Custom View Settings

Topic 1 - Question Set 1

Question #1 *Topic 1*

You have several Conditional Access policies that block noncompliant devices from connecting to services.
You need to identity which devices are blocked by which policies.
What should you use?

A. the Setting compliance report in the Microsoft Endpoint Manager admin center

B. Sign-ins in the Azure Active Directory admin center

C. Activity log in the Cloud App Security admin center

D. Audit logs in the Azure Active Directory admin center

prats005 Highly Voted 4 months ago
https://docs.microsoft.com/en-us/azure/active-directory/conditional-access/troubleshoot-conditional-access | ANSWER is COrrect
upvoted 6 times

theboywonder Most Recent 1 month ago
The given answer is correct:
- The first way is to review the error message that appears. For problems signing in when using a web browser, the error page itself has detailed information. This information alone may describe what the problem is and that may suggest a solution.

- The second method to get detailed information about the sign-in interruption is to review the Azure AD sign-in events to see which Conditional Access policy or policies were applied and why.

source: https://docs.microsoft.com/en-us/azure/active-directory/conditional-access/troubleshoot-conditional-access
upvoted 1 times

CAINBJJ 1 month, 1 week ago
Sorry guys... reading the documentation again... in this part that's clear
"The left side provides details collected at sign-in and the right side provides details of whether those details satisfy the requirements of the applied Conditional Access policies. Conditional Access policies only apply when all conditions are satisfied or not configured."
In the Conditional Access error codes, the code "53000 DeviceNotCompliant"
The answer is correct
upvoted 2 times

CAINBJJ 1 month, 2 weeks ago
Correct answer is A,

Open the Intune Device compliance dashboard:

Sign in to the Microsoft Endpoint Manager admin center.

Select Devices > Overview > Compliance status tab.

https://docs.microsoft.com/en-us/mem/intune/protect/compliance-policy-monitor
upvoted 3 times

IsrarChanna 1 month, 3 weeks ago
https://docs.microsoft.com/en-us/azure/active-directory/conditional-access/troubleshoot-conditional-access
upvoted 2 times

OMPAROZ 2 months ago
Wrong answer, it Should be A
A. the Setting compliance report in the Microsoft Endpoint Manager admin center
This to review a complete list of devices which noncompliant, answer B is for individual users
upvoted 3 times

JoelB 1 month, 2 weeks ago
EPM gives you the list of non-compliant devices but does not tell you which policies are preventing it from signing in. The Sign Ins in AAD provides you with the Conditional Access Policy details, although the export data does not contain information about the individual policies and you need to check each entry.
Honestly, I struggle to identify an easy solution to display all non-compliant devices with the relevant CA policy the way the question is worded.
upvoted 2 times

kiketxu 4 months, 4 weeks ago
given answer is correct.
upvoted 4 times

Question #2 *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 that is associated to a Microsoft Azure Active Directory (Azure AD) tenant named contoso.com.
You use Active Directory Federation Services (AD FS) to federate on-premises Active Directory and the tenant. Azure AD Connect has the following settings:

- Source Anchor: objectGUID
- Password Hash Synchronization: Disabled
- Password writeback: Disabled
- Directory extension attribute sync: Disabled
- Azure AD app and attribute filtering: Disabled
- Exchange hybrid deployment: Disabled

User writeback: Disabled -

-

You need to ensure that you can use leaked credentials detection in Azure AD Identity Protection.
Solution: You modify the Azure AD app and attribute filtering settings.
Does that meet the goal?

A. Yes

B. No

AmerSerhan Highly Voted 1 year, 3 months ago
If your organization uses a hybrid identity solution with pass-through authentication or federation, then you should enable password hash sync for the following two reasons:

The Users with leaked credentials report in the Azure AD management warns you of username and password pairs, which have been exposed on the "dark web." An incredible volume of passwords is leaked via phishing, malware, and password reuse on third-party sites that are later breached. Microsoft finds many of these leaked credentials and will tell you, in this report, if they match credentials in your organization – but only if you enable password hash sync!
upvoted 20 times

doublekill Highly Voted 5 months, 2 weeks ago
The answer is NO, sourceanchor attribute is used to identify the objects. This is that MS says: "The sourceAnchor attribute is defined as an attribute immutable during the lifetime of an object. It uniquely identifies an object as being the same object on-premises and in Azure AD. The attribute is also called immutableId and the two names are used interchangeable."
https://docs.microsoft.com/en-us/azure/active-directory/hybrid/plan-connect-design-concepts#:~:text=%20To%20switch%20from%20objectGUID%20to%20ConsistencyGuid%20as,of%20the%20ms-DS-ConsistencyGuid%20attribute%20in%20your...%20More%20
upvoted 5 times

rkapoor8855 Most Recent 6 months, 3 weeks ago
The answer is NO
upvoted 1 times

svm_Terran 8 months ago
given asnwer is correct.
upvoted 1 times

kiketxu 5 months, 1 week ago
The answer is NO
upvoted 1 times

Question #3 *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 that is associated to a Microsoft Azure Active Directory (Azure AD) tenant named contoso.com.
You use Active Directory Federation Services (AD FS) to federate on-premises Active Directory and the tenant. Azure AD Connect has the following settings:

- Source Anchor: objectGUID
- Password Hash Synchronization: Disabled
- Password writeback: Disabled
- Directory extension attribute sync: Disabled
- Azure AD app and attribute filtering: Disabled
- Exchange hybrid deployment: Disabled
- User writeback: Disabled

You need to ensure that you can use leaked credentials detection in Azure AD Identity Protection.
Solution: You modify the Password Hash Synchronization settings.
Does that meet the goal?

A. Yes

B. No

KeepingITreal Highly Voted 1 year, 3 months ago
Leaked credentials detection in Azure AD Identity Protection requires Password Hash Sync enabled in Azure AD Connect
upvoted 21 times

m2L Highly Voted 1 year, 6 months ago
https://www.microsoft.com/security/blog/2019/05/30/demystifying-password-hash-sync/
upvoted 7 times

PrimeAltariz Most Recent 2 months, 3 weeks ago
The answer is correct, so that it can be validated if the credential is compromised, it must be in Azure AD, in this environment it is achieved with the password has sync: https://docs.microsoft.com/en-us/azure / security / fundamentals / steps-secure-identity # protect-against-leaked-credentials-and-add-resilience-against-outages
upvoted 1 times

kiketxu 5 months, 1 week ago
NO (....but only if you enable password hash sync or have cloud-only identities!)
https://docs.microsoft.com/en-us/azure/security/fundamentals/steps-secure-identity
upvoted 1 times

kiketxu 4 months, 3 weeks ago
You need to ENABLE not modify settings....
upvoted 2 times

bingomutant 4 months, 2 weeks ago
agree - modify does not necessarily mean Enable...
upvoted 1 times

llama321 2 months, 3 weeks ago
It has either enable or disable. Now its in disable state and modify mean enable. What else it could be? half enable?
upvoted 1 times

prats005 4 months ago
what else could it mean?
upvoted 2 times

chaoscreater 1 month, 1 week ago
I guess people are now taking a strict englisn exam rather than an IT exam
upvoted 2 times

kmsrajan 5 months, 2 weeks ago
Answer is no because Leaked credential detection need Password Hash sync enabled
upvoted 2 times

doublekill 5 months, 2 weeks ago
The answer is NO

upvoted 1 times

AshTac 6 months ago

You would need to enable PHS for that..

upvoted 1 times

shanti0091 6 months, 2 weeks ago

The answer is No, Correct.

upvoted 2 times

rkapoor8855 6 months, 3 weeks ago

The answer is NO

upvoted 1 times

Thuthukani 7 months ago

The answer is incorrect because you cannot access premium Identity Protection features like Leaked Credentials without Password Hash Synchronization being enabled

upvoted 1 times

Thuthukani 7 months ago

Apologies I meant the answer is correct

upvoted 1 times

hungryboysl 7 months ago

Answer is correct

upvoted 1 times

svm_Terran 8 months ago

answer is correct

upvoted 1 times

mrcombo 1 year, 1 month ago

Answer:No

upvoted 2 times

Question #4 *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 that is associated to a Microsoft Azure Active Directory (Azure AD) tenant named contoso.com.
You use Active Directory Federation Services (AD FS) to federate on-premises Active Directory and the tenant. Azure AD Connect has the following settings:

- Source Anchor: objectGUID
- Password Hash Synchronization: Disabled
- Password writeback: Disabled
- Directory extension attribute sync: Disabled
- Azure AD app and attribute filtering: Disabled
- Exchange hybrid deployment: Disabled
- User writeback: Disabled

You need to ensure that you can use leaked credentials detection in Azure AD Identity Protection.
Solution: You modify the Source Anchor settings.
Does that meet the goal?

A. Yes

B. No

O365_dude Highly Voted 1 year, 7 months ago
Protect against leaked credentials and add resilience against outages
If your organization uses a hybrid identity solution with pass-through authentication or federation, then you should enable password hash sync for the following two reasons:

The Users with leaked credentials report in the Azure AD management warns you of username and password pairs, which have been exposed on the "dark web." An incredible volume of passwords is leaked via phishing, malware, and password reuse on third-party sites that are later breached. Microsoft finds many of these leaked credentials and will tell you, in this report, if they match credentials in your organization – but only if you enable password hash sync!
upvoted 17 times

CWT Highly Voted 1 year, 8 months ago
Specific details on PHS and ADFS:
https://docs.microsoft.com/en-us/azure/active-directory/hybrid/whatis-phs
https://channel9.msdn.com/Series/Azure-Active-Directory-Videos-Demos/Configuring-AD-FS-for-user-sign-in-with-Azure-AD-Connect
upvoted 6 times

lime568 Most Recent 3 weeks, 1 day ago
https://docs.microsoft.com/en-us/azure/active-directory/identity-protection/concept-identity-protection-risks

Only new leaked credentials found after you enable password hash synchronization (PHS) will be processed against your tenant.
upvoted 1 times

kiketxu 5 months, 1 week ago
Now YES, B for sure
upvoted 1 times

kiketxu 4 months, 4 weeks ago
I was meaning the anwer is NO
upvoted 1 times

doublekill 5 months, 2 weeks ago
The answer is YES, is correct.
upvoted 1 times

shanti0091 6 months, 2 weeks ago
The answer is correct, A
upvoted 1 times

rkapoor8855 6 months, 3 weeks ago
The answer is YES
upvoted 1 times

svm_Terran 8 months ago
modify the Password Hash Synchronization settings is true.

upvoted 3 times

SMHH 1 year, 1 month ago

https://docs.microsoft.com/en-us/azure/security/fundamentals/steps-secure-identity#protect-against-leaked-credentials-and-add-resilience-against-outages

upvoted 1 times

m2L 1 year, 6 months ago

https://www.microsoft.com/security/blog/2019/05/30/demystifying-password-hash-sync/

upvoted 1 times

Question #5

Topic 1

HOTSPOT -

You have a Microsoft 365 subscription that uses a default domain name of contoso.com.

The multi-factor authentication (MFA) service settings are configured as shown in the exhibit. (Click the Exhibit tab.)

multi-factor authentication
users service settings

app passwords (learn more)

- ● Allow users to create app passwords to sign in to non-browser apps
- ○ Do not allow users to create app passwords to sign in to non-browser apps

trusted ips (learn more)

- ☐ Skip multi-factor authentication for requests from federated users on my intranet

Skip multi-factor authentication for requests from following range of IP address subnets

192.168.1.0/27
192.168.1.0/27
192.168.1.0/27

verification options (learn more)

Methods available to users:

- ☐ Call to phone
- ■ Text message to phone
- ■ Notification through mobile app
- ■ Verification code from mobile app or hardware token

remember multi-factor authentication (learn more)

- ☐ Allow users to remember multi-factor authentication on devices they trust
  Days before a device must re-authenticate (1-60): 14

In contoso.com, you create the users shown in the following table.

Display name	Username	MFA status
User1	User1@contoso.com	Enabled
User2	User2@contoso.com	Enabled
User3	User3@contoso.com	Disabled

What is the effect of the configuration? To answer, select the appropriate options in the answer area.

NOTE: Each correct selection is worth one point.

Hot Area:

Answer Area

User1:

Can sign in to the My Apps portal without using MFA	V
Completed the MFA registration	
Must complete the MFA registration at the next sign-in	

User2:

Can sign in to the My Apps portal without using MFA	V
Must use app passwords for legacy apps	
Must use an app password to sign in to the My Apps portal	

btd2020 Highly Voted 1 year, 2 months ago

For User 2- Legacy authentication protocols like POP, SMTP, IMAP, and MAPI don't support MFA. The alternate method is for the user to create App Password for applications supporting legacy authentication. This password would be used instead of the user's regular password to access this application.

upvoted 12 times

hfpb010 Highly Voted 1 year, 2 months ago

Isn't anything missing on the question? Whats the difference between user 1 and user 2?

upvoted 12 times

Fricandel 3 weeks, 4 days ago

The difference between User 1 and User 2 is the number.

upvoted 1 times

Galstonian 1 year, 1 month ago

The difference between the users isn't in the scenario, it is in the answers available.

upvoted 21 times

PrinceVarghese Most Recent 2 months, 3 weeks ago

MFA Status on the the question might be Enabled, Enforced and Disabled. And the answers should be
User 1 ("Enabled") : Must complete the MFA registration at the next sign-in.
User 2 ("Enforced"): Completed the MFA registration (After completing MFA registration the status could be logically change to "Enforced")
User 3 ("Disabled"): Must use app passwords for legacy apps.

upvoted 3 times

prats005 4 months ago

Enabled
Enforced
Disabled
In general, don't move users directly to the Enforced state unless they are already registered for MFA. If you do so, legacy authentication apps stop working because the user hasn't gone through Azure AD Multi-Factor Authentication registration and obtained an app password. In some cases this behavior may be desired, but impacts user experience until the user registers. https://docs.microsoft.com/en-us/azure/active-directory/authentication/howto-mfa-userstates

upvoted 1 times

Ciapek 4 months, 1 week ago

If you use CONDITIONAL ACCESS to forced MFA , Your users will be prompted by 14 days to do it. When you directly set MFA enable to user account it has to register next time.

https://docs.microsoft.com/en-us/azure/active-directory/authentication/howto-mfa-userstates

upvoted 1 times

PrinceVarghese 2 months, 3 weeks ago

Conditional access requires Azure AD premium subscription 1 or 2

upvoted 1 times

gan998 5 months ago

The answer for both is can sign in without MFA.
Enabled does not means MFA is turned on or is required.
Enabled means MFA is OPTIONAL for the user.
Enforced means MFA must be turned on on the next login.

upvoted 2 times

kiketxu 4 months, 3 weeks ago

I'm really freaking out with this explanation... did you really spent 2min googling it? Please...we are here to discuss and learn, but is basic to check anything before post.

None user will be able to log without MFA, except for legacy apps. Both answers are correct, principally because the rest aren't true.

https://docs.microsoft.com/es-es/azure/active-directory/authentication/howto-mfa-userstates#azure-ad-multi-factor-authentication-user-states

upvoted 10 times

shanti0091 6 months, 2 weeks ago

The answer is correct both User1 & 2, because in the real sense, once an account is registered on azure ad MFA it automatically changes from enabled to enforce which I believe reads some meaning to this context as option 3 is wrong.

upvoted 2 times

Timmeh 5 months, 1 week ago

That is not correct.

upvoted 3 times

Mrawrrr 6 months, 4 weeks ago

Answer is correct. If MFA password is enabled it means that user will have to make a registration and download MFA app at next sign in. User can also use password login for legacy apps. Last statement is not true if MFA is enforced. In that case user cant use password for legacy apps.
https://docs.microsoft.com/en-us/azure/active-directory/authentication/howto-mfa-userstates

upvoted 2 times

DrMe 7 months, 3 weeks ago

I don't understand a valid answer for User2 as while MFA is "enabled" legacy authentication works:
https://docs.microsoft.com/en-us/azure/active-directory/authentication/howto-mfa-userstates#:~:text=can%20still%20use%20their%20password%20for%20legacy%20authentication.

upvoted 1 times

penguinperp 7 months ago

Not an expert, but if my understanding is correct, the answer is valid as once user2 finishes the MFA registration they will require app passwords. Basically, Legacy Auth works without impact until the user registers MFA at which point they will require to use app passwords. Maybe someone smarter than I can validate that that is correct.

upvoted 2 times

MOsama1 9 months, 3 weeks ago

Please, what is the deferent between users1 and user2 in the question

upvoted 2 times

zarahome 8 months, 1 week ago

There is no difference between the users, just the drop down options given are different

upvoted 5 times

rdy4u 1 year, 1 month ago

https://docs.microsoft.com/en-us/azure/active-directory/authentication/howto-mfa-app-passwords

upvoted 1 times

rdy4u 1 year, 1 month ago

Some applications, like Office 2010 or earlier and Apple Mail before iOS 11, don't support multi-factor authentication. The apps aren't configured to accept a secondary form of authentication or prompt. To use these applications in a secure way with Azure Multi-Factor Authentication enabled for user accounts, you can use app passwords. These app passwords replaced your traditional password to allow an app to bypass multi-factor authentication and work correctly

upvoted 2 times

BBR 9 months, 2 weeks ago

https://docs.microsoft.com/en-us/azure/active-directory/authentication/howto-mfa-app-passwords

upvoted 1 times

ahhao 1 year, 3 months ago

Shouldn't the answer to User 2 be #3? given that the user's MFA status is enabled and not enforced?

upvoted 2 times

Andrew1234 1 year, 1 month ago

No, App passwords are for specific applications only and can't be used to access the Apps Portal. :)

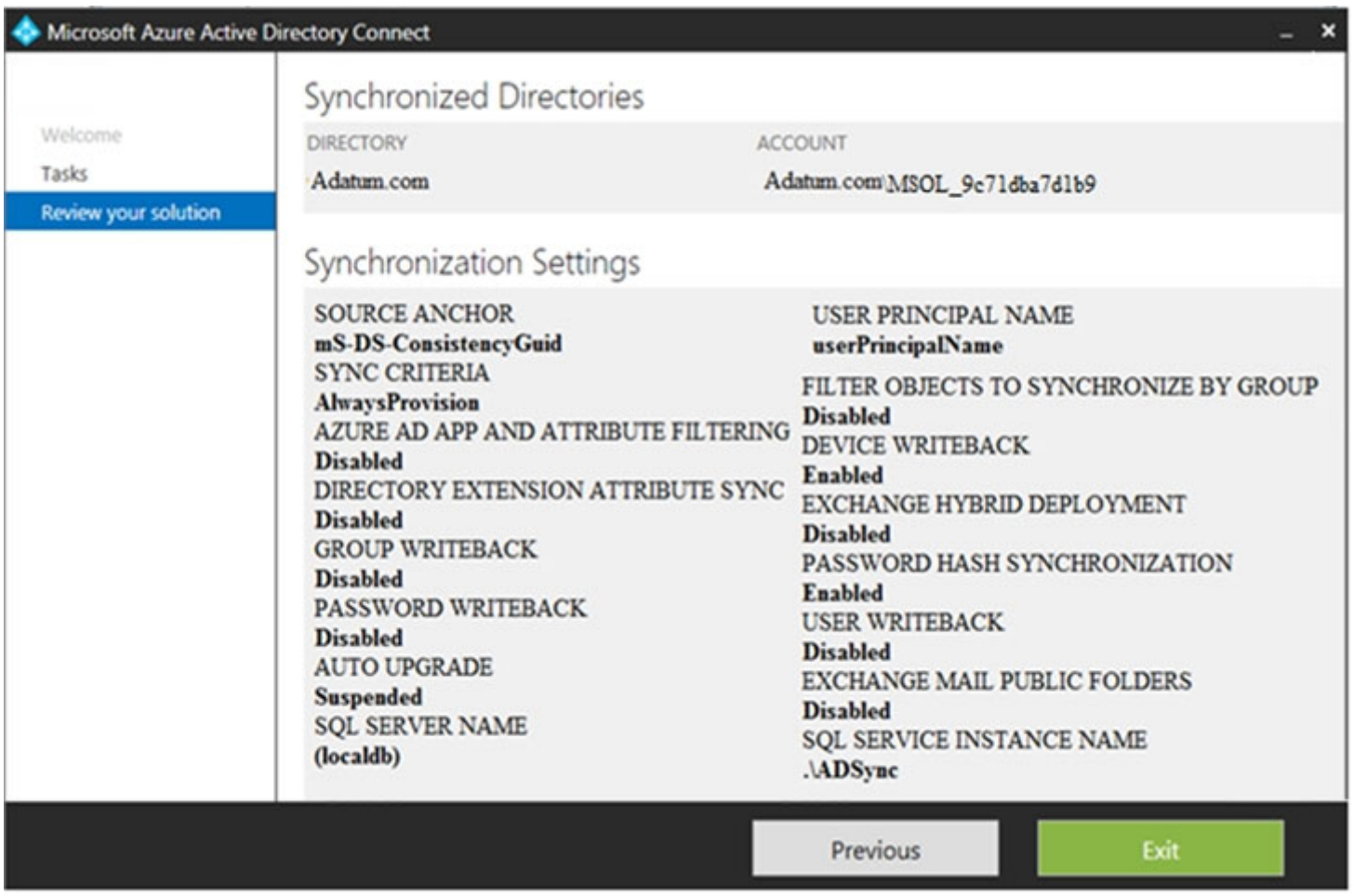
upvoted 1 times

Question #6

Topic 1

HOTSPOT -

You configure Microsoft Azure Active Directory (Azure AD) Connect as shown in the following exhibit.



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

NOTE: Each correct selection is worth one point.

Hot Area:

Answer Area

If you reset a password in Azure AD of a synced user, the password will **[answer choice]**.

be overwritten	V
be synced to Active Directory	
be subject to the Active Directory password policy	

If you join a computer to Azure AD, **[answer choice]**.

an object will be provisioned in the Computers container	V
an object will be provisioned in the RegisteredDevices container	
the device object in Azure will be deleted during synchronization	

TimurKazan Highly Voted 4 months, 3 weeks ago

First is not true. User will not be able to change password in Azure and it will get message about AD policy preventing him from doing it. Hence 1st is subject to Active Directory password policy

upvoted 11 times

Robert__Susin 3 months, 1 week ago

Agreed

upvoted 1 times

Fala_Fel 1 month, 2 weeks ago

Agreed. It will be subject to on prem AD Password policy is the answer.
"When password hash synchronization is enabled, the password complexity policies in your on-premises Active Directory instance override complexity policies in the cloud for synchronized users."
https://docs.microsoft.com/en-us/azure/active-directory/hybrid/how-to-connect-password-hash-synchronization

upvoted 1 times

p2pitu Highly Voted 2 months, 2 weeks ago

The first answer is correct. Admin can change the password in Azure AD but it will be overwritten by AD in next sync because of the password sync enabled.

upvoted 5 times

stromnessian Most Recent 1 week, 6 days ago

Question doesn't make sense because you cannot reset the password of a synced user if password writeback is disabled; you receive this message: "Unfortunately, you cannot reset this user's password because password writeback is not enabled in your tenant.
Learn how to configure password writeback."

upvoted 2 times

someOnePlus 6 days, 20 hours ago

Totally agree

upvoted 1 times

chaoscreater 1 month, 1 week ago

First answer is correct, I've verified this. Question is not asking whether the user can reset the password themselves. It is asking YOU, as an IT admin. If you reset the password as admin, it will work, but of course it will be overwritten by AD password on the next AD sync cycle.

upvoted 3 times

lime568 2 weeks, 3 days ago

Did you try to reset the password for a synced user?. I dont think.

upvoted 1 times

Robert__Susin 3 months, 1 week ago

First given answer is incorrect, the question is about Azure AD, not the on-premisses AD, so if you have password writback disabled, this means you can only change/reset password in on-premisses AD, so the most correct answer for the first question is being subject to AD password policy

upvoted 2 times

kiketxu 4 months, 3 weeks ago

First is true due password writeback isn't enabled.
Second is wrong, the container is "RegisteredDevices"

https://docs.microsoft.com/en-us/azure/active-directory/hybrid/how-to-connect-device-writeback#verify-devices-are-synchronized-to-active-directory

upvoted 3 times

bingomutant 4 months, 3 weeks ago

Given answers are correct IMO, PAssword Writeback is not enabled therefore next AD Sync will overwrite Coud PW. Device Writeback is enabled - So AAD devices are added to the container.

upvoted 2 times

Robert__Susin 3 months, 1 week ago

First answer is not correct, the question is about reseting the password in the Azure AD, there wont be any next AD Sync to respond into this command as you will be prompted error message in trying it.

upvoted 1 times

Question #7 *Topic 1*

You have a hybrid Microsoft 365 environment. All computers run Windows 10 and are managed by using Microsoft Intune.
You need to create a Microsoft Azure Active Directory (Azure AD) conditional access policy that will allow only Windows 10 computers marked as compliant to establish a VPN connection to the on-premises network.
What should you do first?

A. From the Azure Active Directory admin center, create a new certificate

B. Enable Application Proxy in Azure AD

C. From Active Directory Administrative Center, create a Dynamic Access Control policy

D. From the Azure Active Directory admin center, configure authentication methods

paulfns2020 Highly Voted 1 year, 2 months ago
To configure conditional access for VPN connectivity, you need to:

Create a VPN certificate in the Azure portal.
Download the VPN certificate.
Deploy the certificate to your VPN server.
upvoted 20 times

Bl0ckSh3ll 10 months, 3 weeks ago
No doubts on this one, just see paulfns2020 comment and the 7.2 step on this link:

https://docs.microsoft.com/en-us/windows-server/remote/remote-access/vpn/ad-ca-vpn-connectivity-windows10
upvoted 4 times

kiketxu 5 months, 1 week ago
You right,thankies!
upvoted 2 times

Guilherme Highly Voted 1 year, 6 months ago
https://docs.microsoft.com/en-us/windows-server/remote/remote-access/vpn/ad-ca-vpn-connectivity-windows10
upvoted 6 times

Robert__Susin Most Recent 3 months, 1 week ago
Configure root certificates for VPN authentication with Azure AD, which automatically creates a VPN server cloud app in the tenant. Only after this you can use Conditional Access and select Cloud app to VPN Server.
upvoted 1 times

svm_Terran 8 months ago
this is correct.
upvoted 2 times

MSOffice 10 months, 3 weeks ago
The question is what you need to do first in order to create a Microsoft Azure Active Directory (Azure AD) conditional access policy that will allow only Windows 10 computers marked as compliant to establish a VPN connection to the on-premises network.

- We need to configure a Policy to allow windows 10 clients vpn access. Dynamic access policy is the only answer - https://docs.microsoft.com/en-us/windows-server/identity/solution-guides/dynamic-access-control-overview#:~:text=Domain%2Dbased%20Dynamic%20Access%20Control,used%20to%20access%20these%20resources.
upvoted 1 times

VTHAR 10 months, 1 week ago
"C. From Active Directory Administrative Center, create a Dynamic Access Control policy" is definitely NOT the correct answer. That is on-perm technology which has nothing to do with Azure AD and Conditional Access and you also need to deploy Central Access Policies/ Central Access Rules/User claims and device claims which doesn't relate to this question at all.
upvoted 7 times

Robert__Susin 3 months, 1 week ago
Yes the question is very off and confusing the way they wrote, but nonetheless:
To configure conditional access for VPN connectivity, you need to:

Create a VPN certificate in the Azure portal.
Download the VPN certificate.
Deploy the certificate to your VPN server.
upvoted 1 times

junkz 1 year, 1 month ago
the question is not around the actual connection mechanism (which is certificate indeed) but more around the conditions that govern the connection. so dynamic access would be the good option

upvoted 3 times

Robert__Susin 3 months, 1 week ago

Yes the question is very off and confusing the way they wrote, but nonetheless:
To configure conditional access for VPN connectivity, you need to:

Create a VPN certificate in the Azure portal.
Download the VPN certificate.
Deploy the certificate to your VPN server.

upvoted 1 times

Prianishnikov 11 months, 3 weeks ago

https://docs.microsoft.com/en-us/windows-server/remote/remote-access/vpn/ad-ca-vpn-connectivity-windows10

upvoted 1 times

itmp 1 year, 3 months ago

You create the certificate here:
portal.azure.com/#blade/Microsoft_AAD_IAM/ConditionalAccessBlade/Vpn

upvoted 5 times

Question #8 *Topic 1*

You have a Microsoft 365 subscription.

From the Microsoft 365 admin center, you create a new user.

You plan to assign the Reports reader role to the user.

You need to view the permissions of the Reports reader role.

Which admin center should you use?

A. Azure Active Directory

B. Cloud App Security

C. Security & Compliance

D. Microsoft 365

kmsrajan Highly Voted 1 year, 7 months ago

All roles and permission details are available in AAD but in M365 Admin center you see the role, not permission details.

upvoted 15 times

pmr123 10 months, 3 weeks ago

No No..You can also see the permissions as well from M365 portal

upvoted 2 times

sayyidsaif 2 months ago

They Just mentioned M365 portal. Not M365 Admin Center :)

upvoted 1 times

bertik 9 months, 2 weeks ago

Well, in M365 portal you can see only skimmed role permissions description compared to AAD. If in real exam, you can select only one option I would go with AAD, if you can select more options, I would select M365 and AAD.

upvoted 4 times

AB1 Highly Voted 1 year, 10 months ago

You can view the permission in M365 Admin Center as well

upvoted 9 times

JWJUNIOR 1 year, 2 months ago

you completely right. I have just confirmed it in Office 365 Portal

upvoted 4 times

theboywonder Most Recent 1 month ago

The question is Which "ADMIN" center should you use?
As this can be managed from both AAD and M365 Admin centres, both answers are correct A+D

upvoted 1 times

subbuhotmail 1 month, 2 weeks ago

The question stated that it has Microsoft 365 subscription, so the most relevant answer would be D.

upvoted 1 times

Rstilekar 1 month, 4 weeks ago

As Bertik said, its correct answer.... M365 portal you can see only skimmed role permissions description compared to AAD. If in real exam, you can select only one option I would go with AAD, if you can select more options, I would select M365 and AAD.

upvoted 1 times

jsshaker 2 months, 1 week ago

The answer is good. Inside the AAD Console, under "Roles & Administrators", you have all the roles, including Reports Readers.

upvoted 1 times

Xtian_ar 1 month, 2 weeks ago

Yes, but from M365 portal is possible too

upvoted 1 times

Vabene 3 months, 2 weeks ago

I would say its answer D. This exam is related to M365, so as A and D are correct, D is more accurate.

upvoted 1 times

Timzyjay 6 months, 2 weeks ago

Reports Reader based on my check on the licensed demo tenant i have is only available on the Azure AD.

upvoted 1 times

kiketxu 5 months, 1 week ago

you should see the role permissions under roles in the "M365 admin center" but as this isn't literally in the answers I would say AAD.
upvoted 1 times

Vazza98 6 months, 2 weeks ago

Tested in lab environment and verified.
As per TonySuccess' response ; this role shows in both the M365 admin center and Azure AD.
In M365 this actually loads in a tab named 'Azure AD' so is referencing the same location. Azure AD does show more of an advanced view when looking at permissions so is more detailed. Either answer would work here but I think MS are looking for Azure AD so answer is correct.
upvoted 2 times

kiketxu 5 months, 1 week ago

as "M365 admin center" isn't literally in the answers I would say AAD but both places can manage it. OFC AAD more detailed and configurable.
upvoted 1 times

shanti0091 6 months, 2 weeks ago

Both A & B correct, but in this context Azure gives details more when it comes to permissions. I'll go for A.
upvoted 1 times

svm_Terran 8 months ago

Azure AD in general.
upvoted 2 times

TonySuccess 8 months, 1 week ago

It is my opinion, and I recall from a course also that Azure AD Roles section offers more Roles to view and also has more details and options to manage the roles settings.

Infact, whilst checking to validate my comment, I could only actually see Reports Reader Role in Azure AD.

Therefore I would go for the given answer here.
upvoted 2 times

rsolman 10 months, 2 weeks ago

A and D are both correct. just checked it!
upvoted 1 times

pmr123 11 months ago

We can view the permissions from Roles section on Microsoft 365 portal also
upvoted 1 times

examkid 1 year ago

The M365 Portal does a query to the Azure Active Directory and shows the results
Whereas AAD is the source of truth, so I would go for Azure Active Directory
upvoted 3 times

junkz 1 year ago

i imagine there was a time when the 365 portal was showing less info , but nowadays they are prety much on par. the reports reader is a poor example here because indeed, text quantity wise, it shows less than each every action in the role's description in AAD. if you look at application admin for example, you'll see a lot more, comparable to the same in AAD. bottom line is :
1. the question is probably gone from exam because it would be confusing currently
2.i do tend to believe that if someone wants to see what's the role about, it will prefer the way the role is described in a bit more non-technical jargon than AAD, because it's not going to be just global admins that give that role, other persons may be less technical and not realy make sense of the stuff in AAD
upvoted 1 times

mehnaz 1 year ago

Copying the answer from @MawandaH
M365 > Admin Page > Roles > "roleName" > Permissions >
AAD > Dashboard > TenantName > Roles and Administrators > "roleName" > Description
The permission in AAD are quite elaborate compared to M365.
So, will go with the given answer-AAD
upvoted 2 times

Question #9 *Topic 1*

You have a Microsoft 365 E5 subscription.
You need to ensure that users who are assigned the Exchange administrator role have time-limited permissions and must use multi-factor authentication (MFA) to request the permissions.
What should you use to achieve the goal?

A. Security & Compliance permissions

B. Microsoft Azure Active Directory (Azure AD) Privileged Identity Management

C. Microsoft Azure AD group management

D. Microsoft Office 365 user management

prats005 Highly Voted 4 months, 1 week ago
PIM provides JIT access.
upvoted 10 times

kiketxu Highly Voted 4 months, 3 weeks ago
B for sure!
upvoted 5 times

theboywonder Most Recent 1 month ago
PIM is correct!
upvoted 1 times

Question #10 *Topic 1*

Your company has a Microsoft 365 subscription.
The company does not permit users to enroll personal devices in mobile device management (MDM).
Users in the sales department have personal iOS devices.
You need to ensure that the sales department users can use the Microsoft Power BI app from iOS devices to access the Power BI data in your tenant.
The users must be prevented from backing up the appа€™s data to iCloud.
What should you create?

A. a conditional access policy in Microsoft Azure Active Directory (Azure AD) that has a device state condition

B. an app protection policy in Microsoft Endpoint Manager

C. a conditional access policy in Microsoft Azure Active Directory (Azure AD) that has a client apps condition

D. a device compliance policy in Microsoft Endpoint Manager

kiketxu Highly Voted 4 months, 3 weeks ago
Given answer is correct. @Examtopic, here missing the references link

https://docs.microsoft.com/en-us/mem/intune/apps/app-protection-policy#:~:text=You%20can%20use%20Intune%20app,in%20a%20device%20management%20solution.

https://docs.microsoft.com/en-us/mem/intune/apps/app-protection-policy#benefits-of-using-app-protection-policies:~:text=Prevent%20the%20saving%20of%20company%20app%20data%20to%20a%20personal%20storage%20location
upvoted 14 times

Question #11 *Topic 1*

HOTSPOT -

You have a Microsoft 365 E5 subscription.

Users and device objects are added and removed daily. Users in the sales department frequently change their device.

You need to create three following groups:

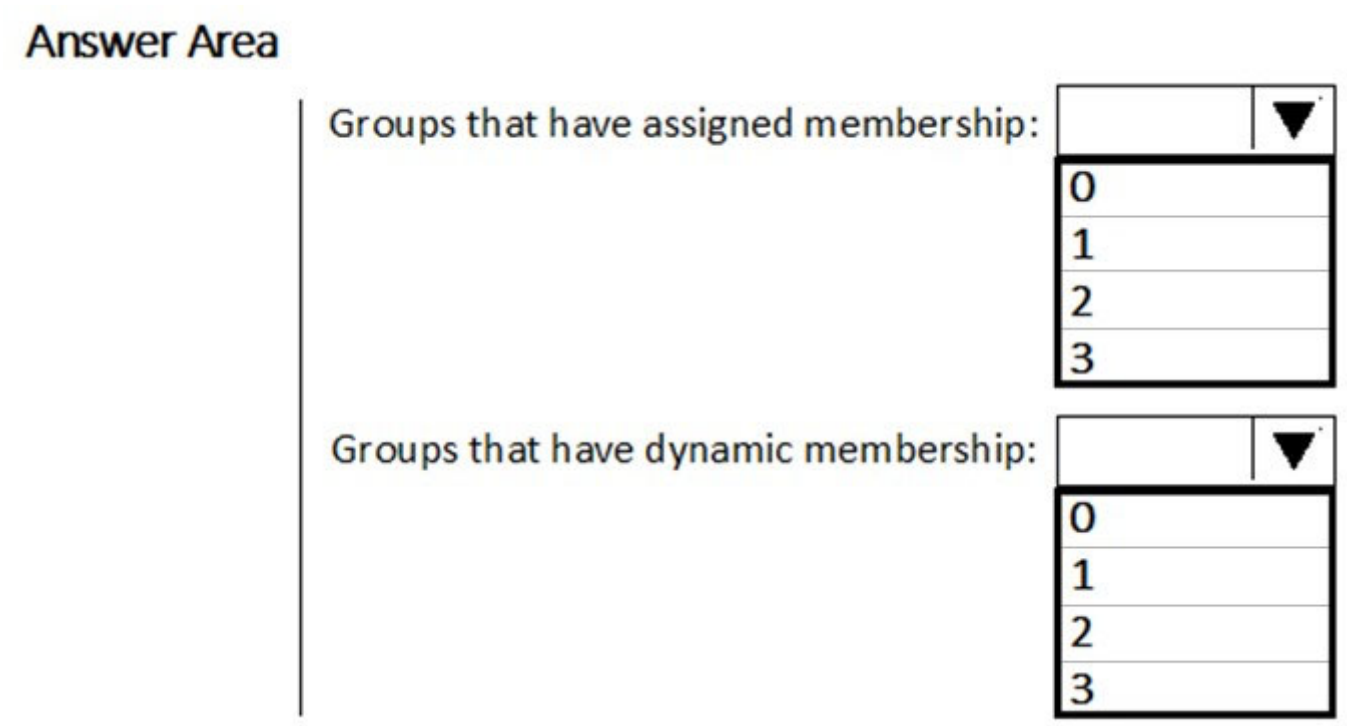
Name	Requirement
Group1	All the devices of users where the `Department` attribute is set to `Sales`
Group2	All the users where the `Department` attribute is set to `Sales`
Group3	All the devices where the `deviceOwnership` attribute is set to `Company`.

The solution must minimize administrative effort.

What is the minimum number of groups you should create for each type of membership? To answer, select the appropriate options in the answer area.

NOTE: Each correct selection is worth one point.

Hot Area:



kiketxu Highly Voted 4 months, 3 weeks ago

Group 1 has to be assigned because you can't create a device group based on the device owners' attributes.
Group 2 can be dynamic because a user does have a department attribute.
Group 3 can be dynamic because a device does have a deviceownership attribute.

https://docs.microsoft.com/en-us/azure/active-directory/enterprise-users/groups-dynamic-membership#rule-builder-in-the-azure-portal

upvoted 7 times

Akc0 4 months, 3 weeks ago

Answer is a bit confusing, Group 1 talks about Department as sales, but you mentioned 'deviceowner' attribute, that is group 3 right?

upvoted 1 times

galangimani97 4 months ago

it means you cannot create a rule of device group with the condition based on user attribute. user attribute is different from the device attribute. you can check more detail in the link below

https://docs.microsoft.com/en-us/azure/active-directory/enterprise-users/groups-dynamic-membership#rules-for-devices

upvoted 4 times

Xtian_ar Most Recent 1 month, 2 weeks ago

The answer is correct, but it is because there is not a rule for department attribute for devices

upvoted 3 times

tarunkantimondal 2 months, 3 weeks ago

answer is confusing

upvoted 1 times

prats005 4 months ago

Answer is correct

upvoted 4 times

prats005 4 months ago

You can create a dynamic group for devices or for users, but you can't create a rule that contains both users and devices.
You can't create a device group based on the device owners' attributes. Device membership rules can only reference device attributes.

https://docs.microsoft.com/en-us/azure/active-directory/enterprise-users/groups-dynamic-membership
upvoted 2 times

Question #12 *Topic 1*

Your company has a main office and a Microsoft 365 subscription.
You need to enforce Microsoft Azure Multi-Factor Authentication (MFA) by using conditional access for all users who are NOT physically present in the office.
What should you include in the configuration?

A. a user risk policy

B. a sign-in risk policy

C. a named location in Azure Active Directory (Azure AD)

D. an Azure MFA Server

AmerSerhan Highly Voted 1 year, 3 months ago
Named locations
With named locations, you can create logical groupings of IP address ranges or countries and regions.
You can access your named locations in the Manage section of the Conditional Access page.
upvoted 19 times

theboywonder 1 month ago
you are right, C is correct. This is how it's done: https://docs.microsoft.com/en-us/azure/active-directory/conditional-access/untrusted-networks
upvoted 1 times

kiketxu Most Recent 5 months, 1 week ago
C for sure.
upvoted 2 times

svm_Terran 7 months, 4 weeks ago
C. Named Location under Azure AD.
upvoted 2 times

junkz 1 year ago
clearly named locations:
Organizations can use this network location for common tasks like:

Requiring multi-factor authentication for users accessing a service when they are off the corporate network.
Blocking access for users accessing a service from specific countries or regions.
The network location is determined by the public IP address a client provides to Azure Active Directory.
upvoted 3 times

xofowi5140 1 year, 3 months ago
"for all users who are NOT physically present in the office"
I think Sign-in risk policy is the best answer.
Administrators can choose to block access, allow access, or allow access but require multi-factor authentication
upvoted 2 times

VTHAR 1 year ago
Sign-in risk policy is extra layer of protection as stated in this link https://docs.microsoft.com/en-us/azure/active-directory/authentication/tutorial-risk-based-sspr-mfa

Therefore, to enforce MFA for out of office access practically, you need to use "Named Locations". It's enforced in my work environment since one and half years ago.
upvoted 5 times

Question #13 *Topic 1*

HOTSPOT -

You have a Microsoft Azure Active Directory (Azure AD) tenant named contoso.com that contains the users shown in the following table.

Name	Member of	Multi-factor authentication (MFA) status
User1	Group1	Disabled
User2	Group1, Group2	Enabled

You create and enforce an Azure AD Identity Protection user risk policy that has the following settings:

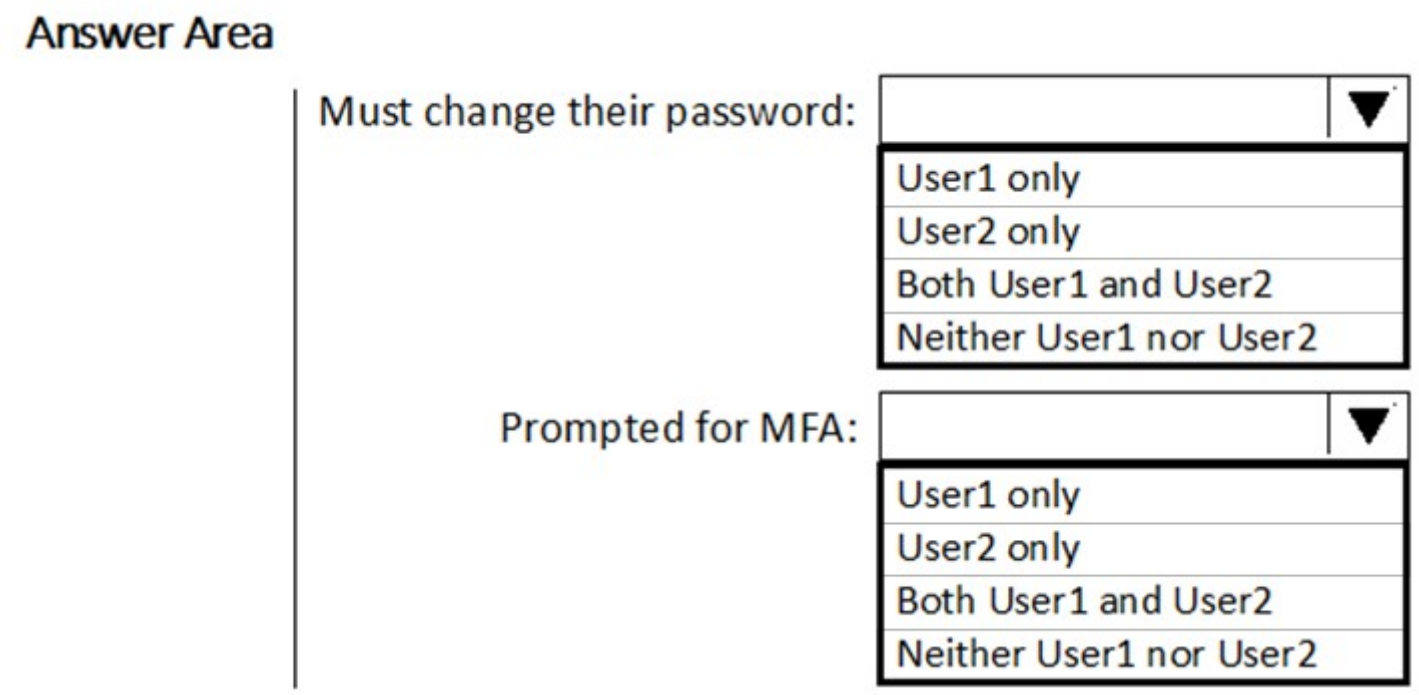
- Assignments: Include Group1, Exclude Group2
- Conditions: Sign-in risk of Low and above
- Access: Allow access, Require password change

You need to identify how the policy affects User1 and User2.

What occurs when User1 and User2 sign in from an unfamiliar location? To answer, select the appropriate options in the answer area.

NOTE: Each correct selection is worth one point.

Hot Area:



kiketxu Highly Voted 4 months, 3 weeks ago

User1 is must change PW.
User2 prompted for MFA

upvoted 27 times

Yetijo 1 month, 3 weeks ago

This is the correct answer. The CA in this scenario is designed for User 1. The user does not have MFA enabled and cannot be challenged, but they can be allowed and prompted action (password change). By nature of MFA a user will be challenged when signing on from an unfamiliar location, without a CA in place.

upvoted 1 times

w00t 4 months, 1 week ago

This is the right answer

upvoted 3 times

Sikula Highly Voted 4 months, 1 week ago

I assume that correct answers are:
User1 must change password (because User2 is excluded from condition)
Neither User1 nor User2 will be prompted (because there is not such condition)

upvoted 17 times

yayoayala 3 months, 3 weeks ago

User1 must change password (because User2 is excluded from condition. Exclusion wins over inclusions.)
User1 nor User2 will be prompted (because there is not such condition)

upvoted 4 times

M3ridi3n 1 month, 4 weeks ago

I think the condition is there : " User1 and User2 sign in from an unfamiliar location"

upvoted 1 times

ellik 3 months, 3 weeks ago

can you elaborate more , why Neither User1 nor User2 will be prompted (because there is not such condition). it is really confusing with all these disscussion.

upvoted 1 times

dcasabona 3 months, 1 week ago

This is because the conditional access policy asks to change the password, not to enforce MFA. On top of that, MFA is disable for user 1 and excluded for user 2 since he is in the exclusion policy, which over take inclusion.

upvoted 1 times

JoelB 1 month, 2 weeks ago

The MFA settings are not in the conditional access policy but the Azure Multi-Factor Authentication blade. This is the per-user AAD MFA (although MS are recommending utilising CA policies for MFA, this is also an option). Since the status of User 2 is set to Enabled, they will have to configure MFA on next login. The user is signing in from unfamiliar location, so they will not exempt from the Trusted IP ranges which can be configured in the per-user AAD MFA. Therefore User 2 will be required to set up MFA if they sign in, second answer is correct. I agree with the exclusion for User 2 and first answer should be User 1 only.

upvoted 3 times

chaoscreater Most Recent 1 month, 1 week ago

Just because it shows Enabled for MFA, doesn't mean user has completed registration. If user has registered for MFA, the status should show Enforced. So technically, user 2 won't be prompted for MFA and instead will be prompted to register for MFA?

upvoted 1 times

Xtian_ar 1 month, 2 weeks ago

Answer is correct.
User1 must change PW (by the conditional policy)
User2 prompted for MFA (by MFA configuration for User2)

upvoted 1 times

Rstilekar 1 month, 4 weeks ago

Correct answer for me is #
User1 must change password (because User2 is excluded from condition. Exclusion wins over inclusions.)
User1 nor User2 will be prompted (because there is not such condition)

upvoted 2 times

bsldwp_2020 2 months ago

Must change their password: User 1 Only
Prompted for password: Neither User 1 nor User 2.
Exclusion take precedence over Inclusions.
Supporting article: https://docs.microsoft.com/en-us/azure/active-directory/conditional-access/concept-conditional-access-users-groups#exclude-users

upvoted 2 times

bsldwp_2020 2 months ago

I mean for Prompted for MFA: User 2 only.

upvoted 1 times

Ocico 2 months, 3 weeks ago

both users are scoped in Group1. prompt for password change has no relation to MFA.
user2 will be prompted for MFA, because user2 is enabled for MFA.
for me, the given answers are correct

upvoted 3 times

arunjana 2 months, 3 weeks ago

User1 must change password
Neither User1 nor User2 will be prompted for MFA

upvoted 2 times

GevedeBe 3 months, 2 weeks ago

The question is" how the policy affects....." MFA is not part of a user sign-in -risk policy so, User 1 and User 2 will NOT be prompted!

upvoted 7 times

Jslei 4 months, 3 weeks ago

This is tricky. I believe answer given is correct. User2 is part of group1 that is included in the policy, so both Users must change password.

upvoted 2 times

Jslei 4 months, 3 weeks ago

Nope I was wrong. Had to test it. User2 got blocked as soon as I removed group2 from the exclusions. When I added group2 back, User2 was no longer blocked. So exlusions wins over inclusions

upvoted 13 times

nramospe 4 months, 3 weeks ago

But user2 also belongs to group1 and I think inclusion has priority over exclusion.
So the answer given is correct

upvoted 1 times

kiketxu 4 months, 3 weeks ago

Not for CA. Exclusion takes priority. Look at this as emergency measure for admins.

upvoted 3 times

MCPsince1999 4 months, 3 weeks ago

Yes: "When organizations both include and exclude a user or group the user or group is excluded from the policy, as an exclude action overrides an include in policy"

upvoted 1 times

BialyFenek 4 months, 4 weeks ago

I think that user 2 doesn't need to change the password because in the settings group 2 is excluded.
Only user 1 needs to change his password.

upvoted 1 times

b00 4 months, 4 weeks ago

I can't understand why user 2 is not excluded

upvoted 1 times

b00 4 months, 4 weeks ago

For me "Must change their password" should be "user 1 only".

upvoted 2 times

Question #14 *Topic 1*

HOTSPOT -

You have a Microsoft Azure Active Directory (Azure AD) tenant named contoso.com that contains the users shown in the following table.

Name	Member of	Multi-factor authentication (MFA) status
User1	Group1, Group2	Disabled
User2	Group1	Disabled

You create and enforce an Azure AD Identity Protection sign-in risk policy that has the following settings:

- Assignments: Include Group1, Exclude Group2
- Conditions: Sign-in risk of Low and above
- Access: Allow access, Require multi-factor authentication

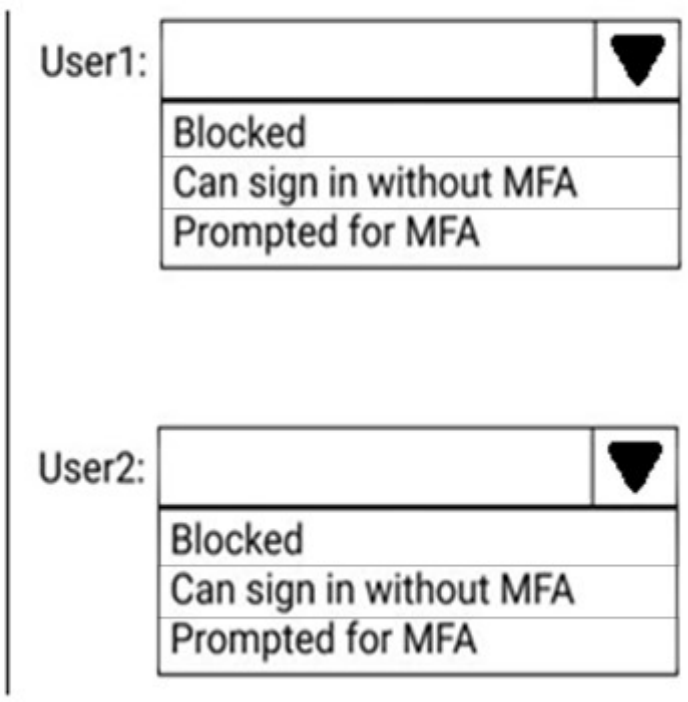
You need to identify how the policy affects User1 and User2.

What occurs when each user signs in from an anonymous IP address? To answer, select the appropriate options in the answer area.

NOTE: Each correct selection is worth one point.

Hot Area:

Answer Area



Sugar123 Highly Voted 4 months, 3 weeks ago

User 2 will be blocked. Watch the video at 1:23 : https://docs.microsoft.com/en-us/azure/active-directory/identity-protection/howto-identity-protection-configure-risk-policies. It says access will be blocked if a user is not registered for MFA

upvoted 24 times

stromnessian 1 week, 6 days ago

Where in the question does it say that the users are not registered?

upvoted 1 times

fuckthisscamsite 3 months, 3 weeks ago

This is wrong, verified in demo tenant lab. If User2 is disabled for MFA, they are prompted to register in this scenario. They are allowed to register, and then allowed to sign in following successful registration. Unfortunately that video is wrong too and would not be the first time that official MS documentation is inaccurate.

upvoted 9 times

chaoscreater 1 month, 1 week ago

I agree. Answer should be "can sign in without MFA", which is technically correct? Prompted to register for MFA and prompted for MFA are different things, so technically the only suitable option is can sign in without MFA?

upvoted 1 times

ellik 3 months, 3 weeks ago

how about user 1 ? is the given answer correct ? can sign-in without MFA as exclusion win ?

upvoted 2 times

bingomutant 4 months, 3 weeks ago

this looks correct - thanks

upvoted 1 times

Lulu77 Highly Voted 1 month, 2 weeks ago

Replicated these settings in my demo tenant. User1 - can sign in without MFA. User2 prompted to register.
upvoted 7 times

Nickske157 Most Recent 1 month, 1 week ago
user 1: can sign-in without mfa
user 2: blocked
https://docs.microsoft.com/en-us/azure/active-directory/identity-protection/howto-identity-protection-configure-risk-policies
Warning

Users must register for Azure AD MFA and SSPR before they face a situation requiring remediation. Users not registered are blocked and require administrator intervention.

Password change (I know my password and want to change it to something new) outside of the risky user policy remediation flow does not meet the requirement for secure password reset.
upvoted 1 times

Rstilekar 1 month, 4 weeks ago
Given answers are correct#

USER1 # User 1 has MFA "disabled".
User 1 is part of Group 1 and Group 2 -- Group 2 is EXCLUDED from this policy, meaning User 1 doesn't participate in this policy.
The policy is what enforced that MFA is required to log in. Because this policy isn't enforced for User 1, they can sign in without MFA.
Reference - Exclusion take precedence over Inclusions: https://docs.microsoft.com/en-us/azure/active-directory/conditional-access/concept-conditional-access-users-groups#exclude-users

USER2 # Answer for MFA part is 'Blocked'
Users must register for Azure AD MFA and SSPR before they face a situation requiring remediation. Users not registered are blocked and require administrator intervention
Reference - Watch the video at 1:23 : https://docs.microsoft.com/en-us/azure/active-directory/identity-protection/howto-identity-protection-configure-risk-policies. It says access will be blocked if a user is not registered for MFA
upvoted 2 times

stromnessian 1 week, 6 days ago
Where does it say that User2 is not registered. Registration has nothing to do with per-user MFA settings.
upvoted 1 times

bsldwp_2020 2 months ago
User 2 will be required to register for MFA. Only after user is registered and sign-in using MFA, the access will be granted.
Also, Exclusion take precedence over Inclusions: https://docs.microsoft.com/en-us/azure/active-directory/conditional-access/concept-conditional-access-users-groups#exclude-users
upvoted 4 times

bsldwp_2020 2 months ago
CORRECTION: Answer for MFA part is 'Blocked'
Users must register for Azure AD MFA and SSPR before they face a situation requiring remediation. Users not registered are blocked and require administrator intervention
upvoted 1 times

chaoscreater 1 month, 1 week ago
The user isn't blocked though, they will be prompted to register for MFA during the sign-in.
upvoted 1 times

JRGR 4 months ago
Why User 1 can sign in without MFA? Both users are members of Group 1, which is included in the policy, so both users will be blocked.
upvoted 2 times

AJWYATT79 4 months ago
Because User 1 is also a member of Group 2, and Group 2 is excluded from the policy. Exclusions win over inclusions
upvoted 6 times

w00t 4 months, 1 week ago
User 1 = Can sign in without MFA
User 2 = Blocked
upvoted 6 times

theboywonder 1 month ago
this is the correct answer, user 2 is blocked due to MFA is disabled. MFA should be enabled first for this user.
upvoted 1 times

prats005 4 months, 1 week ago
How the user will be able to sign in without MFA?
upvoted 1 times

w00t 3 months, 3 weeks ago
User 1 has MFA "disabled".
User 1 is part of Group 1 and Group 2 -- Group 2 is EXCLUDED from this policy, meaning User 1 doesn't participate in this policy.
The policy is what enforced that MFA is required to log in. Because this policy isn't enforced for User 1, they can sign in without MFA.
upvoted 9 times

kiketxu 4 months, 3 weeks ago

User 1 can't sign without MFA.
User 2 will be prompted for MFA.

upvoted 3 times

ellik 3 months, 3 weeks ago

User 2 will be blocked. Sugar123 is right

upvoted 1 times

rinokings 4 months, 3 weeks ago

User 2 will be prompted for MFA

upvoted 1 times

BialyFenek 4 months, 4 weeks ago

User 2 will be prompted for MFA.

upvoted 2 times

bingomutant 4 months, 3 weeks ago

agreed - even if MFA disabled user 2 will still be prompted for it

upvoted 2 times

Question #15 *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 an on-premises Active Directory domain named contoso.com.
You install and run Azure AD Connect on a server named Server1 that runs Windows Server.
You need to view Azure AD Connect events.
You use the Security event log on Server1.
Does that meet the goal?

