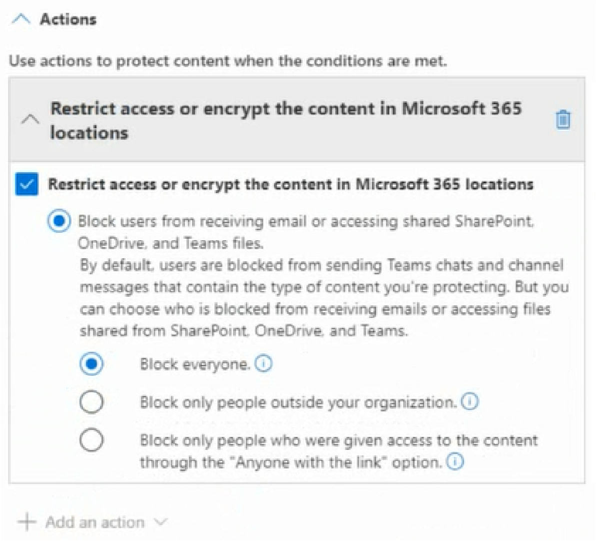
-

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.



Actions

Use actions to protect content when the conditions are met.

Restrict access or encrypt the content in Microsoft 365 locations

☑ Restrict access or encrypt the content in Microsoft 365 locations

● Block users from receiving email or accessing shared SharePoint, OneDrive, and Teams files.
By default, users are blocked from sending Teams chats and channel messages that contain the type of content you're protecting. But you can choose who is blocked from receiving emails or accessing files shared from SharePoint, OneDrive, and Teams.

● Block everyone. ⓘ

○ Block only people outside your organization. ⓘ

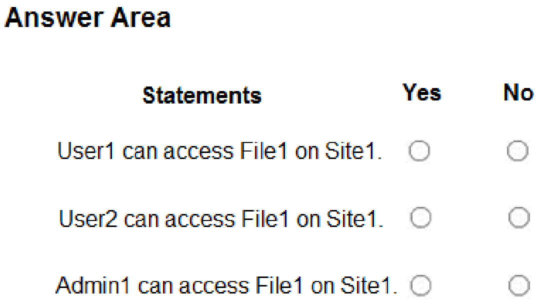
○ Block only people who were given access to the content through the "Anyone with the link" option. ⓘ

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.

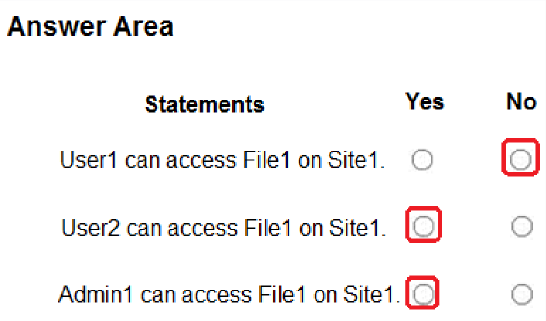
NOTE: Each correct selection is worth one point.



Answer Area

Statements	Yes	No
User1 can access File1 on Site1.	○	○
User2 can access File1 on Site1.	○	○
Admin1 can access File1 on Site1.	○	○

Suggested Answer:



Answer Area

Statements	Yes	No
User1 can access File1 on Site1.	○	[✓ ○]
User2 can access File1 on Site1.	[✓ ○]	○
Admin1 can access File1 on Site1.	[✓ ○]	○

⊟ **CharlieGolf** Highly Voted 2 years, 3 months 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 5 times

⊟ **Domza** 1 year, 4 months ago

Thank you for the link. Y/Y/Y - correct answers~

upvoted 3 times

⊟ **Futfuyfyjfj** 1 year, 4 months ago

There is no clue user 1 is the content owner, he is only the uploader...

upvoted 1 times

⊟ **IndigoRabbit** 10 months, 2 weeks ago

User who uploads a file in SPO is considered the file owner.

upvoted 4 times

⊟ **cris_exam** Highly Voted 2 years 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 5 times

⊟ **cris_exam** 2 years ago

Hence answer is: N / Y / Y

upvoted 3 times

⊟ **ca7859c** Most Recent 1 month, 3 weeks ago

YYY

Explanation for 1st Question: Block everyone. Only the content owner, last modifier, and site admin will continue to have access

https://learn.microsoft.com/en-us/microsoft-365/compliance/dlp-policy-reference?view=o365-worldwide#actions

upvoted 1 times

⊟ **Jideakin** 3 months, 3 weeks ago

Answer is: YYN

Block everyone. Only the content owner, last modifier, and site admin will continue to have access.