A. Yes

B. No

WoneSix Highly Voted 1 year, 7 months ago
While the responses were correct, the URL referenced in the solution on this and the following two questions refers to a third party product, NOT to Azure AD Connect. A correct reference is https://docs.microsoft.com/en-us/azure/active-directory/hybrid/tshoot-connect-object-not-syncing, which shows that the Azure AD Connect events are in the Azure AD Connect tool itself, not in any of the Windows event logs.
upvoted 12 times

Wallace44 1 year, 6 months ago
Even though to a third party product, if you read the page it includes information about where to find logs for AAD Connect. I do agree your link is better, though this link does provide enough context.
upvoted 2 times

WoneSix 1 year, 6 months ago
This is referencing where a third party tool keeps its event logs. From the web page, it appears the third party tool is named AD Connect. This is not the droid you're looking for.
upvoted 1 times

WoneSix 1 year, 6 months ago
After more searching, I was able to find this article that says password hash sync issues are found in the application event log. https://docs.microsoft.com/en-us/azure/active-directory/hybrid/tshoot-connect-password-hash-synchronization
upvoted 2 times

kiketxu Highly Voted 4 months, 3 weeks ago
No, it should be in the application log.
upvoted 8 times

zerowonka Most Recent 3 months ago
Correct answer is No
https://docs.microsoft.com/en-us/azure/active-directory/hybrid/how-to-connect-sync-service-manager-ui
upvoted 1 times

littlelamb 8 months, 1 week ago
I have setup and using AADC for a client, AADC events can be viewed in windows event APPLICATION logs not SECURITY logs
upvoted 6 times

Dumas234 1 year ago
Azure AD Connect is not a 3rd party tool.
upvoted 1 times

jason6311 1 year ago
Ignore the pingidentity.com link (as WoneSix stated). It is to a third party app (Ping Identity) which apparently has a feature called AD Connect, and has nothing to do with Azure AD Connect; the logo doesn't even match the Azure AD Connect logo.
upvoted 2 times

jasscomp 1 year, 3 months ago
https://docs.microsoft.com/en-us/azure/active-directory/hybrid/how-to-connect-sync-service-manager-ui

Logs can be found with Syncronisation Manager which is part of Azure AD Connect.
upvoted 2 times

Question #16 *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 an on-premises Active Directory domain named contoso.com.
You install and run Azure AD Connect on a server named Server1 that runs Windows Server.
You need to view Azure AD Connect events.
You use the Directory Service event log on Server1.
Does that meet the goal?

A. Yes

B. No

WoneSix Highly Voted 1 year, 6 months ago

The solution references a third-party product called AD Connect. This is not AAD Connect. Here is documentation saying where the AAD Connect tool records password hash sync issues: https://docs.microsoft.com/en-us/azure/active-directory/hybrid/tshoot-connect-password-hash-synchronization

upvoted 5 times

kiketxu Most Recent 5 months, 1 week ago

B for sure. You need application event log.
https://docs.microsoft.com/en-us/troubleshoot/azure/active-directory/installation-configuration-wizard-errors#troubleshoot-additional-error-messages

upvoted 4 times

vishg 6 months, 1 week ago

What is the correct answer? Simply put Yes or No. With description.

upvoted 2 times

ochiwi 1 year, 3 months ago

event logss thats where they go...

upvoted 2 times

Question #17 *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 an on-premises Active Directory domain named contoso.com.
You install and run Azure AD Connect on a server named Server1 that runs Windows Server.
You need to view Azure AD Connect events.
You use the System event log on Server1.
Does that meet the goal?

A. Yes

B. No

svm_Terran 7 months, 4 weeks ago
certainly No. needs an Application.
upvoted 4 times

kiketxu 5 months, 1 week ago
Agree. https://docs.microsoft.com/en-us/troubleshoot/azure/active-directory/installation-configuration-wizard-errors#troubleshoot-additional-error-messages
upvoted 3 times

WoneSix 1 year, 6 months ago
The solution references a third-party product called AD Connect. This is not AAD Connect. Here is documentation saying where the AAD Connect tool records password hash sync issues: https://docs.microsoft.com/en-us/azure/active-directory/hybrid/tshoot-connect-password-hash-synchronization
upvoted 4 times

Question #18 *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 an on-premises Active Directory domain named contoso.com.
You install and run Azure AD Connect on a server named Server1 that runs Windows Server.
You need to view Azure AD Connect events.
You use the Application event log on Server1.
Does that meet the goal?

A. Yes

B. No

Gowdhaman Highly Voted 1 year, 8 months ago
Application Event Log is correct. But the reference link is wrong. It should be below.

https://support.microsoft.com/en-us/help/2684395/how-to-troubleshoot-azure-active-directory-sync-tool-installation-and
upvoted 19 times

TDAC 10 months, 3 weeks ago
I agree with this answer. Further information can also be found here: https://docs.microsoft.com/en-us/troubleshoot/azure/active-directory/installation-configuration-wizard-errors - under the heading "Troubleshooting additional error messages", it makes specific mention that DIRECTORY SYNCHRONIZATION LOGGING can be found under the Application log
upvoted 3 times

jasscomp 1 year, 3 months ago
Thanks - the article does explain that these logs can be found in the Event Log. So if Azure AD connect is installed on Server1 then this is the correct answer.
upvoted 2 times

Rstilekar Most Recent 1 month, 4 weeks ago
TDAC is correct # I agree with this answer. Further information can also be found here: https://docs.microsoft.com/en-us/troubleshoot/azure/active-directory/installation-configuration-wizard-errors - under the heading "Troubleshooting additional error messages", it makes specific mention that DIRECTORY SYNCHRONIZATION LOGGING can be found under the Application log
upvoted 1 times

kiketxu 5 months, 1 week ago
At last! this is correct log location.
upvoted 1 times

kiketxu 5 months, 1 week ago
https://docs.microsoft.com/en-us/troubleshoot/azure/active-directory/installation-configuration-wizard-errors#troubleshoot-additional-error-messages
upvoted 1 times

JSmithZTG 1 year, 2 months ago
The answer is incorrect. Only installation events are logged in the Event Log. Azure AD Connect Events are logged within the application itself.
upvoted 3 times

jason6311 1 year ago
Though I take your point, none of the other test questions (at least shown here) give that answer as an option, and these series typically have one correct answer. The fact that installation events for AAD Connect do show in the Application Event log, if I were faced with the same series of questions in the exam, I would choose the Application Event log answer as "yes". But it is an ambiguous question.
upvoted 3 times

VTHAR 12 months ago
Yes, it's very ambiguous question. AADC logs certain events to Application Event Log so this answer must be correct.
https://docs.microsoft.com/en-us/azure/active-directory/hybrid/tshoot-connect-password-hash-synchronization

"No password hash synchronization heartbeat events
Each on-premises Active Directory connector has its own password hash synchronization channel. When the password hash synchronization channel is established and there aren't any password changes to be synchronized, a heartbeat event (EventId 654) is generated once every 30 minutes under the Windows Application Event Log. For each on-premises Active Directory connector, the cmdlet searches for corresponding heartbeat events in the past three hours. If no heartbeat event is found, the following error is returned:"
upvoted 2 times

TonySuccess 8 months, 1 week ago
Don't overthink it bro it's just making sure you know that it's not security logs etc and you go to the correct log area (App logs).
upvoted 8 times

Question #19 *Topic 1*

You have a Microsoft 365 E5 subscription.
Some users are required to use an authenticator app to access Microsoft SharePoint Online.
You need to view which users have used an authenticator app to access SharePoint Online. The solution must minimize costs.
What should you do?

A. From the Security & Compliance admin center, download a report.

B. From Azure Log Analytics, query the logs.

C. From the Security & Compliance admin center, perform an audit log search.

D. From the Enterprise applications blade of the Azure Active Directory admin center, view the sign-ins.

Goseu 2 months, 3 weeks ago
Answer is Correct , you may filter per Application and per Authentication requirement .
upvoted 3 times

kiketxu 4 months, 3 weeks ago
It's clear D to me in this case, but there is something rare in the statement. It's correct yhay you can see if MFA authentication was used filtering by MFA, but I don't see any possibility to confirm they are using the authenticator app.
upvoted 3 times

thecomodor 4 months ago
Actually, you can. If you click on the sign-in, a Details pane will be opened at the bottom which has the authentication Details including what form of MFA has been used
upvoted 1 times

Question #20 *Topic 1*

HOTSPOT -

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

Name	Role
User1	Global administrator
User2	Privileged Role Administrator
User3	Security administrator

You implement Azure Active Directory (Azure AD) Privileged Identity Management (PIM).

From PIM, you review the Application Administrator role and discover the users shown in the following table.

Name	Assignment type
UserA	Permanent
UserB	Eligible
UserC	Eligible

The Application Administrator role is configured to use the following settings in PIM:

- Maximum activation duration: 1 hour
- Notifications: Disable
- Incident/Request ticket: Disable
- Multi-Factor Authentication: Disable
- Require approval: Enable
- Selected approver: No results

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

NOTE: Each correct selection is worth one point.

Hot Area:

Answer Area

Statements	Yes	No
If UserB requests the Application Administrator role, User1 can approve the request of UserB.	○	○
If UserB requests the Application Administrator role, User2 can approve the request of UserB.	○	○
If UserC requests the Application Administrator role, User3 can approve the request of UserC.	○	○

VTHAR Highly Voted 10 months, 1 week ago

YES-YES-NO. If you edit role setting and define no approver, you will see this statement right there at PIM => If no specific approvers are selected, privileged role administrators/global administrators will become the default approvers.

upvoted 26 times

examuser123 Highly Voted 1 year, 1 month ago

Just tested this, no approvers specified, any global admin can approve as well as privileged role admins. Key here is if no approvers are assigned then any GA or PRA can approve

upvoted 22 times

tarunkantimondal Most Recent 1 month, 4 weeks ago

Answer is Y-Y-N

upvoted 1 times

SofieneFerchichi 5 months ago

Correct.....Y Y N with TEST

upvoted 8 times

finolweb 5 months, 2 weeks ago

If no specific approvers are selected, privileged role administrators/global administrators will become the default approvers.

upvoted 4 times

Jullirene 5 months, 2 weeks ago

The answer is CORRECT. The focus on this question is on whether approval is required or no and in this case approval IS required even though there are no approvers selected which means that anyone in the Global Administrator or Privileged Administrator role would be able to approve access to eligible members. If "Require Approval" wasn't configured then the users would be able to self-approve for the roles and the whole elevation process would be automated and time-bound for the 1hr mentioned here

upvoted 2 times

TheHole 5 months, 2 weeks ago

"Only Global Administrators and Privileged Role administrators can delegate administrator roles"
YES
YES
NO

upvoted 5 times

Gamer50 5 months, 3 weeks ago

The answer is YES,YES,NO.

To explain the first YES with regards to the Administrator can approve, check this reference : https://docs.microsoft.com/en-us/azure/active-directory/privileged-identity-management/azure-ad-pim-approval-workflow?tabs=new

A Global admin or Privileged role admin who believes that an approved user should not be active can remove the active role assignment in Privileged Identity Management. Although administrators are not notified of pending requests unless they are an approver, they can view and cancel any pending requests for all users by viewing pending requests in Privileged Identity Management.

upvoted 2 times

LuisLfr 6 months ago

YES
YES
NO

upvoted 2 times

janee 6 months, 3 weeks ago

Yes
Yes
No

upvoted 2 times

Samoanhulk 6 months, 3 weeks ago

No, Yes, No

upvoted 1 times

AlexanderSaad 6 months, 3 weeks ago

The answer is correct. If you create an assignment in PIM and you check its settings you will read that:
"If no specific approvers are selected, privileged role administrators/global administrators will become the default approvers."

upvoted 1 times

Mary_Yvette 7 months, 3 weeks ago

Yes, Yes, No

I checked the portal in PIM and this is what I found:
If no specific approvers are selected, privileged role administrators/global administrators will become the default approvers.

upvoted 3 times

TonySuccess 8 months, 2 weeks ago

I've used my lab to test this because there are so many conflicting answers.

If you assign the App Admin role to someone and make them eligable, they can activate the role themsleves.

Unless, you Edit the role settings and assign approvers for the role. (If you do not assign approvers you ge the following message):

"If no specific approvers are selected, privileged role administrators/global administrators will become the default approvers"

I logged in to PIM as a secondary Global Admin and was able to Activate an assignment for the App Admin role.

Make of that what you will...

upvoted 2 times

TonySuccess 8 months ago

A Global admin or Privileged role admin who believes that an approved user should not be active can remove the active role assignment in Privileged Identity Management. Although administrators are not notified of pending requests unless they are an approver, they can view and cancel any pending requests for all users by viewing pending requests in Privileged Identity Management.

https://docs.microsoft.com/en-us/azure/active-directory/privileged-identity-management/azure-ad-pim-approval-workflow?tabs=new

upvoted 3 times

Ehernandez 6 months, 3 weeks ago

this link is clear, in the last Note.

upvoted 1 times

hamzajeljeli 9 months, 2 weeks ago

Provided answer is correct. Please check this reference https://docs.microsoft.com/en-us/azure/active-directory/roles/permissions-reference#privileged-role-administrator

upvoted 2 times

Dhanger 9 months, 4 weeks ago

Yes-Yes-No
Only Global administrators and Privileged Role administrators can delegate administrator roles. To reduce the risk to your business, we recommend that you assign this role to the fewest possible people in your organization.
https://docs.microsoft.com/en-us/azure/active-directory/users-groups-roles/directory-assign-admin-roles
upvoted 1 times

examcrammer 10 months, 1 week ago
VTHAR is correct!! I upvoted that response and agree YES-YES-NO
upvoted 1 times

Question #21 *Topic 1*

You have a Microsoft 365 E5 subscription.
Some users are required to use an authenticator app to access Microsoft SharePoint Online.
You need to view which users have used an authenticator app to access SharePoint Online. The solution must minimize costs.
What should you do?

A. From the Azure Active Directory admin center, view the sign-ins.

B. From the Security & Compliance admin center, download a report.

C. From the Enterprise applications blade of the Azure Active Directory admin center, view the audit logs.

D. From the Azure Active Directory admin center, view the authentication methods.

kiketxu 4 months, 3 weeks ago
A in this case.
upvoted 4 times

Question #22 *Topic 1*

HOTSPOT -

You have a Microsoft 365 subscription that contains an Azure Active Directory (Azure AD) tenant named contoso.com.

You need to recommend an Azure AD Privileged Identity Management (PIM) solution that meets the following requirements:

- Administrators must be notified when the Security administrator role is activated.
- Users assigned the Security administrator role must be removed from the role automatically if they do not sign in for 30 days.

Which Azure AD PIM setting should you recommend configuring 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

Administrators must be notified when the Security administrator role is activated: [▼]
- Alerts
- Roles
- Access reviews

Users assigned the Security administrator role must be removed from the role automatically if they do not sign in for 30 days: [▼]
- Alerts
- Roles
- Access reviews

kiketxu Highly Voted 4 months, 3 weeks ago

If I'm right....(if not, please appreciated someone point me right)
#1 Role activation alert is in "Roles" under Assignments (or Assignments in the blade directly), select i.e. Security Admin role and go to notifications section in settings.

#2 Despite under Alerts are two triggers that could raise an alert for "Elegible administrators aren't using their privileged roles (<30days)" or "Potential stale accounts in a privileged role (without setting available)" I don't see anywhere an option to automate removal. So, I would answer "Access Reviews" as the only possible way I found to automate action to remove role. https://docs.microsoft.com/en-us/azure/active-directory/privileged-identity-management/pim-how-to-configure-security-alerts?tabs=new#administrators-arent-using-their-privileged-roles

Additional link: https://docs.microsoft.com/es-es/azure/active-directory/privileged-identity-management/pim-how-to-configure-security-alerts?tabs=new

upvoted 16 times

prabhjot 6 days, 21 hours ago

agree 1) role and 2) Access Review

upvoted 1 times

Yetijo 1 month, 3 weeks ago

I believe you are correct.
#1 is Role
#2 Access Review

#1 Should be role, no question. #2 Should be access review based on findings in the lab and supported by the MS docs:
https://docs.microsoft.com/es-es/azure/active-directory/privileged-identity-management/pim-how-to-configure-security-alerts?tabs=new

upvoted 6 times

ellik 3 months, 3 weeks ago

I agree with you as it is mentioned that >>>Regularly review accounts with privileged roles using access reviews and remove role assignments that are no longer needed.
I also checked the AAD and you can specify the role and the action to remove-approve-take recommendation

upvoted 1 times

w00t 4 months, 1 week ago

Pretty positive you're right.
#1 = ROLE
#2 = ALERT

They have the answer backwards.

upvoted 1 times

w00t 4 months, 1 week ago

CONFIRMED
1 - ROLE
2 - ALERT

If you go into PIM > Roles > Select Any Role > Role Settings > "Send notifications when eligible members activate this role" - This is all within ROLE SETTINGS. Has nothing to do with "Alerts".

upvoted 3 times

Rafale Highly Voted 4 months, 1 week ago

Given answers are correct
1- Alert
2- Role

upvoted 10 times

stromnessian Most Recent 1 week, 5 days ago

Dear Microsoft, please employ competent people to write the exam questions.

upvoted 2 times

aaronkho 1 month, 1 week ago

Alert
Access Review

upvoted 1 times

Rstilekar 1 month, 4 weeks ago

I think JRGR is correct # Answer to both is ROLES.
1 - Roles: In the role configuration, in the Notification tab you can set up who receives a notification when the role is activated ((Role activation alert is in "Roles" under Assignments (or Assignments in the blade directly), select i.e. Security Admin role and go to notifications section in settings.))
2 - Roles:In the role configuration, Assignement tab, and then set the assignment duration to 30 days.

2nd answer cant be access reviews as - Stale accounts is based on the last password change date and for access review you can set up this rule only for max 27 days in a month (not 30), also access review is more asking the manager to review.

Also 2nd Answer Cant be 'Alert' as - the "Potential stale accounts in a privileged role" Alert is for 90 days and cannot be changed

upvoted 2 times

DiscussElie 2 months ago

1-Roles
2- Alerts

upvoted 1 times

bsldwp_2020 2 months ago

1- Role (Manage --> Roles --> <Role name> --> Role Settings --> Edit "Send notifications when members are assigned as eligible to this role")

2- Alerts (Manage --> Alerts --> Settings --> Edit "Eligible administrators aren't activating their privileged role")

upvoted 1 times

Lomak 2 months, 1 week ago

#1 - Role: Role Settings
#2 - Role: Assinment End time - set to 30 days

2nd Answer Cant be 'Alert' as the "Potential stale accounts in a privileged role" Alert is for 90 days and cannot be changed

upvoted 1 times

prats005 4 months ago

Roles and Access Review | https://docs.microsoft.com/en-us/azure/active-directory/privileged-identity-management/pim-how-to-start-security-review

upvoted 5 times

JRGR 4 months ago

1 - Roles: In the role configuration, in the Notification tab you can set up who receives a notification when the role is activated
2 - Roles:In the role configuration, Assignement tab, and then set the assignment duration to 30 days.

upvoted 5 times

vijeet 4 months, 2 weeks ago

Answers are:
1. Role (Require approval to activate)
2. Alert (Potential stale accounts in a privileged role)

upvoted 4 times

b00 4 months, 4 weeks ago

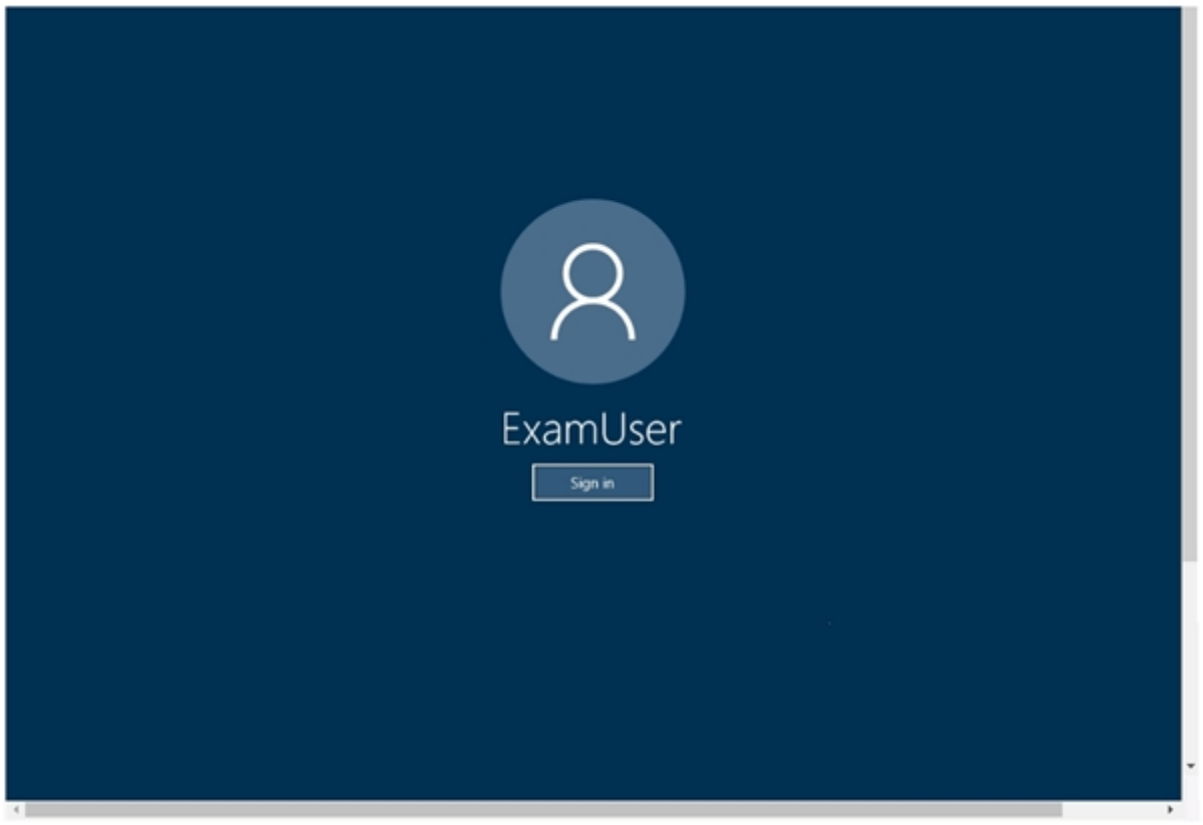
I think this is the other way arround, notifications are in "role" (the alert can trigger if admin is assigned outside of PIM but that's not how I understand the question) and for the second question because it says "if they do not sign in" I would rather use this alert : https://docs.microsoft.com/en-us/azure/active-directory/privileged-identity-management/pim-how-to-configure-security-alerts?tabs=new#administrators-arent-using-their-privileged-roles. The only thing I cannot answer is the automation of the role removal... but maybe the fix for the alert can be considered as automation.

upvoted 2 times

Question #23 *Topic 1*

SIMULATION -
Please wait while the virtual machine loads. Once loaded, you may proceed to the lab section. This may take a few minutes, and the wait time will not be deducted from your overall test time.
When the Next button is available, click it to access the lab section. In this section, you will perform a set of tasks in a live environment. While most functionality will be available to you as it would be in a live environment, some functionality (e.g., copy and paste, ability to navigate to external websites) will not be possible by design.
Scoring is based on the outcome of performing the tasks stated in the lab. In other words, it doesnɹ€™t matter how you accomplish the task, if you successfully perform it, you will earn credit for that task.
Labs are not timed separately, and this exam may more than one lab that you must complete. You can use as much time as you would like to complete each lab.
But, you should manage your time appropriately to ensure that you are able to complete the lab(s) and all other sections of the exam in the time provided.
Please note that once you submit your work by clicking the Next button within a lab, you will NOT be able to return to the lab.

Username and password -



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@LODSe244001.onmicrosoft.com
Microsoft 365 Password: &=Q8v@2qGzYz
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: 11032396 -
You need to ensure that a user named Lee Gu can manage all the settings for Exchange Online. The solution must use the principle of least privilege.
To complete this task, sign in to the Microsoft Office 365 admin center.

Alex_ua1 1 month ago
The task says -To complete this task, sign in to the Microsoft Office 365 admin center. answer is correct
upvoted 1 times

Rstilekar 1 month, 3 weeks ago
Yes given answer is right
upvoted 1 times

ZakS 2 months, 1 week ago
The Exchange Service Admin (aka Azure AD 'Exchange Administrator' role) is a member of the 'Organization Management' role group in EXO.

So, granting someone the Azure AD Exchange Admin role would be the ideal/best practice way to go.

The ans given is technically correct but probably not best practice.
I'd grant the user the Azure AD Exchange Admin role in the exam for this lab exercise.
upvoted 4 times

nidentify 3 weeks, 3 days ago
Yes exchange admin is should be the correct answer
upvoted 1 times

jatinKumar 4 months ago
will this not be .. ADzure AD Role "Exchange Administrator" as it says manage all settings of exchange online.. please advise
upvoted 3 times

Robert__Susin 3 months ago
No as Exchange Administrator is different from Organization Manager role in EXO, the question states Least Privileges into managing settings in EXO, so the given answer is correct.
upvoted 2 times

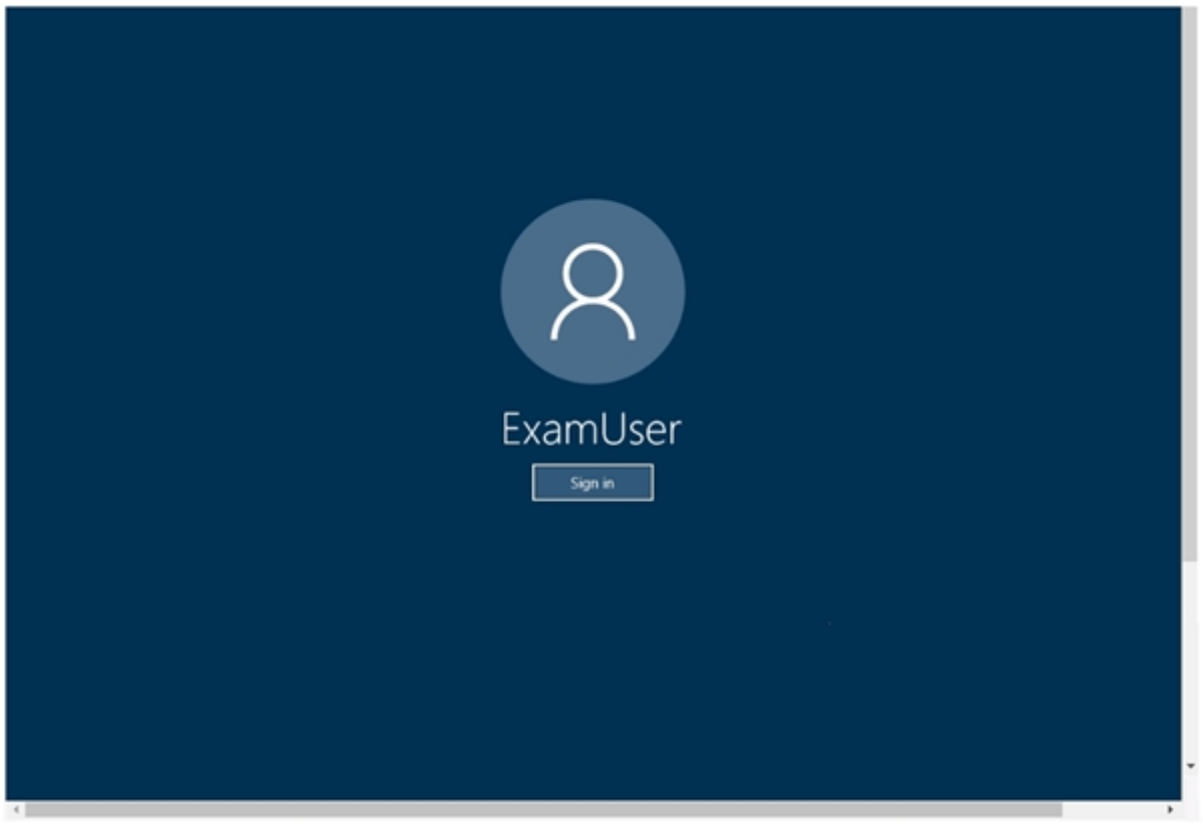
dcasabona 3 months, 1 week ago
I think so too.
upvoted 1 times

ellik 3 months, 3 weeks ago
is it AD Role "Exchange Administrator" ?
upvoted 1 times

Question #24 *Topic 1*

SIMULATION -
Please wait while the virtual machine loads. Once loaded, you may proceed to the lab section. This may take a few minutes, and the wait time will not be deducted from your overall test time.
When the Next button is available, click it to access the lab section. In this section, you will perform a set of tasks in a live environment. While most functionality will be available to you as it would be in a live environment, some functionality (e.g., copy and paste, ability to navigate to external websites) will not be possible by design.
Scoring is based on the outcome of performing the tasks stated in the lab. In other words, it doesnɹ€™t matter how you accomplish the task, if you successfully perform it, you will earn credit for that task.
Labs are not timed separately, and this exam may more than one lab that you must complete. You can use as much time as you would like to complete each lab.
But, you should manage your time appropriately to ensure that you are able to complete the lab(s) and all other sections of the exam in the time provided.
Please note that once you submit your work by clicking the Next button within a lab, you will NOT be able to return to the lab.

Username and password -



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@LODSe244001.onmicrosoft.com
Microsoft 365 Password: &=Q8v@2qGzYz
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: 11032396 -
You need to ensure that each user can join up to five devices to Azure Active Directory (Azure AD).
To complete this task, sign in to the Microsoft Office 365 admin center.

Delli Highly Voted 3 months, 4 weeks ago
Device is now in Microsoft EndPoint Manager Admin Center. So the process is different :

1-Connect on https://endpoint.microsoft.com
2-Go in Devices --> Enrollement restrictions
3-Create or Edit the default device limit restrictions that apply to all users
4-Set Device limit to 5
https://docs.microsoft.com/en-us/mem/intune/enrollment/device-limit-intune-azure#azure-device-limit-restriction
upvoted 8 times

fuckthisscamsite 3 months, 2 weeks ago
The question is about joining devices to Azure AD, not enrolling in Intune. You are wrong
upvoted 16 times

Rstilekar Most Recent 1 month, 3 weeks ago

Agreed. given steps in answer are correct

upvoted 2 times

Donnie21 3 months, 3 weeks ago

You can still use Azure.

upvoted 2 times

Vic08 2 months, 3 weeks ago

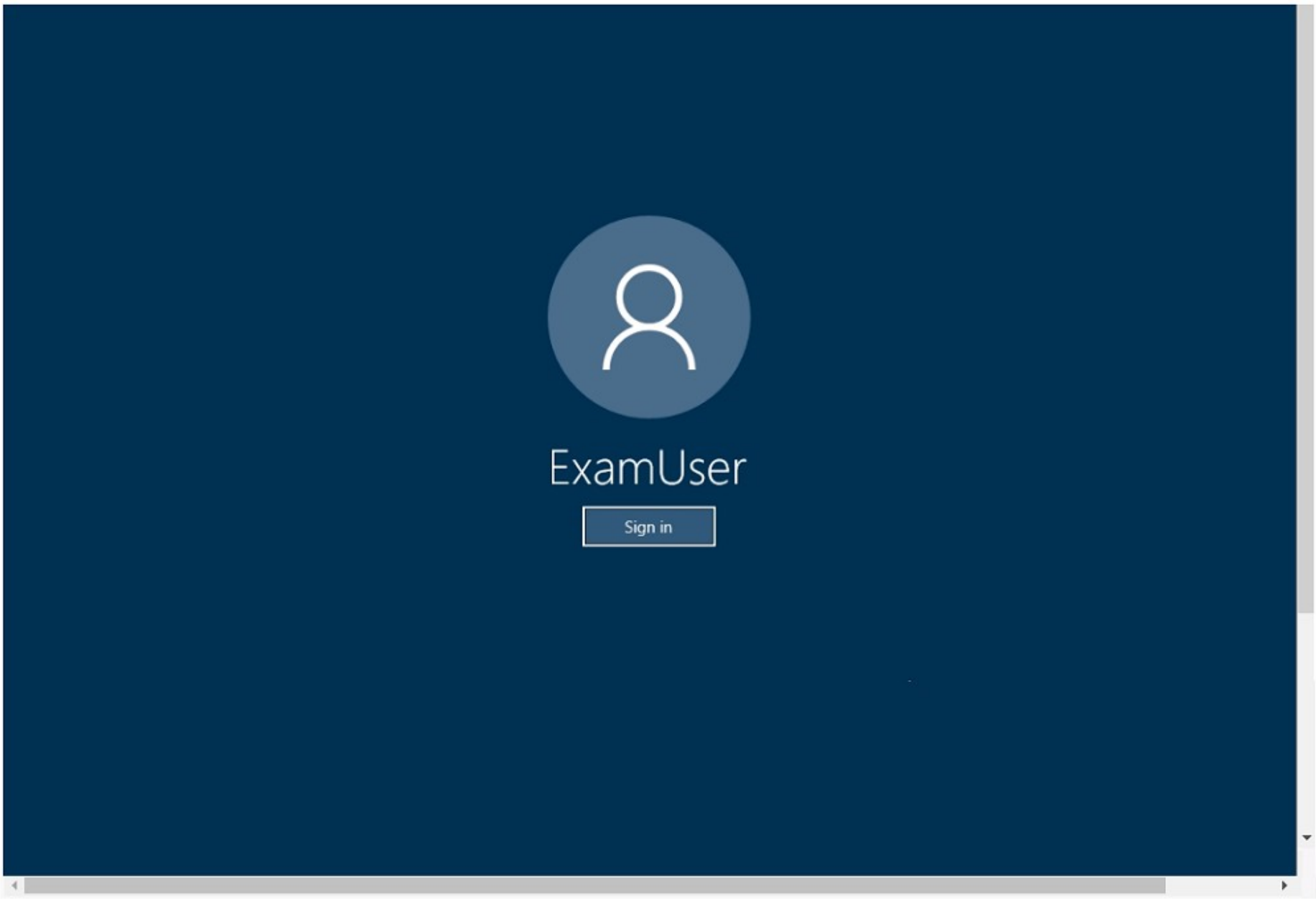
https://portal.azure.com/#blade/Microsoft_AAD_Devices/DevicesMenuBlade/DeviceSettings/menuId/

upvoted 2 times

Question #25 *Topic 1*

SIMULATION -
Please wait while the virtual machine loads. Once loaded, you may proceed to the lab section. This may take a few minutes, and the wait time will not be deducted from your overall test time.
When the Next button is available, click it to access the lab section. In this section, you will perform a set of tasks in a live environment. While most functionality will be available to you as it would be in a live environment, some functionality (e.g., copy and paste, ability to navigate to external websites) will not be possible by design.
Scoring is based on the outcome of performing the tasks stated in the lab. In other words, it doesnɹ€™t matter how you accomplish the task, if you successfully perform it, you will earn credit for that task.
Labs are not timed separately, and this exam may more than one lab that you must complete. You can use as much time as you would like to complete each lab.
But, you should manage your time appropriately to ensure that you are able to complete the lab(s) and all other sections of the exam in the time provided.
Please note that once you submit your work by clicking the Next button within a lab, you will NOT be able to return to the lab.

Username and password -



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@LODSe244001.onmicrosoft.com
Microsoft 365 Password: &=Q8v@2qGzYz
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: 11032396 -
You need to ensure that group owners renew their Office 365 groups every 180 days.
To complete this task, sign in to the Microsoft Office 365 admin center.

Vic08 2 months, 3 weeks ago
https://portal.azure.com/#blade/Microsoft_AAD_IAM/GroupsManagementMenuBlade/Lifecycle
upvoted 1 times

Discuss4certi 4 months, 2 weeks ago

If the email address is required, which one would you enter? Or has it been provided?

upvoted 1 times

mashaeg 2 months, 2 weeks ago

By default is sent to group owner, if there are no owner, it will send the email in "email cotnact fro groups with no owners"- so yourself/amin

upvoted 1 times

Question #26 *Topic 1*

SIMULATION -

You need to ensure that unmanaged mobile devices are quarantined when the devices attempt to connect to Exchange Online.

To complete this task, sign in to the Microsoft 365 portal.

FumerLaMoquette Highly Voted 9 months ago

I think you need to go to exchange control panel > mobile > exchange activesync access settings and verify default is set to quarrantine.
https://docs.microsoft.com/en-us/exchange/troubleshoot/client-connectivity/eas-device-is-blocked-by-abq-list

upvoted 6 times

Dooa Highly Voted 5 months ago

This option is not available in new exchange admin portal..

upvoted 5 times

Rstilekar Most Recent 1 month, 3 weeks ago

The steps are only in Classic EAP and no settings for same in new EAP

upvoted 2 times

TheGuy 4 months, 1 week ago

You can still find this setting in the Classic Exchange Admin Center

upvoted 3 times

yassora 4 months, 2 weeks ago

I agree With Fumer , This answer for the old portal

upvoted 1 times

Question #27 *Topic 1*

SIMULATION -

You need to ensure that all users must change their password every 100 days.

To complete this task, sign in to the Microsoft 365 portal.

Nicholasname Highly Voted 1 year, 1 month ago

2. In the left navigation pane, expand the Settings section then select the "Org Settings" option.

upvoted 12 times

Alpanama 4 months, 1 week ago

Confirmed, the "new" value is "Org Settings".

upvoted 1 times

Ray81 10 months, 4 weeks ago

Yes, thank you @Nicholasname, they skipped that step.

upvoted 2 times

IvanDan 10 months, 3 weeks ago

They didn't, "Org Settings" was just "Settings" before. It was changed a few months ago

upvoted 3 times

shanti0091 6 months, 1 week ago

true gospel

upvoted 1 times

Shahidqk Most Recent 1 week, 4 days ago

Agree with Nicholas, Setting-->Org Settings.
Don't get confuse there are 3 tabs in middle one "Security & Privacy" then double click on "Password expiration Policy"

upvoted 1 times

Question #28 *Topic 1*

SIMULATION -

You need to ensure that a user named Grady Archie can monitor the service health of your Microsoft 365 tenant. The solution must use the principle of least privilege.

To complete this task, sign in to the Microsoft 365 portal.

btd2020 Highly Voted 1 year, 2 months ago

I believe the Service Administrator role is the same as Service Support Administrator. I couldn't even find SA role under roles . But the role description for both is the same.

upvoted 20 times

Bl0ckSh3ll 10 months, 3 weeks ago

That's correct. Service Support Administrator role description:
Creates service requests for Azure, Microsoft 365, and Office 365 services, and monitors service health.

upvoted 11 times

shanti0091 6 months, 1 week ago

This is 100% correct.

upvoted 3 times

Rstilekar Most Recent 1 month, 3 weeks ago

Checked. Its Service Support Administrator role now.

upvoted 1 times

ThBEST 2 months ago

Here is the updated link....
https://docs.microsoft.com/en-us/microsoft-365/business-video/add-admin?view=o365-worldwide

upvoted 1 times

Cogan 4 months, 2 weeks ago

Service Support Admin Role

upvoted 4 times

Mikula 1 year, 2 months ago

User need Service Administrator role.
https://docs.microsoft.com/en-us/office365/enterprise/view-service-health

upvoted 2 times

DrMe 7 months ago

Role has been renamed Service Support Administrator:
https://docs.microsoft.com/en-us/azure/active-directory/roles/permissions-reference#service-support-administrator:~:text=Previously%2C%20this%20role%20was%20called%20%22Service,Graph%20API%2C%20and%20Azure%20AD%20PowerShell.

upvoted 9 times

Question #29 *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 subscription.
You have a user named User1. Several users have full access to the mailbox of User1.
Some email messages sent to User1 appear to have been read and deleted before the user viewed them.
When you search the audit log in Security & Compliance to identify who signed in to the mailbox of User1, the results are blank.
You need to ensure that you can view future sign-ins to the mailbox of User1.
You run the Set-AdminAuditLogConfig -AdminAuditLogEnabled $true
-AdminAuditLogCmdlets *Mailbox* command.
Does that meet the goal?

A. Yes

B. No

yeckto Highly Voted 9 months ago

With Set-AdminAuditLogConfig , you must use -UnifiedAuditLogIngestionEnabled parameter to activate user and admin activities.
https://docs.microsoft.com/en-us/powershell/module/exchange/set-adminauditlogconfig?view=exchange-ps

upvoted 13 times

kiketxu 4 months, 3 weeks ago

thanks!

upvoted 1 times

Goseu Most Recent 2 months, 2 weeks ago

Answer is Correct ,meaning NO .
for cloud based use :-UnifiedAuditLogIngestionEnabled
This is for on prem only

upvoted 2 times

Kalzonee3611 2 months, 2 weeks ago

This is correct? Seen a few conflicting answers. Any advice would be great...

upvoted 1 times

yeckto 9 months ago

Answer is correct. You must use Set-Mailbox -Identity [] -AuditXXXX. https://docs.microsoft.com/es-es/microsoft-365/compliance/enable-mailbox-auditing?view=o365-worldwide

upvoted 3 times

TDAC 10 months, 2 weeks ago

Answer is correct.

The Set-AdminAuditLogConfig powershell cmdlet has nothing to do with logging mailbox access for delgates. The command is used to change auditing parameters once auditing has already been enabled. We know from the question that no auditing has been enabled yet.

You can read more about the PS cmdlet mentioned here: https://docs.microsoft.com/en-us/powershell/module/exchange/set-adminauditlogconfig?view=exchange-ps

upvoted 1 times

Question #30 *Topic 1*

You have a Microsoft 365 subscription that contains a user named User1.

You plan to use Compliance Manager.

You need to ensure that User1 can assign Compliance Manager roles to users. The solution must use the principle of least privilege.

Which role should you assign to User1?

A. Compliance Manager Assessor

B. Global Administrator

C. Portal Admin

D. Compliance Manager Administrator

dzampar Highly Voted 9 months, 1 week ago

My guess is that the answer is wrong as I couldn't find any portal admin role. So regarding the options provided, I would go with the global admin as per the link below.

https://docs.microsoft.com/en-us/microsoft-365/compliance/compliance-manager-setup?view=o365-worldwide#role-types

upvoted 8 times

Mendel Highly Voted 4 months, 1 week ago

Both Portal Admin and Global Admin is correct. Portal Admin is for the classic portal (which will be deprecated) and Global Admin for new portal.

Classic: https://docs.microsoft.com/en-us/microsoft-365/compliance/meet-data-protection-and-regulatory-reqs-using-microsoft-cloud?view=o365-worldwide#permissions-and-role-based-access-control%20//%20Portal%20Admin.
New: https://docs.microsoft.com/en-us/microsoft-365/compliance/compliance-manager-setup?view=o365-worldwide

upvoted 7 times

Yetijo Most Recent 1 month, 3 weeks ago

Global Administrator
The answer is here in the docs. Also reference the table for Role Types in the following section from the link. The last row clearly indicates GA is required for assignments.
https://docs.microsoft.com/en-us/microsoft-365/compliance/compliance-manager-setup?view=o365-worldwide#set-user-permissions-and-assign-roles

upvoted 1 times

Rstilekar 1 month, 3 weeks ago

Global Admin is correct.
Portal Admin role was in old compliance admin portals that is retired now already and not available to use anymore.

upvoted 3 times

ZakS 2 months, 1 week ago

Ans GLOBAL ADMINISTRATOR is correct.

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

"The person holding the global admin role for your organization can set user permissions for Compliance Manager. Permissions can be set in the Office 365 Security & Compliance center as well as in Azure Active Directory (Azure AD)."

upvoted 1 times

DudleyYVR 3 months, 2 weeks ago

It's C. Global Admin is NOT LEAST PRIVILEGE. So that's wrong. RBAC for Portal Admin still exists.

upvoted 2 times

SerhioG 4 months, 1 week ago

Role types
The table below shows the functions allowed by each role in Compliance Manager. The table also shows how each Azure AD role maps to Compliance Manager roles. Users will need at least the Compliance Manager reader role, or Azure AD global reader role, to access Compliance Manager.

Types
User can:Compliance Manager role:Azure AD role

Read but not edit data:Compliance Manager Reader:Azure AD Global reader, Security reader
Edit data:Compliance Manager Contribution:Compliance Administrator
Edit test results:Compliance Manager Assessment:Compliance Administrator
Manage assessments,and template and tenant data:Compliance Manager Administration:Compliance Administrator, Compliance Data Administrator,Security Administrator

Assign users:Global Administrator:Global Administrator
https://docs.microsoft.com/ru-ru/microsoft-365/compliance/compliance-manager-setup?view=o365-worldwide#role-types

upvoted 1 times

Rafale 4 months, 1 week ago

Global Administrator is the correct answer.
No role called Portal Admin.

upvoted 1 times

diazed 4 months, 3 weeks ago

B for sure. The person holding the global admin role for your organization can set user permissions for Compliance Manager.

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

upvoted 2 times

kiketxu 4 months, 3 weeks ago

Seems out of data this question due "Portal Admin", nowdays I hope we can found it updated in the exam.
B for sure! https://docs.microsoft.com/en-us/microsoft-365/compliance/compliance-manager-setup?view=o365-worldwide#role-types

upvoted 3 times

Discuss4certi 4 months, 2 weeks ago

Indeed, i went looking in the permissions section of the compliance admin center. No portal admin to be found. So indeed this question is probably outdated. If i were to get it today i would pick global admin

upvoted 2 times

eltom 5 months ago

Only global administrator can assign Compliance Manager roles to users

https://docs.microsoft.com/en-us/microsoft-365/compliance/compliance-manager-setup?view=o365-worldwide#role-types

Assign users Global Administrator Global Administrator

upvoted 2 times

shanti0091 6 months, 1 week ago

The answer is 100% correct. Portal Admin Role is the least privileged access in this context.
https://docs.microsoft.com/en-us/microsoft-365/compliance/meet-data-protection-and-regulatory-reqs-using-microsoft-cloud?view=o365-worldwide#permissions-and-role-based-access-control%20//%20Portal%20Admin.

upvoted 2 times

la6520117 6 months, 2 weeks ago

Answer is D.Global administrator. Microsoft says
To add or remove users from Compliance Manager roles.
Go to https://servicetrust.microsoft.com.
Sign in with your Azure Active Directory global administrator account.

Reference: https://docs.microsoft.com/en-us/microsoft-365/compliance/meet-data-protection-and-regulatory-reqs-using-microsoft-cloud?view=o365-worldwide#assigning-compliance-manager-roles-to-users

upvoted 2 times

Faith 7 months ago

I have found this statement "Manage users - Users can add other users in their organization to the Reader, Contributor, Assessor, and Administrator roles. Only those users with the Global Administrator role in your organization can add or remove users from the Portal Admin role."

upvoted 1 times

PattiD 7 months, 3 weeks ago

https://docs.microsoft.com/en-us/microsoft-365/compliance/meet-data-protection-and-regulatory-reqs-using-microsoft-cloud?view=o365-worldwide#permissions-and-role-based-access-control // Portal Admin.

upvoted 2 times

Sonia33 8 months, 3 weeks ago

As per this link, C) Portal Admin is correct:
https://docs.microsoft.com/en-us/microsoft-365/compliance/meet-data-protection-and-regulatory-reqs-using-microsoft-cloud?view=o365-worldwide

But notice that this refers to Classic portal, not the latest.

upvoted 1 times

ramingt 7 months, 3 weeks ago

The person holding the global admin role for your organization can set user permissions in the Microsoft 365 compliance center, as well as in Azure Active Directory (Azure AD).

upvoted 1 times

alexgrdi89 8 months, 4 weeks ago

I think B is correct.

Reference: https://docs.microsoft.com/en-us/microsoft-365/compliance/compliance-manager-setup?view=o365-worldwide

upvoted 3 times

Question #31 *Topic 1*

You have a Microsoft 365 subscription linked to an Azure Active Directory (Azure AD) tenant that contains a user named User1.
You have a Data Subject Request (DSR) case named Case1.
You need to allow User1 to export the results of Case1. The solution must use the principle of least privilege.
Which role should you assign to User1 for Case1?

A. eDiscovery Manager

B. Security Operator

C. eDiscovery Administrator

D. Global Reader

shanti0091 Highly Voted 6 months, 1 week ago
The answer is 100% correct. An E-Discovery Administrator role is superior in terms of RBAC than E-Discovery Manager.
upvoted 7 times

Rstilekar Most Recent 1 month, 3 weeks ago
eDiscovery manager role is correct
upvoted 3 times

iwikneerg 2 months ago
Check this page out for the difference between the 2 roles

https://docs.microsoft.com/en-us/microsoft-365/compliance/assign-ediscovery-permissions?view=o365-worldwide

The manager is the least privilege option as it only has access to cases it created or it has been added to.
upvoted 2 times

Enoll 3 months, 1 week ago
"The primary difference between an eDiscovery Manager and an eDiscovery Administrator is that an eDiscovery Administrator can access all cases that are listed on the eDiscovery cases page in the Security & Compliance Center. An eDiscovery manager can only access the cases they created or cases they are a member of."
https://docs.microsoft.com/en-us/microsoft-365/security/office-365-security/permissions-in-the-security-and-compliance-center?view=o365-worldwide#:~:text=The%20primary%20difference%20between%20an,they%20are%20a%20member%20of.
So I think that in this case, since User 1 didn't create Case1, he should be eDiscovery Admin in order to access and export the results. Thoughts?
upvoted 3 times

Azuanuka 2 months, 1 week ago
"An eDiscovery manager can only access the cases they created or cases they are a member of."

Applying the principle of least privilege, assing User1 eDiscovery manager role and make him a member of the Case1. Issue resolved.
upvoted 6 times

Nasser 1 month ago
Totally agree
upvoted 1 times

Enoll 2 months ago
you are right!
upvoted 1 times

NIck207 4 months, 4 weeks ago
E discovery manager is least privilege role, of course admin also correct but clearly stated least privilege,
upvoted 4 times

Faith 7 months ago
I would go for C: eDiscovery Administrator as the requirement is "use the principle of least privilege", as administrator is a member of the manager role with export access.
upvoted 2 times

drbabnik 6 months, 3 weeks ago
It says "Additionally, an eDiscovery Administrator can:" so Administrator is higher role than Manager.
upvoted 2 times

kiketxu 4 months, 3 weeks ago
Agree with eDiscovery Manager.
upvoted 2 times

Tom993 8 months, 3 weeks ago
A is correct; https://docs.microsoft.com/en-us/microsoft-365/compliance/assign-ediscovery-permissions?view=o365-worldwide

upvoted 2 times

Question #32 *Topic 1*

HOTSPOT -

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

Name	Member of
User1	Group1
User2	Group2
User3	Group1, Group2

You create and enforce an Azure Active Directory (Azure AD) Identity Protection sign-in risk policy that has the following settings:

- Assignments: Include Group1, Exclude Group2
- Conditions: User risk level of Medium and above
- Access: Allow access, Require password change

The users attempt to sign in. The risk level for each user is shown in the following table.

User	User risk level
User1	High
User2	Medium
User3	High

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

NOTE: Each correct selection is worth one point.

Hot Area:

Answer Area

Statements	Yes	No
User1 must change his password.	○	○
User2 must change his password.	○	○
User3 must change his password.	○	○

kiketxu Highly Voted 4 months, 3 weeks ago

Yes, (High and included)
No, (Medium but excluded)
No, (High but excluded too)
upvoted 8 times

Rstilekar Most Recent 1 month, 3 weeks ago

Answers are correct and logical (exclusion wins over inclusions for U2 & U3)
upvoted 1 times

Dawid321 3 months, 4 weeks ago

Tricky, sign-in risk policy required MFA confirmation
upvoted 1 times

ellik 3 months, 3 weeks ago

I guess this is user risk policy (different than sign-in risk policy which require MFA) , which requires SSPR to be enabled.
upvoted 1 times

Question #33 *Topic 1*

You configure several Advanced Threat Protection (ATP) policies in a Microsoft 365 subscription.

You need to allow a user named User1 to view ATP reports from the Threat management dashboard.

Which role provides User1 with the required role permissions?

A. Compliance administrator

B. Security reader

C. Message center reader

D. Reports reader

Rstilekar 1 month, 3 weeks ago

What permissions are needed to view the Defender for Office 365 reports?
You need to be a member of one of the following role groups in the Security & Compliance Center:

Organization Management
Security Administrator
Security Reader
Global Reader

upvoted 4 times

Robert__Susin 3 weeks, 1 day ago

Correction: in the Microsoft 365 Defender portal

upvoted 1 times

kiketxu 4 months, 3 weeks ago

from the given answers, Security Reader.
https://docs.microsoft.com/en-us/microsoft-365/security/office-365-security/view-reports-for-atp?view=o365-worldwide#what-permissions-are-needed-to-view-the-defender-for-office-365-reports

upvoted 2 times

Alpanama 4 months, 1 week ago

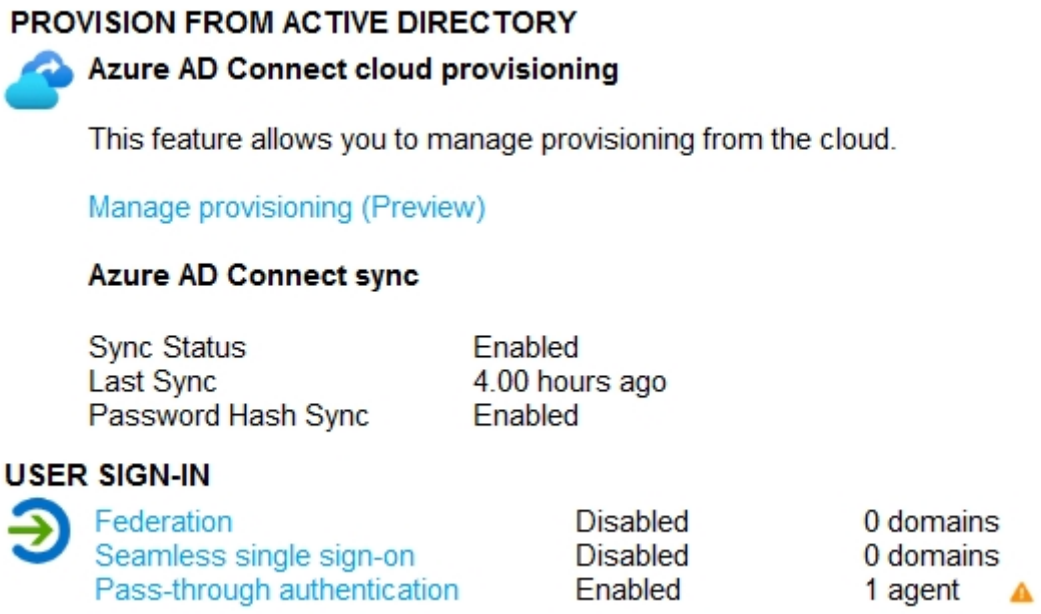
Changed to https://docs.microsoft.com/en-us/microsoft-365/security/office-365-security/view-reports-for-mdo?view=o365-worldwide#what-permissions-are-needed-to-view-the-defender-for-office-365-reports

upvoted 1 times

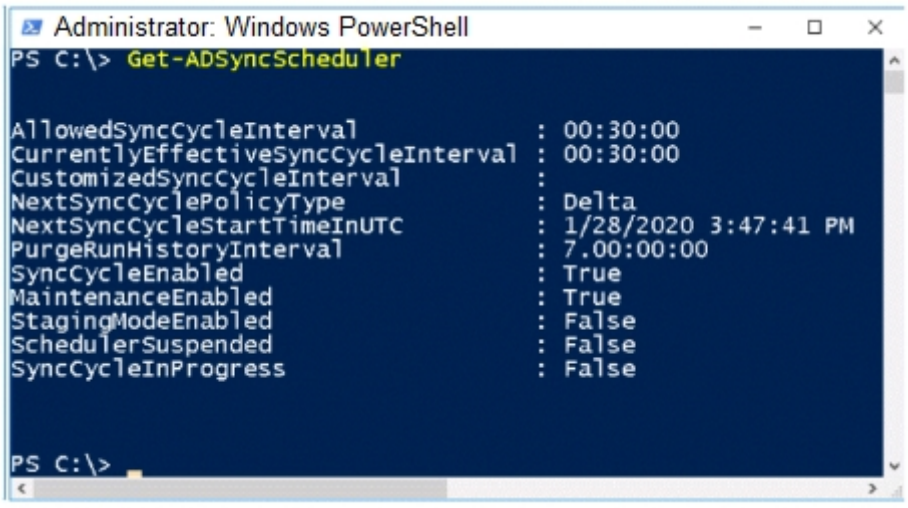
Question #34 *Topic 1*

HOTSPOT -

Your network contains an on-premises Active Directory domain that syncs to Azure Active Directory (Azure AD) as shown in the following exhibit.



The synchronization schedule is configured as shown in the following exhibit.



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

NOTE: Each correct selection is worth one point.

Hot Area:

Answer Area

Which employees can authenticate by using Azure AD?

- Only employees who have an Azure AD user account
- Employees who have an Azure AD user account and a synced on-premises account
- Only employees who have a synced on-premises account

What should you do to remove the warning for pass-through authentication?

- Fix the synchronization server and install Azure AD Connect in staging mode
- Fix the synchronization server and install an additional authentication agent
- Install an additional authentication agent and run the Start-ADSyncSyncCycle cmdlet
- Install Azure AD Connect in staging mode and run the Start-ADSyncSyncCycle cmdlet

2funky Highly Voted 2 months, 3 weeks ago

so which one is correct?

upvoted 6 times

Robert__Susin 3 weeks, 1 day ago

Look at TerenceFung for the first one, the second as is given is correct.

upvoted 1 times

Robert__Susin 3 weeks, 1 day ago

Btw, he means for the first question Azure AD accounts only, as there is no failback into PHS if PTA isnt working.

upvoted 2 times

gisbern Highly Voted 3 months, 3 weeks ago

PTA authentication is used, so whenever account is synced from local AD, logon process for them requires active PTA agent to contact domain controller. So only Azure AD users are able to log in while PTA agent is not working properly.
Am I missing something?

upvoted 6 times

gisbern 3 months, 3 weeks ago

I meant only users created in Azure AD can authenticate against Azure AD, for synced users they will be sent via PTA agent to local AD. Second answer is correct, AAD Connect is in maintenance mode, and changes has to be confirmed before next sync is able to run.

upvoted 1 times

stromnessian Most Recent 1 week, 2 days ago

Azure AD only for the first part surely?

upvoted 2 times

kanag1 1 week, 6 days ago

The question is : Who can authenticate by using Azure AD , means whose credentials are stored in Azure AD NOT by passing through. Hence the answer for the first question is : Whoever got an account created in Azure AD, NOT the ones syncing from on prem. Can someone explain if this is wrong?

upvoted 2 times

TerenceFung 2 months, 3 weeks ago

Pass-through Authentication does not automatically failover to password hash synchronization. To avoid user sign-in failures, you should configure Pass-through Authentication for high availability.

https://docs.microsoft.com/en-us/azure/active-directory/hybrid/how-to-connect-pta-faq

upvoted 4 times

AKyr 2 months, 3 weeks ago

Maintenance enabled: true
that is why 4h from last sync

upvoted 4 times

paperinop541 3 months ago

for me the correct answers are:
option 2 for the first question : azure ad account (cloud only) can also authenticate on Azure AD
option 2 for the secondo question.

upvoted 5 times

kiketxu 4 months, 3 weeks ago

I would say both answers are right, but this isn't a great topic for me. Anyone else could confirm?

upvoted 3 times

MCPsince1999 4 months, 3 weeks ago

I agree for the 1 but for 2, I would choice 3 option just to install additional agent my experience confirm that. I do not see why sync server should be fixed here.

upvoted 1 times

PeterC 4 months, 3 weeks ago

fixed - because, last sync was 4h ago - sync intervall is 30 min. so here is a problem.

upvoted 12 times

Pitch09 3 months, 1 week ago

4hours is too long. PeterC you are correct.

upvoted 1 times

Question #35 *Topic 1*

HOTSPOT -

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

Name	Role
User1	Global administrator
User2	Compliance administrator
User3	Security administrator
User4	Security operator

You plan to implement Azure Active Directory (Azure AD) Identity Protection.

You need to identify which users can perform the following actions:

- Configure a user risk policy.
- View the risky users report.

Which users 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

Configure a user risk policy:

- User1 only
- User1 and User3 only
- User3 and User4 only
- User1, User3, and User4 only
- User1, User2, User3, and User4

View the risky users report:

- User1 only
- User3 and User4 only
- User1, User2, and User3 only
- User1, User3, and User4 only
- User1, User2, User3, and User4

kiketxu Highly Voted 4 months, 3 weeks ago

1.- User1 and User3
2.- User1, User3, User4

Global administrator.Full access to Identity Protection
Compliance Administrator. Can't access to Security in the AAD blade.
Security administrator.Full access to Identity Protection
Security operator. View all Identity Protection reports and Overview blade
"Currently (3/21), the security operator role cannot access the Risky sign-ins report."
ref: https://docs.microsoft.com/en-us/azure/active-directory/identity-protection/overview-identity-protection#permissions

upvoted 14 times

ellik 3 months, 2 weeks ago

the answers are correct, I tested this, for user with security operator role, all Risky sign-ins , Risk detection, Risky users report can be accessed. not sure why the ref you provided mentioned that "the security operator role cannot access the Risky sign-ins report"

upvoted 1 times

iwikneerg Most Recent 2 months ago

https://docs.microsoft.com/en-us/azure/active-directory/identity-protection/overview-identity-protection#permissions

upvoted 1 times

Sethoo 4 months, 2 weeks ago

So the answer for 2 should be 1 &3 as well, but that is not in the options. So we go with 1 3 and 4 for now as in old times

upvoted 1 times

Question #36 *Topic 1*

HOTSPOT -

You have an Azure Active Directory (Azure AD) tenant named contoso.com that contains the users shown in the following table.

Name	Role
Admin1	Groups administrator
Admin2	User administrator

You add internal as a blocked word in the group naming policy for contoso.com.

You add Contoso- as prefix in the group naming policy for contoso.com.

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
Admin1 can create a Microsoft 365 group named Distribution.	○	○
Admin2 can create a Microsoft 365 group named Contoso-FinanceInternal.	○	○
Admin2 can create a security group named Contoso-internal.	○	○

Joshing 1 week, 5 days ago

The answer is N/Y/Y

1. No because the prefix will be Contoso as outlined in the policy so the group would be appended with Contoso-Distribution. They wouldn't be able to create a group named "Distribution".

2. Yes - https://docs.microsoft.com/en-us/microsoft-365/solutions/groups-naming-policy?view=o365-worldwide#custom-blocked-words.

"No sub-string searches are carried out; specifically, an exact match between the user entered name and the custom blocked words is required to trigger a failure." I have tested this. Including a blocked word within a string. Even with special characters such as ./_- doesn't trigger this policy. Only when you have the word itself or with it separated with a space between each word in the group will it trigger.

3.Yes - It's a security group and is not effected by the 365 Group naming policies. Tested this as well any way. But security groups are definitely not effected by this also if it were a 365 the User Administrator bypasses the Naming Policy but in this case it isn't the reason why this is answered as Yes.

upvoted 2 times

Joshing 1 week, 5 days ago

Also as the as the name is separated with a "-" it also wouldn't trigger the policy even if they weren't a user admin and it was a 365 group.

upvoted 1 times

Joshing 1 week, 5 days ago

Sorry, I misinterpreted the last part. Contoso is part of the prefix so they would be naming the group "Internal" which wouldn't be allowed if they weren't a User/Global admin.

upvoted 1 times

TazDevil 3 weeks, 2 days ago

Y - If Admin1 creates a group named Distribution. It will create a group named Contoso-Distribution without a warning or error.
Y - Only naming with just the word "internal" is blocked (not case sensitive). Add a random charater before or after "internal" and the warning disappears
Y - Policy is not enforced on security groups, just Microsoft 365 groups.

upvoted 2 times

Xtian_ar 1 month, 1 week ago

for me N Y Y

upvoted 2 times

Cvy4s 1 month, 2 weeks ago

NYY - https://docs.microsoft.com/en-us/azure/active-directory/enterprise-users/groups-naming-policy#:~:text=Roles%20and%20permissions,User%20Administrator

upvoted 3 times

M3ridi3n 1 month, 3 weeks ago

Can someone tell me if a USER admin (USER !!) can create a security group???

upvoted 1 times

fffffffdeeeeeeeeeee 2 months ago

Y/Y/Y

Admin override
Some administrators are exempted from these policies, across all group workloads and endpoints, so that they can create groups with these blocked words and with their desired naming conventions. The following are the list of administrator roles exempted from the group naming policy.
Global admin
Partner Tier 1 Support
Partner Tier 2 Support
User account admin

https://docs.microsoft.com/en-us/microsoft-365/solutions/groups-naming-policy?view=o365-worldwide

upvoted 4 times

Nasser 1 month ago

Totally agree

upvoted 1 times

Nasser 1 month ago

Hold a second, due to the 1st question the group named "distribution" is conflicted with the policy, the group name should have the Contoso- prefix, also the group admin role is not exempted from the policy. So the correct answer is:
NO, YES, YES

upvoted 2 times

sayyidsaif 2 months, 1 week ago

Ans1. applied policy is Prefix- answer is No.
Ans2. The blocked words are case-insensitive. - answer is Yes
Ans3. User account admin can override group naming policy - answer is Yes

upvoted 1 times

sayyidsaif 2 months, 1 week ago

Ans1. applied policy is suffix - answer is No.
Ans2. The blocked words are case-insensitive. - answer is Yes
Ans3. User account admin can override group naming policy - answer is Yes

upvoted 1 times

sayyidsaif 2 months, 1 week ago

Ans1. User account admin can override group naming policy
Ans2. The blocked words are case-insensitive.
Ans3. No idea why the answer is Yes.

upvoted 2 times

chaoscreater 1 month, 1 week ago

You've spammed 3 comments in a row and each comment contradict each other. Stop spreading useless information and don't bother contributing crap.

Ans 3: This is because admin2 is a user administrator and so it is exempt. Also, "When group naming policy is configured, the policy will be applied to new Microsoft 365 groups". Check the bloody documentation and you'll be able to verify both those points I made.

upvoted 2 times

jaullo 2 months, 2 weeks ago

But internal is part of "blocked words" right?

upvoted 1 times

Azseon 2 months, 2 weeks ago

Based on the context, I would think the answer is N,Y,Y. But I think the response given here is based on the fact that the policy does not apply to Distribution Groups, even though there is no mention of the group "Distribution" being a distribution group.

upvoted 1 times

laugz92 2 months, 2 weeks ago

isn't internal part of the "blocked words" list?

upvoted 1 times

skalolaz 3 months ago

N, Y, Y?
Groups admin is not an exempt.

upvoted 4 times

Ocico 2 months, 3 weeks ago

but Distribution is not a block word, therefore its Y/Y/Y

upvoted 2 times

Ocico 2 months, 3 weeks ago

I am wrong. It will get the name contoso-distribution. sorry ;)

upvoted 2 times

arunjana 2 months, 3 weeks ago

Makes sense. Below are the accounts that are exempted from policies -

Global admin
Partner Tier 1 Support
Partner Tier 2 Support
User account admin

upvoted 1 times

arunjana 2 months, 2 weeks ago

N,Y,Y should be the correct answers

upvoted 2 times

Tam0924 2 months, 2 weeks ago

Hi did we get the answer confirmed to be N,Y,Y

upvoted 4 times

Question #37 *Topic 1*

DRAG DROP -

You have a Microsoft 365 tenant.

User attributes are synced from your companyא€™s human resources (HR) system to Azure Active Directory (Azure AD).

The company has four departments that each has its own Microsoft SharePoint Online site. Each site must be accessed only by the users from its respective department.

You are designing an access management solution that has the following requirements:

☞ Users must be added automatically to the security group of their department.

☞ All security group owners must verify once quarterly that only the users in their department belong to their group.

Which components should you recommend to meet the requirements? To answer, drag the appropriate components to the correct requirements. Each component may only 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.

Select and Place:

Components

- Access packages
- Access reviews
- Azure AD Privileged Identity Management (PIM) role assignments
- Conditional access policies
- Data loss prevention (DLP) policies
- Groups that have a Membership type of Assigned
- Groups that have a Membership type of Dynamic User

Answer Area

Users must be automatically added to the security group for their department: [Components]

Group owners must verify membership of departmental groups: [Components]

kiketxu Highly Voted 4 months, 3 weeks ago

given answers are correct

upvoted 15 times

armandolubaba Most Recent 4 weeks, 1 day ago

The answers are correct

upvoted 1 times

iwikneerg 2 months ago

given answers are correct

upvoted 1 times

Question #38 *Topic 1*

HOTSPOT -

You have a Microsoft 365 E5 subscription that uses Microsoft Endpoint Manager.

The Compliance policy settings are configured as shown in the following exhibit.

These settings configure the way the compliance service treats devices. Each device evaluates these as a "Built-in Device Compliance Policy", which is reflected in device monitoring.

Mark devices with no compliance policy assigned as ⓘ	Compliant / **Not Compliant**
Enhanced jailbreak detection ⓘ	Enabled / **Disabled**
Compliance status validity period (days) ⓘ	30

On February 25, 2020, you create the device compliance policies shown in the following table.

Name	Require BitLocker Drive Encryption (BitLocker)	Require Secure Boot	Mark device as not compliant	Assigned to
Policy1	Yes	No	5 days after noncompliance	Group1
Policy2	No	Yes	10 days after noncompliance	Group1, Group2

On March 1. 2020, users enroll Windows 10 devices in Microsoft Endpoint Manager as shown in the following table

Name	BitLocker enabled	Secure Boot enabled	Member of
Device1	Yes	No	Group1
Device2	No	No	Group2

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
On March 2, 2020, Device2 is marked as compliant.	○	○
On March 6, 2020, Device1 is marked as compliant.	○	○
On March 12, 2020, Device1 is marked as compliant.	○	○

ZakS Highly Voted 2 months, 1 week ago

As per this article, the status of a device should be 'in-grace period' which is different from the 'compliant' state. So, should the answers be N, N, N in that case as the first two would be in the in grace period state?

https://docs.microsoft.com/en-us/mem/intune/protect/compliance-policy-monitor

upvoted 7 times

CAINBJJ Most Recent 1 month, 1 week ago

I a gree with ZakS

upvoted 1 times

Not_A_Bot_ 2 months ago

Disagree with answers
Device 1 won't be marked as compliant on March 6th. It will be marked as compliant once the compliance policy completes its checks. If it is non-compliant it would go in to grace-mode until such a time as it gets marked as non-compliant which would be on the 10th of March due to policy 2

upvoted 3 times

Not_A_Bot_ 1 month, 3 weeks ago

Thinking further about this question. The "in-grace period" that would apply to these devices would be seen as "Compliant" from a CA perspective to allow users and devices to continue accessing corporate resources. If interpreted in this manner, the given answers would be correct I suppose.

upvoted 2 times

Thespy45 1 month, 3 weeks ago

"in-grace period" is stated as a non-compliant status. Please read: https://docs.microsoft.com/en-us/mem/intune/protect/compliance-policy-monitor#device-compliance-status

upvoted 2 times

Topgeer123 3 months, 3 weeks ago

given answers are correct, device1 is assigned to group1 and policy1 and policy2 are both assigned to group1 and policy2 is also assigned to group1. so device1 got both policies and 5 days later the device is still compliant due to the settings of policy2 :)

upvoted 1 times

phantasmagoria 4 months, 2 weeks ago

where it is written device 1 is part of group1 and group2

upvoted 1 times

Mendel 4 months, 1 week ago

I think this is mistyped. It's member of group 1 which as both policies applied to it.

upvoted 2 times

MikeSA 4 months, 2 weeks ago

Although it doesn't say device 1 is in group 1 and 2, it only mentions group 1
Is this missing in the question?

upvoted 1 times

kiketxu 4 months, 3 weeks ago

given answers are OK.

upvoted 4 times

Topic 2 - Question Set 2

Question #1 *Topic 2*

You have a Microsoft 365 subscription that contains several Windows 10 devices. The devices are managed by using Microsoft Endpoint Manager.
You need to enable Windows Defender Exploit Guard (Windows Defender EG) on the devices.
Which type of device configuration profile should you use?

A. Endpoint protection

B. Device restrictions

C. Identity protection

D. Windows Defender ATP

kiketxu Highly Voted 4 months, 3 weeks ago
A for sure.
upvoted 7 times

iwikneerg Most Recent 2 months ago
https://docs.microsoft.com/en-us/mem/intune/protect/endpoint-protection-windows-10#attack-surface-reduction-rules
upvoted 1 times

iwikneerg 2 months ago
Attack surface reduction rules from the following profiles are evaluated for each device the rules apply to:
Devices > Configuration policy > ***Endpoint protection profile*** > Microsoft Defender Exploit Guard > Attack Surface Reduction

Attack surface reduction rules from the following profiles are evaluated for each device the rules apply to:
Devices > Configuration policy > Endpoint protection profile > Microsoft Defender Exploit Guard > Attack Surface Reduction
upvoted 1 times

theboywonder 1 month ago
This is about how the rules get applied in what order and is not a direct answer to the question asked.

The information that is required is:
You can enable attack surface reduction rules by using any of these methods:

Microsoft Intune
Mobile Device Management (MDM)
Microsoft Endpoint Configuration Manager
Group Policy
PowerShell

source: https://docs.microsoft.com/en-us/microsoft-365/security/defender-endpoint/enable-attack-surface-reduction?view=o365-worldwide
upvoted 1 times

Question #2 *Topic 2*

DRAG DROP -

You have a Microsoft 365 E5 subscription.

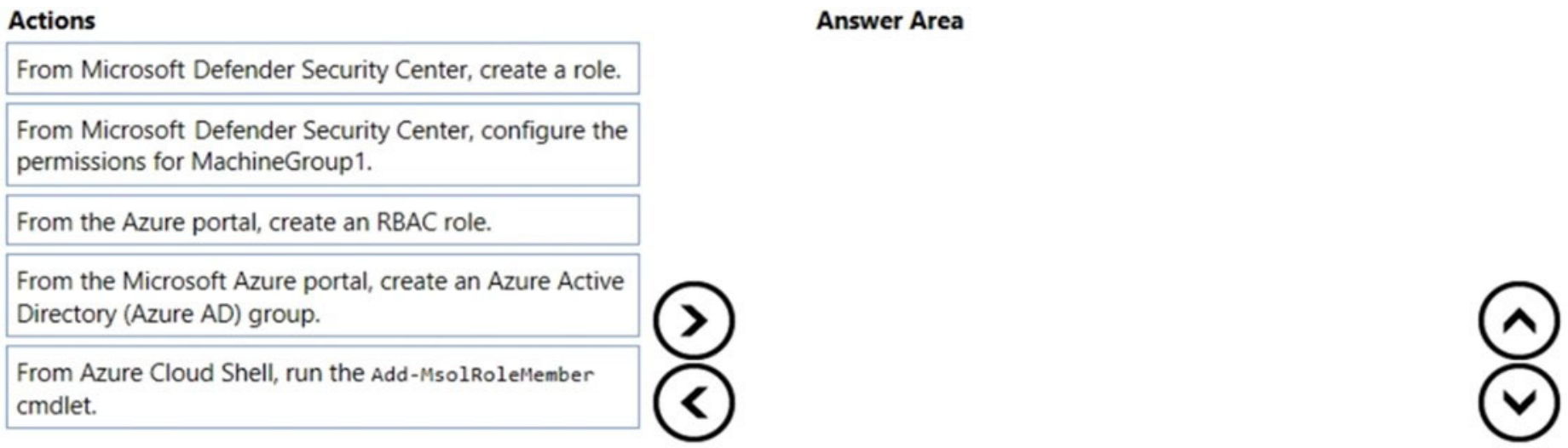
All computers run Windows 10 and are onboarded to Microsoft Defender for Endpoint.

You create a Microsoft Defender for Endpoint machine group named MachineGroup1.

You need to enable delegation for the security settings of the computers in MachineGroup1.

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:



armandolubaba 4 weeks, 1 day ago

The answers are correct

upvoted 1 times

theboywonder 1 month ago

Zaks and ikwikneerg and the given answers seem to be correct

upvoted 1 times

iwikneerg 2 months ago

The following steps guide you on how to create roles in Microsoft Defender Security Center. It assumes that you have already created Azure Active Directory user groups.

Log in to Microsoft Defender Security Center using account with a Security administrator or Global administrator role assigned.

In the navigation pane, select Settings > Roles.

Select Add item.

Enter the role name, description, and permissions you'd like to assign to the role.

Select Next to assign the role to an Azure AD Security group.

Use the filter to select the Azure AD group that you'd like to add to this role to.

Save and close.

Apply the configuration settings.

https://docs.microsoft.com/en-us/microsoft-365/security/defender-endpoint/user-roles?view=o365-worldwide#create-roles-and-assign-the-role-to-an-azure-active-directory-group

upvoted 2 times

ZakS 2 months, 1 week ago

I believe given Ans is correct.

upvoted 2 times

Question #3 *Topic 2*

You have a hybrid Microsoft Exchange Server organization. All users have Microsoft 365 E5 licenses.

You plan to implement a Microsoft Defender for Office 365 anti-phishing policy.

You need to enable mailbox intelligence for all users.

What should you do first?

A. Configure attribute filtering in Microsoft Azure Active Directory Connect (Azure AD Connect)

B. Purchase the Microsoft Defender for Office 365 add-on

C. Select Directory extension attribute sync in Microsoft Azure Active Directory Connect (Azure AD Connect)

D. Migrate the on-premises mailboxes to Exchange Online

Joshing 1 week, 5 days ago

The answer is correct.

Although bare in mind you can use the Exchange Online Protection standalone for On-premises email servers and Hybrid scenarios. But this wasn't an answer. The closest was defender for 365. That only applies to 365 and would still require mailboxes to be migrated whereas EOP standalone wouldn't.

https://docs.microsoft.com/en-us/exchange/standalone-eop/standalone-eop

upvoted 1 times

mahtab 1 month ago

D is correct: Policies to configure anti-phishing protection settings are available in Microsoft 365 organizations with Exchange Online mailboxes, standalone Exchange Online Protection (EOP) organizations without Exchange Online mailboxes, and Microsoft Defender for Office 365 organizatio
https://docs.microsoft.com/en-us/microsoft-365/security/office-365-security/set-up-anti-phishing-policies?view=o365-worldwide

upvoted 2 times

JoeExam 1 month, 1 week ago

It has to be either A or C as the E5 license already has the necessary capabilities, and Microsoft Defender is available for on-prem mailboxes.

upvoted 1 times

chaoscreater 3 weeks, 6 days ago

How is A or C relevant here? You need an Exchange Online mailbox to make use of those policies. A or C talks about AD Connect filtering etc, completely irrelevant to mailboxes.

upvoted 1 times

theboywonder 1 month ago

C has nothing to do with setting up anti-phishing for all your mailboxes in your organization, this is about extending the Azure AD schema to include on-prem AD attributes(https://docs.microsoft.com/en-us/azure/active-directory/hybrid/how-to-connect-sync-feature-directory-extensions)
A enables you to show objects from on-prem AD in Azure AD, so users can have access to a global address list(https://docs.microsoft.com/en-us/azure/active-directory/hybrid/how-to-connect-sync-configure-filtering)

D seems to be the correct answer here (https://docs.microsoft.com/en-us/microsoft-365/security/office-365-security/set-up-anti-phishing-policies?view=o365-worldwide)

upvoted 1 times

JoelB 1 month, 2 weeks ago

B. Purchase the Microsoft Defender for Office 365 add-on

Mailbox Intelligence is part of the Anti-phishing policies in Defender for Office 365. Anti-phishing policies in Microsoft Defender for Office 365 are only available in organizations that have Defender for Office 365. For example:
Microsoft 365 Enterprise E5, Microsoft 365 Education A5, etc.
Microsoft 365 Enterprise
Microsoft 365 Business
Microsoft Defender for Office 365 as an add-on

Microsoft Defender is available for hybrid environments, there is no need to migrate the mailboxes to Exchange Online.

upvoted 1 times

theboywonder 1 month ago

Wrong Xtian is right, read the doc

upvoted 1 times

Xtian_ar 1 month, 1 week ago

E5 licenses already have antiphishing policies capability

upvoted 2 times

Question #4 *Topic 2*

HOTSPOT -

You have a Microsoft Azure Active Directory (Azure AD) tenant named contoso.com.

Four Windows 10 devices are joined to the tenant as shown in the following table.

Name	Has TPM	BitLocker Drive Encryption (BitLocker) -protected C drive	BitLocker Drive Encryption (BitLocker) -protected D drive
Device1	Yes	Yes	No
Device2	Yes	No	Yes
Device3	No	Yes	Yes
Device4	No	No	No

On which devices can you use BitLocker To Go and on which devices can you turn on auto-unlock? To answer, select the appropriate options in the answer area.

NOTE: Each correct selection is worth one point.

Hot Area:

Answer Area

BitLocker To Go:
- Device3 only
- Device1 and Device2 only
- Device1, Device2, and Device3 only
- Device1, Device2, Device3, and Device4

Auto-unlock:
- Device1 and Device2 only
- Device1 and Device3 only
- Device1, Device2, and Device3 only
- Device1, Device2, Device3, and Device4

jack987 Highly Voted 1 year, 1 month ago

Agree with jayze. The answer is correct.

What is BitLocker To Go?
BitLocker To Go is BitLocker Drive Encryption on removable data drives. This includes the encryption of USB flash drives, SD cards, external hard disk drives, and other drives formatted by using the NTFS, FAT16, FAT32, or exFAT file systems.
As with BitLocker, drives that are encrypted using BitLocker To Go can be opened with a password or smart card on another computer by using BitLocker Drive Encryption in Control Panel.
Source: https://docs.microsoft.com/en-us/windows/security/information-protection/bitlocker/bitlocker-to-go-faq

BitLockerAutoUnlock:
You can configure BitLocker to automatically unlock volumes that do not host an operating system. After a user unlocks the operating system volume, BitLocker uses encrypted information stored in the registry and volume metadata to unlock any data volumes that use automatic unlocking.
Source: https://docs.microsoft.com/en-us/powershell/module/bitlocker/enable-bitlockerautounlock?view=win10-ps

upvoted 23 times

TimurKazan 3 months, 2 weeks ago

but how do youk now that: "Yes, you can enable BitLocker on an operating system drive without a TPM version 1.2 or higher, if the BIOS or UEFI firmware has the ability to read from a USB flash drive in the boot environment. " ? there is no information about it in question. the second part of the answer also seems to be incorrect

upvoted 1 times

TimurKazan 3 months, 2 weeks ago

And how do you know device 4 can have Bitlocker To go on it? it does heither have TPM, nor information about BIOS or UEFI firmware has the ability to read from a USB flash drive in the boot environment.

upvoted 1 times

JiDu 1 year ago

Good solid answer.

upvoted 4 times

kiketxu 5 months ago

Absolutely agree, thumbs-up!

upvoted 1 times

jayze Highly Voted 1 year, 2 months ago

complement
Yes, you can enable BitLocker on an operating system drive without a TPM version 1.2 or higher, if the BIOS or UEFI firmware has the ability to read from a USB flash drive in the boot environment.
The auto-unlock feature allows users to access data and removable data drives without having to enter a password each time. It is only valid when using BitLocker to encrypt OS drives.
upvoted 9 times

theboywonder Most Recent 1 month ago
Bitlocker to go is a Windows 10 feature that, it has no other resuirements

Bitlocker auto-unlock, will unlock data-drives automatically when you unlock the OS drive.

The given answers are correct
upvoted 1 times

Marsh 5 months, 3 weeks ago
Auto-unlock feature here is talking about data volumes. It requires bitlocker enabled for OS volume. The answer is correct.
upvoted 2 times

tosanede 9 months, 2 weeks ago
The answer is correct. For the device without a TPM to have been encrypted, an Azure key vault or something else must have been used to store the encryption keys. if the device storing the keys can be read during boot, the decryption can take place automatically
upvoted 2 times

Morne 10 months, 3 weeks ago
Network Unlock clients must have a TPM chip and at least one TPM protector.
Please See:https://docs.microsoft.com/en-us/windows/security/information-protection/bitlocker/bitlocker-how-to-enable-network-unlock
upvoted 1 times

bobbyJ 11 months ago
is the answer for bitlocker to go correct because essentially if a USB drive (in this case the D drive) is available then it can be secured with bitlock to go regardless if it is already protected?
upvoted 1 times

Buddhiman 11 months ago
The answer options for Auto Unlock is little bit confusing. Yes, Network Unlock was introduced in Windows 8 and Windows Server 2012 as a BitLocker protector option for operating system volumes. Network Unlock enables easier management for BitLocker enabled desktops and servers in a domain environment by providing automatic unlock of operating system volumes at system reboot when connected to a wired corporate network.
However, Network Unlock must meet mandatory hardware and software requirements before the feature can automatically unlock domain-joined systems. One of them is Network Unlock clients must have a TPM chip and at least one TPM protector.
Thefore, in my view, answer is only Device 1.
upvoted 1 times

nashers 1 year, 1 month ago
autolock relates to Bitlocker Network Unlock When a computer that is connected to a wired corporate network is rebooted, Network Unlock allows the PIN entry prompt to be bypassed. It automatically unlocks BitLocker-protected operating system volumes by using a trusted key that is provided by the Windows Deployment Services server as its secondary authentication method. Only devices 1 and 3 have encrypted OS drives
https://docs.microsoft.com/en-us/windows/security/information-protection/bitlocker/bitlocker-network-unlock-faq
upvoted 1 times

Pereiraman 1 year, 2 months ago
BitLocker To Go is BitLocker Drive Encryption on removable data drives. drives that are encrypted using BitLocker To Go can be opened with a password or smart card on another computer by using BitLocker Drive Encryption in Control Panel. Device 1,2,3 and 4. CORRECT.
https://docs.microsoft.com/pt-pt/windows/security/information-protection/bitlocker/bitlocker-to-go-faq

Auto-Unlock part is tricky:
You can configure BitLocker to automatically unlock volumes that do not host an operating system. So only Device 2 and 3 have bitlocker enable on D drive.
https://docs.microsoft.com/en-us/powershell/module/bitlocker/enable-bitlockerautounlock?view=win10-ps
However auto-unlock requires TPM or USB or some auto unlock way...
So I would say only Device 2.
There must be something missing in this Question... or answer...
upvoted 3 times

The_Master 1 year, 1 month ago
Auto-unlock answer is correct, it requires bitlocker on the OS drive only.
upvoted 6 times

upstrem 1 year, 4 months ago
What is TPM?
upvoted 1 times

tosanede 9 months, 2 weeks ago
Its is a secure storage device located on the motherboard of a PC for storing encryption keys instead of writing it out or storing on a flash drive
upvoted 1 times

jasscomp 1 year, 3 months ago

Trusted Platform Module.
Not sure if that's there to confuse people but if a machine doesn't have a TPM chip then things like Windows Hello can't be enabled i.e. finger print, facial recognition or PIN (not Bit Locker PIN).

Maybe its there to confuse people

upvoted 3 times

gbabes 1 year, 4 months ago

https://www.microsoft.com/en-US/windows/windows-10-specifications?SilentAuth=1&wa=wsignin1.0
Trusted Platform Module

upvoted 2 times

Question #5 *Topic 2*

HOTSPOT -

You have an Azure Active Directory (Azure AD) tenant named contoso.com that contains the users shown in the following table.

Name	Member of
User1	Group1
User2	Group2

You register devices in contoso.com as shown in the following table.

Name	Platform	Member of	Microsoft Intune managed
Device1	Windows 10	GroupA	Yes
Device2	iOS	GroupB	No

You create app protection policies in Intune as shown in the following table.

Name	Platform	Management state	Assigned to
Policy1	Windows 10	With enrollment	Group1
Policy2	Windows 10	With enrollment	Group2
Policy3	iOS	Apps on Intune managed devices	GroupA
Policy4	iOS	Apps on Intune managed devices	GroupB

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
When User1 uses Device1, Policy3 applies.	○	○
When User2 uses Device1, Policy2 applies.	○	○
When User2 uses Device2, Policy4 applies.	○	○

theboywonder 1 month ago

given answers are correct, a device needs to be intune managed to apply to an APP

upvoted 1 times

Robert__Susin 3 weeks ago

A device dosent need to be intune managed to apply APP, that is why MAM-WE exists for BYOD devices, see: https://docs.microsoft.com/en-us/mem/intune/fundamentals/deployment-guide-enrollment-mamwe

upvoted 2 times

DudleyYVR 3 months, 2 weeks ago

Answer is right. Device 2 is not intune managed so policy does not apply to user 2

upvoted 3 times

prats005 4 months, 1 week ago

which one is correct?

upvoted 1 times

w00t 4 months, 1 week ago

Answer is correct:
Yes, No, Yes.

upvoted 1 times

kiketxu 4 months, 3 weeks ago

I would say here: NO, YES, "YES".
In the third, User2 w/Device2 matches with iOS Policy4 for GroupB.

upvoted 3 times

Sugar123 4 months, 3 weeks ago

I believe it is No, Yes, No. Device 2 is not managed by Microsoft Intuned.

upvoted 10 times

rkapoor8855 4 months, 3 weeks ago

Agreed

upvoted 3 times

kiketxu 4 months, 3 weeks ago

Ohh! You both right. Isn't intune managed. NO, YES, NO.

upvoted 7 times

cebularz 1 month, 1 week ago

No, https://docs.microsoft.com/en-us/mem/intune/apps/app-protection-policy#app-protection-policies-on-devices You have info that is not neccessery to be managed by Intune. So No, YES, YES

upvoted 1 times

Robert__Susin 3 weeks ago

No, you are talking about MAM-WE for BYOD, the policy states that it needs to be intune managed to be applied, so they and the given answer are correct:
N, Y, N

upvoted 1 times

Jslei 4 months, 3 weeks ago

but Device2 is not intune managed?

upvoted 3 times

Question #6 *Topic 2*

DRAG DROP -

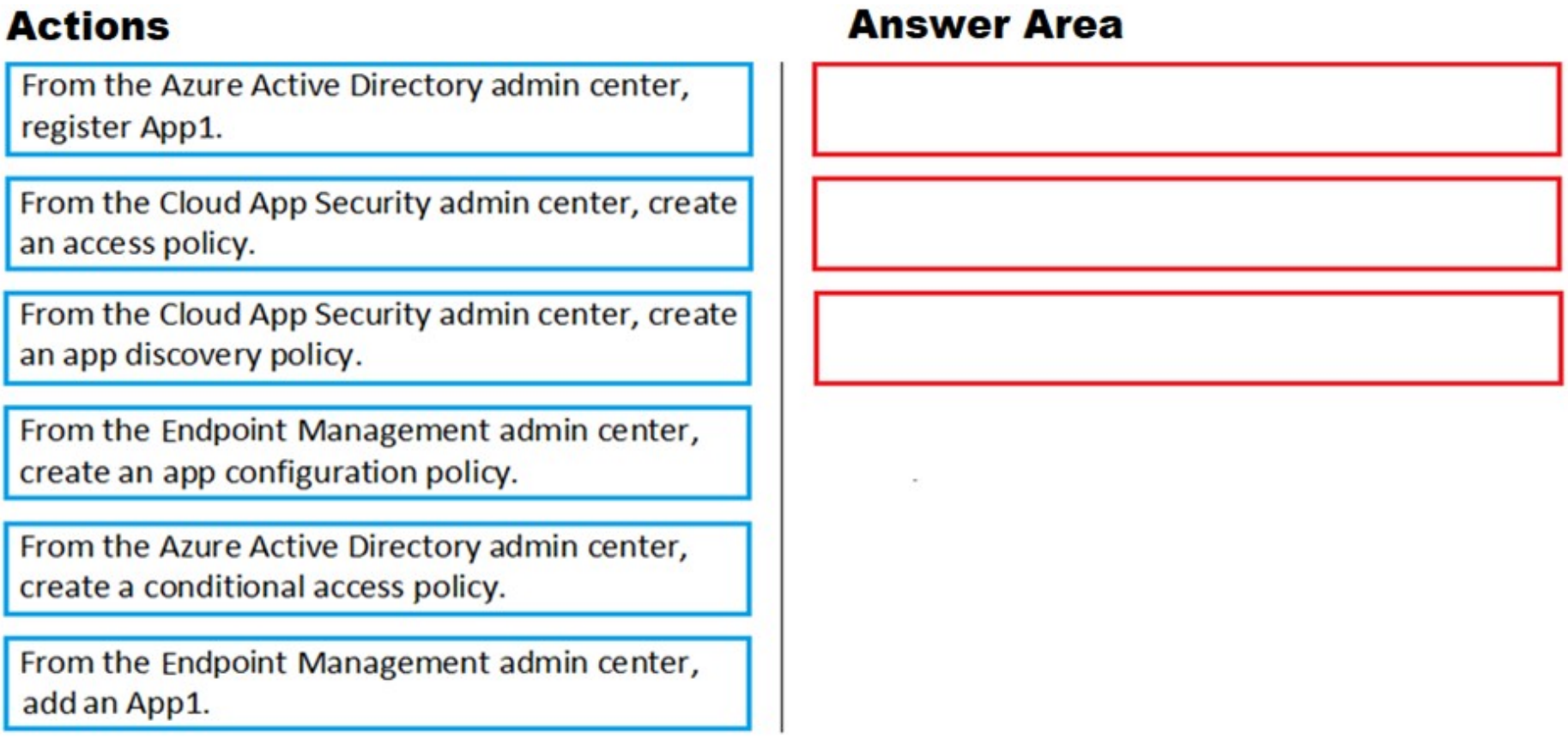
You have a Microsoft 365 subscription that uses an Azure Active Directory (Azure AD) tenant named contoso.com. All the devices in the tenant are managed by using Microsoft Endpoint Manager.

You purchase a cloud app named App1 that supports session controls.

You need to ensure that access to App1 can be reviewed in real time.

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:



Sido1 4 months, 3 weeks ago

correct

upvoted 3 times

kiketxu 4 months, 3 weeks ago

Had to discard my doubts in lab. This is correct.

upvoted 6 times

Question #7 *Topic 2*

You configure several Microsoft Defender for Office 365 policies in a Microsoft 365 subscription.
You need to allow a user named User1 to view Microsoft Defender for Office 365 reports in the Threat management dashboard.
Which role provides User1 with the required role permissions?

A. Security reader

B. Compliance administrator

C. Information Protection administrator

D. Exchange administrator

webhav 3 weeks, 2 days ago
"view" is the keyword
upvoted 1 times

ZakS 2 months, 1 week ago
Correct - Security Reader
upvoted 1 times

Question #8 *Topic 2*

You have a Microsoft 365 Enterprise E5 subscription.
You use Microsoft Defender Advanced Threat Protection (Microsoft Defender ATP). You plan to use Microsoft Office 365 Attack simulator.
What is a prerequisite for running Attack simulator?

A. Enable multi-factor authentication (MFA)

B. Configure Office 365 Advanced Threat Protection (ATP)

C. Create a Conditional Access App Control policy for accessing Office 365

D. Integrate Office 365 Threat Intelligence and Microsoft Defender ATP

Enoll Highly Voted 3 months, 1 week ago
-> Your account needs to be configured for multi-factor authentication (MFA) to create and manage campaigns in Attack Simulator.

https://docs.microsoft.com/en-us/microsoft-365/security/office-365-security/attack-simulator?view=o365-worldwide
upvoted 6 times

kiketxu Most Recent 4 months, 3 weeks ago
A for sure!
upvoted 3 times

Question #9 *Topic 2*

You have a Microsoft 365 E5 subscription and a hybrid Microsoft Exchange Server organization.
Each member of a group named Executive has an on-premises mailbox. Only the Executive group members have multi-factor authentication (MFA) enabled. Each member of a group named Research has a mailbox in Exchange Online.
You need to use Microsoft Office 365 Attack simulator to model a spear-phishing attack that targets the Research group members.
The email addresses that you intend to spoof belong to the Executive group members.
What should you do first?

A. From the Azure ATP admin center, configure the primary workspace settings

B. From the Microsoft Azure portal, configure the user risk policy settings in Azure AD Identity Protection

C. Enable MFA for the Research group members

D. Migrate the Executive group members to Exchange Online

Ronnie123 Highly Voted 1 year, 8 months ago
According to the link, the answer shoud be D. Migrate the Executive group members to Exchange Online.
MFA is only required for the admins, not the users.
upvoted 24 times

mehnaz 1 year ago
will go with D . MFA is only for the one simulating an attack not the recepients.
upvoted 2 times

TheHole 5 months, 2 weeks ago
D is the correct answer.

"Your account needs to be configured for multi-factor authentication (MFA) to create and manage campaigns in Attack Simulator."

An important note is due here – the Launch Attack button will only be available if the account you are using to access Attack Simulator has succeeded in performing a MFA challenge as part of the authentication process. This is alluded to by the "You need to have MFA enabled to schedule or terminate attacks" warning visible on the above screenshot, but the requirement is not only to have MFA enabled on the account, but to actually login by completing a MFA challenge. This might be an inconvenience for organizations that do not enforce MFA or use some form of MFA bypass, however it makes sense to have this additional security verification enabled for working with one of most sensitive functionalities currently available in Office 365.
upvoted 2 times

WoneSix 1 year, 6 months ago
The spoofed address can be any address - only the target accounts (the ones that will receive the spoofed email) need to be in Office 365.
upvoted 5 times

VTHAR Highly Voted 10 months, 1 week ago
There is no correct answer in here. It was in exam and there is another option which is to "enable MFA for your account". That is the correct answer.
upvoted 24 times

kanag1 3 days, 12 hours ago
Hi,
None is the right answer. You dont MFA to be enabled for source or target mailboxes. The source mailbox could even be outside office 365 (gmail).
upvoted 2 times

SSK500 6 months ago
Thanks. But explain how "enable MFA for your account" is correct answer.
upvoted 1 times

dlt_mate 3 weeks, 1 day ago
MFA must be enabled for the admin initiating the simulated attack
upvoted 2 times

MQH Most Recent 1 month, 2 weeks ago
Correct answer, you need to spoof those mailboxes' accounts not targeting them with attack simulation.
upvoted 1 times

swonga 1 month, 2 weeks ago
C is correct. You try to trick the research department by sending spoofed emails that appear from CEO. E.g.,
From: CEO
To: Research department
subject: secret deals.. don't tell anyone

So you need to enable MFA for the research group

upvoted 1 times

TerenceFung 2 months, 3 weeks ago

https://docs.microsoft.com/en-us/microsoft-365/security/office-365-security/attack-simulator?view=o365-worldwide

Each targeted recipient must have an Exchange Online mailbox. If you click Filter and Apply without entering a search criteria, all recipients are returned and added to the campaign.

From (Email): The sender's email address. You can enter a real or fake email address from your organization's email domain, or you can enter a real or fake external email address. A valid sender email address from your organization will actually resolve in the recipient's email client.

upvoted 1 times

elife 3 months, 1 week ago

Answer is D. According to the link: "Attack Simulator only works on cloud-based mailboxes."

upvoted 2 times

Pitch09 3 months, 1 week ago

The answer is correct.
This version of Attack Simulator has been retired.
You can find the new experience at https://security.microsoft.com/attacksimulator. The ability to launch new simulations from this site has been disabled. However, you can still access your reports for simulations run in the past 90 days.
You must enable multi-factor authentication (MFA) to schedule or terminate attacks.

upvoted 2 times

bobicos 6 months, 1 week ago

From https://docs.microsoft.com/en-us/microsoft-365/security/office-365-security/attack-simulator?view=o365-worldwide#what-do-you-need-to-know-before-you-begin, if you read the section on spear fishing campaigns:
Click Address Book to select the recipients (users or groups) for the campaign. Each targeted recipient must have an Exchange Online mailbox.

upvoted 4 times

kiketxu 5 months ago

Pretty clear man! I'm with you. Thank you for confirming D as the right answer.

upvoted 2 times

TimurKazan 4 months, 3 weeks ago

but as in question : "Each member of a group named Research has a mailbox in Exchange Online." means they have already got Online Mailbox. I believe C suits more than other

upvoted 3 times

kiketxu 4 months, 3 weeks ago

You right, I was wrong. Only the target target be in EXO. The answer is C.

upvoted 2 times

Martyvdb 6 months, 2 weeks ago

To simulate an attack, the 'real' sender needs to exist in order for the 'fake' sends to impersonate them. That sender cannot be an on-prem ID.

upvoted 1 times

svm_Terran 8 months ago

answer is correct. the question says "Group"

upvoted 2 times

examcrammer 10 months, 2 weeks ago

The correct answer is C. YOU the attacker, are NOT an executive, so you must be a member of Research (as no other claims are made to your group membership or role assignment) making C the MOST correct answer.

upvoted 1 times

SUBZER0 11 months ago

Microsoft should pay us for doing all this reseach, there are many questions with blurry areas

upvoted 6 times

Bl0ckSh3ll 11 months, 1 week ago

From the provided link in the answer:

"Each targeted recipient must have an Exchange Online mailbox".

The research group members already have an exchange online account.

Really confusing question, but I would go with C.

upvoted 1 times

jason6311 1 year ago

This wouldn't be the first (or the 30th) question I've seen on the site that didn't quite make sense, only to find in the actual test it is clearer. The key bits of info I would take to the test are that MFA is required for the attacking accounts, and EXO is required for the target mailboxes.

upvoted 13 times

TDAC 10 months, 3 weeks ago

^^this guy is right. MFA is only needed for the account running the attack. EXO is required for the accounts receiving the attack. It is spelled out here: https://docs.microsoft.com/en-us/microsoft-365/security/office-365-security/attack-simulator?view=o365-worldwide - "In the Target recipients step, do one of the following steps:

Click Address Book to select the recipients (users or groups) for the campaign. Each targeted recipient must have an Exchange Online mailbox."

upvoted 4 times

Yvesi 1 year ago

Guys the two group are part of the same Hybrid organisation communication from on-prem and exchange online is already established so the group can communicate as internal already.

upvoted 1 times

shaan6810 1 year, 1 month ago

The most upvoted comment here, aka Ronnie123's comment is incorrect. The members in the Executive group need not be migrated because there is no mention that the tenant being used to run Attack Simulator is a tenant belonging to the Executive group. It is merely one of the Executive group's e-mail that is being spoofed.

On the other hand, the answer given here, which is enabling MFA for the research group is also not a requirement, however because in the link provided, it is said that enabling MFA is ideal for all users in the organisation, C is the most suitable answer.

Honestly, this is such a terrible question, like many other questions by Microsoft. Good luck to me and all of your taking the exam.

upvoted 4 times

ginsahec 1 year, 2 months ago

Each member of a group named Executive has an on-premises mailbox.
The firt is migrate to Exchange Online for start the Attacj simulator

upvoted 3 times

ginsahec 1 year, 2 months ago

Sorry the correct is C, it does not influence where the mailbox is to simulate the attack

upvoted 1 times

xofowi5140 1 year, 2 months ago

Scenario "Only the Executive group members have multi-factor authentication (MFA) enabled"
C. Enable MFA for the Research group members

I don't think so.

upvoted 1 times

Question #10 *Topic 2*

You have a Microsoft 365 E5 subscription.

You implement Advanced Threat Protection (ATP) safe attachments policies for all users.

User reports that email messages containing attachments take longer than expected to be received.

You need to reduce the amount of time it takes to receive email messages that contain attachments. The solution must ensure that all attachments are scanned for malware. Attachments that have malware must be blocked.

What should you do from ATP?

A. Set the action to Block

B. Add an exception

C. Add a condition

D. Set the action to Dynamic Delivery

Jhill777 Highly Voted 11 months, 3 weeks ago

Dynamic Delivery eliminates email delays by sending the body of an email message through to the recipient with a placeholder for each email attachment. The placeholder remains until a copy of the attachment is scanned and determined to be safe by ATP Safe Attachments.

As each attachment is cleared, it is available to open or download.

If an attachment is determined to be malicious, it is sent to quarantine, where someone on your organization's security team (such as a global administrator or security administrator) can manage quarantined messages in Office 365.

upvoted 20 times

DrMe 7 months, 2 weeks ago

Agreed, https://docs.microsoft.com/en-us/microsoft-365/security/office-365-security/atp-safe-attachments?view=o365-worldwide#safe-attachments-policy-settings:~:text=Delivers%20messages%20immediately%2C%20but%20replaces%20attachments,until%20Safe%20Attachments%20scanning%20is%20complete.

upvoted 1 times

mahtab Most Recent 1 month ago

D for sure

upvoted 1 times

kiketxu 5 months ago

D for sure!

upvoted 2 times

Question #11 *Topic 2*

HOTSPOT -

Your network contains an Active Directory domain named contoso.com. The domain contains a VPN server named VPN1 that runs Windows Server 2016 and has the Remote Access server role installed.

You have a Microsoft Azure subscription.

You are deploying Microsoft Defender for Identity.

You install a Microsoft Defender for Identity standalone sensor on a server named Server1 that runs Windows Server 2016.

You need to integrate the VPN and Microsoft Defender for Identity.

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

NOTE: Each correct selection is worth one point.

Hot Area:

Answer Area

On VPN1:

Configure an authentication provider.	V
Configure an accounting provider.	
Create a connection request policy.	
Create a RADIUS client.	

On Server1, enable the following inbound port:

443	V
1723	
1813	
8080	
8531	

iwikneerg 2 months ago

https://docs.microsoft.com/en-us/defender-for-identity/install-step6-vpn#configure-vpn-in-defender-for-identity

upvoted 1 times

arunjana 2 months, 3 weeks ago

Given answer is correct.
https://docs.microsoft.com/en-us/defender-for-identity/install-step6-vpn

upvoted 2 times

Question #12 *Topic 2*

HOTSPOT -

You have a Microsoft Defender Advanced Threat Protection (Microsoft Defender ATP) deployment that has the custom network indicators turned on. Microsoft

Defender ATP protects two computers that run Windows 10 as shown in the following table.

Name	Tag
Computer1	Kiosk1
Computer2	Tag1

Microsoft Defender ATP has the machine groups shown in the following table.

Rank	Name	Membership rule
1	Group1	Tag Contains 1
2	Group2	Name Ends with 2 And Tag Equals Tag1
3	Group3	Name Contains comp
Last	Ungrouped machines (default)	*None*

From Microsoft Defender Security Center, you create the URLs/Domains indicators shown in the following table.

URL/Domain	Action	Scope
http://www.contoso.com	Alert and block	Group1
http://www.litwareinc.com	Alert and block	Group2
http://www.litwareinc.com/public	Allow	All machines

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
From a web browser on Computer1, you can open http://www.contoso.com.	○	○
From a web browser on Computer1,you can open http://www.litwareinc.com/public.	○	○
From a web browser on Computer2, you can open http://www.litwareinc.com.	○	○

fred Highly Voted 4 months, 4 weeks ago

that is not correct, computer can be member on just 1 atp group, and priority is used
all both computers are on group1 because contains 1 and group 1 have the higest priority.
response: No Yes Yes

upvoted 17 times

fred Highly Voted 4 months, 4 weeks ago

https://docs.microsoft.com/en-us/windows/security/threat-protection/microsoft-defender-atp/machine-groups
When a device is matched to more than one group, it is added only to the highest ranked group.

upvoted 14 times

kiketxu 4 months, 3 weeks ago

After reading the doc, I'm with you. Thanks!
The Scope2 does not aply to Computer2 as it isn't member of Group2 due tag match with Group1

upvoted 3 times

Rascal_Study Most Recent 1 week, 2 days ago

is this a specificity issue? Group 2 has more conditions which apply only to Computer2 thusly that policy takes effect?

upvoted 1 times

Joshing 1 week, 5 days ago

Agree with Fred.

"Specify the matching rule that determines which device group belongs to the group based on the device name, domain, tags, and OS platform. If a device is also matched to other groups, it's added only to the highest ranked device group"

So Computer 2 matches with Group 1 and is higher ranking. So last answer is Yes.

upvoted 1 times

arunjana 2 months, 3 weeks ago

No Yes Yes - Going by the below logic
https://docs.microsoft.com/en-us/windows/security/threat-protection/microsoft-defender-atp/machine-groups

upvoted 3 times

belyo 4 months, 3 weeks ago

maybe because computer2 has better matching membership rules is evaluated with Group2 rather than Group1

upvoted 1 times

Sido1 4 months, 3 weeks ago

NO YES NO

upvoted 3 times

Question #13 *Topic 2*

SIMULATION -

You need to ensure that a user named Allan Deyoung uses multi-factor authentication (MFA) for all authentication requests.

To complete this task, sign in to the Microsoft 365 admin center.

dlt_mate 3 weeks, 1 day ago

I disagree with this one. Enabling 'app passwords' and 'remember mfa' settings doesn't meet the criteria of "Allan Deyoung uses MFA for ALL authentication requests".

upvoted 2 times

HnTer 1 month, 2 weeks ago

How to enable MFA for whole org:
M365 admin center -> Settings | Org settings -> Modern authentication -> Turn on modern authentication

How to then enable MFA for *a user*:
M365 admin center -> Settings | Org settings -> Multi-factor authentication -> Select a user -> Enable

(MFA now comes enabled by default, so this probably doesn't have to be done anymore).

upvoted 2 times

MCPsince1999 4 months, 3 weeks ago

I would do two steps ((MFA) for all authentication requests):
1. Enable per user MFA
2. disable ability to use app password

upvoted 2 times

Question #14 *Topic 2*

SIMULATION -

You need to ensure that all links to malware.contoso.com within documents stored in Microsoft Office 365 are blocked when the documents are accessed from

Office 365 ProPlus applications.

To complete this task, sign in to the Microsoft 365 admin center.

mashaeg Highly Voted 2 months, 1 week ago

Policy-Safe links-Global Settings-Safe Links settings for your organization
Add URL

upvoted 5 times

Rhukey Most Recent 4 months, 3 weeks ago

From the admin center>>Security>>Threat management >>Policy>>Safe links

upvoted 1 times

Delli 3 months, 4 weeks ago

Then click on Global settings

upvoted 1 times

ellik 3 months, 2 weeks ago

there is no default policy in Safe links, when click on Global settings I just need to add the URL mentioned in question?

upvoted 2 times

fred 4 months, 4 weeks ago

why remove email section ? office 365 proplus contain outlook

upvoted 1 times

Question #15 *Topic 2*

SIMULATION -

You need to protect against phishing attacks. The solution must meet the following requirements:

- Phishing email messages must be quarantined if the messages are sent from a spoofed domain.
- As many phishing email messages as possible must be identified.

The solution must apply to the current SMTP domain names and any domain names added later.

To complete this task, sign in to the Microsoft 365 admin center.

Oz Highly Voted 11 months, 3 weeks ago

To meet the second requirement, it is necessary in Default Antiphishing policy settings to scroll down and find Advanced settings.
Edit it and set Advanced phishing threshold to "Most Aggressive" instead of "Standard"

upvoted 10 times

ThBEST Most Recent 1 month, 4 weeks ago

I agree with Toyo on this one, although Oz is being more cautious, the increased number of false positives is not a good for production or accuracy. However here is the new reference link as of 06/04/2021: https://docs.microsoft.com/en-us/microsoft-365/security/office-365-security/configure-mdo-anti-phishing-policies?view=o365-worldwide

upvoted 1 times

andreiiar 3 months, 2 weeks ago

What about Spoof settings? Default here is move to junk.

===
Editing Spoofing filter settings
Editing Actions
If the person spoofing your domain isn't an allowed sender, we'll apply the action you choose here.
===

upvoted 1 times

w00t 4 months, 1 week ago

* Phishing email messages must be quarantined if the messages are sent from a spoofed domain.
* AS MANY phishing email messages AS POSSIBLE must be identified.

Default Policy
* Impersonation -> Edit
* Add domains to protect -> Automatically Include the Domains I own -> ON
* Actions -> If email is sent by an impersonated user: QUARANTINE
* Actions -> If email is sent by an impersonated domain: QUARANTINE
* Mailbox Intelligence -> If email is sent by an impersonated user: QUARANTINE

* Advanced Settings -> Edit
* Advanced phishing thresholds -> MOST AGGRESSIVE

upvoted 4 times

DrMe 7 months ago

Walk though with video... https://support.microsoft.com/en-us/office/protect-against-phishing-attempts-in-microsoft-365-86c425e1-1686-430a-9151-f7176cce4f2c

Make sure you also also complete Oz's recommendation to change the threshold too.

upvoted 4 times

AJ2021 6 months ago

I agree with Toyo, leave APT asis, also left unchanged in your video link too

upvoted 2 times

Toyo1 11 months, 2 weeks ago

I don't think the Advanced Phishing Threshold should be raised because the question did not request the threshold be raised. Raising the threshold to "Most Aggressive" may result in high number of false positives.

upvoted 4 times

njeske 11 months ago

The problem states "As many phishing email messages as possible must be identified." It doesn't say anything at all about the organizations tolerance level for false positives. Therefore, I'd completely agree with Oz, and would raise the Advanced Phishing Threshold to "Most Agressive."

upvoted 10 times

Question #16 *Topic 2*

Your network contains an on-premises Active Directory domain. The domain contains the servers shown in the following table.

Name	Configuration
DC1	Domain controller
Server1	Member server

You plan to implement Azure Advanced Threat Protection (ATP) for the domain.

You install an Azure ATP standalone sensor on Server1.

You need to monitor the domain by using Azure ATP.

What should you do?