User1 is uploader, hence file owner. No mention that ownership has changed.

So User1 can access

User2 is member of site owners and also last modifier of file.

So User2 can access

Admin1 is SharePoint Administrator, NOT SiteAdmin.

So Admin1 cannot access

No Automatic Site Ownership:
SharePoint administrators do not automatically have owner permissions for all sites within the tenant.
upvoted 1 times

⊟ **Dools** 7 months, 1 week ago
In SharePoint Online, the user who uploads a document typically becomes the document owner. However, the ownership concept in SharePoint is a bit nuanced. Here's a quick breakdown:

Uploader's Role: The person who uploads the document is generally the initial "owner" and has full control over the document's permissions and settings.

Site Ownership: The actual ownership might also be influenced by site-level permissions. For instance, site owners have overarching control over all documents within that site.

Sharing and Permission Changes: The initial owner (uploader) can share the document with others and adjust permissions, potentially assigning ownership or editing rights to other users.

Metadata and Versioning: SharePoint also tracks the document metadata, including who last modified the document, providing a detailed history of document interactions.
upvoted 1 times

⊟ **xswe** 2 years, 2 months 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

⊟ **luissaro** 2 years, 2 months ago
there is no evidence user1 is owner of the file, he just uploaded it
upvoted 3 times

⊟ **pokus00132** 2 years, 2 months 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** 2 years ago
I agree with NO, YES, YES - no mention that user1 is the content owner.
upvoted 1 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

Suggested Answer: *B*

Community vote distribution

B (100%)

Davidf 10 months, 2 weeks ago

Selected Answer: B

Cloud app discovery monitors network traffic to discover apps in the cloud, not local executable

upvoted 2 times

pokus00132 1 year, 2 months 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 1 year, 2 months ago

Nope, app discovery wont succeed with what they are asking for

upvoted 1 times

Question #57 *Topic 2*

HOTSPOT

-

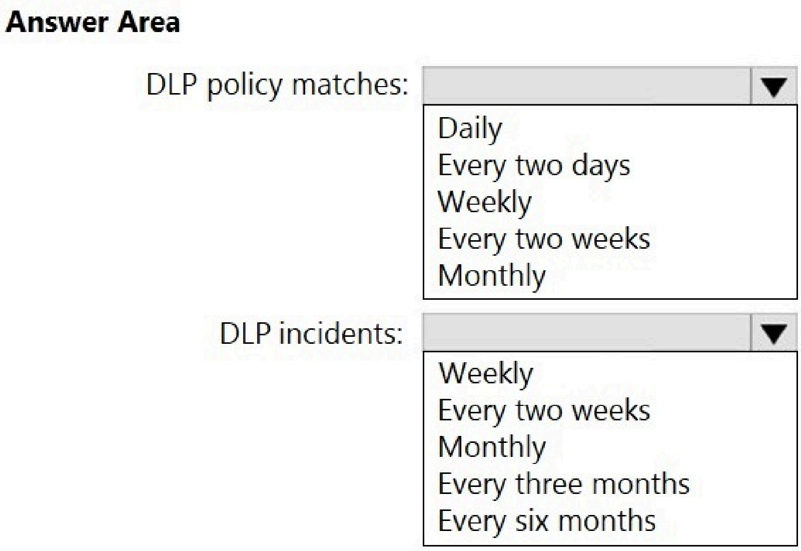
You have a Microsoft 365 E5 subscription that uses data loss prevention (DLP) to protect sensitive information.

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.

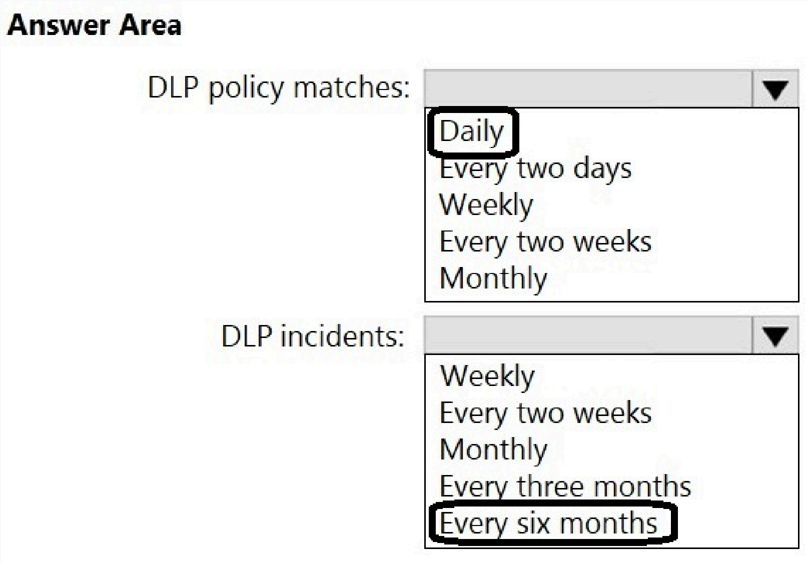


Answer Area

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

Suggested 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]

Dools 7 months, 1 week ago

In Microsoft 365 Purview, the shortest frequency at which a DLP (Data Loss Prevention) policy matches report can be generated is daily. This means you can receive a report every day detailing the matches found by your DLP policies.

In Microsoft 365 Purview, the longest period you can set for generating DLP (Data Loss Prevention) incident reports is 90 days. This allows you to review and analyze incidents over a three-month period, which can be useful for identifying trends and patterns in data loss incidents.

upvoted 1 times

CharlieGolf 1 year, 4 months ago

Defender portal retains incident history for 6 months. https://learn.microsoft.com/en-us/purview/dlp-alert-investigation-learn

upvoted 3 times

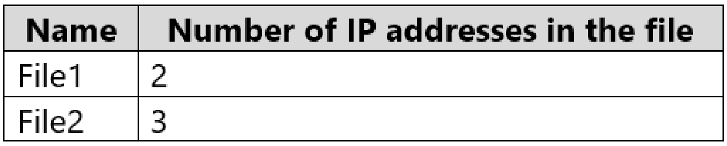
ca7859c 2 months ago

Agreed.

upvoted 1 times

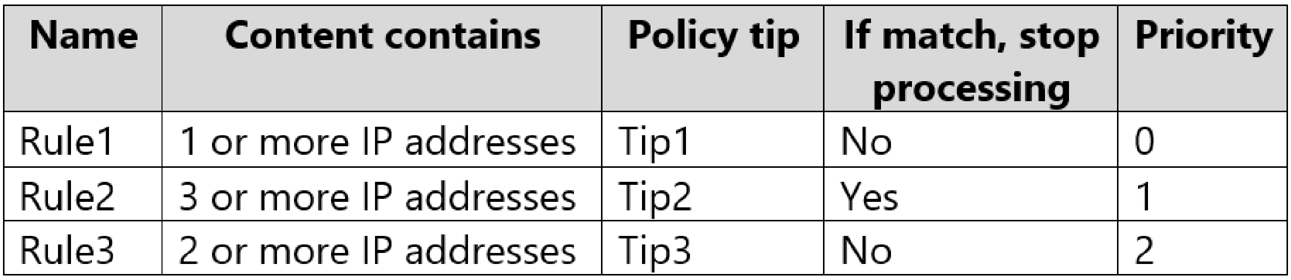
Question #58 *Topic 2*

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

Suggested Answer: *D*

Community vote distribution

D (57%) B (43%)

Kuteron Highly Voted 7 months, 3 weeks ago

Selected Answer: B

Out of Doc Articel: https://learn.microsoft.com/en-us/purview/dlp-policy-reference it is D:

Only the policy tip from the highest priority, most restrictive rule will be shown. For example, a policy tip from a rule that blocks access to content will be shown over a policy tip from a rule that simply sends a notification. This prevents people from seeing a cascade of policy tips.