A. Configure port mirroring for Server1.

B. Install the Microsoft Monitoring Agent on DC1.

C. Install the Microsoft Monitoring Agent on Server1.

D. Configure port mirroring for DC1.

kiketxu 4 months, 3 weeks ago

Seems this question is out of date, given the text on the top of the ref link and the port mirroring workaround
https://docs.microsoft.com/en-us/azure-advanced-threat-protection/configure-port-mirroring
"This article is relevant only if you deploy Microsoft Defender for Identity standalone sensors instead of Defender for Identity sensors."
I agree withthe port mirroring as correct answer here, but not sure if we will see this in the exam.

upvoted 3 times

Robert__Susin 2 weeks, 6 days ago

No, installing standalone sensors are not optional, is mandatory if you are installing the sensor on a dedicated server, so port mirroring is relevant, see: "The installation wizard automatically checks if the server is a domain controller/ AD FS server or a dedicated server. If it's a domain controller / AD FS server, the Defender for Identity sensor is installed. If it's a dedicated server, the Defender for Identity standalone sensor is installed."

upvoted 2 times

Question #17 *Topic 2*

An administrator plans to deploy several Azure Advanced Threat Protection (ATP) sensors.
You need to provide the administrator with the Azure information required to deploy the sensors.
What information should you provide?

A. an Azure Active Directory Authentication Library (ADAL) token

B. the public key

C. the access key

D. the URL of the Azure ATP admin center

DTz Highly Voted 1 year, 1 month ago
Pretty sure this should be C
https://docs.microsoft.com/en-us/azure-advanced-threat-protection/install-atp-step4
upvoted 15 times

Marcelo72 5 months, 2 weeks ago
Access key is just part of the solution. You need to download a customized copy of the package in the portal. So the correct answer is D
upvoted 3 times

mehnaz 1 year ago
The access key is required for the Azure ATP sensor to connect to your Azure ATP workspace.
The access key is a one-time-password for deploying sensors.Its has to be access key
upvoted 4 times

TDAC 10 months, 1 week ago
I agree. The access key is required to install the sensor and is needed if admin guy wants to deploy the sensors on the domain controllers.
upvoted 1 times

kratos13 1 year, 1 month ago
Concur: "Prerequisites
An Azure ATP instance that's connected to Active Directory.
A downloaded copy of your ATP sensor setup package and the access key."
upvoted 2 times

CAINBJJ Most Recent 1 month, 1 week ago
answer is wrong.. Correct is C

Click Download to save the package locally.
Copy the Access key. The access key is required for the Defender for Identity sensor to connect to your Defender for Identity instance. The access key is a one-time-password for sensor deployment, after which all communication is performed using certificates for authentication and TLS encryption. Use the Regenerate button if you ever need to regenerate the new access key, you can, and it won't affect any previously deployed sensors, because it's only used for initial registration of the sensor.
Copy the package to the dedicated server or domain controller onto which you're installing the Defender for Identity sensor. Alternatively, you can open the Defender for Identity portal from the dedicated server or domain controller and skip this step.
https://docs.microsoft.com/en-us/defender-for-identity/install-step3
and
https://docs.microsoft.com/en-us/defender-for-identity/install-step4
upvoted 1 times

CAINBJJ 1 month, 1 week ago
answer is wrong.. Correct is C

Click Download to save the package locally.
Copy the Access key. The access key is required for the Defender for Identity sensor to connect to your Defender for Identity instance. The access key is a one-time-password for sensor deployment, after which all communication is performed using certificates for authentication and TLS encryption. Use the Regenerate button if you ever need to regenerate the new access key, you can, and it won't affect any previously deployed sensors, because it's only used for initial registration of the sensor.
Copy the package to the dedicated server or domain controller onto which you're installing the Defender for Identity sensor. Alternatively, you can open the Defender for Identity portal from the dedicated server or domain controller and skip this step.
https://docs.microsoft.com/en-us/defender-for-identity/install-step3
upvoted 1 times

Xtian_ar 1 month, 1 week ago
For me is C, access key.
upvoted 1 times

Xtian_ar 1 month, 2 weeks ago
Is really necesary to provide the URL of the Admin Portal ? the agent does not know that? or is somehing unique for every installation?

upvoted 2 times

vicks1x 4 months, 3 weeks ago

D is correct

Ref : You can enter the Defender for Identity portal either by logging in to the portal https://portal.atp.azure.com and selecting your instance, or browsing to the instance URL: https://*instancename*.atp.azure.com.

https://docs.microsoft.com/en-us/defender-for-identity/workspace-portal

upvoted 1 times

kiketxu 4 months, 3 weeks ago

Seems something wrong with the statement/answers. Obviously isn't enough with the access key if you don't get the package, but looks pretty poor give just the URL.
I would mark here D but, it should be the sensor package and the access key.

upvoted 2 times

shanti0091 6 months, 1 week ago

Answer - C.
https://docs.microsoft.com/en-us/defender-for-identity/install-step4

upvoted 1 times

mnak 7 months, 3 weeks ago

The answer is correct in that it provides an "Administrator" with the information to get the setup and access key. The access key alone doesn't tell them where to get the setup file.

upvoted 4 times

vmhvm 5 months, 2 weeks ago

I agree.
https://docs.microsoft.com/en-us/defender-for-identity/install-step3

upvoted 1 times

cenil 9 months, 2 weeks ago

You get rge access key from Azure ATP admin center right?

upvoted 1 times

Neharsin 9 months, 2 weeks ago

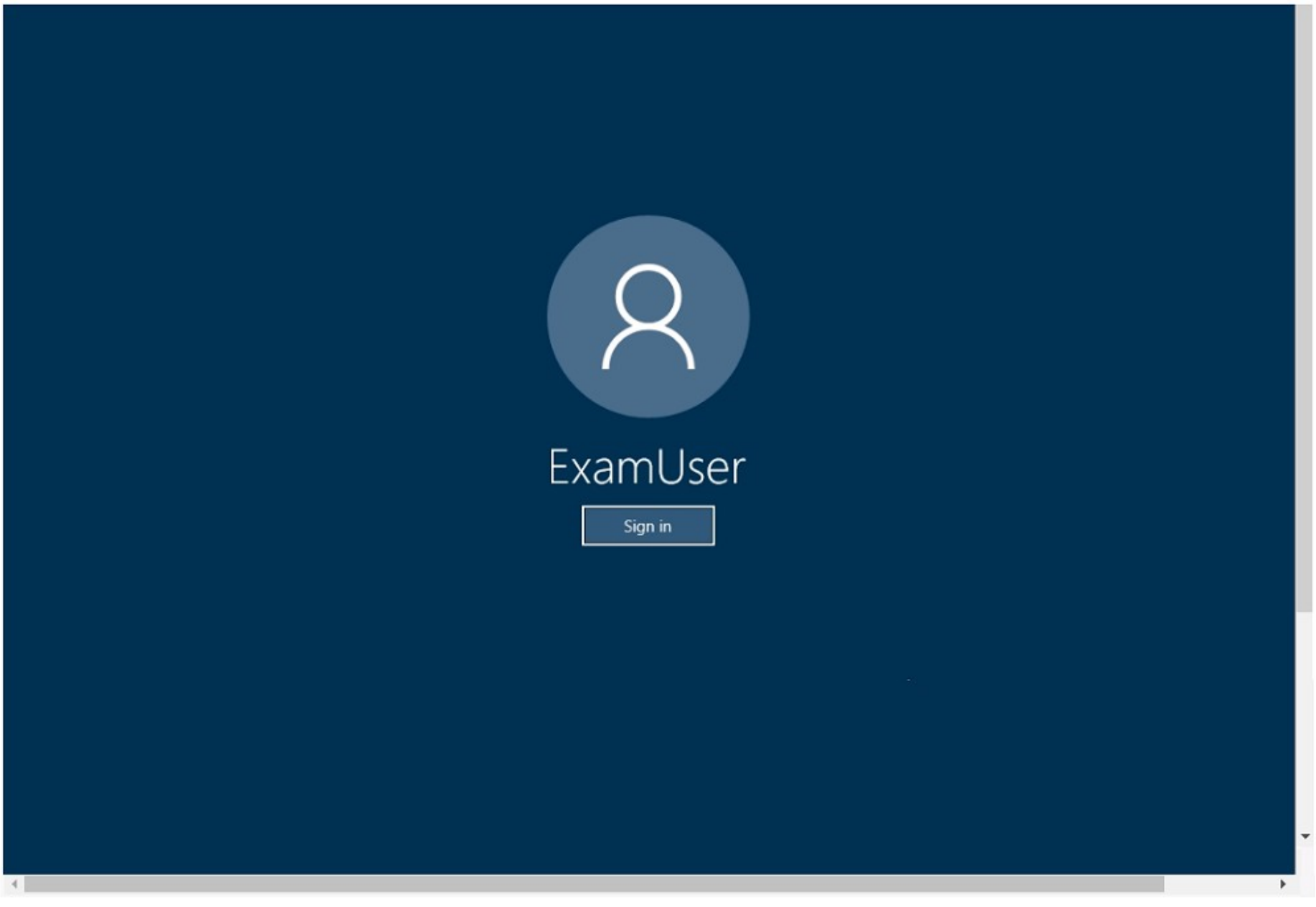
Yes, access key info is available through Azure ATP portal.
https://docs.microsoft.com/en-us/azure-advanced-threat-protection/install-step4

upvoted 1 times

Question #18 *Topic 2*

SIMULATION -
Please wait while the virtual machine loads. Once loaded, you may proceed to the lab section. This may take a few minutes, and the wait time will not be deducted from your overall test time.
When the Next button is available, click it to access the lab section. In this section, you will perform a set of tasks in a live environment. While most functionality will be available to you as it would be in a live environment, some functionality (e.g., copy and paste, ability to navigate to external websites) will not be possible by design.
Scoring is based on the outcome of performing the tasks stated in the lab. In other words, it doesnɹ€™t matter how you accomplish the task, if you successfully perform it, you will earn credit for that task.
Labs are not timed separately, and this exam may more than one lab that you must complete. You can use as much time as you would like to complete each lab.
But, you should manage your time appropriately to ensure that you are able to complete the lab(s) and all other sections of the exam in the time provided.
Please note that once you submit your work by clicking the Next button within a lab, you will NOT be able to return to the lab.

Username and password -



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@LODSe244001.onmicrosoft.com
Microsoft 365 Password: &=Q8v@2qGzYz
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: 11032396 -
You need to ensure that a user named Alex Wilber can register for multifactor authentication (MFA).
To complete this task, sign in to the Microsoft Office 365 admin center.

Joshing 1 week, 5 days ago
Second part technically isn't wrong. Multifactor authentication in this section will prompt the user to set up MFA.

The first part is literally enabling Modern Auth for Exchange but not necessarily required as the steps only ask to allow the user to register for MFA.

MFA registration can also be prompted from here - https://docs.microsoft.com/en-us/azure/active-directory/identity-protection/howto-identity-protection-configure-mfa-policy#policy-configuration

You can enforce registration for MFA through the policy. They can bypass it for up to 14 days then they will need to register for MFA.

upvoted 1 times

Ahmed911 1 month, 3 weeks ago

Wrong. Modern Authentication is for Exchange MFA only

upvoted 1 times

mashaeg 2 months, 1 week ago

Admin-Settings-Org Settings-Services/Modern Authentication

upvoted 1 times

Question #19 *Topic 2*

HOTSPOT -

You have a Microsoft 365 subscription that uses a default domain name of contoso.com.

Microsoft Azure Active Directory (Azure AD) contains the users shown in the following table.

Name	Member of
User1	Group1
User2	Group1, Group2
User3	Group3

Microsoft Endpoint Manager has two devices enrolled as shown in the following table:

Name	Platform
Device1	Android
Device2	Windows 10

Both devices have three apps named App1, App2, and App3 installed.

You create an app protection policy named ProtectionPolicy1 that has the following settings:

- Protected apps: App1
- Exempt apps: App2
- Windows Information Protection mode: Block

You apply ProtectionPolicy1 to Group1 and Group3. You exclude Group2 from ProtectionPolicy1.

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	Yes	No
From Device1, User1 can copy data from App1 to App3.	○	○
From Device2, User1 can copy data from App1 to App2.	○	○
From Device2, User1 can copy data from App1 to App3.	○	○

DTz Highly Voted 1 year, 1 month ago

I believe you guys are thinking in terms of TO instead of FROM. The policy is set to block.
"Block: Blocks enterprise data FROM LEAVING protected apps." The protected app is App1. So the policy would prevent data from LEAVING App1.

1. Device 1 is an Android Device and WIP won't work at all -> Answer YES
2. App2 is exempt, but the policy protects >App1< from data LEAVING it. So the copy gets blocked -> Answer NO
3. This is effectively the same as #2. Sure, App3 is not impacted, but App1 is, and you cannot copy data FROM App1 -> Answer NO

upvoted 76 times

Joshing 1 week, 4 days ago

For anyone who has read DTz answer and is thinking of testing it. Don't bother (I of course wasted my time). He is 100% correct.

As he said data coming from a Protected app is protected. It is protected and is allowed to be used with other Protected apps. You set apps to Exempt if they are unenlightened. You can Deny the app so it won't be able to work with corporate data or Allow it so it can work with corporate data but you have the risk of data being copied out of this app due to the protection not being in place.

Exempting something and using Deny is the same as not including the app within Protected Apps section within WIP. They won't be able to use corporate data.

Here is a great article on this matter - https://campbell.scot/windows-information-protection-wip-app-protection-policies-protected-and-exempt-denied-and-allowed-what-do-they-mean/

upvoted 2 times

ZakS 2 months, 1 week ago

I agree....YES, NO, NO

DTz is correct.

upvoted 2 times

VTHAR 10 months, 4 weeks ago

DTz is correct. It's YES, NO, NO.

upvoted 7 times

Ehernandez 6 months, 3 weeks ago

yes, right, because Divece1 is not in the policy, App2 is exempt but the App1 is Protected it is blocked, if it were App2 -> App1 or App2 -> App3 would work.
for this reason the answer is Yes, No and No

upvoted 2 times

mehnaz 1 year ago

This is perfect. I believe this too.When one creates app protection policy, the option of choosing WIP MODE is applicable only for windows 10 devices which means this policy has been created for Windows 10 devices only.
So answer is YES, NO , NO

upvoted 8 times

Pitch09 3 months ago

https://docs.microsoft.com/en-us/mem/intune/apps/windows-information-protection-policy-create

upvoted 1 times

mehnaz 1 year ago

CORRECT; Its has to be YES, YES NO. because Group 2 is exempted

upvoted 1 times

mehnaz 1 year ago

FINAL Correction: Its has to be Yes ,NO No

upvoted 2 times

ChrisBr Highly Voted 1 year, 9 months ago

I think this is not correct...

1. Device 1 is an Android Device and WIP won't work at all -> Answer YES
2. App 2 is an excempt App so this should work -> Answer YES
3. APP 3 is neither a protected nor an excempt app. WIP should Block -> Answer NO

upvoted 57 times

Toorop 1 year, 8 months ago

I think it should be Yes, Yes, No as well.

upvoted 8 times

matthu 1 year, 3 months ago

pretty sure it's yes yes no. the wording sucks for this question, but it's talking about a WIP app protection policy, not a MAM app protection policy. Only WIP policies have those options specified, MAM policy options are different. androids aren't protected by WIP policies so that's a yes, App 2 is exempt so 1 -> 2 is yes, and 1 -> 3 should be no since it's no because 1 is protected and 3 isn't exempt
https://docs.microsoft.com/en-us/windows/security/information-protection/windows-information-protection/create-wip-policy-using-intune-azure

upvoted 4 times

Sizz 1 year, 7 months ago

Answer is correct if it's just talking about App Protection Policies... These are iOS and Android only... The question confuses matter by talking about WIP at all.

Source - https://docs.microsoft.com/en-us/intune/apps/app-protection-policy#supported-platforms-for-app-protection-policies

upvoted 6 times

Jhill777 11 months, 3 weeks ago

MAM can only manage enlightened apps. Since they call them App1, 2, 3, I don't think we can assume anything.

upvoted 1 times

RonS 1 year, 3 months ago

Answer is correct it is specifically asking about App protection not WIP! Sizz link is correct

upvoted 4 times

xofowi5140 1 year, 3 months ago

ProtectionPolicy1 have Windows Information Protection mode: Block

upvoted 6 times

madmouse256 1 year, 3 months ago

ChrisBr is correct. Here is a link to detailed explanation how WIP App Protection Policies are working https://docs.microsoft.com/en-us/mem/intune/apps/windows-information-protection-policy-create#add-a-protection-mode

upvoted 2 times

Cbruce Most Recent 1 month, 3 weeks ago

Should be Y,Y,N
1. Y - Android not protected with a WIP policy. You need to create one for Android too, to protect data.
2. Y - App2 is exempt from the policy. "List of allowed and exempt apps
Protected apps: These apps are the apps that need to adhere to this policy.
Exempt apps: These apps are exempt from this policy and can access corporate data without restrictions." https://docs.microsoft.com/en-us/mem/intune/apps/windows-information-protection-policy-create
3. N - App3 isn't listed, so data will be blocked from App1. There could be 100s of apps you don't list to block. If the app is not in the list, then it's blocked.

upvoted 2 times

Goseu 2 months, 3 weeks ago

Yes No No , DTz explained everything

upvoted 2 times

Rockalm 3 months, 2 weeks ago

For me it is YNN
1. It's an Android, but the rule applies only to Windows devices. In the meantime also Androids can be protected: https://docs.microsoft.com/en-us/mem/intune/apps/app-protection-policy-settings-android. But this rule uses WIP, so it's only for Win.
2. DTz is right: Block: Blocks enterprise data FROM LEAVING protected app -->N
3. same as 2.-->N

upvoted 2 times

B1G_B3N 6 months, 3 weeks ago

I dont understand how it isnt no no no. An app protection policy in the name surely stops data leaking if the app is protected? Everyone here getting caught up on Android but its an APP protection policy it doesnt care what device as long as the policy is applied. Coupled with WIP surely nothing gets out here? Mucho confusion!

upvoted 4 times

B1G_B3N 6 months, 2 weeks ago

Agree with Dtz, Yes No No

upvoted 1 times

kiketxu 5 months ago

me too, he did explained pretty well. Probably the most voted coment that I saw in this site.

upvoted 2 times

Paulmtx 6 months, 3 weeks ago

So, if you try to create a policy on Intune portal, under Apps->App protection policies, the 1st thing you need to choose is the platform. WIP policy can only be specified if you're creating a policy that target Windows 10. This means that an Android device will not be affected by this policy.
To me, it means that the answer to 1st question should be "yes", since the device is not touched by the policy.
As per question 2, an "exempt" app is one for which the "copy/paste" restrictions won't apply, letting that app be sourse and/or target of a copy/paste action. So, the answer to this for me should be "yes".
As per question 3, app 3 is neither protected nor exempt, so it cannot be used as either source or destination of a copy/paste operation.

upvoted 3 times

Samoanhulk 6 months, 3 weeks ago

App Protection Policies only apply to Android and iOS Platforms as outlined here under row 5 in the table - https://docs.microsoft.com/en-us/mem/intune/apps/app-management#app-management-capabilities-by-platform

Therefore, the provided initial answer is correct. Windows 10 devices will only come into play if we are purely looking at WIP. At the bottom of the table in the link above, there is this comment "Consider using Windows Information Protection to protect apps on devices that run Windows 10."
So answer is No (Device being an Android), Yes (Device being a Win10), Yes (Device being a Win10)

upvoted 1 times

B1G_B3N 6 months, 3 weeks ago

I dont understand? What has android got anything to do with it? The android device has app1 installed and the policy protects app1 and applies to User1 who is using the android device in Q1. If user1 tries moving any data as its a protected app it wont work????

upvoted 1 times

Mary_Yvette 7 months, 2 weeks ago

Yes – it only applies to Windows 10 not Android
Yes – App 2 is exempted so communications between App1 (Protected) and App 2 is okay
No – App 3 is not protected. App 1 is protected. They can not communicate.

https://docs.microsoft.com/en-us/windows/security/information-protection/windows-information-protection/create-wip-policy-using-intune-azure#define-your-enterprise-managed-corporate-identity

If your app is incompatible with WIP, but still needs to be used with enterprise data, you can exempt the app from the WIP restrictions. This means that your apps won't include auto-encryption or tagging and won't honor your network restrictions. It also means that your exempted apps might leak.

upvoted 4 times

Ken88 9 months, 1 week ago

Key word is app protection policy.
It will only works on Android and iOS.
Answer is Yes NO NO.
https://docs.microsoft.com/en-us/mem/intune/apps/app-management#app-management-capabilities-by-platform

upvoted 6 times

Ashton_98 7 months, 2 weeks ago

Isn't this back to front then?

1. Android user is blocked from copying as the APP is applied.
2. Windows user is NOT blocked from copying as the APP is not compatible with Windows.
3. Windows user is NOT blocked from copying as the APP is not compatible with Windows.

upvoted 1 times

Enoll 10 months ago

So I had to sit down and actually test this because I was so certain that it is YES YES NO, but to my surprise it wasn't. Usually, when you exempt an application, this means that you can access your data, say for instance you have put as a cloud resource sharepoint, however it will not be protected and it is subject to data leakage and up until now I strongly believe that even if you exempt an app it can still communicate in terms of cut/copy/paste with protected apps, but no, it doesn't. I did a WIP with enrollment (Since I already have an autopilot test pc) with IE as protected app, Edge as exempt app , block setting and sharepoint as protected cloud resource. I had also Chrome installed, so once the policy was deployed I

cannot browse anything on Chrome, good indicator that it is working :D. I could open sharepoint on both browsers which is what to be expected, however if i try to copy data from one document from IE to EDGE it throws an error - Can't use work content here. So the answers are:

1. Yes - clearly this is a WIP policy, not an Android policy
2. NO - You cannot copy between App 1 (protected) and App 2 (exempt)
3. NO - This is a no brainer.

upvoted 16 times

cabeza 8 months, 3 weeks ago

Exactly this, WIP only ever applies to W for Windows. There is only one app policy created here and it has a WIP condition so the platform must have been windows 10 for the app policy.

upvoted 1 times

dzampar 9 months, 3 weeks ago

Agreed!
more info here
https://docs.microsoft.com/en-us/mem/intune/apps/windows-information-protection-policy-create

upvoted 2 times

xyzzy 10 months, 3 weeks ago

I agree with DTz

upvoted 1 times

Dumas234 11 months, 3 weeks ago

oops - I forgot there is a WIP policy also.

upvoted 1 times

Dumas234 11 months, 3 weeks ago

So answer becomes NO, YES, NO

upvoted 2 times

SUBZER0 11 months ago

If we assume that is compaible with Android and windows which could be https://mattsoseman.wordpress.com/2019/10/06/block-sharing-of-corporate-data-with-windows-information-protection-microsoft-endpoint-dlp/
App2 is exempt and can access company data https://docs.microsoft.com/en-us/mem/intune/apps/windows-information-protection-policy-create
The answer would be NO, YES, NO FINAL (LAST COMMENT)

upvoted 2 times

SUBZER0 11 months ago

Ok so is only for android and ios
https://docs.microsoft.com/es-es/mem/intune/apps/app-management#app-management-capabilities-by-platform Answers are fine NO, YES, YES

upvoted 1 times

SUBZER0 11 months ago

You are not protecting app2 you are protecting app1 from data exfiltration, app 2 doesn't matter becasue is never the source.
The point is if these "app protection policies are compatible with windows or only with android"

upvoted 2 times

Dumas234 11 months, 3 weeks ago

1. WIP doesn't work on Android but App Protection does - NO
2. APP 2 is exempt, but even if it wasn't App Protection not supported on Windows Device - YES
3. App Protection not supported on Windows Device - YES (See Sizz link)

upvoted 2 times

Dumas234 1 year ago

Group 2 is exempted, but only user 2 is in Group 2. All questions are about User 1.

upvoted 2 times

jack987 1 year, 2 months ago

Correct Answer: No Yes No
https://docs.microsoft.com/en-us/mem/intune/apps/windows-information-protection-policy-create

upvoted 5 times

jack987 1 year, 1 month ago

DTz is right.

Correct Answer should be:

1. Device 1 is an Android Device and WIP won't work at all -> Answer YES
2. App2 is exempt, but the policy protects >App1< from data LEAVING it. So the copy gets blocked -> Answer NO
3. This is effectively the same as #2. Sure, App3 is not impacted, but App1 is, and you cannot copy data FROM App1 -> Answer NO

upvoted 9 times

MCPsince1999 4 months, 2 weeks ago

I agree. The point is if the source is protected how it could leave it if we change something on the target...

upvoted 2 times

pmr123 10 months, 3 weeks ago

I too had the same in my mind and was looking for this explanation. When something is protected how can you copy data from it and go away??

upvoted 3 times

Hisagenda 11 months ago

your doc is on mem not wip

upvoted 1 times

Mehodge 1 year, 4 months ago

If we are looking at WIP App Policy then Protected Apps must adhere to the policy and Exempt apps have free access to corp data. As App1 is protected and wants to share with an app (App3) that is not included in protected or exempt then it is blocked. As app 2 is exempt then it has free access to the corp data so it is allowed.
No - Yes - No
https://docs.microsoft.com/en-us/mem/intune/apps/windows-information-protection-policy-create

upvoted 9 times

Question #20 *Topic 2*

You have a Microsoft 365 tenant.
You have 500 computers that run Windows 10.
You plan to monitor the computers by using Microsoft Defender for Endpoint after the computers are enrolled in Microsoft Endpoint Manager.
You need to ensure that the computers connect to Microsoft Defender for Endpoint.
How should you prepare Endpoint Manager for Microsoft Defender for Endpoint?

A. Configure an enrollment restriction

B. Create a device configuration profile

C. Create a conditional access policy

D. Create a Windows Autopilot deployment profile

Pitch09 3 months ago

https://docs.microsoft.com/en-us/mem/intune/protect/advanced-threat-protection-configure

upvoted 4 times

Question #21 *Topic 2*

HOTSPOT -

Your company has a Microsoft 365 subscription that contains the users shown in the following table.

Name	Member of
User1	Group1
User2	Group2
User3	Group3

The company implements Microsoft Defender Advanced Threat Protection (Microsoft Defender ATP). Microsoft Defender ATP includes the roles shown in the following table:

Name	Permission	Assigned user group
Role1	View data, Active remediation actions, Alerts investigation	Group1
Role2	View data, Active remediation actions	Group2
Microsoft Defender ATP administrator (default)	View data, Alerts investigation, Active remediation actions, Manage portal system settings, Manage security settings	Group3

Microsoft Defender ATP contains the machine groups shown in the following table:

Rank	Machine group	Machine	User access
First	ATPGroup1	Device1	Group1
Last	Ungrouped machines (default)	Device2	Group2

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

NOTE: Each correct selection is worth one point.

Hot Area:

Answer Area

Statements	Yes	No
User1 can run an antivirus scan on Device1.	○	○
User2 can collect an investigation package from Device2.	○	○
User3 can isolate Device1.	○	○

Joshing 1 week, 3 days ago

Correct answer is Y/N/Y.

With RBAC logging into this security portal you will get Full Access "Defender for Endpoint Global administrator role" (which is the default) if you are a Global Admin or Security Admin. Security Reader will get Read-only variants.

The same full access Role can be assigned to users as well. Which in this case either has been or has been inherited as the user is a Global/Security Admin.

https://docs.microsoft.com/en-us/microsoft-365/security/defender-endpoint/rbac?view=o365-worldwide#before-you-begin

"Someone with a Defender for Endpoint Global administrator role has unrestricted access to all devices, regardless of their device group association and the Azure AD user groups assignments."

upvoted 3 times

laugz92 2 months, 2 weeks ago

User groups assigned the Microsoft Defender for Endpoint administrator role have access to all device groups.
https://securitycenter.microsoft.com/preferences2/machine_groups -> User Access

upvoted 4 times

Cbruce 1 month, 3 weeks ago

Y,N,Y
1. Y - Correct permissions to run scans on devices in the group

2. N - Does not have access to collect package, needs Alerts Investigation permissions too
3. Y - default administrator, can access all devices, regardless of group

upvoted 7 times

weabey 2 months, 3 weeks ago

Yes - No - No

View Data
- View Data

Alerts investigation
- Manage alerts
- Initiate automated investigations
- Run scans
- Collect investigation packages
- Manage machine tags

Active remediation actions
- Take responsive actions
- Approve or dismiss pending remediation actions

ATP-Administrators – ATP Admins, change settings and manage security roles only

Manage security settings
- Configure alert suppression settings
- Manage allowed/blocked lists for automation
- Manage folder exclusions for automated (applies globally)
- Onboard and offboard machines
- Manage email notifications

upvoted 3 times

kiketxu 4 months, 4 weeks ago

Seems this is repeated question...

Yes, AV scan is in the allowed actions.
No, collection is not allowed.
Yes, despite is not clear in the following link, isolate machine is in the remediations actions.
https://docs.microsoft.com/en-us/windows/security/threat-protection/microsoft-defender-atp/user-roles#permission-options

Check in this other link. https://docs.microsoft.com/en-us/windows/security/threat-protection/microsoft-defender-atp/respond-machine-alerts

upvoted 2 times

Sugar123 4 months, 3 weeks ago

User 3 cannot isolate Device 1 as it does not have access to this device. Only Group 1 has access to Device 1. "The user needs to have access to the device, based on device group settings (See Create and manage device groups for more information)"
https://docs.microsoft.com/en-us/windows/security/threat-protection/microsoft-defender-atp/isolate-machine

So, the answer is correct. Yes - No - No

upvoted 2 times

kiketxu 4 months, 3 weeks ago

Please check this...
https://docs.microsoft.com/en-us/windows/security/threat-protection/microsoft-defender-atp/rbac#before-you-begin

"Someone with a Defender for Endpoint Global administrator role has unrestricted access to all devices, regardless of their device group association and the Azure AD user groups assignments"

upvoted 5 times

Sugar123 4 months, 3 weeks ago

I'm a little confused. The below link implies that a Defender for Endpoint Global Administrator and a Defender for Endpoint Administrator are different. "Users with full access (users that are assigned the Global Administrator or Security Administrator directory role in Azure AD), are automatically assigned the default Defender for Endpoint administrator role, which also has full access. Additional Azure AD user groups can be assigned to the Defender for Endpoint administrator role after switching to RBAC. Only users assigned to the Defender for Endpoint administrator role can manage permissions using RBAC."

I'm not sure if Group 3 consists of Global Administrators, which would make you right, or if they are regular users assigned the default Defender for Endpoint administrator role. If it is the latter, then I believe the answer is Yes - No - No.

https://docs.microsoft.com/en-us/windows/security/threat-protection/microsoft-defender-atp/assign-portal-access

upvoted 3 times

JoelB 1 month, 1 week ago

The role in the question says (default), therefore it should be an AAD Global Admin/Security Admin, the quote you provided explains it.

upvoted 1 times

Question #22

Topic 2

You have a hybrid deployment of Microsoft 365 that contains the users shown in the following table.

Name	User mailbox	Multi-factor authentication (MFA)
User1	On-premises Microsoft Exchange Server	Required
User2	On-premises Microsoft Exchange Server	Disabled
User3	Microsoft Exchange Online	Required
User4	Microsoft Exchange Online	Disabled

You plan to use Microsoft 365 Attack Simulator.

You need to identify the users against which you can use Attack Simulator.

Which users should you identify?

A. User3 only

B. User1, User2, User3, and User4

C. User3 and User4 only

D. User1 and User3 only

kiketxu Highly Voted 4 months, 4 weeks ago

C for sure. Only supported on EXO. Btw, MFA is to create and manage campaings.

upvoted 13 times

ffffffffdeeeeeeeeeee 2 months ago

ANS: A
Attack Simulator only works on cloud-based mailboxes and with MFA enabled.

upvoted 4 times

belyo Highly Voted 4 months, 3 weeks ago

A for sure
*Your account needs to be configured for multi-factor authentication (MFA) to create and manage campaigns in Attack Simulator. For instructions, see Set up multi-factor authentication.

*Attack Simulator only works on cloud-based mailboxes.

upvoted 10 times

kiketxu 4 months, 3 weeks ago

MFA is to create and manage campaings. In the statements says "against"

upvoted 11 times

chaoscreater 1 month, 1 week ago

You're overcomplicating the english. If the sentence were to say - "you need to identify the users which you can use Attack Simulator against", then it means you want to use it on them. "Against" is to use it ON something, not necessarily PREVENT from using it on them. Question here is talking about using it on someone. Answer A is correct.

upvoted 1 times

Joshing Most Recent 1 week, 3 days ago

I don't get the confusion on this one. C is the definitely the correct answer.

If it were asking who could manage the Attack Simulation campaign why would it include the mailbox type being on-prem or EXO? As an admin your only requirement to manage the campaigns is to have MFA on your account. You don't need any mailbox what so ever.

The question is clearly asking what users you can run the campaign against. As in who will be targeted. In this case it will be C. As the requirement to run the campaign is just to have EXO. MFA is only required on the Admin running the campaign.

https://docs.microsoft.com/en-us/microsoft-365/security/office-365-security/attack-simulator?view=o365-worldwide#what-do-you-need-to-know-before-you-begin

upvoted 1 times

Joshing 1 week, 3 days ago

Clarity: The requirement is EXO to be targeted for the campaign. MFA is not required.

upvoted 1 times

ViniciusVidal 4 months ago

For me A is correct (User 3 only), because Attack Simulator only works on cloud-based mailboxes and with MFA enabled.

upvoted 6 times

arunjana 2 months, 3 weeks ago

C is correct. MFA is only required for the admin who initiates the 'Attack Simulator'
upvoted 2 times

Question #23 *Topic 2*

SIMULATION -
You need to implement a solution to manage when users select links in documents or email messages from Microsoft Office 365 ProPlus applications or Android devices. The solution must meet the following requirements:
- Block access to a domain named fabrikam.com
- Store information when the users select links to fabrikam.com

To complete this task, sign in to the Microsoft 365 portal.

mitchg Highly Voted 10 months ago
The settings have been rearranged. Blocking URLs should now be done under "Global Settings", see https://docs.microsoft.com/en-us/microsoft-365/security/office-365-security/configure-global-settings-for-safe-links?view=o365-worldwide
upvoted 7 times

dzampar Highly Voted 9 months, 3 weeks ago
You will need to set up at least one policy so that you can have the global settings applied to users. I've tested in my lab and there was no default policy indeed.

"The features provided by global settings for Safe Links are only applied to users who are included in active Safe Links policies. There is no built-in or default Safe Links policy, so you need to create at least one Safe Links policy in order for these global settings to be active."

https://docs.microsoft.com/en-us/microsoft-365/security/office-365-security/configure-global-settings-for-safe-links?view=o365-worldwide#what-do-you-need-to-know-before-you-begin

So for your policy, I guess you will need to pay attention to these two options.

*Apply Safe Links to email messages sent within the organization: Select this setting to apply the Safe Links policy to messages between internal senders and internal recipients.

*Do not track user clicks: Leave this setting unselected to enable the tracking user clicks on URLs in email messages.
upvoted 6 times

itstudy369 Most Recent 6 months, 2 weeks ago
The features provided by global settings for Safe Links are only applied to users who are included in active Safe Links policies. There is no built-in or default Safe Links policy, so you need to create at least one Safe Links policy in order for these global settings to be active.
upvoted 3 times

Question #24 *Topic 2*

SIMULATION -
You need to configure your organization to automatically quarantine all phishing email messages.
To complete this task, sign in to the Microsoft 365 portal.

techstudent Highly Voted 8 months, 3 weeks ago
https://docs.microsoft.com/en-us/microsoft-365/security/office-365-security/configure-anti-phishing-policies-eop?view=o365-worldwide
https://protection.office.com/antiphishing
Security & Compliance Center, Threat management > Policy > Anti-phishing.
[Default Policy]
Spoof [Edit]
- Actions
If email is sent by someone who's not allowed to spoof your domain:
Quarantine the message
upvoted 7 times

Question #25

Topic 2

You configure several Advanced Threat Protection (ATP) policies in a Microsoft 365 subscription.

You need to allow a user named User1 to view ATP reports in the Threat management dashboard.

Which role provides User1 with the required role permissions?

A. Security administrators

B. Exchange administrator

C. Compliance administrator

D. Message center reader

kiketxu 4 months, 3 weeks ago

A for sure!

upvoted 4 times

Question #26 *Topic 2*

You have a Microsoft 365 subscription and a Microsoft Defender Advanced Threat Protection (Microsoft Defender ATP) subscription.

You have devices enrolled in Microsoft Endpoint Manager as shown in the following table:

Name	Platform
Device1	Windows 10
Device2	Android
Device3	iOS

You integrate Microsoft Defender ATP and Endpoint Manager.

You plan to evaluate the Microsoft Defender ATP risk level for the devices.

You need to identify which devices can be evaluated.

Which devices should you identify?

A. Device1 and Device2 only

B. Device1 only

C. Device1 and Device3 only

D. Device1, Device2 and Device3

vijayvasisht Highly Voted 4 months, 2 weeks ago

its all 3 now (https://techcommunity.microsoft.com/t5/microsoft-defender-for-endpoint/microsoft-defender-for-endpoint-on-ios-is-generally-available/ba-p/1962420)

upvoted 11 times

Nounna Most Recent 2 months, 2 weeks ago

Evaluation of MDE is only available for Windows10, Win srv 2019 and Win srv 2016 (firewall evaluation
https://docs.microsoft.com/en-us/microsoft-365/security/defender-endpoint/evaluate-mde?view=o365-worldwide

upvoted 1 times

andreiiar 3 months, 2 weeks ago

https://docs.microsoft.com/en-us/microsoft-365/security/defender-endpoint/minimum-requirements?view=o365-worldwide#other-supported-operating-systems

Other supported operating systems

Android
iOS
Linux
macOS

upvoted 3 times

DudleyYVR 3 months, 2 weeks ago

MD ATP is not fully integrated with Android.
iOS is NOT macOS. There's a difference.

upvoted 1 times

MCPsince1999 4 months, 2 weeks ago

Answer is A, W10 and Android is supported (not iOS)

upvoted 2 times

bingomutant 4 months, 1 week ago

see vijay below which is now correct

upvoted 1 times

kiketxu 4 months, 3 weeks ago

This answer might change recently. Now there are more supported OS like: Linux, MacOS and Android. ref: https://docs.microsoft.com/en-us/windows/security/threat-protection/microsoft-defender-atp/minimum-requirements#other-supported-operating-systems
Despite in the above is missing iOS, seems is also already available:
https://docs.microsoft.com/es-es/windows/security/threat-protection/microsoft-defender-atp/microsoft-defender-atp-ios

upvoted 3 times

bingomutant 4 months, 3 weeks ago

latest 3 versions of iOS are now supported.

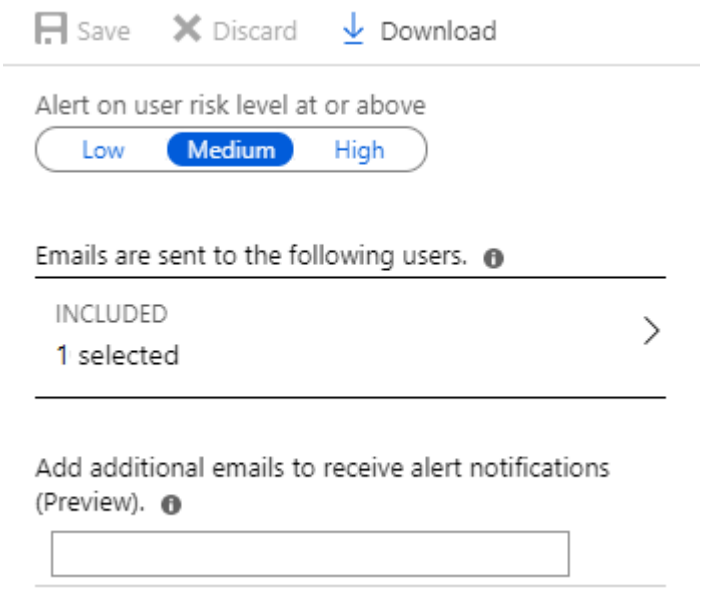
upvoted 2 times

Question #27 *Topic 2*

HOTSPOT -

You have a Microsoft 365 E5 subscription that contains an Azure Active Directory (Azure AD) tenant named contoso.com.

Azure AD Identity Protection alerts for contoso.com are configured as shown in the following exhibit.



A user named User1 is configured to receive alerts from Azure AD Identity Protection.

You create users in contoso.com as shown in the following table.

Name	Role
User2	Security reader
User3	User administrator
User4	*None*
User5	*None*

The users perform the sign-ins shown in the following table.

Time	User	Risk event type
13:00	User4	Sign-ins from infected device
14:00	User4	Sign-in from unfamiliar location
15:00	User5	Sign-ins from anonymous IP address

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

NOTE: Each correct selection is worth one point.

Hot Area:

Answer Area

Statements	Yes	No
User1 receives three email alerts from Azure AD Identity Protection.	○	○
User2 receives three email alerts from Azure AD Identity Protection.	○	○
User3 receives two email alerts from Azure AD Identity Protection.	○	○

kiketxu Highly Voted 4 months, 3 weeks ago

Based on the below risk level severity ("old") table, I would say...

YES. User1 receives 3 alerts as all them are medium and he was manually added.
YES. User2 receives 3 alerts (for the same) but in this case for his Security Reader role.
NO. User3 doesn't receive any because his "User Administrator" role does not permit that.

Users with leaked credentials - High

Sign-ins from anonymous IP addresses - Medium
Impossible travel to atypical locations - Medium
Sign-ins from infected devices -Medium
Sign-ins from unfamiliar locations - Medium

Sign-ins from IP addresses with suspicious activity -Low

NOTE: This table has grew recently, seems now with more alerts, but couldn't get their current level. Not sure when we will see this in exam.
https://docs.microsoft.com/en-us/azure/active-directory/identity-protection/concept-identity-protection-risks#user-risk
upvoted 18 times

Yetijo 1 month, 3 weeks ago

Agree, - Yes, Yes, No.

Per documentation, by default - GA, Security Admin, and Security Reader receive mail.
Source:
https://docs.microsoft.com/en-us/azure/active-directory/identity-protection/howto-identity-protection-configure-notifications#configure-users-at-risk-detected-alerts

All events are flagged in the Sign-In Risk table here.
Source:
https://docs.microsoft.com/en-us/azure/active-directory/identity-protection/concept-identity-protection-risks#sign-in-risk
upvoted 1 times

Kalzonee3611 2 months, 2 weeks ago

How do you which activity falls under which category of threat?
upvoted 1 times

Goseu 2 months, 2 weeks ago

This answer does not apply .
The given answers are correct .
While Microsoft does not provide specific details about how risk is calculated, we will say that each level brings higher confidence that the user or sign-in is compromised
IMO , User 4 first alert will be low , second alert probably medium risk .User 5 low .
Therefore , NO,NO,NO
upvoted 3 times

Sethoo 4 months, 1 week ago

Check the configuration. The alert is configured to go to just 1 email and that is user 1. So why will user 2 get the email alert? I lean YES NO NO
upvoted 2 times

TheGuy 4 months, 1 week ago

From the Identity Protection Alert Blade: "Users in the Global administrator, Security administrator, or Security reader roles are automatically added to this list if that user has a valid "Email" or "Alternate email" configured".

I'd say: Yes, Yes, and No
upvoted 1 times

The_Poet Most Recent 1 week, 4 days ago

Sign-ins from infected device is classified as low. This risk detection identifies IP addresses, not user devices.
isn't right?
upvoted 1 times

ThBEST 3 weeks, 4 days ago

Each of the sign ins are successful so therefore each have a low risk. The infected system has not set off any alerts and the risk remains low. So because of the low risk there will be no alert emails sent to either user at this time. No, No, No.
upvoted 1 times

Destny 2 months, 2 weeks ago

Definitely YYN
upvoted 1 times

Pitch09 3 months ago

YYN- explained here - https://docs.microsoft.com/en-us/azure/active-directory/identity-protection/howto-identity-protection-configure-notifications#:~:text=In%20response%20to%20a%20detected%20account%20at%20risk%2C,you%20should%20immediately%20investigate%20the%20users%20at%20risk.
upvoted 1 times

ismossss 3 months ago

This one most be
no. Sign-ins from infected devices -Low
no. Sign-ins from infected devices -Low
no. Sign-ins from infected devices -Low
upvoted 2 times

Question #28 *Topic 2*

You have an Azure Sentinel workspace that has an Azure Active Directory (Azure AD) connector and a Microsoft Office 365 connector.

You need to assign built-in role-based access control (RBAC) roles to achieve the following tasks:

- Create and run playbooks.
- Manage incidents.

The solution must use the principle of least privilege.

Which two roles should you assign? Each correct answer presents part of the solution.

NOTE: Each correct selection is worth one point.

A. Automation Operator

B. Azure Sentinel responder

C. Automation Runbook Operator

D. Azure Sentinel contributor

E. Logic App contributor

xyzzy Highly Voted 10 months, 3 weeks ago

Azure Sentinel Contributor + Logic App Contributor is correct

upvoted 13 times

JaBe 9 months ago

but according to table
https://docs.microsoft.com/en-us/azure/sentinel/roles#roles-and-allowed-actions
Azure Sentinel Responder is enough to manage incidents. Contributor would be too much in regards to least privilege.
I agree with the Local App contributor

upvoted 8 times

FumerLaMoquette 8 months, 4 weeks ago

I agree.
Azure sentinel responder
Logic app contributor

upvoted 6 times

MrGarak1 8 months, 3 weeks ago

RESPONDER can`t create and run playbooks only CONTRIBUTOR and that is what is asked in the question.
https://docs.microsoft.com/en-us/azure/sentinel/roles#roles-and-allowed-actions

upvoted 2 times

JaBe 8 months, 3 weeks ago

Yes but it's the Logic app contributor role that is handling the create and run playbooks part.

upvoted 1 times

MrGarak1 8 months, 3 weeks ago

With Responder, you CAN`T Create and Run Playbook. Only with Azure Sentinel Contributor + Logic App Contributor

upvoted 2 times

TDAC 10 months, 1 week ago

I agree.
Azure Sentinel Contributor is correct to respond and manage incidents.

A Logic App can be used to trigger a runbook. Therefore the role of Logic App Contributor is correct. Automation runbook operator CANNOT create runbooks. To Logic App Contributor is the logical answer.

upvoted 1 times

naren49 Highly Voted 6 months, 3 weeks ago

the given answer D & E are correct

Azure Sentinel Contributor
Create and edit workbooks, analytic rules, and other Azure Sentinel resources
Manage incidents (dismiss, assign, etc.)
view data, incidents, workbooks, and other Azure Sentinel resources

Logic App Contributor
Create and run playbooks

upvoted 5 times

kiketxu 4 months, 3 weeks ago

Pretty clear!
https://docs.microsoft.com/en-us/azure/sentinel/roles#roles-and-allowed-actions

upvoted 7 times

Fala_Fel 3 weeks, 3 days ago

Yes, section "Azure Sentinel roles and allowed actions" clearly shows answer is correct.
D. Azure Sentinel contributor
E. Logic App contributor

upvoted 1 times

GevedeBe Most Recent 3 months, 1 week ago

I am wrong, the Sentinel contributor on itself cannot create and run playbooks, the combination is with the Logic app to make this happening.

upvoted 1 times

GevedeBe 3 months, 2 weeks ago

This is part of the question, " The solution must use the principle of least privilege." and as such you have two roles, right, so one for manage incidents and one for creating and run. So in this setup it should be Sentinel Contributor and Sentinel Responder, Logic App Contributor, has too much rights - privileges!

upvoted 1 times

NickDouglas 11 months ago

B. Azure Sentinel responder
D. Azure Sentinel contributor

upvoted 2 times

kijken 11 months ago

Responder had no vakje if you put user in contributie
D is needed and because of that B is wrong. Nog site of e is correct

upvoted 2 times

Question #29 *Topic 2*

Your company uses Microsoft Azure Advanced Threat Protection (ATP).

You enable the delayed deployment of updates for an Azure ATP sensor named Sensor1.

How long after the Azure ATP cloud service is updated will Sensor1 be updated?

A. 7 days

B. 24 hours

C. 1 hour

D. 48 hours

E. 12 hours

mnak Highly Voted 1 year, 2 months ago

It was 24 hours, but was updated to 72 hours in 2.62.
https://docs.microsoft.com/en-us/azure-advanced-threat-protection/atp-whats-new#azure-atp-release-262

upvoted 18 times

btd2020 Highly Voted 1 year, 2 months ago

I think the information added to the question is correct- "72 hours after the Azure ATP cloud service is updated, sensors selected for Delayed update start their update process according to the same update process as automatically updated sensors." https://docs.microsoft.com/en-us/azure-advanced-threat-protection/sensor-update

upvoted 13 times

Metasploit 11 months, 2 weeks ago

Would Microsoft base their questions on latest service version or previous? Just asking if presented with both options for 24 and 72 hours.

upvoted 1 times

Davidf 9 months, 2 weeks ago

Did 101 very recently (which has recently been updated) and got 20 and 72 hours as option, went with 72 (and passed)

upvoted 4 times

VTHAR 10 months, 4 weeks ago

Microsoft should not present both value if this question is being asked. As a rule of thumb, it should refer to latest service version. No point asking an outdated service info.

upvoted 1 times

examcrammer 10 months, 1 week ago

To the readers...MS writes exam questions based on the CURRENT configuration of a service at the TIME the question was written. You have to remember, give the MS answer, not what you feel is correct or best practices or 'latest' capabilities. This is why the require you to re-certify every 2 - 3 years.....to stay current.

upvoted 2 times

ginsahec 1 year, 2 months ago

Yes , the answer is 72 hrs.
https://docs.microsoft.com/es-es/azure-advanced-threat-protection/sensor-update

upvoted 8 times

kiketxu Most Recent 4 months, 3 weeks ago

Sensors set to Delayed update are updated on a delay of 72 hours, following the official release of each service update.
https://docs.microsoft.com/es-es/defender-for-identity/sensor-update#delayed-sensor-update

upvoted 2 times

svm_Terran 8 months ago

answer would be 72

upvoted 5 times

Question #30 *Topic 2*

DRAG DROP -

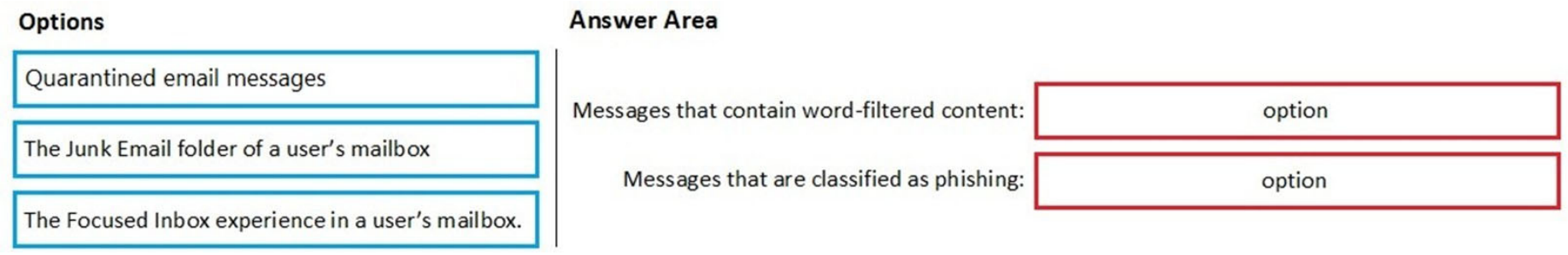
You have a Microsoft 365 E5 subscription. All users use Microsoft Exchange Online.

Microsoft 365 is configured to use the default policy settings without any custom rules.

You manage message hygiene.

Where are suspicious email messages placed by default? To answer, drag the appropriate location to the correct message types. Each option 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.

Select and Place:



asquante Highly Voted 4 months ago

This is incorrect. By default both go to Junk Mail, only high confidence phishing goes to Quarantine.

upvoted 6 times

chaoscreater Highly Voted 1 month, 1 week ago

People should really test and verify themselves before giving answers. Both go to junk mail. The default value for the default anti-philshing policy is that it goes to junk. You have to actually modify it to go into quarantine.

upvoted 5 times

kanag1 3 days, 6 hours ago

You are right mate!!
Only High Confidence Phishing goes to Quarantine, spam , high confidence spam and Phishing goes to Junk.
Others , please check the policy settings before posting here.

upvoted 2 times

SR_OPS Most Recent 1 month, 1 week ago

From: https://docs.microsoft.com/en-us/microsoft-365/security/office-365-security/quarantine-email-messages?view=o365-worldwide

By default, anti-spam polices quarantine phishing messages, and deliver spam and bulk email messages to the user's Junk Email folder.
From this page:
https://docs.microsoft.com/en-us/microsoft-365/security/office-365-security/advanced-spam-filtering-asf-options?view=o365-worldwide
"Messages that contain words from the sensitive word list in the subject or message body are marked as high confidence spam."

From the above I understand that:
Word filtered content would go to users junk because they are marked as spam, while the phishing would go to quarantine

upvoted 3 times

SimoneV 1 month, 2 weeks ago

Answer seems correct to me.

"By default, anti-spam polices quarantine phishing messages, and deliver spam and bulk email messages to the user's Junk Email folder."
https://docs.microsoft.com/en-us/microsoft-365/security/office-365-security/quarantine-email-messages?view=o365-worldwide

Also check the table on this page. The * marks the default action:
https://docs.microsoft.com/en-us/microsoft-365/security/office-365-security/quarantine-email-messages?view=o365-worldwide

upvoted 1 times

Cbruce 1 month, 3 weeks ago

Both go to Junk Mail. "Move messages to the recipients' Junk Email folders: This is the default value. The message is delivered to the mailbox and moved to the Junk Email folder. " https://docs.microsoft.com/en-us/microsoft-365/security/office-365-security/set-up-anti-phishing-policies?view=o365-worldwide#advanced-phishing-thresholds-in-anti-phishing-policies-in-microsoft-defender-for-office-365

upvoted 2 times

kiketxu 4 months, 3 weeks ago

given answer are correct.
Junk and Quarantine.

upvoted 4 times

Question #31 *Topic 2*

You have a Microsoft 365 subscription.

You create a Microsoft Defender for Identity safe attachments policy.

You need to configure the retention duration for the attachments in quarantine.

Which type of threat management policy should you create?

A. Anti-phishing

B. DKIM

C. Anti-spam

D. Anti-malware

stromnessian 1 week, 4 days ago

Defender for Identity???

upvoted 1 times

SR_OPS 1 month, 1 week ago

C - Anti-Spam Policy

From this page: https://docs.microsoft.com/en-us/microsoft-365/security/office-365-security/manage-quarantined-messages-and-files?view=o365-worldwide#BKMK_ModQuarantineTime

Quarantined messages are retained for a default period of time before they're automatically deleted:

30 days for messages quarantined by anti-spam policies (spam, phishing, and bulk email). This is the default and maximum value. To configure (lower) this value, see Configure anti-spam policies.

upvoted 1 times

ffffffffdeeeeeeeeeee 2 months ago

C - Anti-spam

Quarantined messages are retained for a default period of time before they're automatically deleted:

30 days for messages quarantined by anti-spam policies (spam, phishing, and bulk email). This is the default and maximum value. To configure (lower) this value, see Configure anti-spam policies.
15 days for messages that contain malware.
15 days for files quarantined by Safe Attachments for SharePoint, OneDrive, and Microsoft Teams in Defender for Office 365.

upvoted 2 times

M1crsoftPro 2 months ago

Correct answer is D
they are asking about attachments retention and not the emails.
therefor the answer is anti-malware.
anti-spam is addressing spam and phishing emails and the anti-malware is addressing to the attachments.

upvoted 3 times

chaoscreater 1 month, 1 week ago

I agree. Question is asking about attachments and if you go to the policies under Threat Management, it is anti-malware that deals with attachments.

upvoted 1 times

chaoscreater 1 month, 1 week ago

Actually, I take it back, answer is correct.

"Attachments will be quarantined by Anti-Malware policies, however the only place to configure quarantine retention is in the Anti-Spam policy"

https://www.examtopics.com/discussions/microsoft/view/8009-exam-ms-500-topic-2-question-11-discussion/

upvoted 1 times

Goseu 2 months, 2 weeks ago

Correct answer
30 days for messages quarantined by anti-spam policies (spam, phishing, and bulk email). This is the default and maximum value. To configure (lower) this value, see Configure anti-spam policies.

upvoted 2 times

TimurKazan 3 months ago

Just checked it in the lab, the answer is correct - C - Anti-spam

upvoted 3 times

elife 3 months ago

Correct Answer is "D": Anti-malware.
https://docs.microsoft.com/en-us/microsoft-365/security/office-365-security/configure-anti-malware-policies?view=o365-worldwide

upvoted 1 times

fred99 3 months ago

wrong, it is anti-spam: Quarantined messages are retained for a default period of time before they're automatically deleted: 30 days for messages quarantined by anti-spam policies (spam, phishing, and bulk email). This is the default and maximum value. To configure (lower) this value, see Configure anti-spam policies.

upvoted 1 times

Question #32 *Topic 2*

Your company has 500 computers.

You plan to protect the computers by using Microsoft Defender for Endpoint. Twenty of the computers belong to company executives.

You need to recommend a remediation solution that meets the following requirements:

- Microsoft Defender for Endpoint administrators must manually approve all remediation for the executives
- Remediation must occur automatically for all other users

What should you recommend doing from Microsoft Defender Security Center?

A. Configure 20 system exclusions on automation allowed/block lists

B. Configure two alert notification rules

C. Download an offboarding package for the computers of the 20 executives

D. Create two machine groups

SlimBoy 2 months, 1 week ago

The answer is correct

upvoted 1 times

Question #33 *Topic 2*

You have a Microsoft 365 Enterprise E5 subscription.

You use Microsoft Defender for Endpoint.

You need to integrate Microsoft Defender for Office 365 and Microsoft Defender for Endpoint.