upvoted 5 times

Jideakin Most Recent 3 months, 3 weeks ago

Selected Answer: A

Rule1 will be evaluated because it has the highest priority, then followed by Rule2. Rule3 will NOT be evaluated because Rule2 has the option to stop processing further rules. Then Rule1 will be applied because it has the highest priority.

upvoted 1 times

belyo 8 months ago

Selected Answer: B

correct answer B

upvoted 1 times

Ruslan23 1 year, 2 months ago

Selected Answer: D

Multiple tips can be displayed, both Rule1 and Rule2 are applied, the second one has stop if matches so Rule3 is not applied.

upvoted 1 times

SDiwan 1 year, 3 months ago

Selected Answer: B

Tip 2 only is the right answer.

Rule 2 is the most restrictive and so wins

upvoted 1 times

> **mb0812** 1 year, 3 months ago
>
> Incorrect. It will be D.
>
> Rule one does not stop processing after it is matched. After Tip 1, the rule 2 gets executed as it is next in the priority. Rule 2 has the condition set as "Stop processing after match found". Hence both rule 1 and 2 execute, which means Tip1 and Tip 2
>
> upvoted 3 times
>
> > **Jideakin** 3 months, 3 weeks ago
> >
> > It will process both rules but only one will get enforce, that is the higher priority one Rule1 and the policy tip there is Tip1 hence Tip1 will get applied. Answer is A
> >
> > upvoted 1 times

CharlieGolf 1 year, 4 months ago

Selected Answer: D

Rule1 with Priority 0 is the highest priority and runs first. It matches, displays the tip, and proceeds to Rule2, which matches, runs its tip action, and then halts further processing. Unlike policies which will only execute the highest priority with most restrictive actions, multiples rules can and will execute if matched and until a stop-processing is reached. https://learn.microsoft.com/en-us/purview/dlp-policy-reference

upvoted 4 times

> **Jideakin** 3 months, 3 weeks ago
>
> This is from the page you reference. Please read it well. Multiple rules will NOT execute.
> 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 doesn't 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.
>
> upvoted 1 times

sonstevold 1 year, 5 months ago

Selected Answer: B

If you have multiple rules in a policy, you can use the Additional options to control further rule processing if there's a match to the rule you're editing as well as setting the priority for evaluation of the rule.

https://learn.microsoft.com/en-us/purview/dlp-policy-reference#additional-options

upvoted 1 times

Romeokton 1 year, 7 months ago

Selected Answer: B

I agree with ae88d96

upvoted 1 times

ae88d96 1 year, 7 months 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 4 times

> **Jideakin** 3 months, 3 weeks ago
>
> No Rule2 does NOT have a higher priority than Rule1 whose priority is "0"
>
> upvoted 1 times

Futfuyfyjfj 1 year, 4 months ago

Rule 2 as a higher priority than rule3?

upvoted 1 times

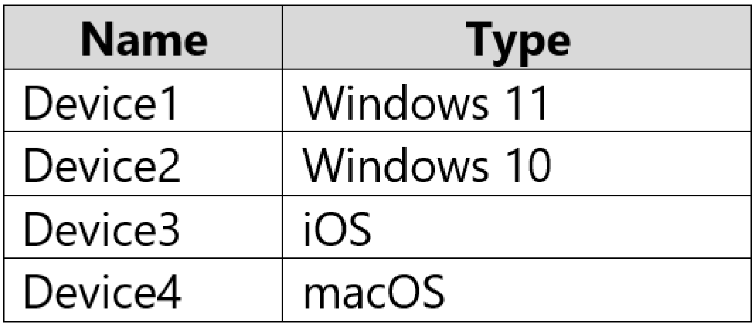
Pablosanchez 1 year, 7 months ago

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

Suggested Answer: *D*

Community vote distribution

D (100%)

Domza 1 year ago

Repeat question. There is one before.. Win10/11 and macOs

upvoted 1 times

Romeokton 1 year, 1 month ago

Selected Answer: D

Definitely D

upvoted 1 times

Domza 1 year, 1 month ago

Win10/11 and macOs

upvoted 2 times

izgi43 1 year, 1 month ago

on the exam thu nov 9

upvoted 2 times

Pablosanchez 1 year, 1 month 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

Suggested Answer: *A*

Community vote distribution

U (100%)

JanioHSilva 7 months, 1 week ago

To identify which Data Loss Prevention (DLP) rules include conditions that can trigger DLP policies in Microsoft 365 E5, the most appropriate report to use from the Microsoft Purview compliance portal would be one that details DLP policy matches . This report provides an overview of the triggered rules and can help you understand what specific conditions are leading to the policies being activated.

The most appropriate option, therefore, would be:

A. DLP policy matches
This report will help identify the rules that have been triggered, providing insights into the specific conditions under which DLP policies are being applied. This is crucial for tuning and optimizing DLP policies to reduce false positives and ensure effective protection of sensitive data.
upvoted 3 times

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

Suggested Answer: *D*

Dools 8 months ago

Selected Answer: D

Tricky question. *.contoso.com would block web1 and web2 but it would also block web3.contoso.com, web4.... and so on.

I believe D is the least administrative effort.

upvoted 1 times

Domza 1 year, 5 months ago

Link: https://learn.microsoft.com/en-us/purview/dlp-configure-endpoint-settings#browser-and-domain-restrictions-to-sensitive-data

upvoted 2 times

kingAzure 1 year, 6 months ago

Seems correct? You can't do web*, because maybe there is a web3.contoso.com that they don't want to restrict?

upvoted 4 times

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.

Suggested Answer: *C*

Community vote distribution

C (88%) 13%

PsiCzar 10 months, 3 weeks ago

While the answer appears to be C based on Romeokton's link, D. would be less administrative effort. Just create an advanced DLP rule that includes a group condition AND NOT "Sender is" and include user1 and user2's email addresses. No need for a distribution group.

upvoted 1 times

SDiwan 1 year, 3 months ago

Selected Answer: C

Basically to exclude users from a policy, we need to create an Advanced DLP rule where we need to create a NOT group and specify sender/recipient is a member of a selected distribution group.

Now, the question asks "what should you do first?". So, in this case before we can configure advanced DLP rule , we must create the distribution group to be excluded from the rule condition.

So answer is C

upvoted 2 times

Domza 1 year, 5 months ago

Its asking to "exclude" two users named User1 and User2 from DLP1 - Your first step is create advanced rule? Really?

upvoted 1 times

kingAzure 1 year, 6 months ago

Selected Answer: C

C is correct.

"If you choose to include specific distribution groups in Exchange, the DLP policy is scoped only to the emails sent by members of that group. Similarly, excluding a distribution group excludes all the emails sent by the members of that distribution group from policy evaluation".

https://learn.microsoft.com/en-us/purview/dlp-policy-reference

upvoted 3 times

Romeokton 1 year, 7 months ago

Selected Answer: C

After reviewing carefully I agree with C.

https://learn.microsoft.com/en-us/purview/dlp-policy-reference#policy-scoping

upvoted 2 times

Romeokton 1 year, 7 months 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

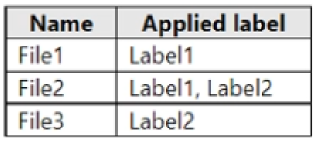
Question #63 *Topic 2*

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:

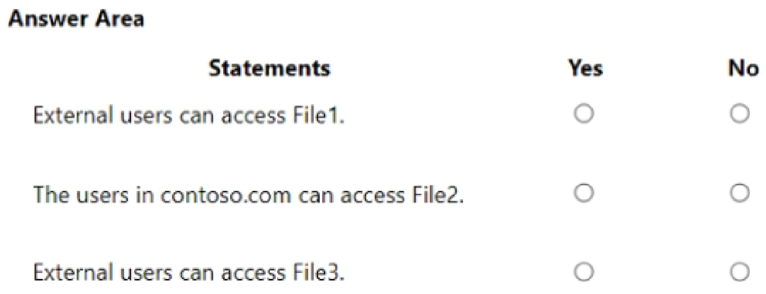
- Conditions: Label1 or Label2
- Actions: Restrict access to the content
- Priority: 1

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.	○	○