Where should you configure the integration?

A. From the Microsoft 365 admin center, select Settings, and then select Services & add-ins.

B. From the Microsoft 365 security admin center, select Threat management, and then select Explorer.

C. From the Microsoft 365 admin center, select Reports, and then select Security & Compliance.

D. From the Microsoft 365 security admin center, select Threat management and then select Threat tracker.

arunjana Highly Voted 2 months, 3 weeks ago

B is correct.

Security & Compliance> In the navigation pane, choose Threat management > Explorer. In the upper right corner of the screen, choose Defender for Endpoint Settings (MDE Settings).

upvoted 5 times

kanag1 Most Recent 3 days, 6 hours ago

M365--> Security Portal --> Settings -->EndPoints -->General --> Advanced features -->Microsoft Intune connection

upvoted 1 times

Question #34 *Topic 2*

Your network contains an on-premises Active Directory domain. The domain contains servers that run Windows Server and have advanced auditing enabled.
The security logs of the servers are collected by using a third-party SIEM solution.
You purchase a Microsoft 365 subscription and plan to deploy Azure Advanced Threat Protection (ATP) by using standalone sensors.
You need to ensure that you can detect when sensitive groups are modified and when malicious services are created.
What should you do?

A. Turn off Delayed updates for the Azure ATP sensors.

B. Configure auditing in the Office 365 Security & Compliance center.

C. Turn on Delayed updates for the Azure ATP sensors.

D. Integrate SIEM and Azure ATP.

kiketxu Highly Voted 4 months, 3 weeks ago
Look at the answer and the clone question ref.
https://www.examtopics.com/discussions/microsoft/view/28219-exam-ms-500-topic-2-question-41-discussion/
upvoted 6 times

Question #35 *Topic 2*

You have an Azure Sentinel workspace that has an Azure Active Directory (Azure AD) connector and a Microsoft Office 365 connector.
You need to use a Fusion rule template to detect multistage attacks in which users sign in by using compromised credentials, and then delete multiple files from
Microsoft OneDrive.
Based on the Fusion rule template, you create an active rule that has the default settings.
What should you do next?

A. Add data connectors.

B. Add a workbook.

C. Add a playbook.

D. Create a custom rule template.

kiketxu 4 months, 3 weeks ago
Agree with B.
upvoted 2 times

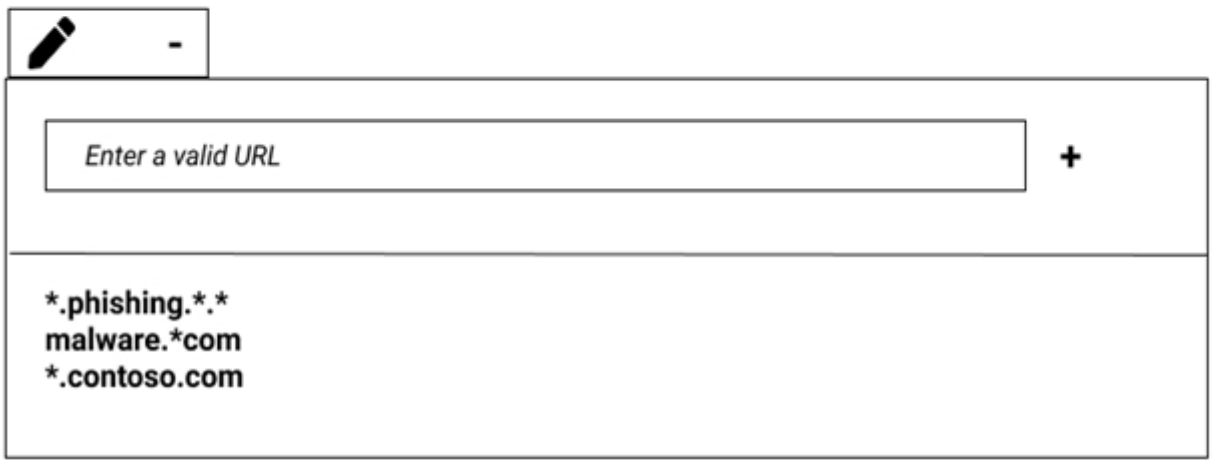
Question #36 *Topic 2*

You have a Microsoft 365 subscription that uses a default domain name of fabrikam.com.

You create a safe links policy, as shown in the following exhibit.

Safe links policy for your organization

Settings that apply to content across Office 365
When users click a blocked URL, they're redirected to a web page that explains why the URL is blocked.
Block the following URLs:



Settings that apply to content except email
These settings don't apply to email messages. If you want to apply them for email, create a safe links policy for email receipients.

Use safe links in:

☑ Office 356 ProPlus, Office for iOS and Android
☑ Office Online of above applications

For the locations selected above:
☑ Do not track when users click safe links:
☑ Do not let users click through safe links to original URL:

Which URL can a user safely access from Microsoft Word Online?

A. fabrikam.phishing.fabrikam.com

B. malware.fabrikam.com

C. fabrikam.contoso.com

D. www.malware.fabrikam.com

WoneSix Highly Voted 1 year, 6 months ago

Since the malware.*com filter has no leading wildcard, www.malware.fabrikam.com can be accessed. All others match one or the others of the filters.

upvoted 34 times

authentic Highly Voted 6 months, 1 week ago

The second option in the exam is: malware.*.com

upvoted 6 times

Yetijo 1 month, 3 weeks ago

Thanks, this was throwing me a bit.

upvoted 1 times

Joshing Most Recent 1 week, 1 day ago

You can tell there is a missing "." with malware.*com as if this was the case. Two answers would be allowed. B and D. Reasoning is that the URL's are malware.fabrikam.com and www.malware.fabrikam.com, the blocked URL setting is looking specifically for "malware.(TLD ending in "com") which neither of these are. They end .com and not like malware.examplecom if you get me.

There should only be one correct answer. So the correct setting in blocked URL would be malware.*.com as Authentic suggested.

As there is no preceding * in the blocked URL. The correct answer is D as the rule doesn't apply to subdomains unless you start it with "*.". If it were *.malware.*.com then D would be blocked also.

upvoted 1 times

Mary_Yvette 7 months, 2 weeks ago

I test this, and everything are blocked.

upvoted 2 times

Dasdweqs 8 months, 1 week ago

D seems correct to me. https://docs.microsoft.com/en-us/microsoft-365/security/office-365-security/atp-safe-links?view=o365-worldwide#block-the-following-urls-list-for-safe-links

upvoted 2 times

kiketxu 5 months ago

I would say the same after confirm that all these syntax are allowed to enter as blocked urls within safe links global policy settings .

upvoted 2 times

Shamos 8 months, 4 weeks ago

I think it should be B since its subdomain

upvoted 2 times

namco23 9 months ago

I think it should be B.
According to the image, the URL should start with malware

upvoted 2 times

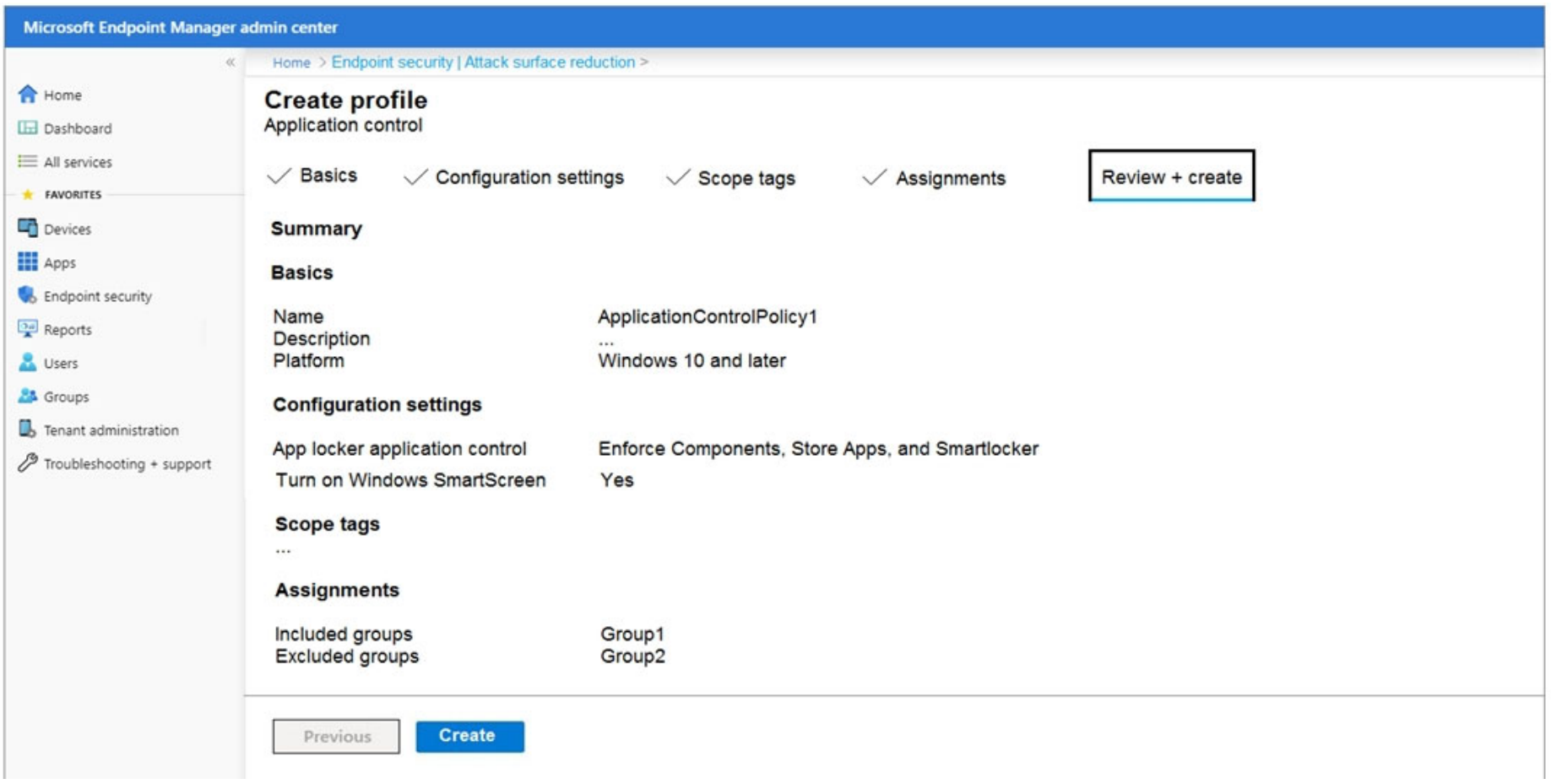
Question #37

Topic 2

HOTSPOT -

You have a Microsoft 365 tenant.

You create an attack surface reduction policy that uses an application control profile as shown in the following exhibit.



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

NOTE: Each correct selection is worth one point.

Hot Area:

Answer Area

When only a member of Group1 connects to a site that is identified as dangerous by application control, **[answer choice]**

- the site will open without warning
- the site will be blocked from opening
- the member will receive a security warning

When only a member of Group2 connects to a site that is identified as dangerous by application control, **[answer choice]**

- the site will open without warning
- the site will be blocked from opening
- the member will receive a security warning

kiketxu 4 months, 3 weeks ago

I would say given answers are correct as SmartScreen firstly shows a warning and exclusions are selected to avoid the policy.

upvoted 2 times

Question #38 *Topic 2*

DRAG DROP -

You have an on-premises Hyper-V infrastructure that contains the following:

- An Active Directory domain
- A domain controller named Server1
- A member server named Server2

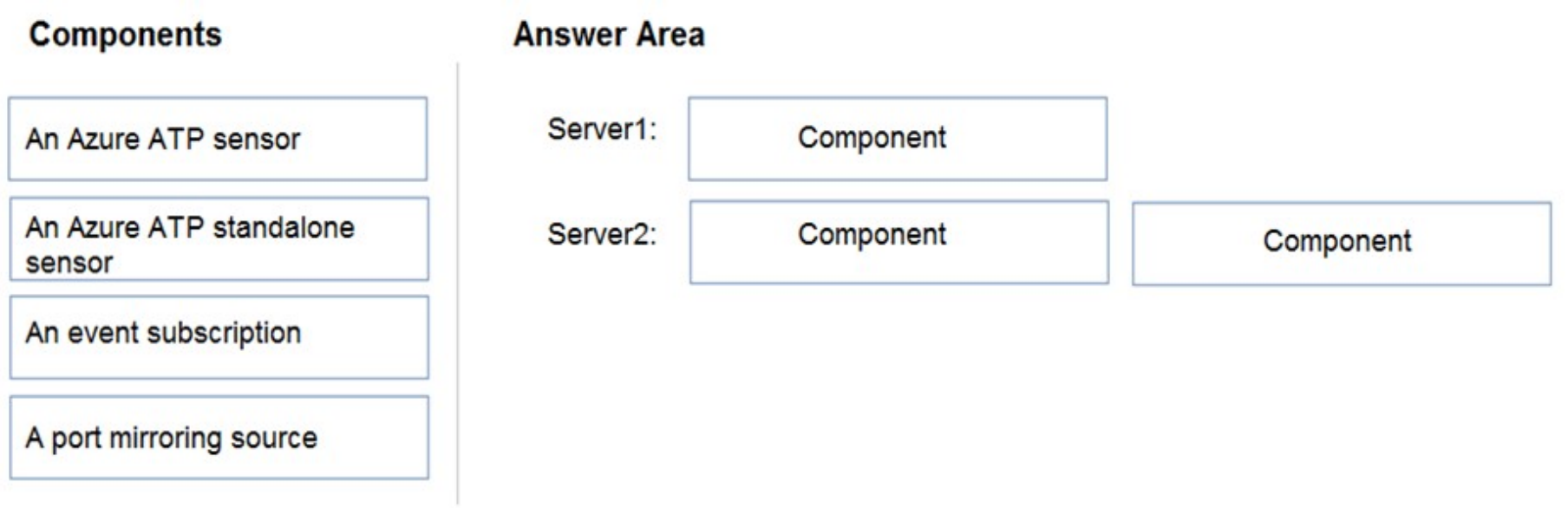
A security policy specifies that Server1 cannot connect to the Internet. Server2 can connect to the Internet.

You need to implement Azure Advanced Threat Protection (ATP) to monitor the security of the domain.

What should you configure on each server? To answer, drag the appropriate components to the correct servers. Each component may only 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.

Select and Place:



PeterC Highly Voted 4 months, 3 weeks ago

Correct is :
Server1 - a port mirroring Source
Server2 - an Azure ATP Standalone sensor & an Event subscription

"For port mirroring, configure port mirroring for each domain controller to be monitored, as the source"
https://docs.microsoft.com/en-us/defender-for-identity/configure-port-mirroring

"After you configured port mirroring from the domain controllers to the Defender for Identity standalone sensor, follow the following instructions to configure Windows Event forwarding using Source Initiated configuration."
https://docs.microsoft.com/en-us/defender-for-identity/configure-event-forwarding

upvoted 29 times

Joshing 1 week, 1 day ago

You shouldn't install standalone sensor on a DC. It most likely wouldn't allow you when it runs the checks on the server. So as everyone said the answer is wrong. Agreed with PeterC

upvoted 1 times

chaoscreater 1 month, 1 week ago

Agree. I've seen similar questions like this and DC requires port mirroring in all of them.

upvoted 1 times

TimurKazan 4 months ago

I would go with it too, as DC does not have Internet access it is logically correct that it should use port mirroring to some standalone sensor

upvoted 1 times

hhaywood 4 months, 3 weeks ago

Agreed

upvoted 2 times

Question #39 *Topic 2*

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

Name	Role
User1	Application administrator
User2	Security administrator
User3	Security operator
User4	User administrator

You need to identify which user can enable Microsoft Defender Advanced Threat Protection (Microsoft Defender ATP) roles.

Which user should you identify?

A. User1

B. User4

C. User3

D. User2

kiketxu Highly Voted 4 months, 3 weeks ago

Only GA and SA can assign roles in DFE.

upvoted 9 times

mashaeg Most Recent 2 months, 1 week ago

Initially, only those with Azure AD Global Administrator or Security Administrator rights will be able to create and assign roles in Microsoft Defender Security Center, therefore, having the right groups ready in Azure AD is important.

upvoted 1 times

Question #40 *Topic 2*

You have an Azure Sentinel workspace.

You need to manage incidents based on alerts generated by Microsoft Cloud App Security.

What should you do first?

A. From the Cloud App Security admin center, configure security extensions.

B. From the Cloud App Security admin center, configure app connectors.

C. From the Cloud App Security admin center, configure log collectors.

D. From the Microsoft 365 compliance center, add and configure a data connector.

TDAC Highly Voted 10 months, 1 week ago

Answer is correct. In Cloud App Security click the settings cog -> Security Extensions -> SIEM Agents -> Click the "Plus" -> Azure Sentinel.

BBQ Sauce: https://docs.microsoft.com/en-us/cloud-app-security/siem-sentinel

upvoted 9 times

kiketxu Most Recent 4 months, 3 weeks ago

A for sure!
https://docs.microsoft.com/en-us/cloud-app-security/siem-sentinel#integrating-with-azure-sentinel

upvoted 3 times

Question #41 *Topic 2*

Your network contains an on-premises Active Directory domain. The domain contains servers that run Windows Server and have advanced auditing enabled.
The security logs of the servers are collected by using a third-party SIEM solution.
You purchase a Microsoft 365 subscription and plan to deploy Azure Advanced Threat Protection (ATP) by using standalone sensors.
You need to ensure that you can detect when sensitive groups are modified and when malicious services are created.
What should you do?

A. Configure Event Forwarding on the domain controllers.

B. Configure auditing in the Office 365 Security & Compliance center.

C. Turn on Delayed updates for the Azure ATP sensors.

D. Enable the Audit account management Group Policy setting for the servers.

belyo 5 months ago
Given the statement there is a SIEM solution, event forwarding isnt necessary.
It should be a standalone sensor configuration not listed in answers...
upvoted 3 times

kiketxu 5 months ago
Agree with you.
upvoted 2 times

kiketxu 4 months, 3 weeks ago
Note: I'm agree, seems event forwarding ins't necessary if the SIEM is collecting. But given the answers, is the only choice here. Hope this will be fixed in the exam
upvoted 2 times

Cybersecgirl 12 months ago
This is the exact same question as the one above but totally different solution and choices? Can you please correct this Examtopics.
upvoted 4 times

Metasploit 11 months, 2 weeks ago
The answer to *this question is correct:

"These events can be received from your SIEM or by setting Windows Event Forwarding from your domain controller."

ref:
https://docs.microsoft.com/en-us/azure-advanced-threat-protection/configure-event-collection

****
Use for the other same Question above as well, Examtopics has the incorrect answer over there.
upvoted 7 times

Joepelus 10 months, 3 weeks ago
If you want to use SIEM you should integrate it. If you pick this "correct" answer your SIEM will break. Do we want that? no.
upvoted 2 times

Question #42 *Topic 2*

Several users in your Microsoft 365 subscription report that they received an email message without the attachment.
You need to review the attachments that were removed from the messages.
Which two tools can you use? Each correct answer presents a complete solution.
NOTE: Each correct selection is worth one point.

A. the Exchange admin center

B. the Azure ATP admin center

C. Outlook on the web

D. the Security & Compliance admin center

E. Microsoft Azure Security Center

rdy4u Highly Voted 1 year, 1 month ago
https://docs.microsoft.com/en-us/microsoft-365/security/office-365-security/manage-quarantined-messages-and-files?view=o365-worldwide

Use the Security & Compliance Center to manage quarantined email messages
Use Exchange Online PowerShell or standalone EOP PowerShell to view and manage quarantined messages and files
upvoted 14 times

Cbruce Most Recent 1 month, 3 weeks ago
This is an old question and the quarantine cannot be viewed in Exchange any longer. From the Exchange Admin center, quarantine, this pops up: "Quarantine has a new home and improved functionality. By December 1, 2020 – the quarantine experience will be removed from the Exchange admin center. Please use the updated experience in the Security and Compliance Center, Quarantine page. Learn more about the new quarantine experience."
upvoted 4 times

Robert__Susin 2 weeks, 4 days ago
Isnt on Security and Compliance anymore, now is under Defender 365 Portal
upvoted 2 times

Paulmtx 6 months, 3 weeks ago
Documentation talks about Security Center and Exchange Powershell. How can the Exchange Admin center be a correct answer?? For those who claim that Exchange Admin center is correct, please show the path/screens in the EXO admin center where you can see the deleted attachments, please, because I couldn't find it.
upvoted 2 times

kiketxu 5 months ago
A & D. From both, EXO Classic and SCC portal. (Not found quarantine in the new EXO portal btw)
upvoted 2 times

Marsh 5 months, 4 weeks ago
Not sure how to post a screenshot. Here is the statement shown in my EAC - "Quarantine has a new home and improved functionality. By December 1, 2020 – the quarantine experience will be removed from the Exchange admin center. Please use the updated experience in the Security and Compliance Center".
upvoted 3 times

shanti0091 6 months, 2 weeks ago
It's simple, if you've been working with an Exchange environment, EOP policies can prevent attachment due to policies set. this was a norm before the introduction of ATP.
upvoted 3 times

svm_Terran 8 months ago
A,D are correct.
upvoted 2 times

Vishbsoni 8 months, 2 weeks ago
You view and manage quarantined messages in the Security & Compliance Center or in PowerShell (Exchange Online PowerShell for Microsoft 365 organizations with mailboxes in Exchange Online; standalone EOP PowerShell for organizations without Exchange Online mailboxes)

https://docs.microsoft.com/en-us/microsoft-365/security/office-365-security/manage-quarantined-messages-and-files?view=o365-worldwide#manage-quarantined-messages-and-files-as-an-admin-in-eop:~:text=You%20view%20and%20manage%20quarantined%20messages,for%20organizations%20without%20Exchange%20Online%20mailboxes).
upvoted 2 times

karank19 9 months ago
Correct Answer: AD
upvoted 4 times

Question #43 *Topic 2*

You have a hybrid Microsoft 365 deployment that contains the Windows 10 devices shown in the following table.

Name	Trusted Platform Module (TPM) version	Joined to	Microsoft Intune enrolled
Device1	v2.0	Active Directory	Yes
Device2	v2.0	Azure Active Directory (Azure AD)	Yes
Device3	v1.3	Azure Active Directory (Azure AD)	Yes

You assign a Microsoft Endpoint Manager disk encryption policy that automatically and silently enables BitLocker Drive Encryption (BitLocker) on all the devices.

Which devices will have BitLocker enabled?

A. Device1, Device2, and Device3

B. Device2 only

C. Device1 and Device2 only

D. Device2 and Device3 only

ZakS 2 months, 1 week ago

B - Device 2 Only. Ans is correct.
Please refer to article.

https://docs.microsoft.com/en-us/mem/intune/protect/encrypt-devices#manage-bitlocker

A device must meet the following conditions to be eligible for silently enabling BitLocker:

If end users log in to the devices as Administrators, the device must run Windows 10 version 1803 or later.
If end users log in to the the devices as Standard Users, the device must run Windows 10 version 1809 or later.
The device must be Azure AD Joined or Hybrid Azure AD Joined.
Device must contain TPM (Trusted Platform Module) 2.0
The BIOS mode must be set to Native UEFI only.

upvoted 2 times

Resquia 2 months, 3 weeks ago

B is correct.

A device must meet the following conditions to be eligible for silently enabling BitLocker:

If end users log in to the devices as Administrators, the device must run Windows 10 version 1803 or later.
If end users log in to the the devices as Standard Users, the device must run Windows 10 version 1809 or later.
The device must be Azure AD Joined or Hybrid Azure AD Joined.
Device must contain TPM (Trusted Platform Module) 2.0
The BIOS mode must be set to Native UEFI only.

upvoted 2 times

Question #44 *Topic 2*

HOTSPOT -

You have an Azure Sentinel workspace.

You configure a rule to generate Azure Sentinel alerts when Azure Active Directory (Azure AD) Identity Protection detects risky sign-ins. You develop an Azure

Logic Apps solution to contact users and verify whether reported risky sign-ins are legitimate.

You need to configure the workspace to meet the following requirements:

☞ Call the Azure logic app when an alert is triggered for a risky sign-in.

☞ To the Azure Sentinel portal, add a custom dashboard that displays statistics for risky sign-ins that are detected and resolved.

What should you configure in Azure Sentinel to meet each requirement? To answer, select the appropriate options in the answer area.

NOTE: Each correct selection is worth one point.

Hot Area:

Answer Area

Call the logic app: [▼]
- An entity mapping
- A hunting query
- A notebook
- A playbook
- A workbook

Displays statistics for risky sign-ins: [▼]
- An entity mapping
- A hunting query
- A notebook
- A playbook
- A workbook

fred99 Highly Voted 3 months ago

to display stats, should not it be Workbook instead of playbook?

upvoted 14 times

prabhjot 6 days, 21 hours ago

playbook (logic app) is for integration only so therefor to display reports and sats- Workbook shines

upvoted 1 times

arunjana 2 months, 3 weeks ago

Absolutely right. Answers should be 1) Playbook, 2) Workbook

upvoted 8 times

M1crsoftPro Most Recent 2 months ago

call the logic app is indeed the playbook
display the risky sing in logs is workbook
https://docs.microsoft.com/en-gb/azure/azure-monitor/visualize/workbooks-overview

upvoted 1 times

saregi 2 months ago

Please review the correct response because I highly doubt a playbook can display statistics in a custom dashboard as others have noticed already. A workbook is the right tool for that job.

upvoted 2 times

Topic 3 - Question Set 3

Question #1 *Topic 3*

You have a Microsoft 365 subscription that includes a user named User1.
You have a conditional access policy that applies to Microsoft Exchange Online. The conditional access policy is configured to use Conditional Access App
Control.
You need to create a Microsoft Cloud App Security policy that blocks User1 from printing from Exchange Online.
Which type of Cloud App Security policy should you create?

A. an app permission policy

B. an activity policy

C. a Cloud Discovery anomaly detection policy

D. a session policy

Vishbsoni Highly Voted 8 months, 2 weeks ago
The answer is D: Session Policy
Enforce read-only mode for external users in real time
Prevent company data from being exfiltrated by external users, by blocking print and copy/paste activities in real-time, utilizing Cloud App Security's session controls.

https://docs.microsoft.com/en-us/cloud-app-security/policies-information-protection#enforce-read-only-mode-for-external-users-in-real-time:~:text=.-,Enforce%20read%2Donly%20mode%20for%20external%20users%20in%20real%20time,Prevent%20company%20data%20from%20being%20exfiltrated%20by%20external%20users%2C%20by%20blocking%20print%20and%20copy%2Fpaste%20activities%20in%20real%2Dtime%2C%20utilizing%20Cloud%20App%20Security's%20session%20controls.,-Prerequisites
upvoted 14 times

TonySuccess Highly Voted 7 months, 4 weeks ago
I tried to test this in Cloud App Security and to be honest as a novice in CAS I was struggling. My results were inconclusive, so I sent Microsft an Email and they replied confirming the given answer is correct.

This is completed by creating a Session Control Policy in CAS. Then 'Use Custom Policy' in Conditional Access and select the policy you created in Cloud App Security from the list.

x
upvoted 9 times

Joshing Most Recent 1 week, 1 day ago
The correct answer is a Session Policy.

You set up a Session policy. Session control type of Block. Put in the filter for the activity of printing and then use the action to block.

Activity Policies are for generating alerts and using Governance action to Suspend users etc. Based on x activity or repeat activities suspend user/confirm user compromised etc.
upvoted 1 times

TimurKazan 3 months ago
I have tested this in lab, it is D- Session Policy
upvoted 2 times

Vishbsoni 8 months, 2 weeks ago
With the access and session policies, you can:

Prevent data exfiltration: You can block the download, cut, copy, and print of sensitive documents on, for example, unmanaged devices.

https://docs.microsoft.com/en-us/cloud-app-security/proxy-intro-aad#how-it-works:~:text=With%20the%20access%20and%20session%20policies%2C,documents%20on%2C%20for%20example%2C%20unmanaged%20devices.
upvoted 4 times

kiketxu 5 months ago
Thanks for the research and highlinting dude! ;)
upvoted 1 times

ellik 3 months, 2 weeks ago
Session control applies to browser-based apps.
To block access from mobile and desktop apps, create an Access policy
upvoted 1 times

LoFix 8 months, 3 weeks ago

Why not "Activity policy", we can define there an "Activity type" filter?
https://docs.microsoft.com/en-us/cloud-app-security/user-activity-policies

upvoted 1 times

musiman 8 months, 3 weeks ago

I also think it's B, an activity policy. You cannot select the option to deny printing is a session policy (I can't find it there). So, I would choose answer B.

upvoted 1 times

ellik 3 months, 2 weeks ago

Session control applies to browser-based apps.
To block access from mobile and desktop apps, create an Access policy

upvoted 1 times

vishg 6 months, 1 week ago

What is the correct answer?

upvoted 1 times

Omar89 1 year, 7 months ago

reference: https://docs.microsoft.com/en-us/cloud-app-security/session-policy-aad

upvoted 4 times

Question #2 *Topic 3*

HOTSPOT -

You have a Microsoft 365 E5 subscription.

From Microsoft Azure Active Directory (Azure AD), you create a security group named Group1. You add 10 users to Group1.

You need to apply app enforced restrictions to the members of Group1 when they connect to Microsoft Exchange Online from non-compliant devices, regardless of their location.

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

NOTE: Each correct selection is worth one point.

Hot Area:

Answer Area

From the Azure portal, create a conditional access policy and configure:

Users and groups, Cloud apps, and Session settings Users and groups, Cloud apps, and Conditions settings Users and groups, Conditions, and Session settings	V

From an Exchange Online Remote PowerShell session, run:

New-OwaMailbox Policy and Set-OwaMailboxPolicy New-ClientAccessRule and Test-ClientAccessRule Get-CASMailbox and Set-CASMailbox	V

kiketxu Highly Voted 4 months, 3 weeks ago

I would say both are correct. Look at this article:
https://techcommunity.microsoft.com/t5/outlook-blog/conditional-access-in-outlook-on-the-web-for-exchange-online/ba-p/267069

Also you can find there the old thread discussion:
https://www.examtopics.com/discussions/microsoft/view/6139-exam-ms-500-topic-3-question-8-discussion/

upvoted 7 times

ellik 3 months, 2 weeks ago

yes , the cmdlet is Set-OwaMailboxPolicy. That cmdlet contains the parameter ConditionalAccessPolicy.

upvoted 1 times

Joshing Most Recent 1 week ago

Correct answer for 1 is Users and Groups, Cloud Apps, Session.

You then configure a new OwaMailboxPolicy and then set the ConditionalAccessPolicy setting with either ReadOnly or the ReadOnly and blocking attachments. You can then assign the policy to individual mailboxes.

Documentation: https://techcommunity.microsoft.com/t5/outlook-blog/conditional-access-in-outlook-on-the-web-for-exchange-online/ba-p/267069

upvoted 1 times

james1 1 month, 3 weeks ago

This is not possible with the given answers, not anymore atleast since targeting of non-compliant devices has moved to Conditions (Now in Preview)
Users and Groups to target -> Group 1
Cloud Apps to select -> Exchange Online
Conditions to target -> Non-compliant devices
Session to apply -> app-enforced restrictions

upvoted 1 times

ZakS 2 months, 1 week ago

First one should be Users and Groups, Cloud Apps, Session

Second one is correct.

https://techcommunity.microsoft.com/t5/outlook-blog/conditional-access-in-outlook-on-the-web-for-exchange-online/ba-p/267069

upvoted 2 times

averyfree 3 months ago

Answer A is wrong. You don't need to specify any conditions. It also says you need to enforce App Enforced Restrictions which is an option you can select in Session.

Correct answer is Users and Groups, Cloud Apps, Session

upvoted 3 times

TimurKazan 3 months ago

Actually, this should be - Users and groups - Cloud Apps - Conditions - Session
but there is no such answer

upvoted 3 times

prats005 4 months ago

Which one is correct? | https://c7solutions.com/2018/12/read-only-and-attachment-download-restrictions-in-exchange-online

upvoted 1 times

PeterC 4 months, 3 weeks ago

1. correct, 2. incorrect.

2. is : New-ClientAccessRule, Test-ClientAccessRule
https://docs.microsoft.com/en-us/powershell/module/exchange/new-clientaccessrule?view=exchange-ps

upvoted 1 times

PeterC 4 months, 3 weeks ago

It is get/Set-casmailbox here you can block devices!
https://docs.microsoft.com/en-us/powershell/module/exchange/set-casmailbox?view=exchange-ps

upvoted 1 times

Question #3 *Topic 3*

SIMULATION -

You discover that Microsoft SharePoint content is shared with users from multiple domains.

You need to allow sharing invitations to be sent only to users in an email domain named contoso.com.

To complete this task, sign in to the Microsoft 365 portal.

Sido1 4 months, 3 weeks ago

correct

upvoted 2 times

shanti0091 6 months, 1 week ago

The steps are accurate.

upvoted 1 times

Question #4 *Topic 3*

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. You create a label named CompanyConfidential in Microsoft Azure Information Protection. You add CompanyConfidential to a global policy.
A user protects an email message by using CompanyConfidential and sends the label to several external recipients. The external recipients report that they cannot open the email message.
You need to ensure that the external recipients can open protected email messages sent to them.
You modify the encryption settings of the label.
Does that meet the goal?

A. Yes

B. No

javilova Highly Voted 1 year, 7 months ago
needs to resend email in order to apply changes in the label.
upvoted 9 times

averyfree Most Recent 3 months ago
This is incorrect. You DO go to Encryption settings to modify permissions for users/groups to access the files with the label applied. You can add external users here.
upvoted 3 times

kiketxu 5 months ago
Modify encryption isn't enough to resolve this escenario. You need to add external users into the "encryption" settings within the label, but then, you need to relabel the document or message and send it again.
This answer is correct to me.
upvoted 4 times

kiketxu 4 months, 3 weeks ago
I believe it don't need to relabel, just opening the file and saving again it will take the new published permissions. Mandatory send it back as they are externals.
upvoted 1 times

melki_zedek 8 months, 3 weeks ago
"In addition to reauthentication, the encryption settings and user group membership is reevaluated. This means that users could experience different access results for the same document or email if there are changes in the encryption settings or group membership from when they last accessed the content."
https://docs.microsoft.com/en-us/microsoft-365/compliance/encryption-sensitivity-labels?view=o365-worldwide

So changes in setting will affect the encryption but because the email is already sent the old policy will stay with it until the default use license validity period for a tenant is 30 days. So the missing word to make this a good answer is "Instruct the user to resend the message"
upvoted 3 times

pmr123 10 months, 3 weeks ago
I was thinking if we remove the encryption then users can able to view it without any restrictions..whats the deal here and why they said no
upvoted 1 times

NatP 9 months ago
I think the scenario is that the label is for confidential internal information, thus the name. Removing the encryption defeats the purpose especially, having the label name as CompanyConfidential and then sending it out to external recipients.
upvoted 2 times

luutuananh 10 months, 2 weeks ago
I think you also need to change the permission, chaging only the encryption settings is not enough.
upvoted 1 times

melki_zedek 8 months, 3 weeks ago
permissions is part of the Encryption Setting. Ref try creating a sensitivity label in M365 Security & Compliance
upvoted 4 times

wasmith12 1 year, 1 month ago
I think this is actually the correct answer
https://docs.microsoft.com/en-us/microsoft-365/compliance/encryption-sensitivity-labels?view=o365-worldwide
upvoted 2 times

SUBZER0 11 months ago

if you remove the encryption then is not protected anymore.
you have to ensure that thre recipients can open PROTECTED email messages

upvoted 3 times

TimurKazan 3 months ago

SUBZERO, there are no words about removing, it says "changing"
you can add external users in encryption settings

upvoted 1 times

wasmith12 1 year, 1 month ago

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

upvoted 1 times

profitchannel 1 year, 6 months ago

Not sure if he really needs to resend the e-mail. As long as the label ID stays the same, a lookup for the label rules will happen. And if the encryption settings changes to allow specific external recipient access to the content, these external users now can access the content.
Can anybody verify this?

upvoted 1 times

WoneSix 1 year, 6 months ago

Nope. Your encryption settings don't change who has access to the item. You need to change the groups to whom the label is available to include everyone.

upvoted 7 times

NatP 9 months ago

Agree. The document inherits any restrictions that comes with the label upon application. Any changes made after that don't change the restrictions on the document that were applied with the label prior.

upvoted 1 times

Question #5 *Topic 3*

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. You create a label named CompanyConfidential in Microsoft Azure Information Protection. You add CompanyConfidential to a global policy.
A user protects an email message by using CompanyConfidential and sends the label to several external recipients. The external recipients report that they cannot open the email message.
You need to ensure that the external recipients can open protected email messages sent to them.
You modify the content expiration settings of the label.
Does that meet the goal?

A. Yes

B. No

AlistairMarini Highly Voted 1 year, 2 months ago
No. content expiration doesn't change who has access to the item. Need to change the groups to whom the label is available
upvoted 7 times

WoneSix Highly Voted 1 year, 6 months ago
Modifying the expiration won't allow the external users to view the message, regardless of whether the email is resent or not.
upvoted 7 times

kiketxu Most Recent 5 months ago
B for sure.
upvoted 1 times

pmr123 10 months, 3 weeks ago
I am not understanding, why content expiration won't allow external users to view messages.If we extend the expiry date until that date they can access the content right.Whats wrong tin this.
upvoted 1 times

NatP 9 months ago
I also think that the question is poorly written. I think it should say that email protected with the label was sent to external users instead of label was sent to external users.
upvoted 1 times

NatP 9 months ago
Ìt doesn't allow them because the name itself gives the idea that the encryption applies to employees only. External recipients, from the start, have no access to the document or not part of the allowed users. Thus, modifying retention doesn't do anything related to external user access.
upvoted 1 times

javilova 1 year, 7 months ago
needs to resend email in order to apply changes in the label.
upvoted 3 times

Question #6 *Topic 3*

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 a Microsoft Azure Active Directory (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	Office 365	Assigned
Group14	Mail-enabled security group	Assigned

You create an Azure Information Protection policy named Policy1.

You need to apply Policy1.

To which groups can you apply Policy1? To answer, select the appropriate options in the answer area.

NOTE: Each correct selection is worth one point.

Hot Area:

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

kiketxu Highly Voted 4 months, 3 weeks ago

Question 1 - Mail Enabled Groups Only.
https://docs.microsoft.com/en-us/azure/information-protection/prepare#azure-information-protection-requirements-for-user-accounts
Question 2 - No Security Groups allowed.
https://docs.microsoft.com/en-us/azure/information-protection/prepare#azure-information-protection-requirements-for-group-accounts

From the old discussion thread:
https://www.examtopics.com/discussions/microsoft/view/12234-exam-ms-500-topic-3-question-12-discussion/

upvoted 11 times

w00t 4 months, 1 week ago

Thank you!

upvoted 1 times

lime568 Most Recent 2 weeks, 2 days ago

To be easy: the supported groups must to have an email address

upvoted 1 times

Ocico 2 months, 3 weeks ago

mail-enabled sec groups are supported: https://docs.microsoft.com/en-us/azure/information-protection/prepare#azure-information-protection-requirements-for-group-accounts

upvoted 1 times

Question #7

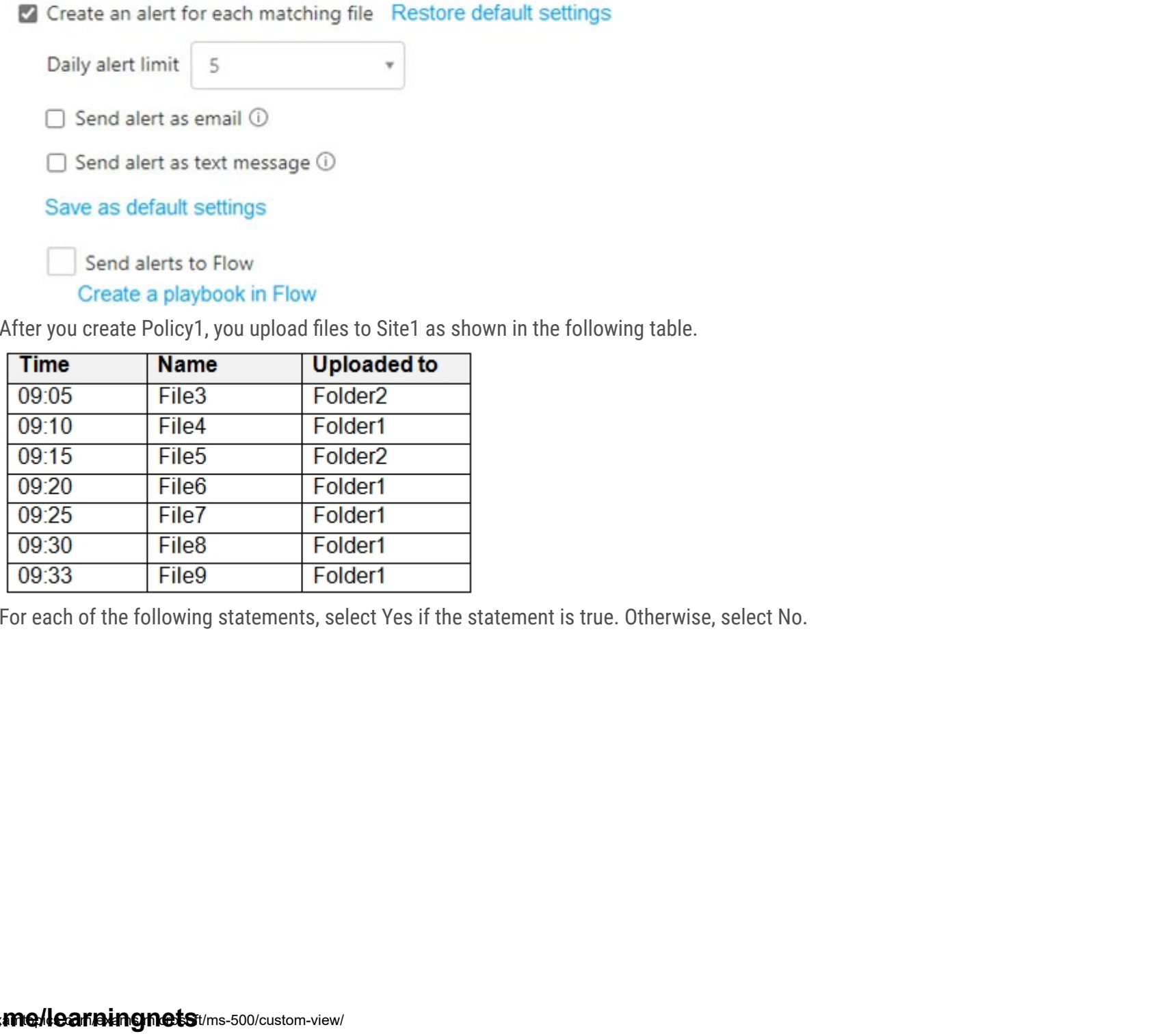
Topic 3

HOTSPOT -

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

Name	File in folder
Folder1	File1
Folder2	File2

At 09:00, you create a Microsoft Cloud App Security policy named Policy1 as shown in the following exhibit.



After you create Policy1, you upload files to Site1 as shown in the following table.

Time	Name	Uploaded to
09:05	File3	Folder2
09:10	File4	Folder1
09:15	File5	Folder2
09:20	File6	Folder1
09:25	File7	Folder1
09:30	File8	Folder1
09:33	File9	Folder1

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

NOTE: Each correct selection is worth one point.

Hot Area:

Answer Area

Statements	Yes	No
File1 triggers an alert from Policy1.	○	○
File3 triggers an alert from Policy1.	○	○
File9 triggers an alert from Policy1.	○	○

Sugar123 Highly Voted 4 months, 3 weeks ago

The conditions of the policy is that an alert will be created for any of the files in Folder 1 of Microsoft Sharepoint. However, the alert limit is set at 5. After the 5th alert, there will be no more alerts.

From this rationale, File 1 triggers an alert since it is already in the Sharepoint Folder 1. File 3 does not trigger an alert because it is in Folder 2 (not applicable to the policy). File 9 does not trigger an alert because it would be the 6th alert and the alert threshold is 5.

upvoted 37 times

kiketxu 4 months, 3 weeks ago

Bit confused as the statment does not clarifies it's a file policy.
Perfectly explained @Sugar123, thanks.

upvoted 3 times

b00 4 months, 3 weeks ago

Thanks Sugar123 !

upvoted 1 times

b00 Highly Voted 4 months, 3 weeks ago

I do not understand the logic here.

upvoted 6 times

kazaki Most Recent 4 months, 2 weeks ago

1 & 9 shall create alerts

upvoted 2 times

Sido1 4 months, 3 weeks ago

confusing

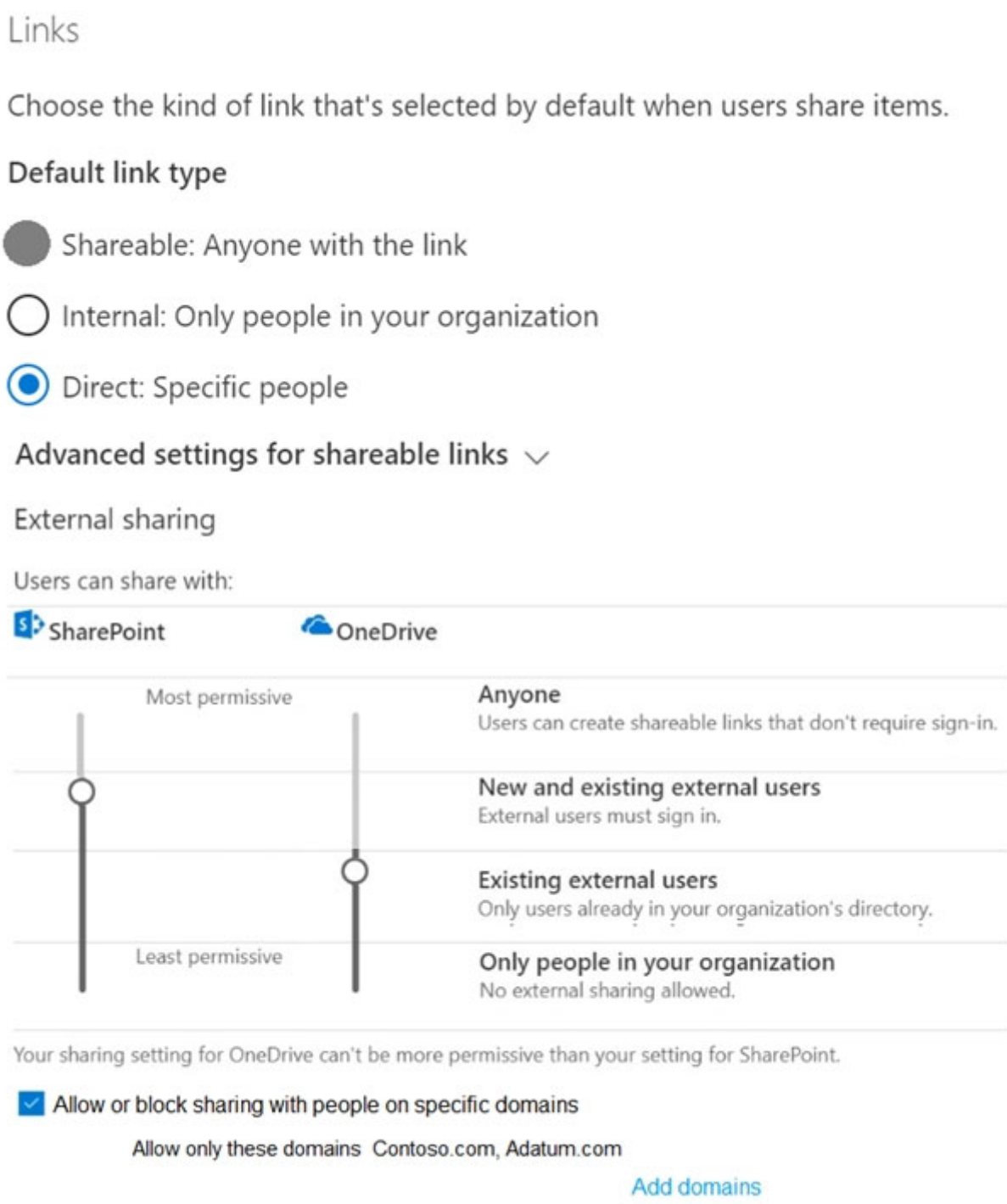
upvoted 4 times

Question #8 *Topic 3*

HOTSPOT -

You have a Microsoft 365 subscription that uses a default domain name of litwareinc.com.

You configure the Sharing settings in Microsoft OneDrive as shown in the following exhibit.



Hot Area:

Answer Area

A user who has an email address of user1@fabrikam.com

- cannot access OneDrive content
- can access OneDrive content after a link is created
- must be added to a group before the user can access shared files

If a new guest user is created for user2@contoso.com,

- the user cannot access OneDrive content
- the user can access OneDrive content after a link is created
- must be added to a group before the user can access shared files

kiketxu Highly Voted 4 months, 3 weeks ago

given answers are right to me. Fabrikam isn't allowed, however Contoso it is.

upvoted 10 times

ellik Most Recent 3 months, 2 weeks ago

I got confused with this question as when you choose specific domain , there is message saying that , These limitations will not apply when users share files and folders using Anyone links. in this question Anyone with the link is selected ! please help

upvoted 1 times

GeO15 1 month, 1 week ago

Anyone with the link - This option is available only if your external sharing setting is set to "Anyone." (https://docs.microsoft.com/en-us/sharepoint/turn-external-sharing-on-or-off) - The "Anyone with the link setting is greyed out" I think the second answer should be "must be added to a group".

upvoted 1 times

TimurKazan 3 months, 3 weeks ago

what does it mean "after a link is created"?

upvoted 1 times

TimurKazan 3 months, 3 weeks ago

if onedrive in this question permits only existing users, how new guest can have access?

upvoted 2 times

AJWYATT79 3 months, 1 week ago

Existing guests
Allow sharing with only people already in your directory. These users may exist in your directory because they previously accepted sharing invitations or because they were manually added. (You can tell an external user because they have #EXT# in their user name.) It states "after the user is created", so the guest account must have been created manually

upvoted 4 times

chaoscreater 1 month ago

where does it state "after the user is created"? All it says is "if a new guest user is created", which means it hasn't been done already, hence IF.

upvoted 2 times

Joshing 5 days ago

They are saying "If a new guest user is created" as in for the following answer consider the guest will be created before the link is shared with them.

So there will be an "Existing Guest" for the last question. So they can have a share link created for them as they are both on the allowed domain list and have a guest account.

They wouldn't include the statement "if a new guest user is created" without wanting you to consider that for the answer. They may as well not have said a thing and you would answer they couldn't access onedrive.

I have used this process for a client before who were restrictive. I changed their sharing policy to be less restrictive and allow Existing Guests and got appropriate permission to create the guest user and asked the user to create share link with a specific person. Worked fine from there.

upvoted 1 times

Question #9 *Topic 3*

HOTSPOT -

You have a Microsoft 365 subscription that uses an Azure Active Directory (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 thatа€™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 thatа€™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.

Hot Area:

Statements	Yes	No
External users can access File1	○	○
The users in contoso.com can access File2	○	○
External users can access File3	○	○

jack987 Highly Voted 1 year, 1 month ago

Answer:
No - No - No
All of them will match Rule2 because it is the most restrictive.

When content is evaluated against rules, the rules are processed in priority order. If content matches multiple rules, the rules are processed in priority order and 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: only notifies users

Rule 5: restricts access

Rule 6: notifies users, restricts access, and does not allow user overrides

Source: https://docs.microsoft.com/en-us/microsoft-365/compliance/data-loss-prevention-policies?view=o365-worldwide
upvoted 39 times

paperinop541 2 months, 3 weeks ago
the users in contoso.com can access to the file because they are internal, no ?
upvoted 3 times

chaoscreater 1 month ago
Did you not read jack's comment? - "If content matches multiple rules, the rules are processed in priority order and the most restrictive action is enforced". File2 has both label1 and label2 applied. Rule2 condition applies to label1 or label2 and the action is restrict access to the content. It doesn't care about if the user is internal or external.
upvoted 2 times

gills Highly Voted 1 year, 3 months ago
Should be NO-NO-NO. As per the URL, https://docs.microsoft.com/en-us/microsoft-365/compliance/data-loss-prevention-policies?view=o365-worldwide#the-priority-by-which-rules-are-processed, "When content is evaluated against rules, the rules are processed in priority order. If content matches multiple rules, the rules are processed in priority order and the most restrictive action is enforced."

So all three rules are evaluated and Rule 2 is the most restrictive and that applies.
upvoted 18 times

Dooa Most Recent 5 months, 1 week ago
@smoo is right..
YES, = user can override and rule is on highest priority
NO, 2nd rule causing this
NO, Third rule causing this.
upvoted 2 times

kiketxu 5 months ago
yeah, but once it pass that override matches with the rule 2, so external user won't ever access to file1.
I will expect similar questions for DLP, hope they will much clear than here. It hasn't sense the thirth policy and nobody will access to Label2 files.
upvoted 2 times

CalST 5 months, 2 weeks ago
https://docs.microsoft.com/en-us/microsoft-365/compliance/sensitivity-labels?view=o365-worldwide a doc can have both a retention lanel and sensitivy label. Given Doc 2 has both labels (and this is possible as DLP can use retention or senstivity labels) then both policy 1 and 2 apply to Doc 2. Then most restrictive setting applies ie Policy 2. Block all access
upvoted 1 times

Marsh 5 months, 3 weeks ago
I agree with the answer (Yes-No-No). One small thing is that each file can only have one sensitivity label. It is not possible for File2 has both Labe1 and Label2 applied.
upvoted 2 times

PeeyushS 5 months, 4 weeks ago
THere are two parts to this Question : One is Rules and Other is Priority. If multiple rules are there with same priority then most restrictive should apply. However if the priorities are different then 0 highest priority will be applied. It appears the priority will take a more importance here 1st. So the answer seems to be correct. If someone can test that will be great.
upvoted 2 times

Andy555 6 months, 2 weeks ago
https://docs.microsoft.com/en-us/microsoft-365/compliance/data-loss-prevention-policies?view=o365-worldwide
When content is evaluated against rules, the rules are processed in priority order. If content matches multiple rules, the rules are processed in priority order and 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: only notifies users

Rule 5: restricts access

Rule 6: notifies users, restricts access, and does not allow user overrides
upvoted 2 times

B1G_B3N 6 months, 3 weeks ago
Answer is no no no. In black and white from MS Docs "When content is evaluated against rules, the rules are processed in priority order. If content matches multiple rules, the rules are processed in priority order and the most restrictive action is enforced."

This states regardless of priority if a label matches multiple rules the most restriction is enforced.
upvoted 2 times

Dhanger 10 months ago

Yes-No-Yes
Label one has override On
Label one condition is only for external users so label two applies for internal users
Label two blocks access for everyone

upvoted 1 times

TonySuccess 8 months ago

But rule 1 applies to both Labels and has Piroty 1, which means it is king of the hill. Renders the other rules applying to the labels useless.

Rule 2:
-Conditions: Label1 or Label2
-Actions: Restrict access to the content
-Priority: 1

All Files are covered by label 1 and 2 therefore ain't nobody getting their paws on the files.

No, No, No.

x

upvoted 4 times

kiketxu 5 months ago

I'm with you too

upvoted 1 times

dzampar 10 months, 2 weeks ago

I'm convinced that all 3 options are NO as they match the most restrictive rule despite the priority order.

"When content is evaluated against rules, the rules are processed in priority order. If content matches multiple rules, the rules are processed in priority order and the most restrictive action is enforced."

https://docs.microsoft.com/en-us/microsoft-365/compliance/data-loss-prevention-policies?view=o365-worldwide

upvoted 4 times

gustangelo 1 year, 1 month ago

The answer is correct. If Microsoft 365 docs talk about it. The use can justify and send, share or modify the content. See here:
https://docs.microsoft.com/en-us/microsoft-365/compliance/data-loss-prevention-policies?view=o365-worldwide

upvoted 1 times

VTHAR 10 months, 3 weeks ago

Rule 2 in the question is the most restrictive which is in turn enforced for this scenario and it also doesn't allow user override. Therefore, the answer would be NO-NO-NO.

upvoted 2 times

STFN2019 1 year, 1 month ago

all No's unless there is a typo in the question.

upvoted 3 times

Smoo 1 year, 2 months ago

I think it is Yes-No-No
Rule 1 is "Actions: Restrict access to the content for external users" but allows user overrides, that means a contoso.com (internal user) could overwrite it and allow external user access:

File 2 is " Actions: Restrict access to the content" - subtly different, this restricts it to everyone including contoso users

File 3 again is restrict access to the content - again everyone is blocked

upvoted 2 times

xofowi5140 1 year, 3 months ago

Why File2 is NO?
The users are in contoso.com

upvoted 2 times

shaan6810 1 year, 1 month ago

Because Rule 2 restricts access to content, despite being internal or external

upvoted 4 times

yaco33 1 year, 4 months ago

Internal users can override the policy, no external users so NO-NO-NO

upvoted 4 times

nitram 1 year, 8 months ago

Must be three times "no" see link
https://docs.microsoft.com/en-us/microsoft-365/compliance/data-loss-prevention-policies
roughly in the middle of the page

upvoted 13 times

Mehodge 1 year, 4 months ago

Anchored Link
https://docs.microsoft.com/en-us/microsoft-365/compliance/data-loss-prevention-policies?view=o365-worldwide#the-priority-by-which-rules-are-processed

upvoted 3 times

WoneSix 1 year, 6 months ago

I agree with you, nitram, since DLP will use the most restrictive policy. Both label1 and label2 are in Rule2, which is the most restrictive. It blocks everything that is done with label1 or label2.

upvoted 7 times

Jogre 1 year, 4 months ago

Rule2 is lower priority than Rule1. Rule1 allows them to access file via override and at that point the rules would stop processing before it gets to Rule2 which would block without override.

upvoted 3 times

btd2020 1 year, 2 months ago

I agree with Wonesix "When content is evaluated against rules, the rules are processed in priority order. If content matches multiple rules, the rules are processed in priority order and the most restrictive action is enforced." https://docs.microsoft.com/en-us/microsoft-365/compliance/data-loss-prevention-policies?view=o365-worldwide#the-priority-by-which-rules-are-processed

upvoted 1 times

Windows311 1 year, 4 months ago

By this logic, File2 should also be YES.
Answer is IMO correct, YES-NO-NO because:
File1 restriction can be overridden as pr Rule1 (Label1)
File2 and File3 cannot be overridden as pr Rule2, the most restrictive (Label2)

upvoted 6 times

Smemory 1 year, 9 months ago

Why the first answer is "YES"?

upvoted 2 times

lindyd 1 year, 8 months ago

User override is on meaning user can bypass the policy but needs to provide a justification

upvoted 2 times

WoneSix 1 year, 6 months ago

But user override is on for both rule 1 and rule 3, so your logic has a flaw.

upvoted 3 times

wizrd049 1 year, 4 months ago

But the priority sets 1 first and 3 last

upvoted 4 times

Question #10 *Topic 3*

You have a Microsoft 365 subscription for a company named Contoso, Ltd. All data is in Microsoft 365.
Contoso works with a partner company named Litware, Inc. Litware has a Microsoft 365 subscription. Microsoft OneDrive has the default settings.
You need to allow users at Contoso to share files from Microsoft OneDrive to specific users at Litware.
Which two actions should you perform from the OneDrive admin center? Each correct answer presents part of the solution.
NOTE: Each correct selection is worth one point.

A. Increase the permission level for OneDrive External sharing

B. Modify the Links settings

C. Change the permissions for OneDrive External sharing to the least permissive level

D. Decrease the permission level for OneDrive External sharing

E. Modify the Device access settings

F. Modify the Sync settings

TimurKazan 3 months ago
Given answers are correct
upvoted 2 times

Jdlr 4 months, 3 weeks ago
Shouldn't it be A. Increasing permission level for OneDrive external sharing means more permissive to allow users outside your organization?
upvoted 1 times

asquante 4 months ago
Default is "Allow anonymous sharing", so decreasing makes sense to only allow sharing with people in Litware
upvoted 4 times

kiketxu 4 months, 3 weeks ago
Given answers are correct to me. The point is clarify what does mean decrease and increase in this context. (btw, is an awfull statement)
https://docs.microsoft.com/en-us/sharepoint/turn-external-sharing-on-or-off
Old discussion: https://www.examtopics.com/discussions/microsoft/view/12239-exam-ms-500-topic-3-question-14-discussion/
upvoted 4 times

Question #11 *Topic 3*

You have a Microsoft 365 subscription.

Some users access Microsoft SharePoint Online from unmanaged devices.

You need to prevent the users from downloading, printing, and syncing files.

What should you do?

A. Run the Set-SPOTenant cmdlet and specify the -ConditionalAccessPolicy parameter.

B. From the SharePoint admin center, configure the secure control settings.

C. From the Microsoft Azure portal, create an Azure Active Directory (Azure AD) Identity Protection sign-in risk policy.

D. From the Microsoft Azure portal, create an Azure AD Identity Protection user risk policy.

kiketxu 4 months, 3 weeks ago

I would select A, because in SPO admin center is really called "access controls" which was correctly named in another similar question.
https://www.examtopics.com/discussions/microsoft/view/9396-exam-ms-500-topic-3-question-27-discussion/

Btw, seems this is something that you can already configure directly with Conditional Access.We will see how they spell it.

upvoted 2 times

mbbhimji 4 months, 2 weeks ago

The question you saw with a similar answer was calling AssignmentCollection which is not a option for this command

So this answer is correct IMO

upvoted 1 times

Question #12 *Topic 3*

HOTSPOT -

You have the Microsoft Azure Information Protection conditions shown in the following table.

Name	Pattern	Case sensitivity
Condition1	Product1	Off
Condition2	Product2	On

You have the Azure Information Protection labels shown in the following table.

Name	Use condition	Label is applied
Label1	Condition1	Automatically
Label2	Condition2	Automatically

You have the Azure Information Protection policies shown in the following table.

Name	Applies to	Use label	Set the default label
Global	*Not applicable*	*None*	None
Policy1	User1	Label1	None
Policy2	User1	Label2	None

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

NOTE: Each correct selection is worth one point.

Hot Area:

Answer Area

Statements	Yes	No
If User1 types "Product1 and Product2" in a document and saves the document in Microsoft Word, the document will be assigned Label1 sensitivity automatically.	○	○
If User1 types "Product2 and Product1" in a document and saves the document in Microsoft Word, the document will be assigned Label2 sensitivity automatically.	○	○
If User1 types "product2" in a document and saves the document in Microsoft Word, the document will be assigned Label2 sensitivity automatically.	○	○

b00 Highly Voted 4 months, 3 weeks ago

correct - https://docs.microsoft.com/en-us/azure/information-protection/configure-policy-delete-reorder. "If you configure conditions for your labels that might apply to more than one label, you must order the labels from least sensitive to most sensitive. This ordering ensures that the most sensitive label is applied when the conditions are evaluated."
so:
1)Label 1 and Label 2 are triggered but Label 2 is the last in the policies so most sensitive so applied in priority, it wons over Label 1 so NO
2)same, Label 2 wons so YES
3)Label 2 is based on Condition 2 which is case sensitive so NO

upvoted 9 times

Yetijo 1 month, 3 weeks ago

This is correct. Here is the supporting article.
https://docs.microsoft.com/en-us/azure/information-protection/configure-policy-delete-reorder

upvoted 1 times

McChickenHawk 4 months, 3 weeks ago

Do you care to explain the “Priority” you mentioned? The question has no mention of priority so I curious why you mentioned it.

upvoted 3 times

Discuss4certi 4 months, 2 weeks ago

That's the purpose of the third table. There the priority order is listed.

upvoted 2 times

kiketxu 4 months, 3 weeks ago

Agree. NO, YES, NO.

upvoted 2 times

mashaeg Most Recent 2 months, 1 week ago

If you configure conditions for your labels that might apply to more than one label, you must order the labels from least sensitive to most sensitive. This ordering ensures that the most sensitive label is applied when the conditions are evaluated.

upvoted 1 times

Question #13 *Topic 3*

HOTSPOT -

Your company has a Microsoft 365 subscription, a Microsoft Azure subscription, and an Azure Active Directory (Azure AD) tenant named contoso.com.

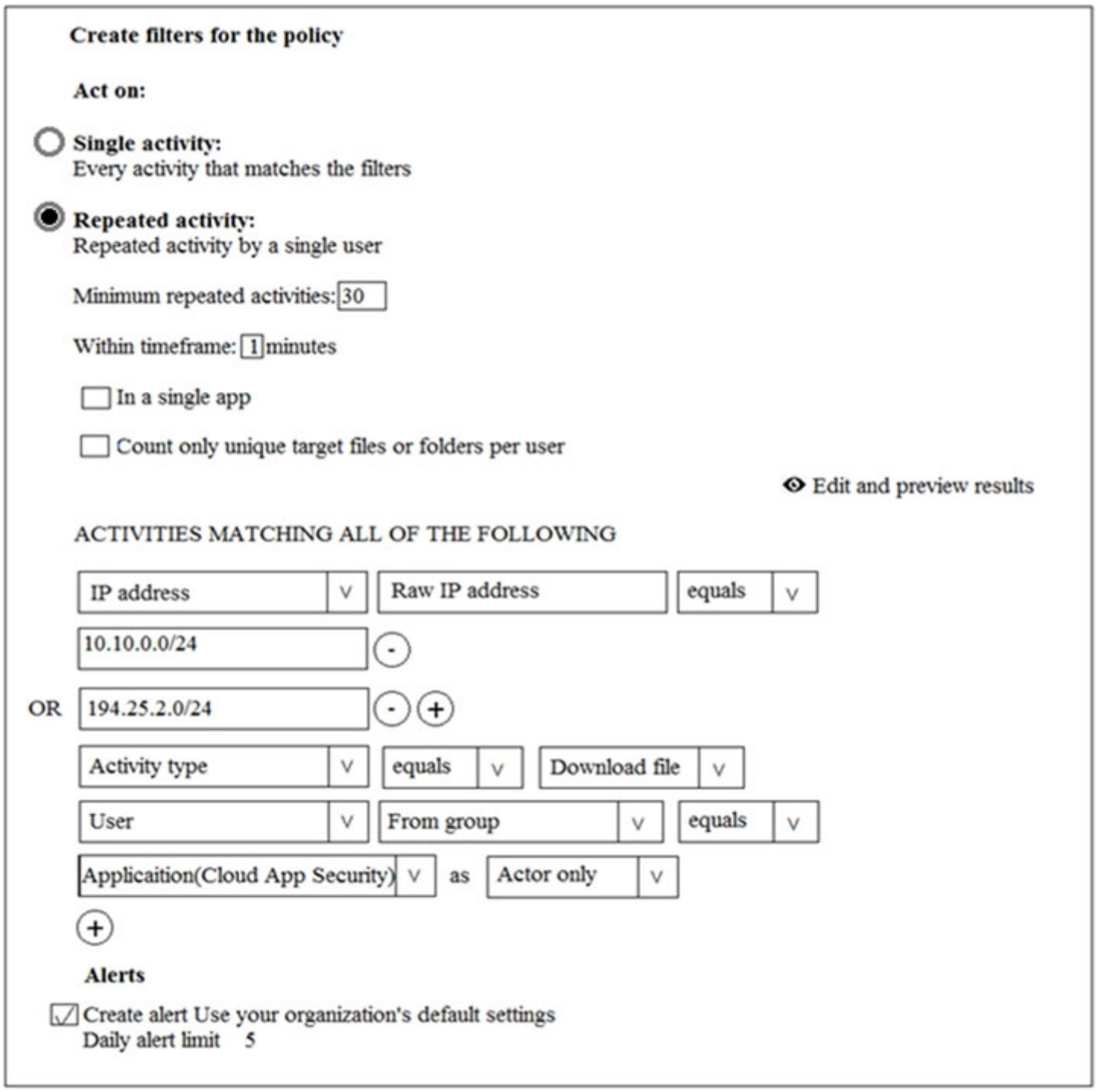
The company has the offices shown in the following table.

Location	IP address space	Public NAT segment
Montreal	10.10.0.0/24	190.15.1.0/24
Seattle	172.16.0.0/16	194.25.2.0/24
New York	192.168.0.0/16	198.35.3.0/24

The tenant contains the users shown in the following table.

Name	Email address
User1	User1@contoso.com
User2	User2@contoso.com

You create the Microsoft Cloud App Security policy shown in the following exhibit.



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
In the Montreal office, if User1 downloads 40 files in 30 seconds, an alert will be created.	○	○
In the Seattle office, if User2 downloads one file per second for two minutes, an alert will be created.	○	○
In the New York office, if User1 downloads 40 files in 10 seconds, an alert will be created.	○	○

lime568 2 weeks, 1 day ago

N-Y-N only if you have an internal server you could use the internal ip ranges

upvoted 1 times

SR_OPS 1 month, 1 week ago

I was a bit suspect about the first response being yes, but based on this it appears that you CAN use internal IP ranges in these policies: https://docs.microsoft.com/en-us/cloud-app-security/ip-tags

upvoted 1 times

kiketxu 4 months, 3 weeks ago

I would say is correct as both first matches with defined IP ranges in the activity scope. The third as isn't included won't raise any alert.

upvoted 1 times

cicekadam 4 months, 2 weeks ago

I dont get it :(10.10.0.0/24 is private IP space, people in the montreal access to system by 190.15.1.0/24 IP address space. How MCAS is gonna notice that?

upvoted 5 times

jetnam 1 month, 1 week ago

I think cicekadam is correct. Correct answer must be N-Y-N.

upvoted 1 times

synflood 3 months, 3 weeks ago

You can conntect MCAS to your Firwall/Proxy or use Defender for Endpoint. So they should also know your private IP

upvoted 2 times

Goseu 2 months, 2 weeks ago

You assume too many things ..

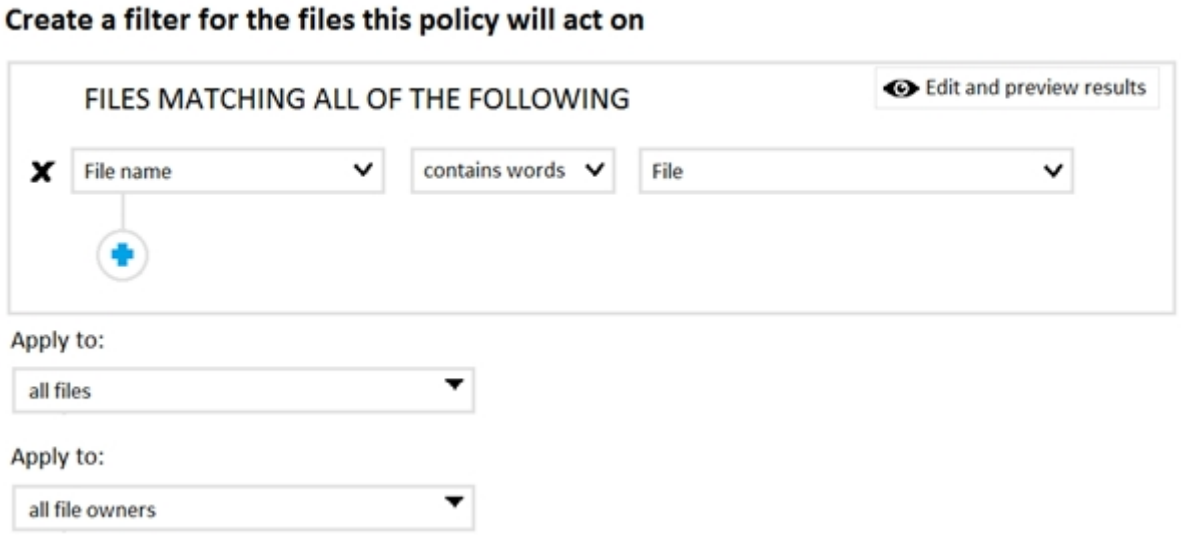
upvoted 5 times

Question #14 *Topic 3*

A user stores the following files in Microsoft OneDrive:

- File.docx
- ImportantFile.docx
- File_Important.docx

You create a Microsoft Cloud App Security file policy Policy1 that has the filter shown in the following exhibit.



To which files does Policy1 apply?

A. File_Important.docx only

B. File.docx, ImportantFile.docx, and File_Important.docx

C. File.docx only

D. ImportantFile.docx only

E. File.docx and File_Important.docx only

TimurKazan Highly Voted 3 months ago

Based on the article I would go with E

upvoted 11 times

Yetijo 1 month, 3 weeks ago

Agree. Supporting excerpt:
"When using the file policy filters, Contains will search only for full words – separated by comas, dots, spaces or underscores to search."

upvoted 1 times

Fala_Fel 3 weeks, 1 day ago

Here is another link with slightly different wording. And again suggests E is the correct answer.
https://docs.microsoft.com/en-us/cloud-app-security/data-protection-policies
"When using the policy filters, Contains searches only for full words – separated by comas, dots, spaces, or underscores. For example if you search for malware or virus, it finds virus_malware_file.exe but it does not find malwarevirusfile.exe"

upvoted 1 times

PHARDY Highly Voted 3 months, 2 weeks ago

I just tested and the right answer is C

upvoted 8 times

sdeyoung 1 month, 4 weeks ago

I have to agree with you PHARDY. Tested this as well in my tenant and C was the answer for me.

upvoted 3 times

jsshaker Most Recent 2 months, 1 week ago

Exactly, the answer should be E. Based on this: When using the file policy filters, Contains will search only for full words – separated by comas, dots, spaces or underscores to search.

upvoted 2 times

b00 4 months, 3 weeks ago

I'm confused by the link as it says :"When using the file policy filters, Contains will search only for full words – separated by comas, dots, spaces or underscores to search." So based on that I would say ImportantFile is not find because Important and File are not separated. However the string contains File so without the link I would have say YES....

upvoted 5 times

Goseu 2 months, 2 weeks ago

I think that applies to the search box only , not the results box.

upvoted 1 times

mroczyslaw 1 month, 4 weeks ago

I think applies to results not search box: "If you want to search for a string, enclose the words in quotation marks. This functions like AND, for example: if you search for "malware" "virus", it will find virus_malware_file.exe but it will not find malwarevirusfile.exe "

upvoted 1 times

kiketxu 4 months, 3 weeks ago

Good point dude, appreciated your comment.
Reading the article, I see the conflict if you uses string to filter. https://docs.microsoft.com/en-us/cloud-app-security/file-filters#Filefilters
In this case, as it's a simple word it will match for every file.

upvoted 1 times

Question #15 *Topic 3*

SIMULATION -

You need to create an Azure Information Protection label to meet the following requirements:

- Content must expire after 21 days.
- Offline access must be allowed for 21 days only.
- Documents must be protected by using a cloud key.
- Authenticated users must be able to view content only.

To complete this task, sign in to the Microsoft 365 admin center.

DaveGrain 3 months, 2 weeks ago

Agree with asquate, If you go to the location in the Azure portal it links you off to the Compliance center, where this task should be done

upvoted 1 times

asquante 4 months ago

Labels should be created from Compliance Center, not Azure AIP portal anymore.

upvoted 3 times

ctazie 3 months, 2 weeks ago

you are correct, Azure AIP stopped being supported on 1 April 2021

upvoted 1 times

ellik 3 months, 2 weeks ago

yes I cannot change anything from Azure portal, it is read only now, should be created from Compliance Center

upvoted 2 times

HSBNZ 4 months ago

This works, all the given information is correct.

upvoted 2 times

Question #16 *Topic 3*

You have a Microsoft 365 subscription.

You have a Microsoft SharePoint Online site named Site1.

You have a Data Subject Request (DSR) case named Case1 that searches Site1.

You create a new sensitive information type.

You need to ensure that Case1 returns all the documents that contain the new sensitive information type.

What should you do?

A. From the Security & Compliance admin center, create a new Search by ID List

B. From Site1, modify the search dictionary

C. From the Security & Compliance admin center, create a new Guided search

D. From Site1, initiate a re-indexing of Site1

kiketxu 4 months, 3 weeks ago

Agree.

upvoted 1 times

PattiD 7 months, 3 weeks ago

https://docs.microsoft.com/en-us/sharepoint/make-site-content-searchable#crawl-and-re-index-a-site

upvoted 4 times

Question #17 *Topic 3*

SIMULATION -

You need to ensure that a user named Allan Deyoung can perform searches and place holds on mailboxes, SharePoint Online sites, and OneDrive for Business locations. The solution must use the principle of least privilege.

To complete this task, sign in to the Microsoft 365 admin center.

mashaeg 2 months, 1 week ago

Out of both, the least priveleged - E-discovery manager
Compliance-Permissions-Compliance center roles- Edit eDiscovery Manager- Select Member

upvoted 1 times

kiketxu 4 months, 3 weeks ago

If needs to follow PoLP, eDiscovery Manager is the right answer.
Compliance Administrator is practically full-admin in the old and new SCC.

upvoted 2 times

shanti0091 6 months, 1 week ago

The answer is E-Discovery manager as it can only view and edit all cases to which it has access?

upvoted 1 times

shanti0091 6 months, 1 week ago

Scratch that, The compliance administrator is the right answer. It has the capability to search and place a mailbox on hold only.

upvoted 1 times

jaz600 9 months, 1 week ago

Members can perform searches and place holds on mailboxes, SharePoint Online sites, and OneDrive for Business locations. Members can also create and manage eDiscovery cases, add and remove members to a case, create and edit Content Searches associated with a case, and access case data in Advanced eDiscovery.

https://docs.microsoft.com/en-us/microsoft-365/security/office-365-security/permissions-in-the-security-and-compliance-center?view=o365-worldwide

Answer is correct: eDiscovery Manger

upvoted 3 times

pmac 11 months, 4 weeks ago

Surely Compliance Administrator follows principal of least privilege
Compliance Administrator can Search and place Holds

upvoted 1 times

JiDu 10 months, 2 weeks ago

The e-discovery manager role only shows in the Office 365 protection.microsoft portal and not in the newer MS365 compliance/security portals.
Therefore I would choose Compliance Administrator also.
According to the link below.
An eDiscovery Administrator is a member of the eDiscovery Manager role group...
https://docs.microsoft.com/en-us/microsoft-365/compliance/assign-ediscovery-permissions?view=o365-worldwide

upvoted 1 times

Question #18 *Topic 3*

SIMULATION -

You need to prevent any email messages that contain data covered by the U.K. Data Protection Act from being sent to recipients outside of your organization, unless the messages are sent to an external domain named adatum.com.

To complete this task, sign in to the Microsoft 365 admin center.

Anker 1 week, 6 days ago

Compliance Center --> Create Policy --> Privacy Category --> U.K. Data Protection Act --> Select Exchange Location only --> Create or Customize Advanced DLP Rules --> Edit (on both Low and High volumes) --> Add Exception --> "Except if recipient domain is" --> Add Adatum.com domain to domain exception field and click "Add" once complete. --> Actions --> Restrict Access or Encrypt the content in M365 locations --> Block users from accessing shared SharePoint, OneDrive, and Teams Content in Microsoft 365 locations (this includes EXO) --> Block only people outside of your organization. --> Save.

upvoted 4 times

sayyidsaif 2 months ago

Classic Exchange Admin center --> Compliance Management -->press + Button -->New DLP Policy From Template-->choose template "U.K. Data protect Act" -->save --> Edit policy -->Rules-->select each rule and add exception using add exception option and go to "domain is" and specify Domain name there

upvoted 2 times

CJCoolio 2 months, 2 weeks ago

You cannot use the Compliance Console as you cannot specify specific domains to be excluded.
This must be done through Exchange Admin still.

upvoted 1 times

Anker 1 week, 6 days ago

Not true, just tested this in the Compliance Center and you indeed can specify domains to exclude in the rule.

upvoted 1 times

andreiiar 3 months, 1 week ago

Testing I found out you could use Template "UK Data Protection Act" and manually edit policy settings to exclude.

upvoted 2 times

Dodier 4 months, 1 week ago

DLP on the new console complice:
Compliance > Policies > DLP > Create Policy > Custom > etc.

upvoted 3 times

fred 4 months, 4 weeks ago

not correct, use new dlp on the new console compliance

upvoted 4 times

Question #19 *Topic 3*

SIMULATION -

You need to ensure that a user named Allan Deyoung receives incident reports when email messages that contain data covered by the U.K. Data Protection Act are sent outside of your organization.

To complete this task, sign in to the Microsoft 365 admin center.

techtest848 Highly Voted 1 year ago

I think number of instances also should be 1 instead of 10 as if the number of incidents is less than 10, the user will not receive the incident report

upvoted 5 times

shanti0091 6 months, 1 week ago

validpoint

upvoted 1 times

itsRay Highly Voted 1 year, 2 months ago

Why in step 4 'All locations', while the question mentions 'email' only?

upvoted 5 times

AJ2021 6 months ago

Correct, it should not be 'All locations', that should be changed to 'Let me choose specific locations', Next, then untick everything except for 'Exchange Email', as the question relates to email

upvoted 2 times

Rick123123 5 months, 4 weeks ago

And what about MS Teams. Can you not send content to external users via Teams??

upvoted 1 times

chaoscreater 1 month ago

"when email messages that contain data ...." -> Is Teams the same as email? NO.

upvoted 1 times

btd2020 1 year, 2 months ago

Very good point!

upvoted 1 times

Question #20 *Topic 3*

SIMULATION -

You need to ensure that a global administrator is notified when a document that contains U.S. Health Insurance Portability and Accountability Act (HIPAA) data is identified in your Microsoft 365 tenant.

To complete this task, sign in to the Microsoft Office 365 admin center.

Donnie21 3 months, 3 weeks ago

You do not have to select global administrators by default email are send to them.

upvoted 3 times

shanti0091 6 months, 1 week ago

The steps are correct but when you get to the part to deselect, you need to select instead and make sure you uncheck the all the box that selects all users, owners and select the add tab to include the global administrator account only.

upvoted 2 times

Question #21 *Topic 3*

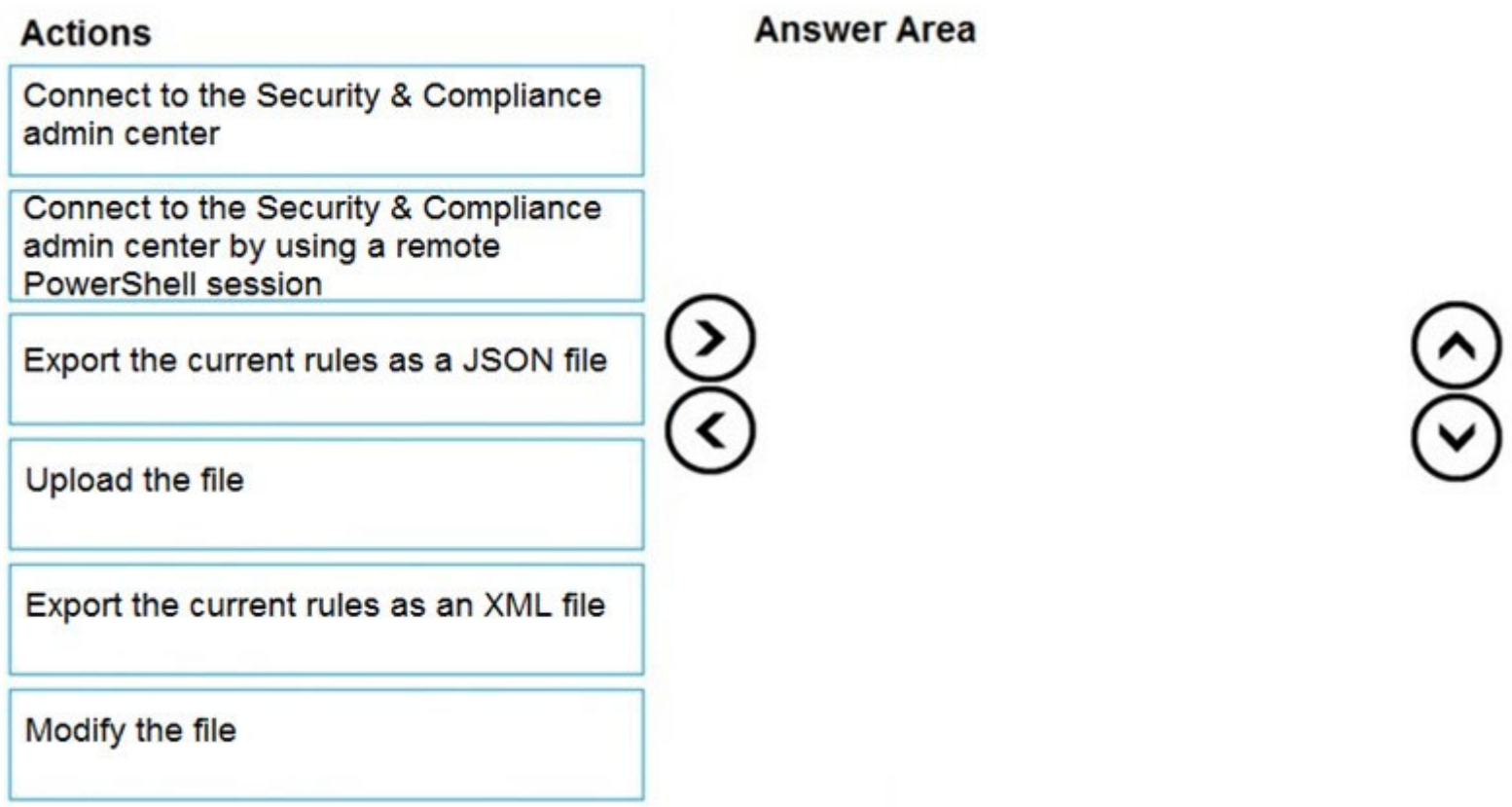
DRAG DROP -

You have a Microsoft 365 subscription.

You need to include a custom sensitive information type in Data Subject Request (DSR) cases.

Which four 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:



kiketxu 4 months, 3 weeks ago

Note this is really a new custom infotype creation, so forget "Data Subject Request (DSR) cases."
It's Ok to me. It connects to SCC by PWSH, download XML file, modifies and upload.

upvoted 4 times

Question #22 *Topic 3*

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. You create a label named CompanyConfidential in Microsoft Azure Information Protection.
You add CompanyConfidential to a global policy.
A user protects an email message by using CompanyConfidential and sends the label to several external recipients. The external recipients report that they cannot open the email message.
You need to ensure that the external recipients can open protected email messages sent to them.
You create a new label in the global policy and instruct the user to resend the email message.
Does that meet the goal?

A. Yes

B. No

Millsy Highly Voted 6 months, 4 weeks ago

I Don't see how this fixes it, no where does it state the settings on this 'new label' so how do we know it would work, also no where does it state that we tell the user about this new label so if they simply resend the email why would this new label that no one knows anything about just be assumed to fix the issue?

upvoted 9 times

kiketxu 5 months ago

This will never fix external access while they aren't added in the label permissions as authorized (viewer,reviewer,coauthor,owner or custom permissions). This is missing in the statement so simply creating another label and publising in the GP you do nothing.

Alternative, could be creating another label with UDP (user defined permissions) where if you label an email it can only apply "DO NOT FORWARD" protected template, allowing the recipients to view and reply, but not copy, print or forward. (with UDP you will be prompted for users/role only with Word,Excel, Powerpoint)

upvoted 3 times

Zorag Highly Voted 1 year, 5 months ago

This is correct as you configure protection settings in the label

upvoted 6 times

Mayurgowda Most Recent 1 year, 2 months ago

This is correct

upvoted 1 times

kmsrajan 1 year, 5 months ago

The answer is confusing. Even new label is created with recipients only then the sender have to reapply the label. The statement say create new label and resend the mail how does change the protection on the label which is already in place?

upvoted 2 times

Fuji_56 1 year, 5 months ago

Typically ambiguous and open ended answers by MS SMEs eh? I don't think that this would be the route I would choose, IRL. I would be even more conscious of the access and lean towards accepted domain exceptions.

upvoted 1 times

Question #23 *Topic 3*

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 a Microsoft Azure Active Directory (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	Office 365	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.

Hot Area:

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

hhaywood 4 months, 3 weeks ago

Only correct if the specific ADDS groups have been synced into AAD - this is not specified so have to 'assume' which is poor

upvoted 1 times

TimurKazan 3 months, 3 weeks ago

it is said that domain is synced

upvoted 2 times

kiketxu 4 months, 3 weeks ago

repeated question, but it's correct.

upvoted 3 times

M3ridi3n 1 month, 3 weeks ago

Not that repeated, the other was about "Policy1".

upvoted 1 times

Question #24 *Topic 3*

HOTSPOT -

You have a Microsoft 365 subscription.

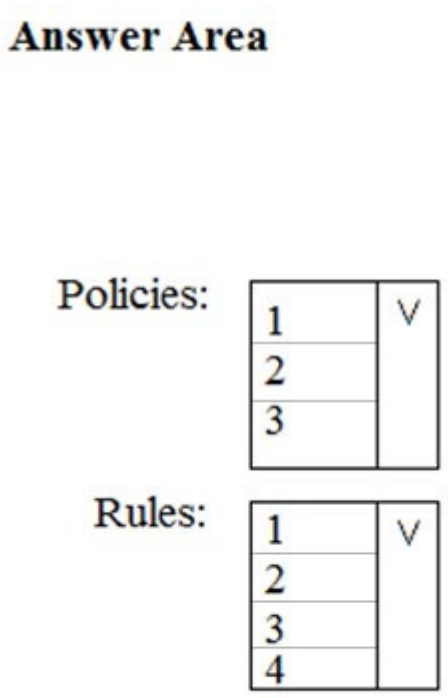
You identify the following data loss prevention (DLP) requirements:

- Send notifications to users if they attempt to send attachments that contain EU Social Security Numbers (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.

Hot Area:



kiketxu Highly Voted 4 months, 3 weeks ago

POLICY1 with Exchange selected as location.
Rule (A) with:
- EU social security - NOTIFY the user who sent - Notify Admin.
Rule (B) with:
- Credit card numbers - BLOCK - Notify Admin.

POLICY2 with OneDrive selected as location.
Rule (C) with:
- EU passport numbers - BLOCK - Notify Admin.

Credits to @itmp in:
https://www.examtopics.com/discussions/microsoft/view/12036-exam-ms-500-topic-3-question-3-discussion/
upvoted 14 times

Yetijo 1 month, 3 weeks ago

Created these polies & rules in lab. This is correct, 2 policies, 3 rules as described.
upvoted 1 times

BialyFenek 4 months, 3 weeks ago

Correct, answer is 2 policies and 3 rules
upvoted 5 times

vijeet 4 months, 2 weeks ago

How about teams?
upvoted 2 times

lime568 Most Recent 2 weeks, 1 day ago

if you do it with excange is 2 policies and 3 rules but with compliance are 3 and 3
upvoted 1 times

prats005 4 months ago

Correct answer is 2 policies and 3 rules | First policy will have 2 rules | second policy will have 1 rule.
upvoted 2 times

Question #25

Topic 3

You have a Microsoft 365 subscription.

Some users access Microsoft SharePoint Online from unmanaged devices.

You create a conditional access policy in Azure Active Directory.

You need to prevent the users from downloading, printing, and syncing files.

What should you do?

A. From the Microsoft Azure portal, create an Azure Active Directory (Azure AD) Identity Protection user risk policy.

B. From the Microsoft Azure portal, create an Azure Active Directory (Azure AD) conditional access policy.

C. From the SharePoint admin center, configure the Access control settings.

D. From the Microsoft Azure portal, create an Azure Active Directory (Azure AD) Identity Protection sign-in risk policy.

Question #26 *Topic 3*

You have a Microsoft 365 tenant.

You have a database that stores customer details. Each customer has a unique 13-digit identifier that consists of a fixed pattern of numbers and letters.

You need to implement a data loss prevention (DLP) solution that meets the following requirements:

☞ Email messages that contain a single customer identifier can be sent outside your company.

☞ Email messages that contain two or more customer identifiers must be approved by the companyя€™s data privacy team.

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

NOTE: Each correct selection is worth one point.

A. a sensitive information type

B. a sensitivity label

C. a retention label

D. a DLP policy

E. a mail flow rule

kiketxu Highly Voted 4 months, 3 weeks ago

You need to create sensitivity infotype for sure but M365 DLP not yet support message approval. Instead you need to use mail flow rule.
https://docs.microsoft.com/es-es/exchange/security-and-compliance/mail-flow-rules/common-message-approval-scenarios#example-4-forward-messages-that-match-one-of-several-criteria
Additional interesting discussion:
https://www.reddit.com/r/Office365/comments/f1ux42/create_approval_workflow_with_office_365_dlp/

upvoted 5 times

subbuhotmail Most Recent 1 month, 2 weeks ago

Firstly, the question is, it asked to create DLP policy.
Second, it didn't mention as approvers, it says approved identifiers by data Privacy team. "two or more customer identifiers must be approved by the companyя€™s data privacy team"

So answer is A&D Only.

upvoted 2 times

james1 1 month, 3 weeks ago

This is correct as you can add an Action to forward for approval to specific approvers within the DLP Policy

upvoted 1 times

bsldwp_2020 2 months ago

Answer should be A & E.

A - Sensitivity Info. Used to create the sensitivity info type - 13 digit identifiers.
E - Mail flow rule. Used to create rule to block messages outside org. if min count of Sensitive info matches 2.

upvoted 3 times

bsldwp_2020 2 months ago

Correction: Even the same rule can be created via the DLP policy as well. So, D is also right.

upvoted 2 times

belyo 4 months ago

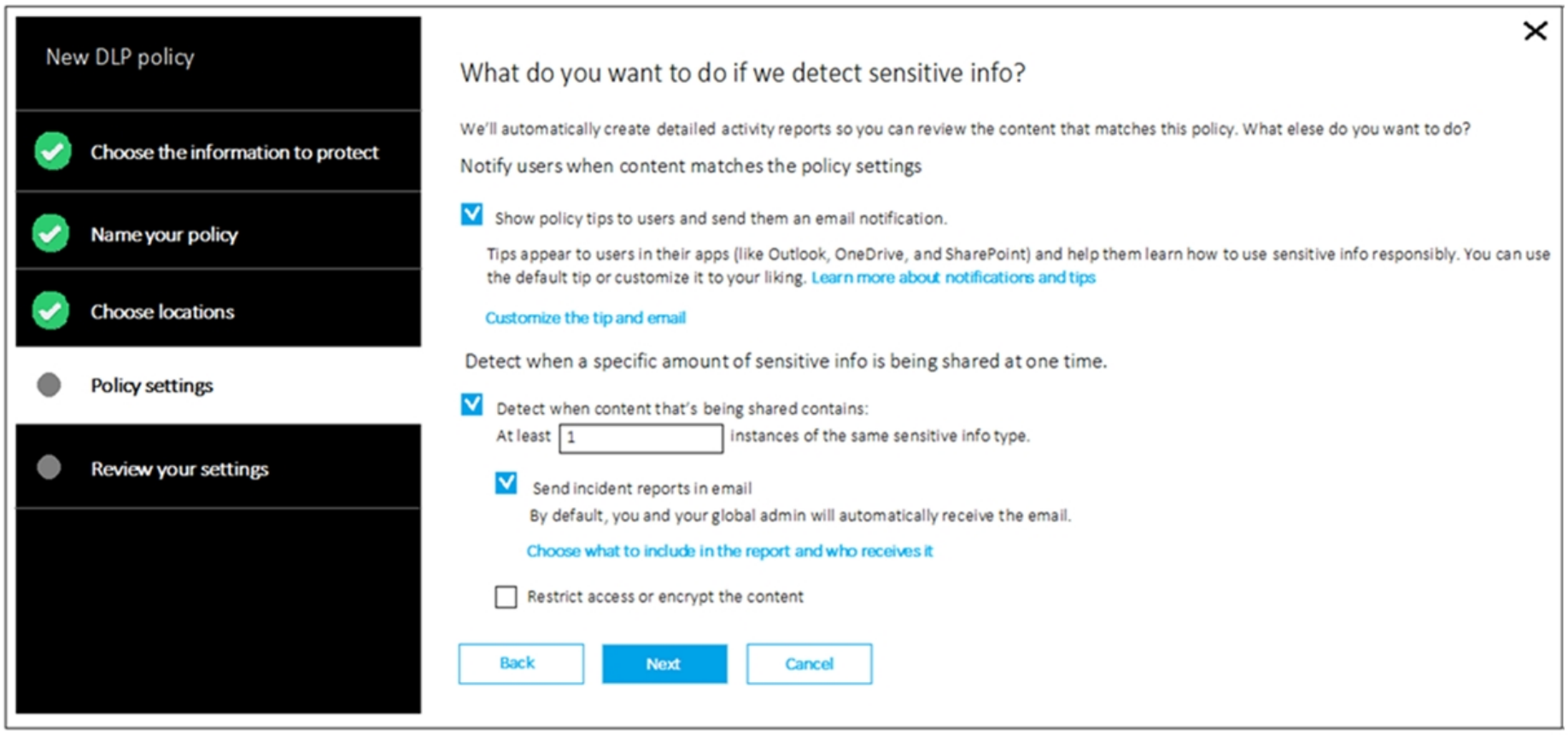
IMO this solution should be D,A,E
you need first a DLP, after that a sensitive type and at last an exchange transport rule
But since question stands only for which 'TWO' the answer is supposed to be correct...

upvoted 1 times

Question #27

Topic 3

You create a data loss prevention (DLP) policy as shown in the following exhibit:



What is the effect of the policy when a user attempts to send an email message that contains sensitive information?

A. The user receives a notification and can send the email message

B. The user receives a notification and cannot send the email message

C. The email message is sent without a notification

D. The email message is blocked silently

kiketxu 4 months, 3 weeks ago

A for sure!

upvoted 2 times

ellik 3 months, 2 weeks ago

Hi Kiketxu, I tried to test this and I found this when you select protection actions and then Next yu will see "Customize access and override settings
By default, users are blocked from sending email and Teams chats and channel messages that contain the type of content you're protecting. But you can choose who has access to shared SharePoint and OneDrive files. You can also decide if you want to let people override the policy's restrictions."

upvoted 4 times

SimoneV 1 month, 1 week ago

"Also, if you want to actually block or restrict access to content that is in violation of policy, you need to configure an action on the rule to do so."
Not all templates have a block access action defined in their rules . And the box to restrict content isn't checked. So wouldn't it be safe to assume that the user CAN send the mail?
https://docs.microsoft.com/en-us/microsoft-365/compliance/create-test-tune-dlp-policy?view=o365-worldwide#where-to-start-with-data-loss-prevention

upvoted 1 times

arunjana 2 months, 3 weeks ago

Going by ellik's comments, the answer should be B) User receives notification and cannot send e-mail (Assuming the default options)

upvoted 2 times

Kalzonee3611 2 months, 2 weeks ago

Default setting is to block, do we just presume that is the case?

upvoted 1 times

SR_OPS 1 month, 1 week ago

The bottom checkbox for restricting access is not ticked, so it will not be blocked

upvoted 7 times

Question #28 *Topic 3*

You have a Microsoft 365 subscription.
You need to create data loss prevention (DLP) queries in Microsoft SharePoint Online to find sensitive data stored in sites.
Which type of site collection should you create first?

A. Records Center

B. eDiscovery Center

C. Enterprise Search Center

D. Document Center

asquante 4 months ago
This has not been the case for years now - only valid for SP 2016, not SPO.
upvoted 4 times

kiketxu 4 months, 3 weeks ago
Seems out of date question. Currently it should run from Compliance Center to get full features as eDiscovery in the old portal is in retiring process.
https://docs.microsoft.com/en-gb/microsoft-365/compliance/ediscovery?view=o365-worldwide

https://docs.microsoft.com/en-gb/microsoft-365/compliance/legacy-ediscovery-retirement?view=o365-worldwide
upvoted 2 times

kiketxu 4 months, 3 weeks ago
https://www.examtopics.com/discussions/microsoft/view/11872-exam-ms-500-topic-3-question-6-discussion/
upvoted 2 times

Topic 4 - Question Set 4

Question #1 *Topic 4*

You have a Microsoft 365 subscription.

The Global administrator role is assigned to your user account. You have a user named Admin1.

You create an eDiscovery case named Case1.

You need to ensure that Admin1 can view the results of Case1.

What should you do first?

A. From the Azure Active Directory admin center, assign a role group to Admin1.

B. From the Microsoft 365 admin center, assign a role to Admin1.

C. From the Security & Compliance admin center, assign a role group to Admin1.

Yogi06 Highly Voted 11 months, 3 weeks ago

correct. Only security and complaince centre includes permission role i.e edisocvery manger in order to see cases

upvoted 6 times

Hogg Most Recent 2 months ago

C is correct - Only security and compliance center includes permission role

Reference - https://docs.microsoft.com/en-us/office365/securitycompliance/assign-ediscovery-permissions

upvoted 1 times

Rafale 4 months, 1 week ago

C is correct

upvoted 1 times

kiketxu 5 months ago

C for sure

upvoted 1 times

svm_Terran 8 months ago

this is correct

upvoted 1 times

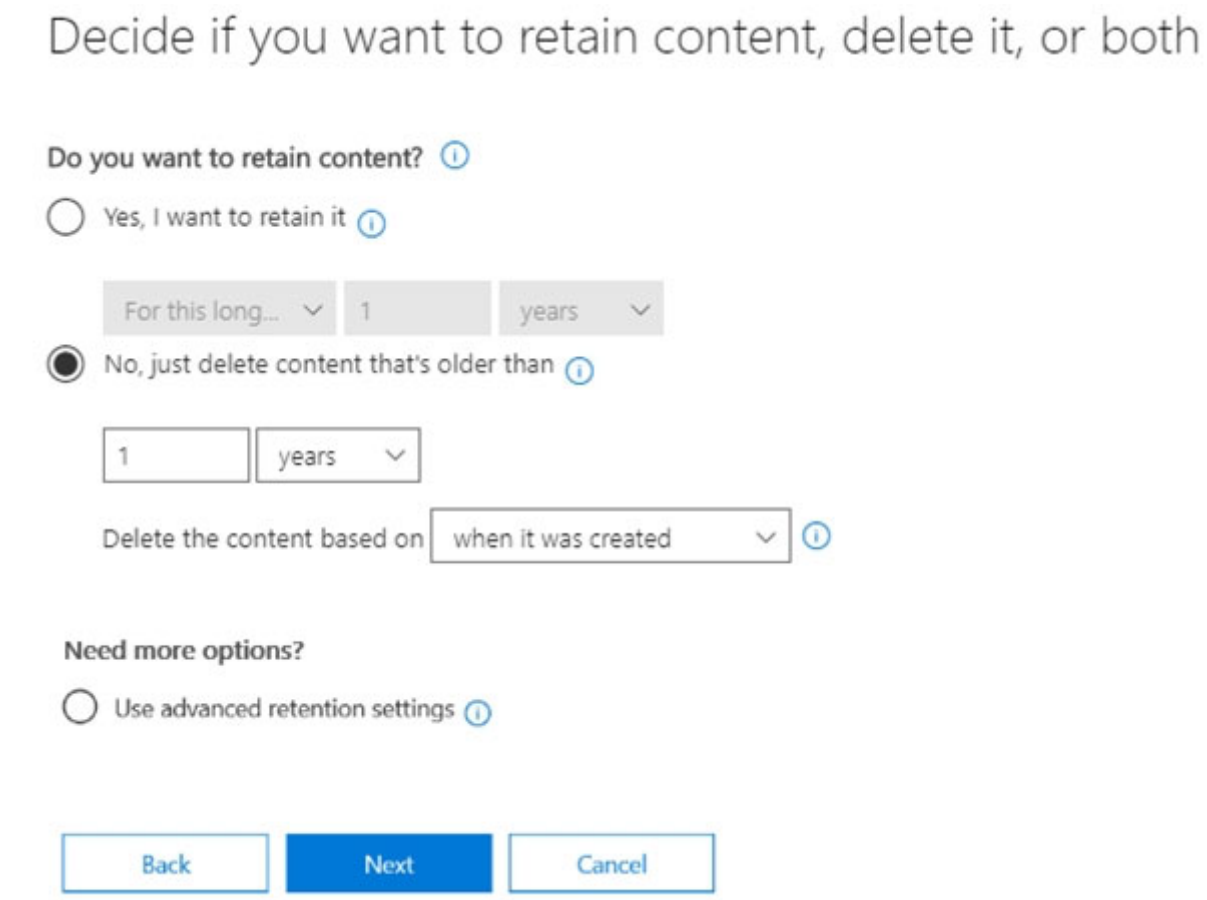
Question #2 *Topic 4*

HOTSPOT -

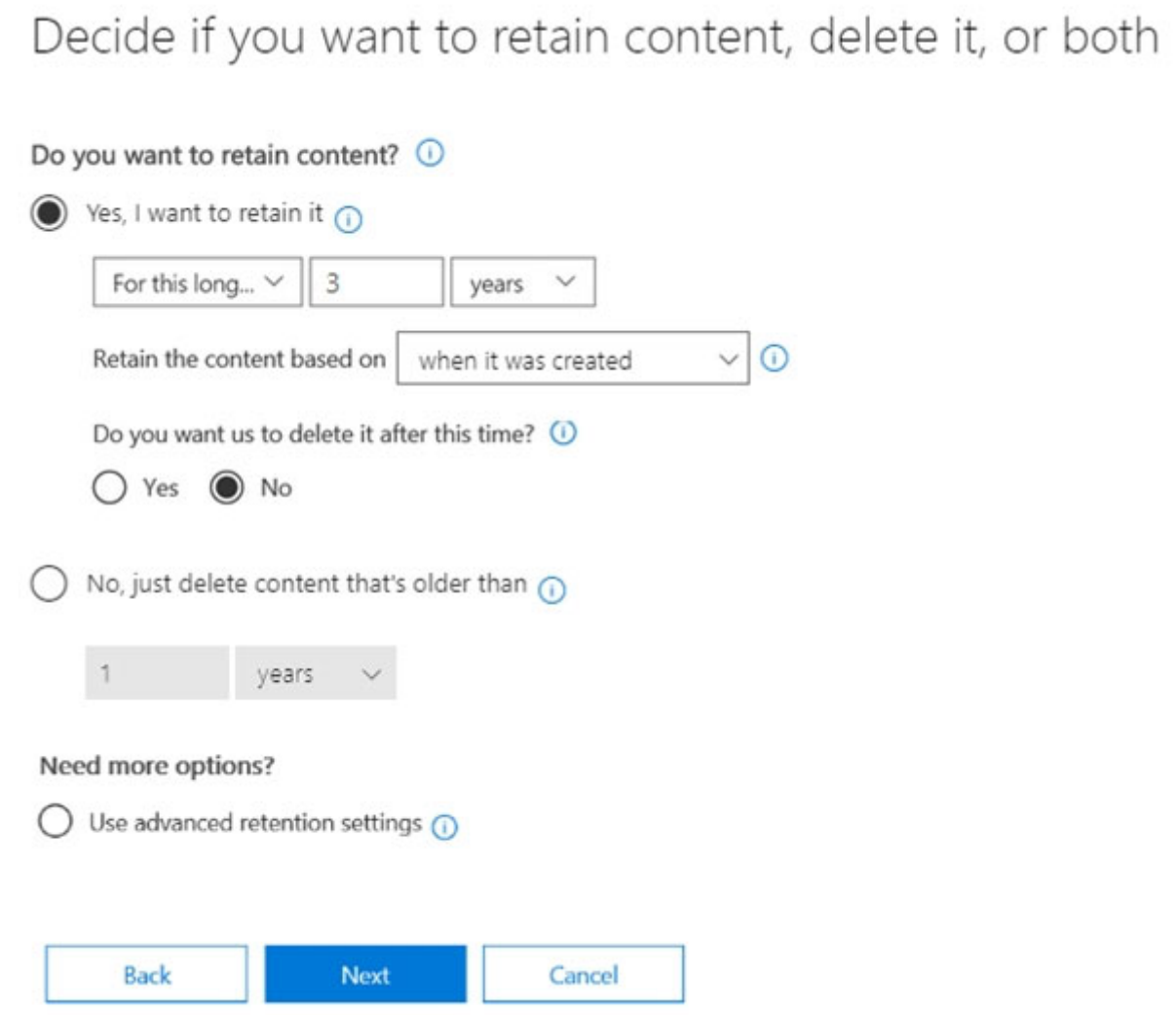
You have a Microsoft 365 subscription. From the Security & Compliance admin center, you create the retention policies shown in the following table.

Name	Location
Policy1	OneDrive accounts
Policy2	Exchange email, SharePoint sites, OneDrive accounts, Office 365 groups

Policy1 if configured as showing in the following exhibit.

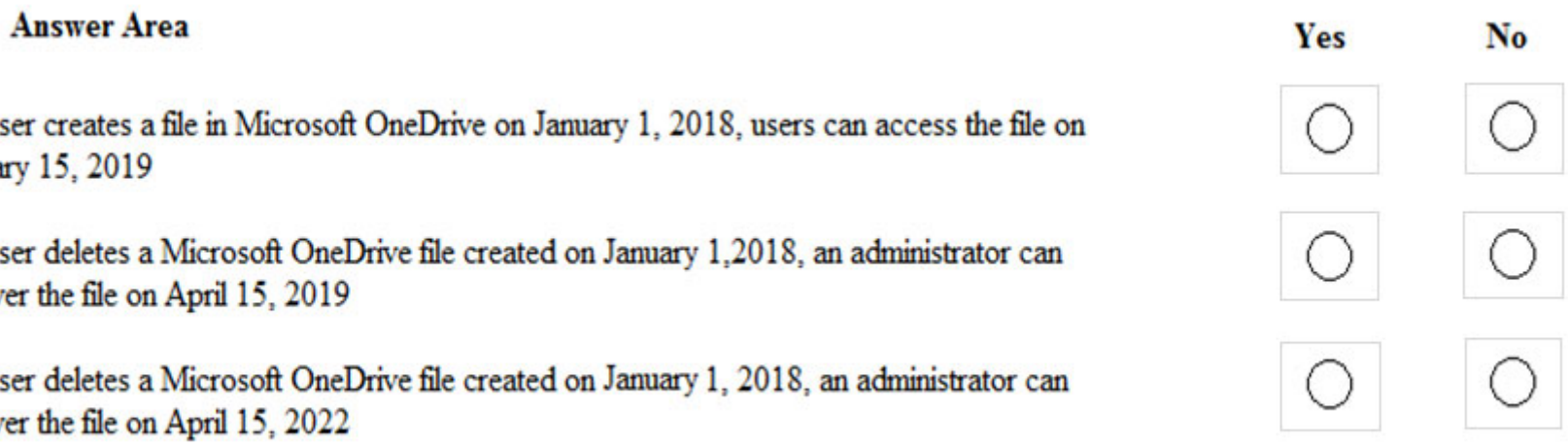


Policy2 is configured as shown in the following exhibit.



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

Hot Area:



kiketxu Highly Voted 4 months, 3 weeks ago

YES, YES, NO.
Principles of retention:
- Retention wins over deletion
- Longest retention period wins
- Explicit inclusion wins over implicit inclusion
- Shortest deletion period wins

Source: https://docs.microsoft.com/en-us/microsoft-365/compliance/retention-policies?view=o365-worldwide#the-principles-of-retention-or-what-takes-precedence

upvoted 22 times

chaoscreater 1 month ago

Why is the answer for the first question Yes? The file is deleted for the user, so they shouldn't be able to access the file. Retention policy will still keep the file but only an admin is able to restore/access the file at that point. Question is asking about whether the "user" can access the file.

upvoted 2 times

lime568 2 weeks, 1 day ago

who said that the user deleted the file? The user created the file

upvoted 1 times

chaoscreater 1 month ago

https://www.examtopics.com/exams/microsoft/ms-100/view/26/#

upvoted 1 times

chaoscreater 3 weeks, 3 days ago

nevermind, the answer in the question I linked is wrong

upvoted 1 times

stromnessian Most Recent 1 week, 4 days ago

NYN, because...
"...Retention wins over deletion. Content won't be permanently deleted when it also has retention settings to retain it. While this principle ensures that content is preserved for compliance reasons, the delete process is still initiated and can remove the content from user view and searches. For SharePoint, for example, a document moves from the original folder to the Preservation Holds folder. However, permanent deletion is suspended..."
Reference: https://docs.microsoft.com/en-us/microsoft-365/compliance/retention?view=o365-worldwide

upvoted 2 times

Question #3 *Topic 4*

You have a Microsoft 365 subscription.

You need to enable auditing for all Microsoft Exchange Online users.

What should you do?

A. From the Exchange admin center, create a journal rule

B. Run the Set-MailboxDatabase cmdlet

C. Run the Set-Mailbox cmdlet

D. From the Exchange admin center, create a mail flow message trace rule.

krrunal Highly Voted 1 year, 8 months ago

Starting in January 2019, Microsoft is turning on mailbox audit logging by default for all Office 365 organizations. This means that certain actions performed by mailbox owners, delegates, and admins are automatically logged, and the corresponding mailbox audit records will be available when you search for them in the mailbox audit log. Before mailbox auditing was turned on by default, you had to manually enable it for every user mailbox in your organization.

upvoted 11 times

kiketxu 5 months ago

I'm agree with this is only for the new tenants. To answer the question in the context I would say the answer is correct.

upvoted 5 times

ThibaultSentinel 1 year, 2 months ago

IMO, this new settings is only for new tenants

upvoted 2 times

DrMe Highly Voted 7 months, 2 weeks ago

Answer reference:
https://docs.microsoft.com/en-us/microsoft-365/compliance/enable-mailbox-auditing?view=o365-worldwide#change-the-mailbox-actions-to-audit:~:text=You%20can%20use%20the%20AuditAdmin%2C%20AuditDelegate%2C,365%20group%20mailboxes%20can't%20be%20customized).

upvoted 6 times

kiketxu 4 months, 3 weeks ago

Crystal clear, thanks! ;)

upvoted 2 times

Question #4 *Topic 4*

Note: This question is part of a series of questions that present the same scenario. Each question in the series contains a unique solution that might meet the stated goals. Some question sets might have more than one correct solution, while others might not have a correct solution.

After you answer a question in this section, you will NOT be able to return to it. As a result, these questions will not appear in the review screen.

You have a Microsoft 365 subscription that contains 1,000 user mailboxes.

An administrator named Admin1 must be able to search for the name of a competing company in the mailbox of a user named User5.

You need to ensure that Admin1 can search the mailbox of User5 successfully. The solution must prevent Admin1 from sending email messages as User5.

Solution: You modify the permissions of the mailbox of User5, and then create an eDiscovery case.

Does this meet the goal?

A. Yes

B. No

kiketxu 4 months, 3 weeks ago

Correct answer. Won't possible create case without eDiscovery role.

upvoted 3 times

Mayurgowda 1 year, 2 months ago

Correct answer

upvoted 3 times

Question #5 *Topic 4*

Note: This question is part of a series of questions that present the same scenario. Each question in the series contains a unique solution that might meet the stated goals. Some question sets might have more than one correct solution, while others might not have a correct solution.
After you answer a question in this section, you will NOT be able to return to it. As a result, these questions will not appear in the review screen.
You have a Microsoft 365 subscription that contains 1,000 user mailboxes.
An administrator named Admin1 must be able to search for the name of a competing company in the mailbox of a user named User5.
You need to ensure that Admin1 can search the mailbox of User5 successfully. The solution must prevent Admin1 from sending email messages as User5.
Solution: You start a message trace, and then create a Data Subject Request (DSR) case.
Does this meet the goal?

A. Yes

B. No

kiketxu 4 months, 3 weeks ago
Of course don't....
upvoted 3 times

Question #6 *Topic 4*

Note: This question is part of a series of questions that present the same scenario. Each question in the series contains a unique solution that might meet the stated goals. Some question sets might have more than one correct solution, while others might not have a correct solution.
After you answer a question in this section, you will NOT be able to return to it. As a result, these questions will not appear in the review screen.
You have a Microsoft 365 subscription that contains 1,000 user mailboxes.
An administrator named Admin1 must be able to search for the name of a competing company in the mailbox of a user named User5.
You need to ensure that Admin1 can search the mailbox of User5 successfully. The solution must prevent Admin1 from sending email messages as User5.
Solution: You assign the eDiscovery Manager role to Admin1, and then create an eDiscovery case.
Does this meet the goal?

A. Yes

B. No

TheSkyMan Highly Voted 1 year, 2 months ago

A couple new questions I remember from the exam are:
What type of groups can be used with a supervision policy?
https://docs.microsoft.com/en-us/microsoft-365/compliance/configure-supervision-policies?view=o365-worldwide

How to apply an access review. Specifically, what users will have access to an app after the access review has ended.
https://docs.microsoft.com/en-us/azure/active-directory/governance/perform-access-review
upvoted 9 times

kiketxu Most Recent 4 months, 3 weeks ago

This time YES, is right.
upvoted 2 times

Sido1 4 months, 3 weeks ago

the answer doesn't solve the second scenerio "preventing admin1 from sending email message to user5"
upvoted 1 times

Sido1 4 months, 3 weeks ago

oh i got it..i think its right !. "AS"
upvoted 2 times

Nicholasname 1 year, 1 month ago

"Following the release of communication compliance in Microsoft 365 Compliance in February 2020, Supervision in Office 365 is being retired. Supervision policies will no longer be available for creation, and policies will eventually be removed, after an extended period of read only access."
https://docs.microsoft.com/en-us/microsoft-365/compliance/configure-supervision-policies?view=o365-worldwide
upvoted 2 times

Question #7 *Topic 4*

SIMULATION -

You need to ensure that all the email messages in the mailbox of a user named Allan Deyoung are retained for a period of 90 days, even if the messages are deleted.

To complete this task, sign in to the Microsoft 365 admin center.

ms5000 Highly Voted 1 year ago

A better, more updated answer can be found by following these instructions: https://docs.microsoft.com/en-us/microsoft-365/compliance/create-retention-policies?view=o365-worldwide

upvoted 11 times

njc 6 months, 1 week ago

I agree. You now create the retention policy for Exchange in the Security and Compliance Centre

upvoted 2 times

shanti0091 6 months, 1 week ago

Agreed, you can configure retention policy from compliance.Microsoft.com

upvoted 1 times

CJCoolio Most Recent 2 months, 2 weeks ago

Hello, you can create a retention policy for Exchange in the Security and Compliance Centre, however you can set 90 days, on 29 days. You can set 3 months but I don't know if that qualifies for the criteria.
I would lean more towards creating it in Exchange Admin Center for this reason.

upvoted 1 times

chaoscreater 1 month ago

3 months = 90 days wtf are you on about...

upvoted 1 times

Steve_B 2 months ago

If you create a retention policie in compliance center you can choose "custom" an set it how you want to

upvoted 1 times

Question #8 *Topic 4*

SIMULATION -

You need to create a retention policy that contains a data label. The policy must delete all Microsoft Office 365 content that is older than six months.

To complete this task, sign in to the Microsoft 365 admin center.

Nicholasname Highly Voted 1 year, 1 month ago

Reference is to 3rd party site. Content is also out of date.

You can now create both retention Labels AND Label Policies via 'Classification' OR 'Information Governance' options in the left-hand menu from the Security Compliance centre (protection.office.com). Both will create Labels that are the same and show in either area.

upvoted 6 times

mitchg Most Recent 10 months ago

Here's the correct URL: https://docs.microsoft.com/en-us/microsoft-365/compliance/data-loss-prevention-policies?view=o365-worldwide#using-a-retention-label-as-a-condition-in-a-dlp-policy

upvoted 2 times

Question #9 *Topic 4*

SIMULATION -

You need to create an eDiscovery case that places a hold on the mailbox of a user named Allan Deyoung. The hold must retain email messages that have a subject containing the word merger or the word Contoso.

To complete this task, sign in to the Microsoft 365 admin center.

sayyidsaif 2 months ago

Query missing in the answer. we can do it in two ways
1. Enter the below key word in Query conditions
subject:merger
subject:Contoso
2. add two condition each with subject contains merger and Contoso

upvoted 2 times

Question #10 *Topic 4*

SIMULATION -

You plan to create a script to automate user mailbox searches. The script will search the mailbox of a user named Allan Deyoung for messages that contain the word injunction.

You need to create the search that will be included in the script.

To complete this task, sign in to the Microsoft 365 admin center.

mashaeg 2 months, 1 week ago

eDiscovery- Searches-Keyword

upvoted 2 times

Question #11 *Topic 4*

You have a Microsoft 365 subscription.

You create a supervision policy named Policy1, and you designate a user named User1 as the reviewer.

What should User1 use to view supervised communications?

A. a team in Microsoft Teams

B. the Security & Compliance admin center

C. Outlook on the web

D. the Exchange admin center

Nicholasname Highly Voted 1 year, 1 month ago

Supervision has been depreciated.

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

upvoted 9 times

kiketxu Most Recent 4 months, 3 weeks ago

Deprecated question for sure! xD

upvoted 2 times

kratos13 1 year, 1 month ago

Answer is correct ~

"View the Supervision report :
1) Sign into the Compliance center with credentials for an admin account with permissions to view supervision reports."

upvoted 3 times

Question #12

Topic 4

SIMULATION -

Please wait while the virtual machine loads. Once loaded, you may proceed to the lab section. This may take a few minutes, and the wait time will not be deducted from your overall test time.

When the Next button is available, click it to access the lab section. In this section, you will perform a set of tasks in a live environment. While most functionality will be available to you as it would be in a live environment, some functionality (e.g., copy and paste, ability to navigate to external websites) will not be possible by design.

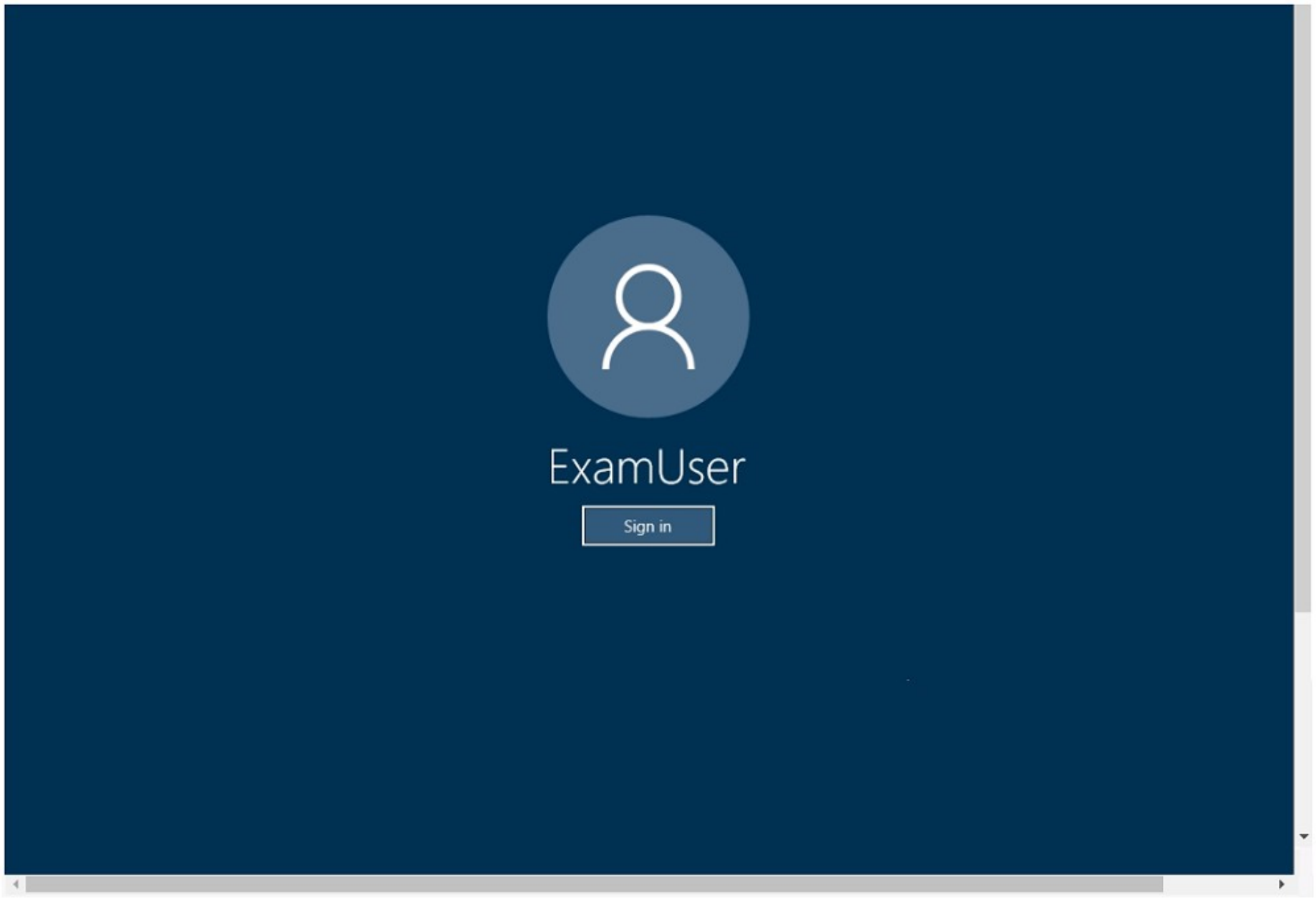
Scoring is based on the outcome of performing the tasks stated in the lab. In other words, it doesnɹ€™t matter how you accomplish the task, if you successfully perform it, you will earn credit for that task.

Labs are not timed separately, and this exam may more than one lab that you must complete. You can use as much time as you would like to complete each lab.

But, you should manage your time appropriately to ensure that you are able to complete the lab(s) and all other sections of the exam in the time provided.

Please note that once you submit your work by clicking the Next button within a lab, you will NOT be able to return to the lab.

Username and password -



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@LODSe244001.onmicrosoft.com

Microsoft 365 Password: &=Q8v@2qGzYz

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: 11032396 -

You need to ensure that when users tag documents as classified, a classified watermark is applied to the documents.

To complete this task, sign in to the Microsoft Office 365 admin center.

SteveBe 3 months ago

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

upvoted 3 times

Nuuk 3 months ago

For me you have to go through Unified Labeling, to create a lable which will watermark documents based on a policy you'll design before creating the label and applying it to a policy. please correct me if I'm wrong or if there is another way.

upvoted 1 times

Rockalm 3 months, 1 week ago

It seems this has completely changed. I can't get this done in my lab. Does anybody have a hint where to start from?

upvoted 1 times

mashaeg 2 months, 1 week ago

Compliance-Information protection-labels
Content marking-Add a watermak

upvoted 3 times

ablackwood 1 month, 3 weeks ago

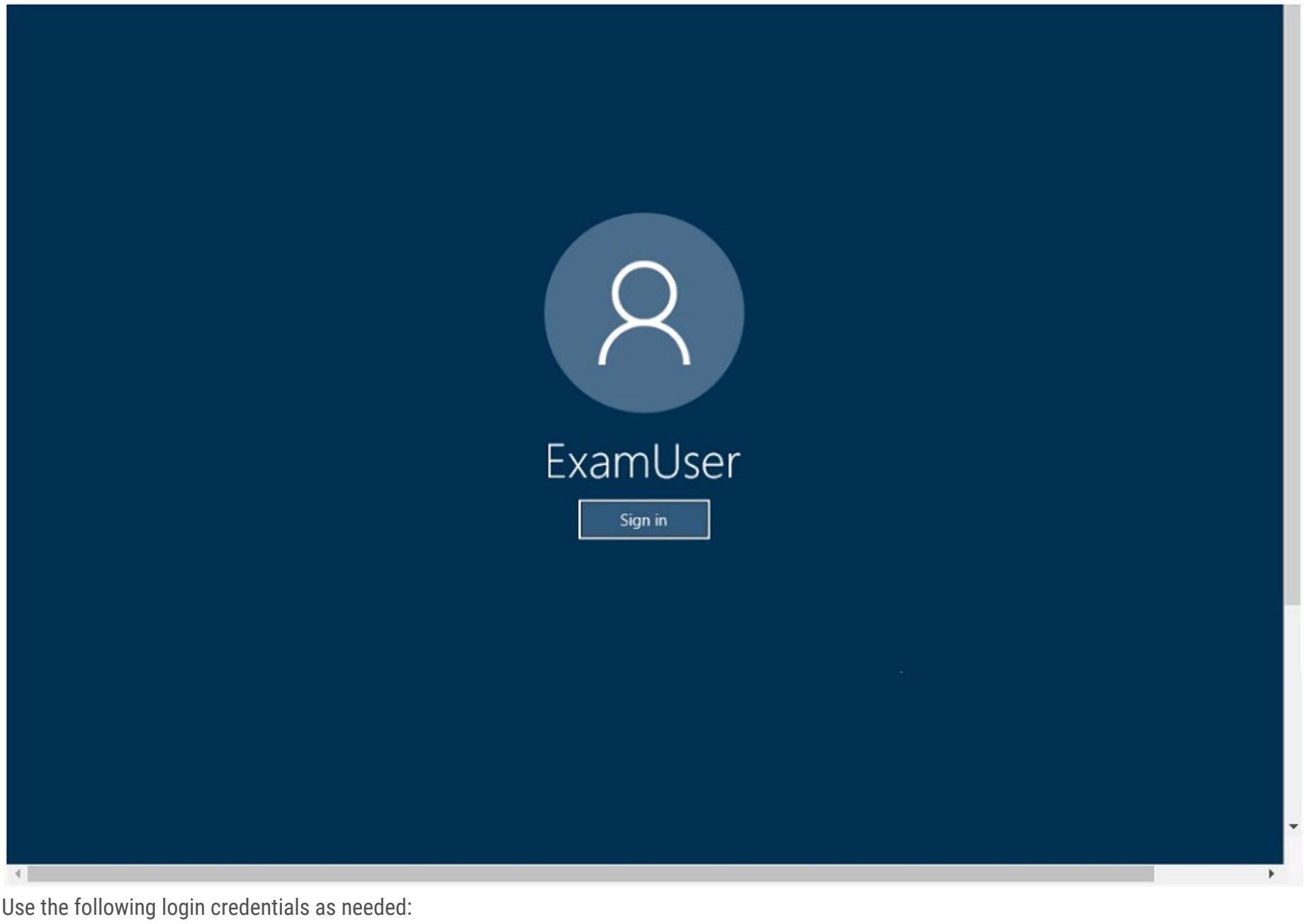
yup - worked perfectly for me

upvoted 1 times

Question #13 *Topic 4*

SIMULATION -
Please wait while the virtual machine loads. Once loaded, you may proceed to the lab section. This may take a few minutes, and the wait time will not be deducted from your overall test time.
When the Next button is available, click it to access the lab section. In this section, you will perform a set of tasks in a live environment. While most functionality will be available to you as it would be in a live environment, some functionality (e.g., copy and paste, ability to navigate to external websites) will not be possible by design.
Scoring is based on the outcome of performing the tasks stated in the lab. In other words, it doesnɹ€™t matter how you accomplish the task, if you successfully perform it, you will earn credit for that task.
Labs are not timed separately, and this exam may more than one lab that you must complete. You can use as much time as you would like to complete each lab.
But, you should manage your time appropriately to ensure that you are able to complete the lab(s) and all other sections of the exam in the time provided.
Please note that once you submit your work by clicking the Next button within a lab, you will NOT be able to return to the lab.

Username and password -



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@LODSe244001.onmicrosoft.com
Microsoft 365 Password: &=Q8v@2qGzYz
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: 11032396 -
You need to ensure that email messages in Exchange Online and documents in SharePoint Online are retained for eight years.
To complete this task, sign in to the Microsoft Office 365 admin center.

kazaki 4 months, 1 week ago
Why are u using retention in exchange it shall be done from compliance and security
upvoted 2 times

arunjana 2 months, 3 weeks ago

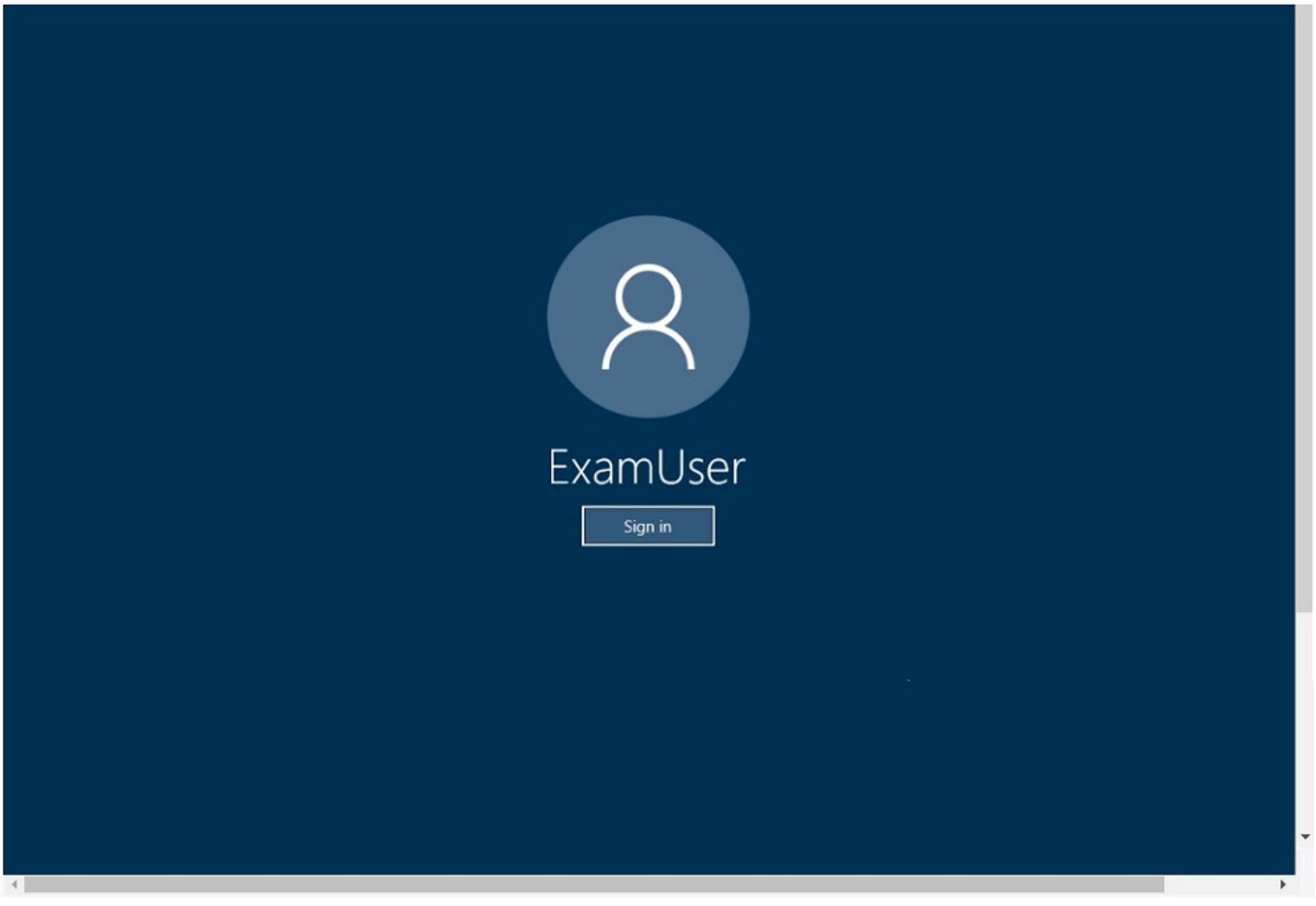
You're right. Can be done on the compliance center - https://compliance.microsoft.com/informationgovernance?viewid=retention

upvoted 2 times

Question #14 *Topic 4*

SIMULATION -
Please wait while the virtual machine loads. Once loaded, you may proceed to the lab section. This may take a few minutes, and the wait time will not be deducted from your overall test time.
When the Next button is available, click it to access the lab section. In this section, you will perform a set of tasks in a live environment. While most functionality will be available to you as it would be in a live environment, some functionality (e.g., copy and paste, ability to navigate to external websites) will not be possible by design.
Scoring is based on the outcome of performing the tasks stated in the lab. In other words, it doesnɹ€™t matter how you accomplish the task, if you successfully perform it, you will earn credit for that task.
Labs are not timed separately, and this exam may more than one lab that you must complete. You can use as much time as you would like to complete each lab.
But, you should manage your time appropriately to ensure that you are able to complete the lab(s) and all other sections of the exam in the time provided.
Please note that once you submit your work by clicking the Next button within a lab, you will NOT be able to return to the lab.

Username and password -



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@LODSe244001.onmicrosoft.com
Microsoft 365 Password: &=Q8v@2qGzYz
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: 11032396 -
You need to ensure that SharepointAdmins@contoso.com receives an alert when a user establishes a sync relationship to a document library from a computer that is a member of an Active Directory (AD) domain.
To complete this task, sign in to the Microsoft Office 365 admin center.

Ahmed911 1 month, 3 weeks ago

Tested it in my lab
Security & Compliance >> Alerts >> Alerts Policy >> Create new alert and choose in "Activity" (Upload files to document library)
upvoted 1 times

Rockalm 3 months, 1 week ago

you have to go to the dashboard --> Other alerts --> Activity alerts
upvoted 3 times

arunjana 2 months, 3 weeks ago

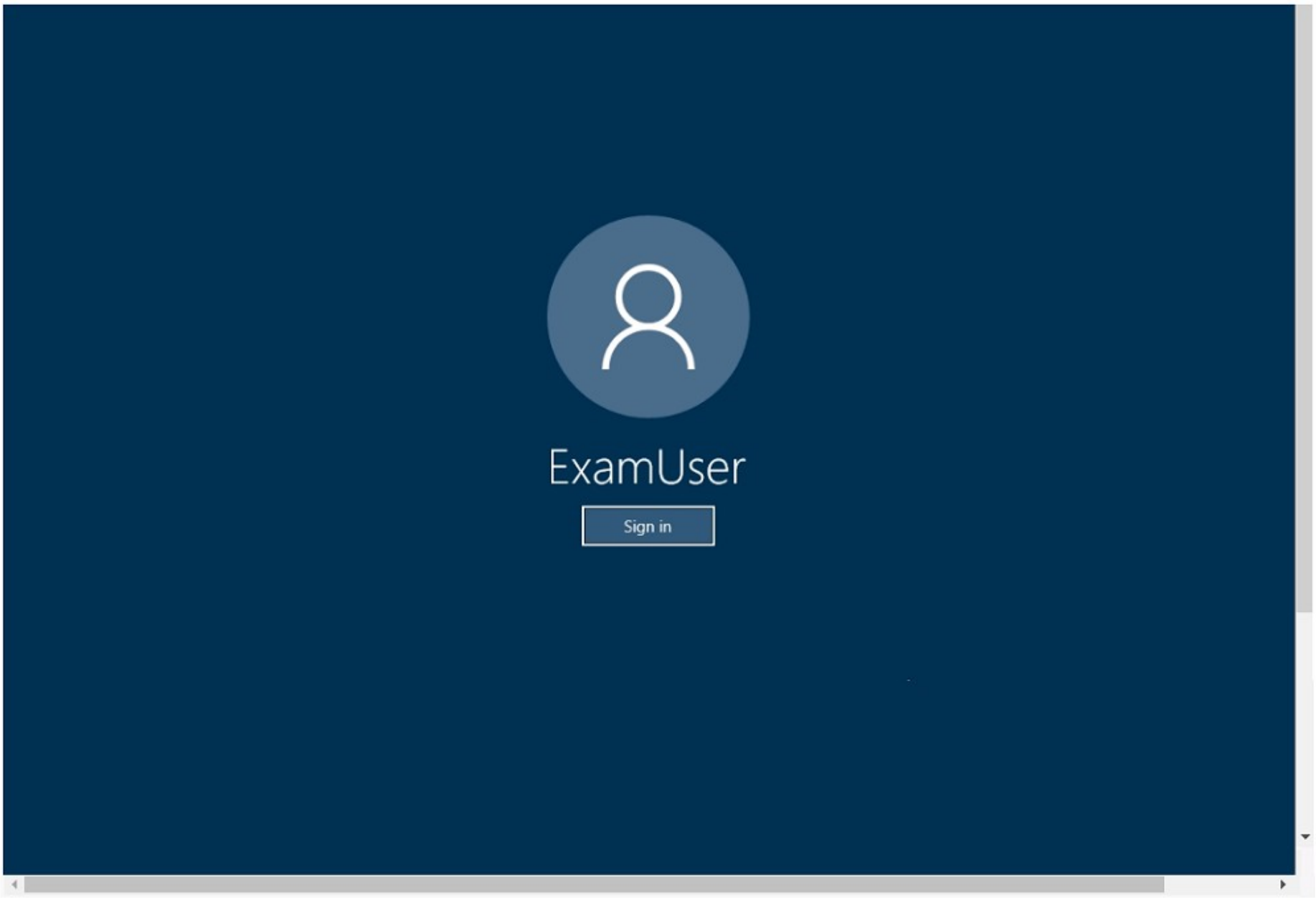
https://protection.office.com/managealerts

Activities > Synchronization Activities
upvoted 2 times

Question #15 *Topic 4*

SIMULATION -
Please wait while the virtual machine loads. Once loaded, you may proceed to the lab section. This may take a few minutes, and the wait time will not be deducted from your overall test time.
When the Next button is available, click it to access the lab section. In this section, you will perform a set of tasks in a live environment. While most functionality will be available to you as it would be in a live environment, some functionality (e.g., copy and paste, ability to navigate to external websites) will not be possible by design.
Scoring is based on the outcome of performing the tasks stated in the lab. In other words, it doesnɹ€™t matter how you accomplish the task, if you successfully perform it, you will earn credit for that task.
Labs are not timed separately, and this exam may more than one lab that you must complete. You can use as much time as you would like to complete each lab.
But, you should manage your time appropriately to ensure that you are able to complete the lab(s) and all other sections of the exam in the time provided.
Please note that once you submit your work by clicking the Next button within a lab, you will NOT be able to return to the lab.

Username and password -



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@LODSe244001.onmicrosoft.com
Microsoft 365 Password: &=Q8v@2qGzYz
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: 11032396 -
You need to create a case that prevents the members of a group named Operations from deleting email messages that contain the word IPO.
To complete this task, sign in to the Microsoft Office 365 admin center.

Question #16 *Topic 4*

DRAG DROP -

You have a Microsoft 365 subscription.

You have a site collection named SiteCollection1 that contains a site named Site2. Site2 contains a document library named Customers.

Customers contains a document named Litware.docx. You need to remove Litware.docx permanently.

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	Answer Area
From PowerShell, run `Remove-SPOUserProfile`	
Delete Litware.docx from the Recycle Bin of Site2.	
From PowerShell, run `Set-SPOSite`.	
Delete Litware.docx from the Recycle Bin of SiteCollection1.	
From Powershell, run `Remove-SPOUserInfo`	
Delete Litware.docx from Customers.	

kiketxu Highly Voted 4 months, 3 weeks ago

given answers are correct

upvoted 5 times

Joshing Most Recent 1 day, 23 hours ago

These are the best answer but to be correct for Sharepoint online at least you would do the same first two steps but then go to site settings, Under Site Collection Administration select Recycle Bin and then choose Second Stage Recycling Bin and then delete the file from there.

upvoted 1 times

bingomutant 4 months, 2 weeks ago

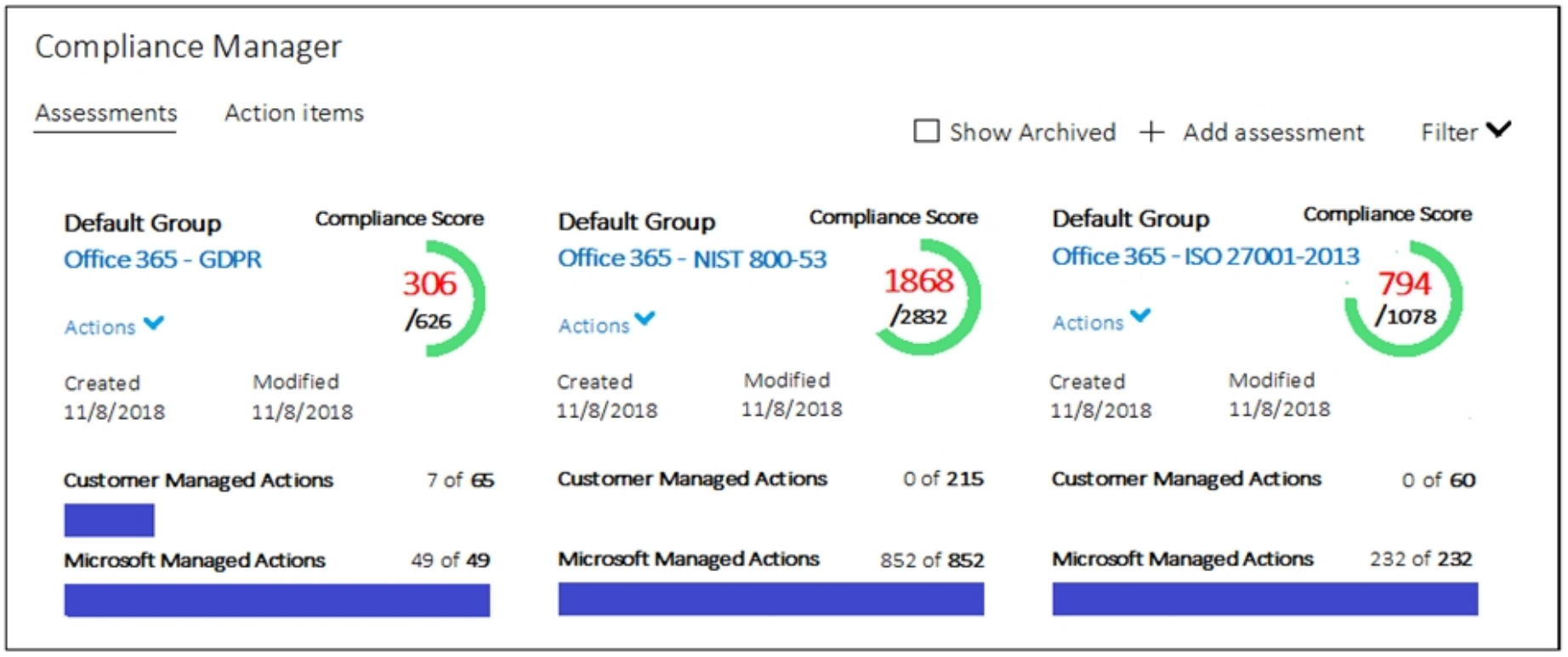
note for edxam no PS commands used :)

upvoted 4 times

Question #17 *Topic 4*

HOTSPOT -

You view Compliance Manager as shown in the following exhibit.



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

NOTE: Each correct selection is worth one point.

Hot Area:

Answer Area

To increase the GDPR Compliance Score for Microsoft Office 365, you must **[answer choice]**.

assign action items	V
review actions	
perform an assessment	
create a service request with Microsoft	

The current GDPR Compliance Score **[answer choice]**.

proves that the organization is non-compliant	V
proves that the organization is compliant	
shows that actions are required to evaluate compliance	

yaco33 Highly Voted 1 year, 4 months ago

Correction:
Assign Action itemshttps://docs.microsoft.com/en-us/microsoft-365/compliance/meet-data-protection-and-regulatory-reqs-using-microsoft-cloud?view=o365-worldwide#assessments-in-compliance-manager
-Shows that actions are required to evaluate compliance
the compliance manager can't be used to determine if an org is "compliant or not."
The Compliance Score does not express an absolute measure of organizational compliance with any particular standard or regulation. It expresses the extent to which you have adopted controls which can reduce the risks to personal data and individual privacy. No service can guarantee that you are compliant with a standard or regulation, and the Compliance Score should not be interpreted as a guarantee in any way.

upvoted 36 times

jack987 1 year, 1 month ago

I agree with Yaco33.

Answer:
Assign Action
Shows that actions are required to evaluate compliance

upvoted 14 times

yaco33 Highly Voted 1 year, 4 months ago

I think it should be:
- Review Actions
-Shows that actions are required to evaluate compliance

upvoted 11 times

Joshing Most Recent 1 day, 22 hours ago

Technical neither assigning or reviewing the Improvement Actions will increase the compliance score. It's only when you change the implementation and testing to passed will it improve the score but I guess by Microsoft's documentation you would in an ideal world assign the action to someone to implement.

An assessment isn't required as the image shows there are already three assessments in progress. It even shows they are on the assessments tab in Compliance Manager. GDPR wouldn't show up here if the assessment hadn't been created. So definitely not the correct answer.

The second answer is correct though.

upvoted 1 times

TimurKazan 3 months, 3 weeks ago

I would go with "perform an assessment" and "shows that actions are required to evaluate compliance
"

upvoted 2 times

Sugar123 4 months, 3 weeks ago

Correct Answers are:
Assign action items. See "Improvement actions" section : https://docs.microsoft.com/en-us/microsoft-365/compliance/compliance-manager?view=o365-worldwide
Shows that actions are required to evaluate compliance.
"If I have a high score, does it mean I'm fully compliant?
No. Your compliance score measures your progress in completing recommended actions that help reduce risks around data protection and regulatory standards. It does not express an absolute measure of organizational compliance with regard to a particular standard or regulation. Compliance Manager, and your compliance score, should not be interpreted as a guarantee in any way." https://docs.microsoft.com/en-us/microsoft-365/compliance/compliance-manager-faq?view=o365-worldwide

upvoted 3 times

Martyvdb 6 months, 2 weeks ago

You are likely to find that many of the noted actions are already complete when you review them. You simply need to review them, set an implementation and test date, and earn the points.
The noted score does not mean you are not compliant. It means you need to assess the recommended actions and confirm if you have them set or not.

upvoted 1 times

SSK500 6 months ago

So the answer should be "perform an assessment"?

upvoted 2 times

BBR 8 months, 4 weeks ago

1. To increase the GDPR Compliance Score for Microsoft Office 365, you must: Perform an assessment.
"Compliance Manager displays the total score for Office 365 ASSESSMENTS in the upper right-hand corner of the tile. This is the overall total Compliance Score for the Assessment and is the accumulation of points received for each control assessment..." From:
https://docs.microsoft.com/en-us/microsoft-365/compliance/meet-data-protection-and-regulatory-reqs-using-microsoft-cloud?view=o365-worldwide#understanding-the-compliance-score

upvoted 6 times

TonySuccess 8 months ago

Yep, looks to be another one of those things that has updated and changed recently.

You need to 'Add Assessment' this then provides you with the improvement actions to increase the score.

I can't even see assign action items or rewview actions anymore when in: https://compliance.microsoft.com/compliancemanager

upvoted 1 times

Dhanger 9 months, 3 weeks ago

Organization is non complaint:

The Compliance Score is a core component of the way that Compliance Manager helps organizations understand and manage their compliance. The Compliance Score for an assessment is an expression of the company's compliance with a given standard or regulation as a number, where the higher the score (up to the maximum number of points allocated for the Assessment), the better the company's compliance posture. Understanding the compliance scoring methodology in which assessment controls are assigned risk severity values between 1- 10 (low to high), and how completed control assessments add to the total compliance score is crucial to organizations for prioritizing their actions.
https://docs.microsoft.com/en-us/microsoft-365/compliance/meet-data-protection-and-regulatory-reqs-using-microsoft-cloud?view=o365-worldwide#understanding-the-compliance-score

upvoted 1 times

junkz 1 year ago

the score is comprised by many improvement action. some actions require just to be read/reviewed, some require interactive approach and mitigation. but the score only changes if these action items are being handled. and you can assign individual items to users in orderfor them to cary out whatever is required for that action, being a simple review or something else. remember that IT dep is not going to be responsible for the way the data is clasified by business for example. so it cannot and should not even attempt to handle each of the improvement actions that are surfaced in the portal. So assigning items is the right answer here

upvoted 2 times

mehnaz 1 year ago

How is the organization non-compliant? Do we need to complete certain percentage of "customer managed actions" for being compliant.

upvoted 2 times

mehnaz 1 year ago

could be because only 7/63 customer managed actions completed.

upvoted 1 times

examuser123 1 year, 1 month ago

This is a tricky one. Last one is correct (does not prove if compliant). Based on the wording it could either be review or perform an assessment. When clicking review for an action item it does give you the option to state it has been implemented which increases your score. Poor wording/answer selection as usual

upvoted 1 times

FableFa 1 year, 1 month ago

Assigning or reviewing action doesn't increase the score ! You need to pass the assessment ... For me answer are : 1. Perform an assessment & 2. Show that actions are required to evaluate compliance.

upvoted 4 times

musiman 8 months, 3 weeks ago

You are right. You need to do an assessment:
Each Assessment includes a total Compliance Score based on the shared responsibility model. Microsoft's implementation and testing of controls for Office 365 contributes a portion of the total possible points associated with a GDPR assessment. As the customer implements and tests each of the customer Actions, the Compliance Score for the Assessment will increase by the value assigned to the control.

upvoted 3 times

billy22 1 year, 2 months ago

Yaco is right, check this link: https://docs.microsoft.com/en-us/microsoft-365/compliance/compliance-score-faq?view=o365-worldwide#if-i-have-a-high-score-does-it-mean-im-fully-compliant

upvoted 2 times

[Removed] 1 year, 4 months ago

More exactly, why is the organization non-compliant?

upvoted 1 times

itmp 1 year, 3 months ago

view yaco33 answer.

upvoted 1 times

Question #18 *Topic 4*

You have a Microsoft 365 subscription.

All computers run Windows 10 Enterprise and are managed by using Microsoft Endpoint Manager.

You plan to view only security-related Windows telemetry data.

You need to ensure that only Windows security data is sent to Microsoft.

What should you create from the Endpoint Management admin center?

A. a device configuration profile that has device restrictions configured

B. a device configuration profile that has the Endpoint Protection settings configured

C. a device compliance policy that has the System Security settings configured

D. a device compliance policy that has the Device Health settings configured

arunjana 2 months, 3 weeks ago

Given answer is correct. You create a device configuration profile with device restrictions

upvoted 2 times

Question #19 *Topic 4*

You create a label that encrypts email data. Users report that they cannot use the label in Outlook on the web to protect the email messages they send.

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

What should you do?

A. Modify the priority order of label policies

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

C. Create a label policy

D. Create a new sensitive information type

Ronnie123 Highly Voted 1 year, 8 months ago

I believe this is C. Create a label policy, because labels need to be published in order to be visisble. See: https://docs.microsoft.com/en-us/microsoft-365/compliance/sensitivity-labels#what-label-policies-can-do

upvoted 44 times

STFN2019 1 year, 1 month ago

I will go with C on the exam as well. Thanks!

upvoted 7 times

mehnaz 1 year ago

It is C for sure. One creates a label but for users to use it, admin has to publish labels by creating label policy.

upvoted 8 times

VTHAR 10 months, 1 week ago

Yes, the label need to be published (create policy). Answer is C.

upvoted 3 times

kiketxu Most Recent 4 months, 3 weeks ago

Missing the label policy publishing so, C should be the right answer.

upvoted 2 times

kuome 6 months ago

You make your sensitivity labels available to users by publishing them in a sensitivity label policy that appears in a list on the Sensitivity policies tab on the Label policies page. https://docs.microsoft.com/en-us/microsoft-365/compliance/sensitivity-labels#what-label-policies-can-do

upvoted 1 times

GregD133 8 months, 2 weeks ago

I say C based off of what is in the portal after creating an encryption label:

 Your label was created
Ready to put this label to work? There are a couple options: publish it or automatically apply it to content.

upvoted 3 times

NatP 9 months ago

Question lacks details. Doesn't say that the label was published.

upvoted 2 times

Morne 10 months, 3 weeks ago

Policy Creation

The next thing you need to do is create a Policy to publish your labels.

https://thevaliantway.com/2019/01/encrypting-email-office-365-azure-information-protection/

upvoted 2 times

Blue 11 months, 3 weeks ago

The Question has stated "You create a label that encrypts email data" But it does not state that you have created a policy for the label. So I beleive that the correct answer would be C based on "After you create your sensitivity labels, you need to publish them, to make them available to people and services in your organization."
Ref- https://docs.microsoft.com/en-us/microsoft-365/compliance/sensitivity-labels?view=o365-worldwide#what-label-policies-can-do

upvoted 2 times

Soumia_Djenan 1 year, 2 months ago

The answer given is correct wait for 6 hours "taken from Alex de jong a Microsoft certified trainer during a Microsoft MS-500 training webinar"

upvoted 3 times

MahmoudEldeep 8 months ago

When publishing a label it does not take this long to appear to users.. i believe it is matter of publishing the label.

upvoted 2 times

Xten 1 year, 1 month ago

Did you not ask for a proof for this, I have heard 48 hrs for ATP report submission, 1hr for blacklisted IP or sometimes 7days for retention policy(though now 24hrs) etc but never 6hrs.... I go with publish the label.

upvoted 2 times

gills 1 year, 3 months ago

Question said it "created a label". No mention of publish a label.
C is correct.

B just not right. Only mention is 24 hours wait. Nothing about 6 hours.

upvoted 2 times

itmp 1 year, 3 months ago

B.) because: "It's the label policy that publishes the labels"
https://docs.microsoft.com/en-us/microsoft-365/compliance/create-sensitivity-labels?view=o365-worldwide
*Also, could not find anything about the '6hour wait period'...

upvoted 1 times

matthu 1 year, 3 months ago

from Ronnie's link: "After you create a label policy that assigns sensitivity labels to users and groups, allow up to 24 hours for these users to see the labels in their Office apps."

so 6hrs doesn't really seem right, I mean I guess it's possible, but seems like the best answer here would be to create the policy since it didn't explicitly state that it was created, and it's required to deploy sensitivity labels.

upvoted 3 times

JRodJ 8 months ago

From link itmp sent: "Until you publish your labels, they won't be available to select in apps or for services. To publish the labels, they must be added to a label policy." There is a comment about 24 hours, but that seems to be only related to changing a label that has already been published

upvoted 1 times

JRodJ 8 months ago

Which I forgot to say means correct answer is C: Create a label policy

upvoted 1 times

kmsrajan 1 year, 5 months ago

Both B an C is correct. The question is not clear

upvoted 1 times

Ashton_98 7 months, 2 weeks ago

Because it doesn't say it works in local Outlook either, it's most likely the newly created label hasn't been published.

upvoted 1 times

BobInTheMoon 1 year, 6 months ago

Create a label policy.

upvoted 4 times

Question #20 *Topic 4*

You have a Microsoft 365 subscription that includes a user named Admin1.

You need to ensure that Admin1 can retain all the mailbox content of users, including their deleted items.

The solution must use the principle of least privilege.

What should you do?

A. From the Microsoft 365 admin center, assign the Exchange administrator role to Admin1.

B. From the Exchange admin center, assign the Security Administrator role to Admin1.

C. From the Azure Active Directory admin center, assign the Service administrator role to Admin1.

D. From the Exchange admin center, assign the Recipient Management admin role to Admin1.

kiketxu 4 months, 3 weeks ago

These answers seems not correct. It should be eDiscovery Management role which missing here. https://docs.microsoft.com/es-es/exchange/permissions-exo/permissions-exo

https://www.examtopics.com/discussions/microsoft/view/15096-exam-ms-500-topic-4-question-7-discussion/

The only possile role applicable is EX admin, but this is not compliance with the PoPL.

upvoted 4 times

masger 2 weeks ago

The key is the requested action, it says 'can retain' which refers the possibility to create a retention policy over the user mailbox, nothing to do with eDiscovery...

upvoted 2 times

chaoscreater 1 month ago

What's PoPL?

upvoted 2 times

GeraldB 1 month ago

Principle of least privilege i assume

upvoted 1 times

Question #21 *Topic 4*

You have a hybrid Microsoft 365 environment.

All computers run Windows 10 Enterprise and have Microsoft 365 Apps for enterprise installed. All the computers are joined to Active Directory.

You have a server named Server1 that runs Windows Server 2016. Server1 hosts the telemetry database. You need to prevent private details in the telemetry data from being transmitted to Microsoft.

What should you do?

A. On Server1, run readinessreportcreator.exe

B. Configure a registry entry on Server1

C. Configure a registry entry on the computers

D. On the computers, run tdadm.exe

DudleyYVR Highly Voted 3 months, 2 weeks ago

seriously we're expected to know this level of detail for exam cert?

upvoted 12 times

sparkynz 2 months, 3 weeks ago

Welcome to Microsoft exams, where you're expected to know what normal people LOOK UP :)

upvoted 9 times

kiketxu Highly Voted 4 months, 3 weeks ago

https://docs.microsoft.com/en-us/deployoffice/compat/manage-the-privacy-of-data-monitored-by-telemetry-in-office#to-enable-file-obfuscation-by-using-the-registry:~:text=The%20following%20example%20enables%20file%20obfuscation,it%20on%20the%20monitored%20client%20computers.

upvoted 6 times

Question #22 *Topic 4*

Your company has a Microsoft 365 subscription that includes a user named User1.

You suspect that User1 sent email messages to a competitor detailing company secrets.

You need to recommend a solution to ensure that you can review any email messages sent by User1 to the competitor, including sent items that were deleted.

What should you include in the recommendation?

A. Enable In-Place Archiving for the mailbox of User1

B. From the Security & Compliance, perform a content search of the mailbox of User1

C. Place a Litigation Hold on the mailbox of User1

D. Configure message delivery restrictions for the mailbox of User1

belyo 4 months ago

just another bad formed question...
you need first to place it on hold and after that to do a content search
or eDiscovery case could do both but Microsoft...

upvoted 2 times

kiketxu 4 months, 3 weeks ago

Rigth answer.
https://docs.microsoft.com/en-us/exchange/security-and-compliance/in-place-and-litigation-holds

upvoted 3 times

nzboy123 5 months, 3 weeks ago

Why wouldn't it be B?

upvoted 1 times

chaoscreater 1 month ago

How is your answer B gonna deal with this - "including sent items that were deleted."

upvoted 1 times

PattiD 7 months, 3 weeks ago

https://docs.microsoft.com/en-us/exchange/policy-and-compliance/holds/litigation-holds?view=exchserver-2019

https://docs.microsoft.com/en-us/exchange/security-and-compliance/in-place-and-litigation-holds

upvoted 3 times

Zorag 1 year, 5 months ago

Although it is not an option the correct way to do this would be via retention policies. https://docs.microsoft.com/en-us/microsoft-365/compliance/retention-policies?view=o365-worldwide

upvoted 1 times

tintin_ 1 year, 2 months ago

retention policies apply only for retaining some content excluding any litigation issues. Here, as the company suspects one of its employees, it can use the legal advisory to put a litigation hold and check it out

upvoted 12 times

Question #23 *Topic 4*

You have a Microsoft 365 subscription.

Yesterday, you created retention labels and published the labels to Microsoft Exchange Online mailboxes.

You need to ensure that the labels will be available for manual assignment as soon as possible.

What should you do?

A. From the Security & Compliance admin center, create a label policy

B. From Exchange Online PowerShell, run Start-RetentionAutoTagLearning

C. From Exchange Online PowerShell, run Start-ManagedFolderAssistant

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

junkz Highly Voted 1 year ago

Correct answer.
The Managed Folder Assistant uses the retention policy settings of users' mailboxes to process retention of items. This mailbox processing occurs automatically. You can use the Start-ManagedFolderAssistant cmdlet to immediately start processing the specified mailbox.

upvoted 17 times

kiketxu Most Recent 4 months, 3 weeks ago

C for sure!

upvoted 3 times

Morne 10 months, 3 weeks ago

The Managed Folder Assistant uses the retention policy settings of users' mailboxes to process retention of items. This mailbox processing occurs automatically. You can use the Start-ManagedFolderAssistant cmdlet to immediately start processing the specified mailbox.

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

upvoted 2 times

paulfns2020 1 year, 2 months ago

https://docs.microsoft.com/en-us/powershell/module/exchange/start-managedfolderassistant

upvoted 3 times

paulfns2020 1 year, 2 months ago

https://docs.microsoft.com/en-us/exchange/security-and-compliance/messaging-records-management/messaging-records-management

upvoted 1 times

[Removed] 1 year, 7 months ago

https://docs.microsoft.com/en-us/microsoft-365/compliance/labels#how-long-it-takes-for-retention-labels-to-take-effect

upvoted 1 times

[Removed] 1 year, 7 months ago

https://docs.microsoft.com/en-us/microsoft-365/compliance/labels

upvoted 1 times

Question #24 *Topic 4*

You have a Microsoft 365 subscription.
Your company uses Jamf Pro to manage macOS devices.
You plan to create device compliance policies for the macOS devices based on the Jamf Pro data.
You need to connect Microsoft Endpoint Manager to Jamf Pro.
What should you do first?

A. From the Azure Active Directory admin center, add a Mobility (MDM and MAM) application.

B. From the Endpoint Management admin center, add the Mobile Threat Defense connector.

C. From the Endpoint Management admin center, configure Partner device management.

D. From the Azure Active Directory admin center, register an application.

sdeyoung 2 months, 2 weeks ago
Is this even on the exam?
upvoted 3 times

kiketxu 4 months, 3 weeks ago
I'm agree. Given answer is right.
https://docs.microsoft.com/en-us/mem/intune/protect/conditional-access-integrate-jamf
upvoted 4 times

DTz 1 year, 1 month ago
The correct answer is C.

Source:
https://docs.microsoft.com/en-us/mem/intune/protect/conditional-access-integrate-jamf

Enable Intune to integrate with Jamf Pro
1. Sign in to the Microsoft Endpoint Manager admin center.
2. Select Tenant administration > Connectors and tokens > Partner device management.
upvoted 1 times

efinotti 1 year, 1 month ago
But first you need to register a new application.
Given answer is correct. D
Source: https://docs.microsoft.com/en-us/mem/intune/protect/conditional-access-integrate-jamf#create-an-application-in-azure-active-directory
upvoted 21 times

Buddhiman 10 months, 2 weeks ago
@efinotti is right. First, you need to register before integration.

Connect Intune to Jamf Pro

To connect Intune with Jamf Pro:

Create a new application in Azure.
Enable Intune to integrate with Jamf Pro.
Configure Conditional Access in Jamf Pro.

Once registration is complete, you will receive App ID for integration.
upvoted 3 times

Question #25 *Topic 4*

Note: This question is part of a series of questions that present the same scenario. Each question in the series contains a unique solution that might meet the stated goals. Some question sets might have more than one correct solution, while others might not have a correct solution.
After you answer a question in this section, you will NOT be able to return to it. As a result, these questions will not appear in the review screen.
You have a Microsoft 365 subscription that contains 1,000 user mailboxes.
An administrator named Admin1 must be able to search for the name of a competing company in the mailbox of a user named User5.
You need to ensure that Admin1 can search the mailbox of User5 successfully. The solution must prevent Admin1 from sending email messages as User5.
Solution: You modify the privacy profile, and then create a Data Subject Request (DSR) case.
Does this meet the goal?

A. Yes

B. No

GevedeBe 3 months, 2 weeks ago
DSR is not part of a search for competing company (see question). DSR is part of GDPR privacy information, so editing the profile is ok, but the rest of the answer, suggested is wrong, so B!
upvoted 1 times

ellik 3 months, 2 weeks ago
In the EAC, navigate to Recipients > Mailboxes.

In the list of mailboxes, select the mailbox that you want to assign permissions for, and then select EditEdit icon.

On the mailbox properties page, select Mailbox Delegation.

To assign permissions to delegates, select AddAdd icon under Full Access to display a page that lists all recipients in your Exchange organization that can be assigned the permission. Select the recipients you want, add them to the list, and then select OK. You can also search for a specific recipient by typing the recipient's name in the search box and then selecting Search Search icon.

The Full Access permission allows a delegate to open a user's mailbox and access the contents of the mailbox.

Note

Assigning the Full Access permission doesn't allow the delegate to send email from the mailbox.You have to assign the delegate the Send As or the Send on Behalf permission to send email.

https://docs.microsoft.com/en-us/exchange/troubleshoot/user-and-shared-mailboxes/how-to-access-other-mailboxes
upvoted 2 times

Rafale 4 months, 1 week ago
The correct answer is A
upvoted 1 times

chaoscreater 1 month ago
The correct answer is you're an idiot who spams useless info in the comments.
upvoted 4 times

kiketxu 4 months, 3 weeks ago
I don't see this could complies the statement without an eDiscovery role
upvoted 2 times

Question #26 *Topic 4*

SIMULATION -
You need to ensure that administrators can publish a label that adds a footer to email messages and documents.
To complete this task, sign in to the Microsoft Office 365 portal.

Question #27 *Topic 4*

SIMULATION -

You plan to publish a label that will retain documents in Microsoft OneDrive for two years, and then automatically delete the documents.

You need to create the label.

To complete this task, sign in to the Microsoft Office 365 portal.

Rockalm 3 months, 2 weeks ago

go to compliance --> Information Governance --> Labels. Create the label and the go to label policies --> publish

upvoted 3 times

Question #28 *Topic 4*

SIMULATION -

You plan to add a file named ConfidentialHR.docx to a Microsoft SharePoint library.

You need to ensure that a user named Megan Bowen is notified when another user accesses ConfidentialHR.xlsx.

To complete this task, sign in to the Microsoft 365 portal.

nineten Highly Voted 10 months, 1 week ago

I think 'Activity is' being set to 'Accessed file' makes more sense than 'Any file or folder activity.'

upvoted 7 times

Dickson Most Recent 10 months, 3 weeks ago

docx or xlsx.....?

upvoted 3 times

Question #29 *Topic 4*

SIMULATION -

You need to create a policy that identifies content in Microsoft OneDrive that contains credit card numbers.

To complete this task, sign in to the Microsoft 365 portal.

AndersPsYnet Highly Voted 1 year, 1 month ago

Hmm... the ask is to identify if credit card information is stored in OneDrive. Auto-labeling is used if you also want to set a sensitivity label of files that include this information. Correct answer would be to define a DLP policy for Credit card information in OneDrive since this will give you information if this excist.

upvoted 12 times

MBraga 1 year, 1 month ago

I agree,
https://docs.microsoft.com/en-us/microsoft-365/compliance/create-a-dlp-policy-from-a-template?view=o365-worldwide

upvoted 1 times

jaz600 Highly Voted 9 months, 1 week ago

1.Security & Compliance
2.Dataloss Prevention -> Policy
3.Create Policy
4.Under Choose locations select -> Let me choose location- Select One Drive only
5.Under Find Content that contains -> Edit -> Add -> Sensitive info types -> Add -> Type Credit Card Number -> Click Add
6.Reduce instances to 1
7.Yes, turn it on right away -> Save

upvoted 12 times

JakubK64 Most Recent 2 weeks, 3 days ago

Shouldn't it be just data classification instead of DLP? There is nothing about protecting this data, just identify it. Credit card pattern is built-in in data classification types

upvoted 1 times

Rockalm 3 months, 2 weeks ago

I also vote for DLP. With auto labeling you can choose certain user locations like this "https://contoso-my.sharepoint.com/personal/rsimone_contoso_onmicrosoft_com" to check for credit cards or stuff. 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 1 times

loudlumi 9 months ago

The answer is correct, you use DLP to detect exfiltration of sensitive data. DLPs do not identify they only detect when data is being transferred.

upvoted 2 times

Garrethk 8 months, 2 weeks ago

First Point on article referenced by MBraga above:
"With a DLP policy, you can:

Identify sensitive information across many locations, such as Exchange Online, SharePoint Online, OneDrive for Business, and Microsoft Teams.

For example, you can identify any document containing a credit card number that's stored in any OneDrive for Business site, or you can monitor just the OneDrive sites of specific people."

upvoted 2 times

phopyi 1 year ago

Why didn't use MCAS instead?

upvoted 3 times

MahmoudEldeep 7 months, 3 weeks ago

MCAS is the most accurate solution for detecting such data on cloud storage apps

upvoted 1 times

Question #30 *Topic 4*

SIMULATION -

Your company plans to merge with another company.

A user named Debra Berger is an executive at your company.

You need to provide Debra Berger with all the email content of a user named Alex Wilber that contains the word merger.

To complete this task, sign in to the Microsoft 365 portal.

Question #31 *Topic 4*

Note: This question is part of a series of questions that present the same scenario. Each question in the series contains a unique solution that might meet the stated goals. Some question sets might have more than one correct solution, while others might not have a correct solution.

After you answer a question in this section, you will NOT be able to return to it. As a result, these questions will not appear in the review screen.

You have a Microsoft 365 subscription.

You have a user named User1. Several users have full access to the mailbox of User1.

Some email messages sent to User1 appear to have been read and deleted before the user viewed them.

When you search the audit log in Security & Compliance to identify who signed in to the mailbox of User1, the results are blank.

You need to ensure that you can view future sign-ins to the mailbox of User1.

You run the Set-Mailbox -Identity "User1" -AuditEnabled $true command.

Does that meet the goal?

A. Yes

B. No

Jpower5000 5 months, 1 week ago

Typo in the command "set-maibox" otherwise this is correct.

upvoted 1 times

JOKERO 5 months, 2 weeks ago

Exchange server: https://docs.microsoft.com/en-us/exchange/policy-and-compliance/mailbox-audit-logging/enable-or-disable?view=exchserver-2019

MS365 : https://docs.microsoft.com/en-us/microsoft-365/compliance/enable-mailbox-auditing?view=o365-worldwide#change-the-mailbox-actions-to-audit:~:text=You%20can%20use%20the%20AuditAdmin%2C%20AuditDelegate%2C,365%20group%20mailboxes%20can't%20be%20customized).

upvoted 2 times

DrMe 7 months, 2 weeks ago

https://docs.microsoft.com/en-us/powershell/module/exchange/set-mailbox?view=exchange-ps#parameters:~:text=The%20AuditEnabled%20parameter%20specifies%20whether%20to,mailbox%20audit%20logging%20for%20the%20mailbox.

upvoted 3 times

svm_Terran 8 months ago

A. Yes

upvoted 1 times

TDAC 10 months, 2 weeks ago

Answer is correct.

Source: https://docs.microsoft.com/en-us/exchange/policy-and-compliance/mailbox-audit-logging/enable-or-disable?view=exchserver-2019

With mailbox audit logging in Exchange Server, you can track logons to a mailbox as well as what actions are taken while the user is logged on.

upvoted 3 times

Question #32 *Topic 4*

Note: This question is part of a series of questions that present the same scenario. Each question in the series contains a unique solution that might meet the stated goals. Some question sets might have more than one correct solution, while others might not have a correct solution.
After you answer a question in this section, you will NOT be able to return to it. As a result, these questions will not appear in the review screen.
You have a Microsoft 365 subscription.
You have a user named User1. Several users have full access to the mailbox of User1.
Some email messages sent to User1 appear to have been read and deleted before the user viewed them.
When you search the audit log in Security & Compliance to identify who signed in to the mailbox of User1, the results are blank.
You need to ensure that you can view future sign-ins to the mailbox of User1.
You run the Set-AuditConfig -Workload Exchange command.
Does that meet the goal?

A. Yes

B. No

paulfns2020 Highly Voted 1 year, 2 months ago
Answer is NO

"Use the Set-AuditConfig cmdlet to configure the auditing configuration in the Security & Compliance Center. The auditing configuration specifies where auditing is allowed in Microsoft Office 365."
upvoted 11 times

tintin_ Highly Voted 1 year, 2 months ago
NO audit logging for a single user can't be enable by this command. Also the reference link proves the statement
upvoted 7 times

VTHAR 10 months, 3 weeks ago
Agreed. It doesn't meet the goal. So, answer is "NO".
upvoted 2 times

kiketxu Most Recent 4 months, 3 weeks ago
I understand the goal is enable the Audit to allow check the sign-ins for user1. Of course it will audit all Exchange, but it complies with the goal so it's correct.
If the case was audit to all users, it should be included in the statement and in that case, this command is overzised and the answer wasn't valid.
upvoted 2 times

diggity801 1 year, 4 months ago
https://docs.microsoft.com/en-us/powershell/module/exchange/policy-and-compliance-audit/set-auditconfig?view=exchange-ps

Answer is YES
upvoted 1 times

ettinhart77 1 year, 3 months ago
Answer is correct.

https://docs.microsoft.com/en-us/exchange/policy-and-compliance/mailbox-audit-logging/enable-or-disable?view=exchserver-2019
upvoted 1 times

Question #33 *Topic 4*

You have a Microsoft 365 subscription.

You have a Microsoft SharePoint Online site named Site1. The files in Site1 are protected by using Microsoft Azure Information Protection.

From the Security & Compliance admin center, you create a label that designates personal data.

You need to auto-apply the new label to all the content in Site1.

What should you do first?

A. From PowerShell, run Set-ManagedContentSettings.

B. From PowerShell, run Set-ComplianceTag.

C. From the Security & Compliance admin center, create a Data Subject Request (DSR).

D. Remove Azure Information Protection from the Site1 files.

jack987 Highly Voted 1 year, 1 month ago

Answer is correct.

Sensitivity labels are currently recommended for applying labels to files on premises and in other cloud services and providers. These are also recommended for files in Microsoft 365 that require Azure Information Protection encryption for data protection, such as trade secret files.

At this time, using Azure Information Protection to apply encryption is not recommended for files in Microsoft 365 with data that is subject to the GDPR. Microsoft 365 services currently cannot read into AIP-encrypted files. Therefore, the service can't find sensitive data in these files.

Source: https://docs.microsoft.com/en-us/microsoft-365/compliance/apply-labels-to-personal-data-in-office-365?view=o365-worldwide

upvoted 27 times

Kalzonee3611 2 months, 2 weeks ago

Brilliant, thanks for that!

upvoted 1 times

Thuthukani 7 months, 4 weeks ago

Great explanation!

upvoted 2 times

kiketxu Most Recent 4 months, 3 weeks ago

The answer is correct to me. You can't use automatic labeling for documents and emails that were previously manually labeled, or previously automatically labeled with a higher sensitivity.
As the statement does not clarify if the previous was also an automated labeling nor their priority order, the solution won't work if you don't remove the previous label.

https://docs.microsoft.com/en-us/microsoft-365/compliance/apply-sensitivity-label-automatically?view=o365-worldwide#when-automatic-or-recommended-labels-are-applied

NOTE for Examtopics: The reference link hasn't relation with the question or solution. Same than other links shared in the discussion. They are all deprecated.

upvoted 3 times

SUBZER0 11 months ago

https://docs.microsoft.com/es-es/microsoft-365/compliance/apply-labels-to-personal-data-in-office-365?view=o365-worldwide#older-auto-apply-policies-win

If there are multiple rules that assign an auto-apply label and content meets the conditions of multiple rules, the label for the oldest rule is assigned. For this reason, it's important to plan the label policies carefully before configuring them. If an organization requires a change to the priority of the label policies, they'll need to delete and recreate them.

upvoted 4 times

WoneSix 1 year, 6 months ago

Specifically, https://docs.microsoft.com/en-us/microsoft-365/compliance/apply-labels-to-personal-data-in-office-365#prioritize-auto-apply-label-policies - older labels win out (manual or auto applied).

upvoted 4 times

Question #34 *Topic 4*

You have a Microsoft 365 subscription.

You need to be notified by email whenever an administrator starts an eDiscovery search.

What should you do from the Security & Compliance admin center?

A. From Search & investigation, create a guided search.

B. From Events, create an event.

C. From Alerts, create an alert policy.

D. From Search & investigation, create an eDiscovery case.

TDAC Highly Voted 10 months, 2 weeks ago

Answer is correct.

Alerts are created in protection.office.com -> Alerts -> New Alert Policy

In here you can specify an alert to be generated when "An eDiscovery search was started or exported".

upvoted 12 times

Question #35 *Topic 4*

You have a Microsoft 365 subscription.

You have a Data Subject Request (DSR) case named Case1.

You need to ensure that Case1 includes all the email posted by the data subject to the Microsoft Exchange Online public folders.

Which additional property should you include in the Content Search query?

A. kind:externaldata

B. itemclass:ipm.externaldata

C. itemclass:ipm.post

D. kind:email

shanti0091 6 months, 1 week ago

The answer is 100% Correct

upvoted 3 times

Morne 10 months, 1 week ago

Correct

itemclass:ipm.post AND "<email address of the data subject>"

upvoted 3 times

Oz 11 months, 3 weeks ago

I think the answer should be D
The question is asking about finding all e-mails, it should be kind:email
answer D is about notes, check the reference.
https://docs.microsoft.com/en-us/microsoft-365/compliance/keyword-queries-and-search-conditions?view=o365-worldwide#search-conditions

upvoted 1 times

saran1987 11 months, 2 weeks ago

No, the answer is correct. Just refer the link shared in the answer.

" The built-in search in a DSR case will only return email messages that the data subject sent to a mail-enabled public folder or messages that someone else sent to a public folder and also copied the data subject. It doesn't return messages that the data subject posted to a public folder. To search for items that the data subject posted to a public folder, you can create a separate create a separate Content Search that searches for any item posted to a public folder by the data subject"

In the Keywords box, use the following search query:

PowerShell

Copy
itemclass:ipm.post AND "<email address of the data subject>"
Search all Exchange public folders

upvoted 11 times

TDAC 10 months, 1 week ago

^ 100% agree. Answer is correct.

upvoted 3 times

kiketxu 4 months, 3 weeks ago

Agree.

upvoted 3 times

Question #36 *Topic 4*

You have a Microsoft 365 E5 subscription.

A security manager receives an email message every time a data loss prevention (DLP) policy match occurs.

You need to limit alert notifications to actionable DLP events.

What should you do?

A. From the Security & Compliance admin center, modify the Policy Tips settings of a DLP policy.

B. From the Cloud App Security admin center, apply a filter to the alerts.

C. From the Security & Compliance admin center, modify the User overrides settings of a DLP policy.

D. From the Security & Compliance admin center, modify the matched activities threshold of an alert policy.

TDAC Highly Voted 10 months, 2 weeks ago

Answer is correct.

When the alert is triggered - You can configure a setting that defines how often an activity can occur before an alert is triggered. This allows you to set up a policy to generate an alert every time an activity matches the policy conditions, when a certain threshold is exceeded, or when the occurrence of the activity the alert is tracking becomes unusual for your organization.

Source: https://docs.microsoft.com/en-us/microsoft-365/compliance/alert-policies?view=o365-worldwide

upvoted 10 times

kiketxu Most Recent 4 months, 3 weeks ago

D for sure!

upvoted 3 times

PeeyushS 5 months, 3 weeks ago

The confusion on "Updated User" is clarified in the two links below. Update user will look at Sign In Risk , User Risk ...and not an attributes that have changed, Thus "Update User" is not correct for this scenario.
https://docs.microsoft.com/en-us/microsoft-365/compliance/search-the-audit-log-in-security-and-compliance?view=o365-worldwide
https://docs.microhttps://docs.microsoft.com/en-us/azure/active-directory/reports-monitoring/concept-audit-logsoft.com/en-us/azure/active-directory/reports-monitoring/concept-audit-logs

upvoted 1 times

Question #37 *Topic 4*

HOTSPOT -

You have a Microsoft 365 subscription. Auditing is enabled.

A user named User1 is a member of a dynamic security group named Group1.

You discover that User1 is no longer a member of Group1.

You need to search the audit log to identify why User1 was removed from Group1.

Which two activities should you use in the search? To answer, select the appropriate activities in the answer area.

NOTE: Each correct selection is worth one point.

Hot Area:

itmp Highly Voted 1 year, 3 months ago

Got the time and tested this.
Answer is:
-Removed member from group
-Updated group

"Updated User" yields no results!

Removed member from group:
=> shows the user that was removed (by modifying dynamic the query)

Updated group
=> shows what user 'updated' the group.

upvoted 25 times

SUBZER0 11 months ago

-----"Updated User" yields no results! ->
unless the user is eddited therefore kicked out from the group

----Updated group=> shows what user 'updated' the group.
Probably because you edited the gruop to kick out the user

If only 1 user is affected probably the change was made in the user and not in the group.
I would say answers are right, anyway you have more chances to find the root cause if you look at to different things, the group and the user.

upvoted 2 times

junkz 1 year ago

I think you need to lay out the test conditions too. the scenario talks about one single user being removed, so , in order for the modification of the dynamic query to affect a single user, it means it was trumping on a property that was not present on the other users. which, in real life, is rather unlikely. Gill's reasoning is valid here.

upvoted 2 times

mehnaz 1 year ago

The above answer is correct according to the document.
https://docs.microsoft.com/en-us/microsoft-365/compliance/search-the-audit-log-in-security-and-compliance?view=o365-worldwide.

upvoted 1 times

ranc1d Highly Voted 1 year, 4 months ago

Action 1: Updated user
an admin changed an attribute of a user
Action 2: Removed user from group
Dynamic group management removes user from the dynamic group as the needed attribute is no longer valid. This action is listed as "Initiated by actor: Microsoft Approval Management" in audit logs

upvoted 22 times

g87123 Most Recent 2 months, 3 weeks ago

the answer is correct. tested it
1. create the dynamic group and add rules (eg. Department or Location)
2. make sure a user account matched or contains the correct department or location
3. Wait for a few minutes or more to take effect. --> Audit Logs > "updated user" will show up
4. to remove the user from Dynamic group > update the user's Department/Location in AAD > wait a few minutes to take effect. > "Removed member from group" will show up in audit logs

You need patience because it will take some time to really show up the result without manually changing it.

upvoted 1 times

nzboy123 5 months, 2 weeks ago

Hi Everyone,

I tested this in my lab and the answers given are correct.

If you look in the user audit logs, the results are:
- Remove Member from group
- Update User

If you look in the dynamic group audit logs, the results are:
- Removed member from group.

upvoted 6 times

Timmeh 5 months, 1 week ago

Cheers, makes sense.

upvoted 2 times

kiketxu 4 months, 3 weeks ago

given answers makes sense to me too as usually in this scenario you check the user1 audit log to see what happened.

upvoted 1 times

Jejechu 8 months, 1 week ago

I think the good answers are "Updated user" and "updated group".
Question is about to find how the user have been removed from the dynamic group. 2 possibilities here : either user's attributes have been modified (so Uptaded user), either dynamic group filtering has been modified (updated group).

So to know why the user has been removed, we must check for "updated user" and "updated group".

upvoted 3 times

saran1987 11 months, 2 weeks ago

I tested this scenario. When I modified the group dynamic rule, one user is removed from the group. I couldnt see any logs for this even in security & compliance as it would take 24 hours but when I checked the audit logs in Azure AD, I see two events as 1.Updated Group 2. Removed member from group. When I edited one of the user's properties, I see the logs as 1. Removed member from group and 2. update user. So my conclusion is Remove member from group is definitely one answer. The second we could either user update user or Update group. Both will improve the chances to see what happened to a particular user being removed from the group

upvoted 3 times

JiDu 11 months, 1 week ago

The testing is excellent. I think as the question states only User1 is no longer a member of the group and not all members, then the change has occured in the attributes of that user and the result is 'updated user' compared to 'updated group', assuming the above is correct.

upvoted 2 times

JaBe 9 months, 1 week ago

Based on your testing, I'd conclude Remove member from group is not an answer. Look, we know the user is removed from the group, the question states you want to know _why_. As you verified, the reason can be one of the two update conditions, hence you need both these update conditions to search on. Only then you can be sure why the remove has taken place.

upvoted 2 times

GregD133 8 months, 2 weeks ago

Jabe, Absolutely correct. The question specifically asks WHY the user was removed. If we wanted to know WHEN, then Remove member would be helpful. A user can only be removed from a dynamic group if the user changes, or the group changes.

upvoted 2 times

jack987 1 year, 1 month ago

Agree with itmp.

--> Updated user Administrator changes one or more properties of a user account. For a list of the user properties that can be updated, see the "Update user attributes" section in Azure Active Directory Audit Report Events.
--> Removed member from group A member was removed from a group.
--> Updated group A property of a group was changed.

Source: https://docs.microsoft.com/en-us/microsoft-365/compliance/search-the-audit-log-in-security-and-compliance?view=o365-worldwide

upvoted 2 times

tintin_ 1 year, 2 months ago

UPDATED USER AND UPDATED GROUP

upvoted 2 times

Piper 1 year, 3 months ago

I thought one answer would be 'updated group' because someone may have changed the rules of the dynamic group.

upvoted 1 times

gills 1 year, 3 months ago

My $0.02, changing a rule of the dynamic group affects a lot of users. So usually this is not the case when only one use user is affected.

upvoted 2 times

Jogre 1 year, 4 months ago

Was under the impression you can't manually remove a user from a Dynamic Group so why is Remove User from Group correct? Either you change the user attributes so they no longer matched the Dynamic Group settings (Updated User) or you changed the Dynamic Group settings (Updated Group)?

upvoted 8 times

nicolonsky 1 year, 4 months ago

Totally agree.

upvoted 2 times

Question #38 *Topic 4*

You have a Microsoft 365 subscription.

You create and run a content search from the Security & Compliance admin center.

You need to download the results of the content search.

What should you obtain first?

A. an export key

B. a password

C. a certificate

D. a pin

kratos13 Highly Voted 1 year, 1 month ago

Definitely not made rightfully clear, but the answer is in the URL, as step#2 under "Step 2: Download the search results" ::
* Under Export key, click Copy to clipboard. You use this key in step 5 to download the search results.

upvoted 12 times

Crni 5 months, 2 weeks ago

Totally clear - Export key is exactly what we need

upvoted 1 times

DrMe 7 months, 2 weeks ago

Agreed, direct link: https://docs.microsoft.com/en-us/microsoft-365/compliance/export-search-results?view=o365-worldwide#step-2-download-the-search-results:~:text=Paste%20the%20export%20key%20that%20you%20copied%20in%20step%203%20in%20the%20appropriate%20box.

upvoted 2 times

kiketxu Most Recent 4 months, 3 weeks ago

A for sure!

upvoted 3 times

PeterC 4 months, 3 weeks ago

Simple test after search and export. you can download the report an see the export key, with this information:

The export key below is required to download the search results.

upvoted 2 times

Question #39 *Topic 4*

You have an Azure Active Directory (Azure AD) tenant that has a Microsoft 365 subscription.

You recently configured the tenant to require multi-factor authentication (MFA) for risky sign-ins.

You need to review the users who required MFA.

What should you do?

A. From the Microsoft 365 admin center, review a Security & Compliance report

B. From the Security & Compliance admin center, run an audit log search and download the results to a CSV file

C. From the Azure Active Directory admin center, review the Authentication methods activities

D. From the Azure Active Directory admin center, download the sign-ins to a CSV file

kiketxu 4 months, 3 weeks ago

I would say D as correct answer here, because I don't believe the answer C is up-to-date or isn't complete. I mean.... currently (3/21) you don't need to donwload the csv. Just go to:
AAD blade -> Security (missing in the C answer) -> Authentication methods -> Registration and reset events (not activities like C answer)

https://docs.microsoft.com/en-us/azure/active-directory/authentication/howto-authentication-methods-activity#registration-and-reset-events
upvoted 3 times

Robert__Susin 1 week, 3 days ago

I dont see where registration and reset of MFA relates to MFA prompt for risky sign-ins/risky users
upvoted 1 times

kiketxu 4 months, 3 weeks ago

*is complete
upvoted 2 times

PattiD 7 months, 3 weeks ago

https://docs.microsoft.com/en-us/azure/active-directory/authentication/howto-mfa-reporting#powershell-reporting-on-users-registered-for-mfa
upvoted 1 times

PattiD 7 months, 3 weeks ago

Correct Answer: D
upvoted 1 times

PattiD 7 months, 3 weeks ago

Get-MsolUser -All | Select-Object @{N='UserPrincipalName';E={$_.UserPrincipalName}},

@{N='MFA Status';E={if ($_.StrongAuthenticationRequirements.State){$_.StrongAuthenticationRequirements.State} else {"Disabled"}}},

@{N='MFA Methods';E={$_.StrongAuthenticationMethods.methodtype}} | Export-Csv -Path c:\MFA_Report.csv -NoTypeInformation
upvoted 1 times

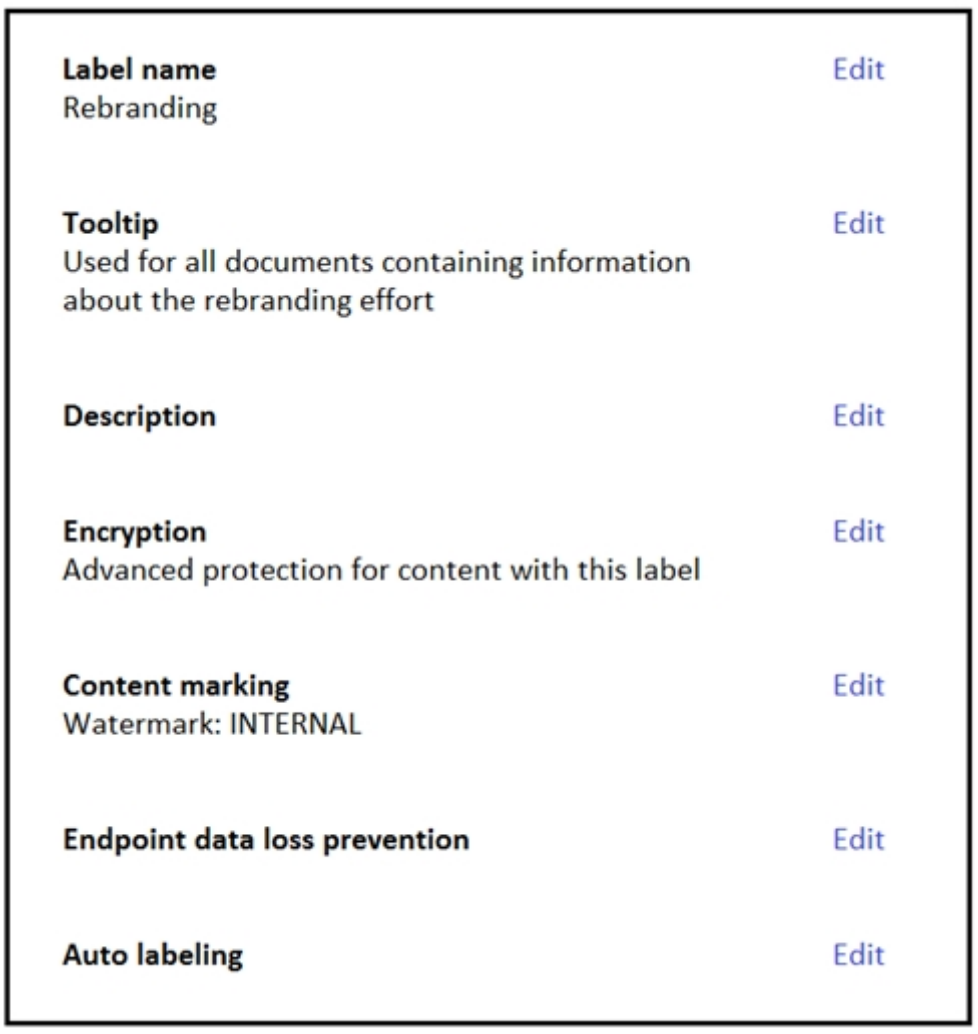
maf001 8 months, 1 week ago

To review and understand Azure AD Multi-Factor Authentication events, you can use the Azure Active Directory (Azure AD) sign-ins report. This report shows authentication details for events when a user is prompted for multi-factor authentication, and if any Conditional Access policies were in use. For detailed information on the sign-ins report
upvoted 4 times

Question #40 *Topic 4*

HOTSPOT -

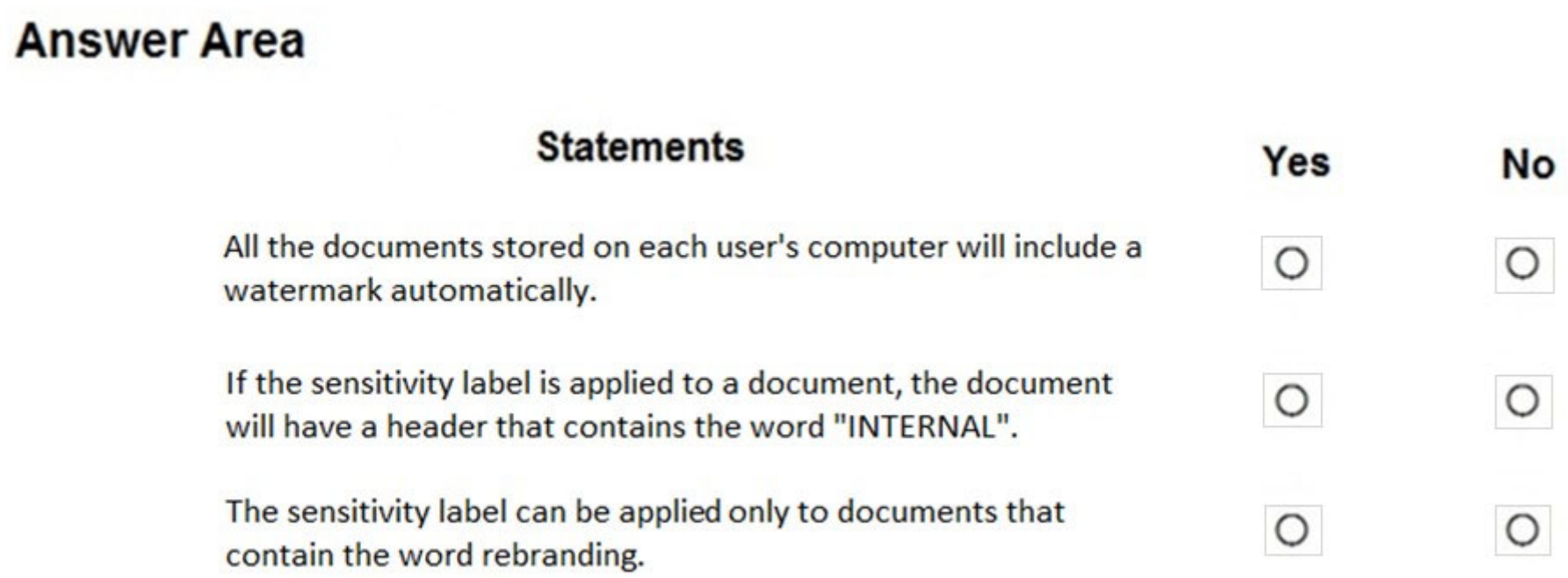
You have a Microsoft 365 sensitivity label that is published to all the users in your Azure Active Directory (Azure AD) tenant as shown in the following exhibit.



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:



kiketxu Highly Voted 4 months, 3 weeks ago

I would say also NO, NO, NO based on the following:
1. Autolabel only applies to Office files.
2. Content marking is a watermark, not header.
3. We don't know the conditions for autolabel. Rebranding is the label name only.

upvoted 10 times

Robert__Susin 1 week, 3 days ago

Autolabel DOES apply to non Office files, you are forgeting AIP scanner with MCAS.
The most correct reason 1 is NO is because "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

ellik Most Recent 3 months, 1 week ago

for the first answer, it should be 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.

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 2 times

Noku_Dee 4 months, 2 weeks ago

Answer should be No, No, No

For the first statement:
The tooltip specifies the documents to which the label applies, ie "all documents containing information about rebranding" NOT all documents stored on each user's computer. Therefore the answer should be NO.

For the 2nd and 3rd statements, I have no objections.

upvoted 2 times

Sido1 4 months, 3 weeks ago

very correct

upvoted 1 times

PeterC 4 months, 3 weeks ago

3 times "NO" - How should the autolabeling work on all the documents on the computer?
Only if the answer is "all Office documents" then yes -

https://docs.microsoft.com/en-us/microsoft-365/compliance/sensitivity-labels-office-apps?view=o365-worldwide#when-office-apps-apply-content-marking-and-encryption

upvoted 3 times

b00 4 months, 3 weeks ago

I would go for NO, NO, NO as first one says Watermarking and not Content Marking.

upvoted 2 times

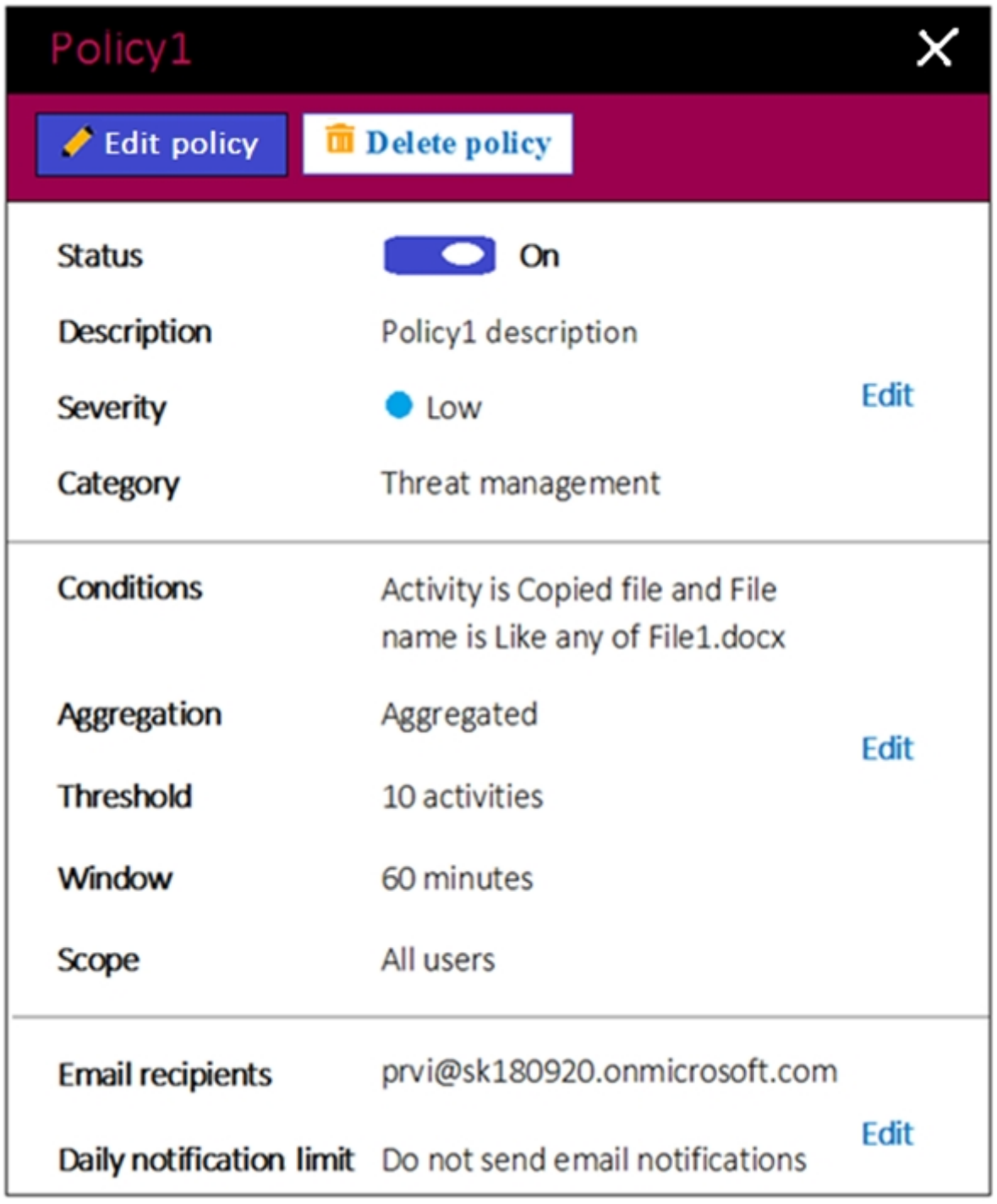
Question #41 *Topic 4*

HOTSPOT -

You have a Microsoft 365 subscription that includes three users named User1, User2, and User3.

A file named File1.docx is stored in Microsoft OneDrive. An automated process updates File1.docx every minute.

You create an alert policy named Policy1 as shown in the following exhibit.



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

NOTE: Each correct selection is worth one point.

Hot Area:

Answer Area

If User1 runs a scheduled task that copies File1.docx to a local folder every five minutes. [answer choice].

- Policy1 will not be triggered
- Policy1 will be triggered after 45 minutes
- Policy1 will be triggered after 60 minutes

If User1, User2, and User3 each run a scheduled task that copies File1.docx to a local folder every 10 minutes. [answer choice].

- Policy1 will not be triggered
- Policy1 will be triggered within 20 minutes
- Policy1 will be triggered within 45 minutes
- Policy1 will be triggered after 60 minutes

jack987 Highly Voted 1 year, 1 month ago

Answer:
Policy1 will be triggered after 45 minutes
Policy1 will be triggered within 45 minutes

Explanation:

1 user -> 5 mins
60/5 = 12

10th copy, t=50 mins

---

3 users -> 10 mins
t=0 -> 3 activites
t=10 -> 6 activites in total
t=20 -> 9 activites in total
t=30 -> 12 activites in total -> Alert is triggered

upvoted 23 times

DTz Highly Voted 1 year, 1 month ago

When you go to create an alert like this, you options say:
More than or equal to # activities
During the last # minutes

The key being "during the last # minutes". So it is assessing the trailing 60 minutes (each minute perhaps). So this pretty much nullifies the given answers of 60 minutes. If it were a report, I could see it happening after 60 minutes, but that would make useless alert wouldn't it!

The other thing is that the choices in the first question says will be triggered 'AFTER' # minutes. So clearly is has to be "Policy1 will be triggered after 45 minutes"

On the second question, notice on the 20 and 45 it says will be triggered 'WITHIN' # minutes. The 60 says 'AFTER'. We know it could not be within 20 minutes. 10 activities would take 30 minutes, so therefore the answer has to be 'within 45 minutes'.

Simple process of elimination.

upvoted 21 times

mehnaz 1 year ago

This is perfect. The policy will wait max of 60 seconds(the windows) but if it reaches threshold before that, it will trigger.In both cases we have policy matching threshold before 60 seconds. So 45 seconds is the answer in both cases.

upvoted 2 times

STFN2019 1 year, 1 month ago

of course, 100%

upvoted 2 times

TimurKazan Most Recent 3 months ago

I believe no policy will be trigered, because:
File is not updated, it is copied, which will not trigger alert

upvoted 1 times

prats005 4 months ago

Answer for question 1 is
Policy will be triggered AFTER 45 min

Logic:
Answer 1 Answer 1
Time User 1 Total Activity
0:00 1 1
0:05 1 2
0:10 1 3
0:15 1 4
0:20 1 5
0:25 1 6
0:30 1 7
0:35 1 8
0:40 1 9
0:45 1 10

Answer for question 2 is
Policy will be triggered WITHIN 45 min
Logic:
Answer 2
Time User 1 User 2 User 3 Total activitty
0:00 1 1 1 3
0:10 1 1 1 6
0:20 1 1 1 9
0:30 1 1 1 12

upvoted 3 times

Sethoo 4 months, 1 week ago

Interesting discussion. To me, the given answers are right. Both will trigger after 60 minutes. The policy is set to trigger after 60 minutes if the threshold is met. In both cases, within the 60 minutes window, they exceeded the threshold and so the trigger will happen at then 60 minutes window. This is more of the time trigger than the number of activity trigger. The question is , within one the one hour has the copying met or exceeded the threshold, if yes, trigger. Otherwise, no trigger.

upvoted 4 times

Cbruce 1 month, 3 weeks ago

I also agree with the answers provided. It will trigger it after 60 minutes for both because it is setup to alert after 60 minutes if the action does occur within the 60 minutes. This will limit the number of notifications to a reasonable number.

upvoted 1 times

mroczyslaw 1 month, 3 weeks ago

You are wrong. When activity occurs, system check last 60 minutes and sum activites. So, when 10th activity begin, system check if last 60 minutes was 10 times. There was, but time from last (10) to first (1) was 45 minutes, not 60 minutes.
So: answer 1: 45 minutes
answer 2: within 45 minutes (on 30 minutes there will be 12 times activity)

upvoted 1 times

kiketxu 4 months, 3 weeks ago

Both answers are wrong to me too. As above folks did the maths....
Policy1 will be triggered after 45 minutes when 10th
Policy1 will be triggered within 45 minutes (as there isn't after 30min)

upvoted 3 times

Arjanussie 5 months ago

docs.microsoft
When the alert is triggered - You can configure a setting that defines how often an activity can occur before an alert is triggered. This allows you to set up a policy to generate an alert every time an activity matches the policy conditions, when a certain threshold is exceeded, or when the occurrence of the activity the alert is tracking becomes unusual for your organization.
https://docs.microsoft.com/en-us/microsoft-365/compliance/alert-policies?view=o365-worldwide#:~:text=How%20alert%20policies%20work,-Here%27s%20a%20quick&text=A%20user%20performs%20an%20activity,in%20the%20Security%20%26%20Compliance%20Center.

so the answers should be wrong

upvoted 1 times

PeeyushS 5 months, 3 weeks ago

Based on the link the image given in Qaestion is "Window = 60 Mins" However once we read the link then it is "During the last 60 Mins" . Thus answer is right there is nothing like Window..this is to create a confusion.

upvoted 2 times

itstudy369 6 months, 2 weeks ago

Tested and both given answers are correct!

upvoted 2 times

DLM 6 months, 2 weeks ago

The key here is Aggregated. It's going to to wait 60 minutes then tell you how many times it hit with a Hit Count.
"When events that match the same alert policy occur within the aggregation interval, details about the subsequent event are added to the original alert."
https://docs.microsoft.com/en-us/microsoft-365/compliance/alert-policies?view=o365-worldwide

upvoted 3 times

Martyvdb 6 months, 2 weeks ago

It is 45 minutes until the event is triggered based on the activity.
Aggregation means that further triggers within the time frame will only be added as hits to the original trigger, and not create new alerts.

upvoted 3 times

B1G_B3N 6 months, 2 weeks ago

I agree with you DLM, to add to your thinking the link you supplied also states the following: " If the same event occurs within the aggregation interval, then Microsoft 365 adds details about the new event to the existing alert instead of triggering a new alert. The goal of alert aggregation is to help reduce alert "fatigue" and let you focus and take action on fewer alerts for the same event." From that I take that the trigger could activate multiple times within the alert window but to reduce 'alert fatigue' it will only display 1 alert.

upvoted 2 times

Mary_Yvette 7 months ago

Tested this the alert was created even before it hits the 60 minutes.

upvoted 2 times

JRodJ 8 months ago

Lots of comments on this, but anyone found references to official MS docs?

upvoted 2 times

DrMe 7 months, 2 weeks ago

This is one reference:
https://docs.microsoft.com/en-us/microsoft-365/compliance/alert-policies?view=o365-worldwide#alert-policy-settings:~:text=when%20a%20certain%20threshold%20is%20exceeded

upvoted 1 times

OhBee 8 months, 3 weeks ago

Guys, I think you are all forgetting the 0th minute here. I believe this needs to be included as well.

So for the first one, if the user copies the file every 5 mins and we include the 0th minute, that is 45 mins exactly.

Same goes for the second one (20 mins exactly). The confusing thing is that it says "within" 20 mins not after...so it might actually be 45 mins with this wording.

upvoted 2 times

cabeza 8 months, 3 weeks ago

Yes you are correct, after 45 and within 45. The 60min window is the trigger to reset the counter for the number of times the files is copied, not when to send the alert.

upvoted 1 times

itmaster 9 months, 3 weeks ago

I think the right answer is 45 minutes for the single user and 20 minutes for the 3 users. it's a scheduled task every 10 minutes, so at second 0 a copy will take place, at minute 10, a second copy, at minute 20, a third copy, so 3 copies per user, so 12 coppices for 3 users in 20 minutes.

upvoted 1 times

itmaster 9 months, 3 weeks ago

it's 30* minutes not 20. in One hour the policy will be triggered twice.

upvoted 1 times

AntUser 11 months ago

Answer is correct. It checks for the threshold (10) after 60mins, the cycle for checks is 60mins. If it's not up to 10 after every 60mins, it will not send alert.

upvoted 4 times

STFN2019 1 year, 1 month ago

Clearly both answers should be as follows:

Box 1: Policy1 will be triggered after 45 mins, why?
5 mins x 10 activites = 50mins

Box 2: Policy1 will be triggered within 45 mins, why?
3 activites every 10 mins so it'll trigger alert as soon as the threshold is hit so e.g. 12 activites = 40 mins

upvoted 3 times

tintin_ 1 year, 2 months ago

Verified; Alert 1 option 2, Alert 2 option 3

upvoted 3 times

Question #42 *Topic 4*

You have a Microsoft 365 subscription.

All users are assigned a Microsoft 365 E5 license.

How long will auditing data be retained?

A. 30 days

B. 90 days

C. 365 days

D. 5 years

ML76 Highly Voted 1 year, 5 months ago

Answer is C:
Office 365 or Microsoft 365 E5 or users with a Microsoft 365 E5 Compliance add-on license: Audit records for Azure Active Directory, Exchange, and SharePoint activity are retained for one year by default.

Da <https://docs.microsoft.com/en-us/microsoft-365/compliance/search-the-audit-log-in-security-and-compliance>

upvoted 21 times

Ton2025 1 year, 5 months ago

I agree , E3 default is 90 days , E5 default is 365 days.
The question is E5.

upvoted 23 times

jack987 Highly Voted 1 year, 1 month ago

The correct answer is C.

For users assigned an Office 365 E5 or Microsoft 365 E5 license (or users with a Microsoft 365 E5 Compliance or Microsoft 365 E5 eDiscovery and Audit add-on license), audit records for Azure Active Directory, Exchange, and SharePoint activity are retained for one year by default. Organizations can also create audit log retention policies to retain audit records for activities in other services for up to one year.

For users assigned any other (non-E5) Office 365 or Microsoft 365 license, audit records are retained for 90 days. For a list of Office 365 and Microsoft 365 subscriptions that support unified audit logging

Source: https://docs.microsoft.com/en-us/microsoft-365/compliance/search-the-audit-log-in-security-and-compliance?view=o365-worldwide

upvoted 8 times

DudleyYVR Most Recent 3 months, 2 weeks ago

365days
For users assigned an Office 365 E5 or Microsoft 365 E5 license (or users with a Microsoft 365 E5 Compliance or Microsoft 365 E5 eDiscovery and Audit add-on license), audit records for Azure Active Directory, Exchange, and SharePoint activity are retained for one year by default.

upvoted 1 times

Rafale 4 months, 1 week ago

Answer is B based one Microsoft Docs:
https://docs.microsoft.com/en-us/microsoft-365/compliance/advanced-audit?view=o365-worldwide

All audit records generated in other services that aren't covered by the default audit log retention policy (described in the previous section) are retained for 90 days. But you can create customized audit log retention policies to retain other audit records for longer periods of time up to 10 years.

upvoted 1 times

kiketxu 4 months, 3 weeks ago

C for sure for E5 (365), for the rest 90 days.
https://docs.microsoft.com/en-us/microsoft-365/compliance/audit-log-retention-policies?view=o365-worldwide#default-audit-log-retention-policy

upvoted 4 times

PattiD 7 months, 3 weeks ago

How long are the audit records retained for?

As previously explained, audit records for activities performed by users assigned an Office 365 E5 or Microsoft E5 license (or users with a Microsoft 365 E5 add-on license) are retained for one year. For all other subscriptions that support unified audit logging, audit records are retained for 90 days.

upvoted 2 times

svm_Terran 8 months ago

Shouldnt be 90 days?

upvoted 1 times

TonySuccess 8 months ago

If you look above your comment, you will see other comments which explain clearly why the answer is C.

upvoted 1 times

MaenQ 8 months ago

"You can retain audit logs for up to 10 years. "
check this please: https://docs.microsoft.com/en-us/microsoft-365/compliance/audit-log-retention-policies?view=o365-worldwide#:~:text=You%20can%20retain%20audit%20logs,users%20or%20by%20specific%20users

upvoted 1 times

JRodJ 8 months ago

https://docs.microsoft.com/en-us/microsoft-365/compliance/search-the-audit-log-in-security-and-compliance?view=o365-worldwide#frequently-asked-questions

How long are the audit records retained for?

As previously explained, audit records for activities performed by users assigned an Office 365 E5 or Microsoft E5 license (or users with a Microsoft 365 E5 add-on license) are retained for one year. For all other subscriptions that support unified audit logging, audit records are retained for 90 days.

Answer is C. E5 is one year, all others are 90 days.

upvoted 3 times

TonySuccess 8 months, 1 week ago

The default audit log retention policy (1 Year) is applied to E5 users \ E Discovery and Audit Add-on Licensed users:

For example, if one of my E5 users signs into Exchange Online this activity will be retained for a year.

If they do not have the above license and just have E3 with no add-on, then it's 90 days.

Confirmed with Microsoft Support via support request in my Lab.

Thanks

upvoted 3 times

mnak 8 months, 2 weeks ago

MS just changed to 90 days even for E5, so now the answer is correct.

upvoted 3 times

bingomutant 5 months ago

nonsense

upvoted 1 times

SSK500 6 months ago

https://docs.microsoft.com/en-us/office365/securitycompliance/search-the-audit-log-in-security-and-compliance
See this, it was updated 2 weeks back and it says one year.

upvoted 2 times

raybishop15 5 months, 4 weeks ago

Also agree with SSK500. I dug a little deeper into the reference link

For users assigned an Office 365 E5 or Microsoft 365 E5 license (or users with a Microsoft 365 E5 Compliance or Microsoft 365 E5 eDiscovery and Audit add-on license), audit records for Azure Active Directory, Exchange, and SharePoint activity are retained for one year by default. Organizations can also create audit log retention policies to retain audit records for activities in other services for up to one year. For more information, see Manage audit log retention policies.

upvoted 1 times

Gracemade 10 months, 3 weeks ago

C for sure

upvoted 2 times

jfish4391 1 year, 1 month ago

"How long are the audit records retained for?

As previously explained, audit records for activities performed by users assigned an Office 365 E5 or Microsoft E5 license (or users with a Microsoft 365 E5 add-on license) are retained for one year. For all other subscriptions that support unified audit logging, audit records are retained for 90 days."

upvoted 3 times

VTHAR 10 months, 1 week ago

Yes, answer is C for E5.

upvoted 1 times

nenar 1 year, 3 months ago

Default audit log retention policy
Advanced Audit in Microsoft 365 provides a default audit log retention policy for all organizations. This policy retains all Exchange, SharePoint, and Azure Active Directory audit records for one year. This default policy retains audit records that contain the value of AzureActiveDirectory, Exchange, or SharePoint for the Workload property (which is the service in which the activity occurred). The default policy can't be modified. See the More information section in this article for a list of record types for each workload that are included in the default policy.

Note

The default audit log retention policy only applies to audit records for activity performed by users who are assigned an Office 365 or Microsoft 365 E5 license or have a Microsoft 365 E5 Compliance add-on license. If you have non-E5 users in your organization, their corresponding audit records are retained for 90 days.

from:
https://docs.microsoft.com/en-us/microsoft-365/compliance/search-the-audit-log-in-security-and-compliance?view=o365-worldwide

upvoted 6 times

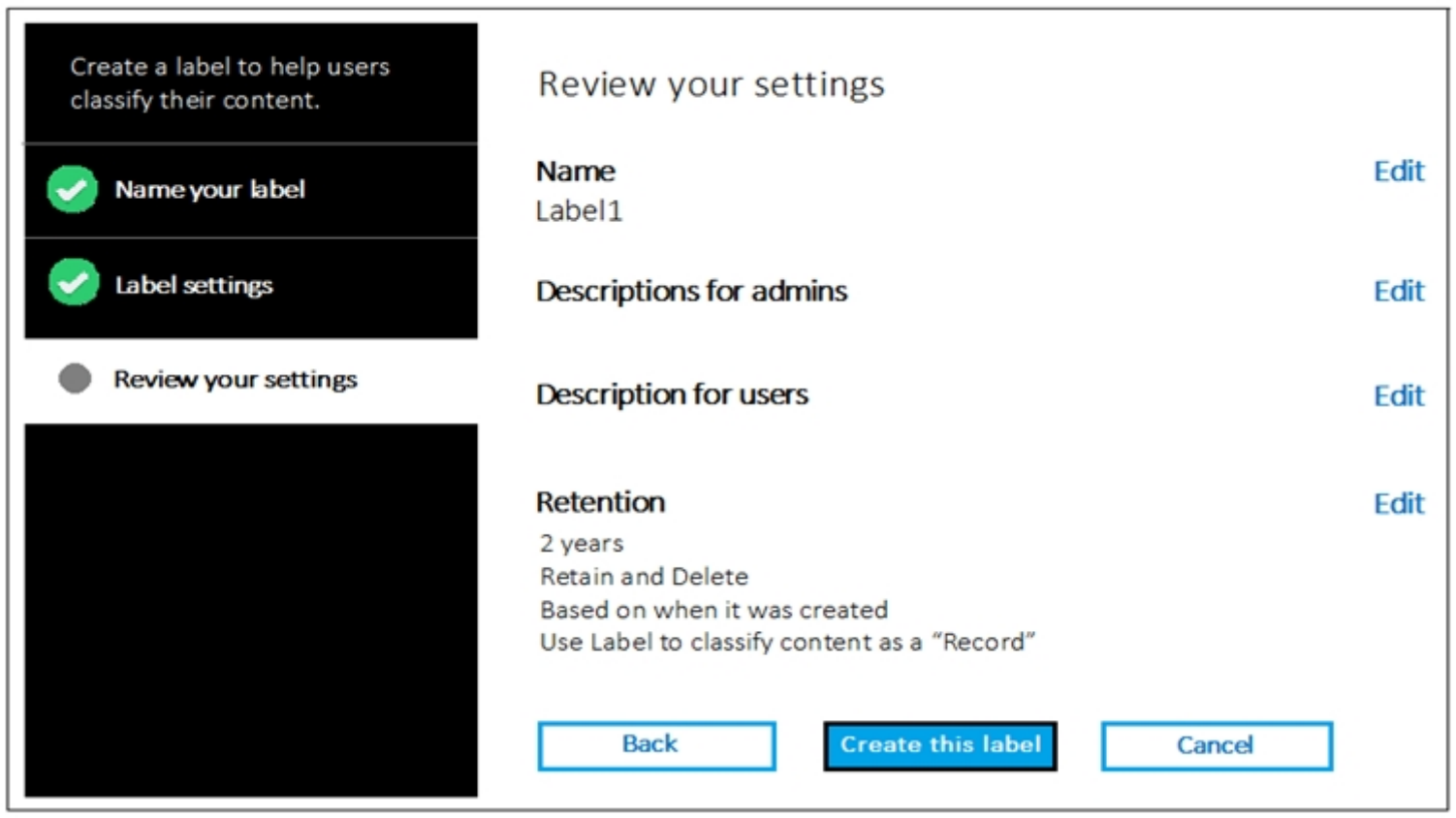
Question #43

Topic 4

HOTSPOT -

You have a Microsoft 365 subscription.

You create a retention label named Label1 as shown in the following exhibit.



You publish Label1 to SharePoint sites.

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

NOTE: Each correct selection is worth one point.

Hot Area:

Answer Area

If you create a file in a Microsoft SharePoint library on January 1, 2019, you can [answer choice].

- never delete the file.
- delete the file before January 1, 2021.
- delete the file after January 1, 2021.

If you create a file in a Microsoft SharePoint library on March 15, 2019, the file will [answer choice].

- always remain in the library.
- remain in the library until you delete the file.
- be deleted automatically on March 15, 2021.

jack987 Highly Voted 1 year, 1 month ago

Correct answer is:
1. never delete the file - because of: Use Label to classify content as "Record"
2. be deleted automatically on March 15, 2021

Explanation:
Additionally, retention labels support records management for email and documents across Microsoft 365 apps and services. You can use a retention label to classify content as a record. When this happens, the label can't be changed or removed, and the content can't be edited or deleted.
Source: https://docs.microsoft.com/en-us/microsoft-365/compliance/labels?view=o365-worldwide

upvoted 44 times

Alvaroll 9 months ago

On the second case, if the file is marked as a record, why is it deleted automatically?

upvoted 1 times

FumerLaMoquette 9 months ago

Answer is correct. To add to this, justification for second answer:

Mark the content as a record as part of the label settings, and always have proof of disposition when content is deleted at the end of its retention period.
Source: https://docs.microsoft.com/en-us/microsoft-365/compliance/retention?view=o365-worldwide

upvoted 1 times

Ronnie123 Highly Voted 1 year, 8 months ago

Not correct, the second statement should be C.
See: https://docs.microsoft.com/en-us/microsoft-365/compliance/records

At a high level, declaring content as a record means that:
The item becomes immutable (a record can't be modified or deleted)
Additional activities about the item are logged
Records are disposed of after their stated retention period is past

upvoted 36 times

dyerjohn42 Most Recent 1 month, 2 weeks ago

i think this question is missing information.

upvoted 1 times

belyo 3 months, 3 weeks ago

BOTH answers should be the same "never delete / always retain" or 'deleted auto after retention lifecycle'. For me its autodeletion because is screenshot the retention label is marked as ordinary 'Record' rather than Immutable 'Regulatory Record' which cannot be deleted at all.

upvoted 2 times

Sollutions 4 months, 3 weeks ago

https://docs.microsoft.com/en-us/microsoft-365/compliance/records-management?view=o365-worldwide#records
This document shows that if a file is labeled as a record, deletion is blocked.

upvoted 1 times

kiketxu 4 months, 3 weeks ago

A. Never delete
B. Auto delete in March.

upvoted 4 times

Dasdweqs 8 months, 1 week ago

At no point does it say the label is actually applied to the file, it's just available right? So possible the file in question does not have the label applied and thus the correct answer would be B and B.

upvoted 3 times

Paulmtx 6 months, 2 weeks ago

I agree, this question is poorly stated. We might assume that the label was applied, but since there are 2 answers that would be correct if the label wasn't applied at all, the question should be more clear.

upvoted 1 times

majidhussain85 8 months, 1 week ago

A timer job periodically cleans up the Preservation Hold library. This job compares all content in the Preservation Hold library to all queries used by the retention settings for that content. Content that is older than their configured retention period is deleted from the Preservation Hold library, and the original location if it is still there. This timer job runs every seven days, which means that it can take up to seven days for content to be deleted.

upvoted 1 times

Xten 1 year, 1 month ago

You can use a retention label to classify content as a record. When this happens and the content remains in Microsoft 365, the label can't be changed or removed, and the content can't be edited or deleted.

upvoted 2 times

FableFa 1 year, 1 month ago

Records are deleted at the end of their retention period. In this case, delete can occur at the end of the retention period. Answers of JACK987 are correct.

upvoted 3 times

TheSkyMan 1 year, 2 months ago

"If a user attempts to delete a record in a SharePoint, an error is displayed say that the item wasn't deleted, and remains in the library."

"Records are disposed of after their stated retention period is past."

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

upvoted 1 times

Coolman 1 year, 5 months ago

Items labels AS a record Will not be deleated until the label is removed from the item. Since the retention policy want to delete the item after x days, that Wont happen. Only admin Can manuelt remove the record label.= answer is correct never deleated

upvoted 2 times

AK311 1 year, 2 months ago

Records are immutable, and labels cant be removed. It will auto-delete after expiry.
https://docs.microsoft.com/en-us/microsoft-365/compliance/records?view=o365-worldwide
upvoted 4 times

Lewist 1 year, 7 months ago

Implement records management across Office 365, including both email and documents. You can use a retention label to classify content as a record. When this happens, the label can't be changed or removed, and the content can't be edited or deleted.
upvoted 2 times

WoneSix 1 year, 6 months ago

True - an end user can't delete the record. But the retention label is set to delete the items after two years, not to trigger a disposition review. If it was the latter, the items would be retained until the review, but since it's not, the items will be automativcally deleted at the end of the two-year period.
upvoted 2 times

btd2020 1 year, 2 months ago

So why does the file in the second case "always remain in the library" after the two year mark?
upvoted 3 times

ifex380 1 year, 7 months ago

How about the first statement.

You should be able to delete the file after January 21 2021
upvoted 1 times

d3an 1 year, 6 months ago

You can never delete the file as it is classified as a Record. It will be deleted automatically by the Retention label that has been applied on Jan 21st 2021, but the drop-down options for the first statement are only for user-driven deletion, rather than auto-deletion like in the second statement.
upvoted 16 times

WoneSix 1 year, 6 months ago

ifex380, d3an is right - the file will be deleted automatically before you have a chance to delete it. Never Delete is the correct answer.
upvoted 1 times

itmp 1 year, 2 months ago

If so, the 2nd answer is wrong.
upvoted 1 times

letterload 8 months, 1 week ago

itmp - agree, the 2nd answer is wrong, I believe Ronnie123 is correct with choice C i.e. auto delete in March.
upvoted 1 times

Duncan 1 year, 8 months ago

Agree with Ronnie123 here.
upvoted 4 times

Question #44 *Topic 4*

You have a Microsoft 365 subscription.

You create a retention policy and apply the policy to Exchange Online mailboxes.

You need to ensure that the retention policy tags can be assigned to mailbox items as soon as possible.

What should you do?

A. From Exchange Online PowerShell, run Start-RetentionAutoTagLearning

B. From Exchange Online PowerShell, run Start-ManagedFolderAssistant

C. From the Security & Compliance admin center, create a data loss prevention (DLP) policy

D. From the Security & Compliance admin center, create a label policy

Ronnie123 Highly Voted 1 year, 8 months ago

I think this should be B. From Exchange Online PowerShell, run Start-ManagedFolderAssistant
Policy tags are handled by the MFA

upvoted 45 times

Sizz 1 year, 7 months ago

Indeed - either a misleading question, or an incorrect answer...
If the answer is definitely around Labels, then it is adhering to the guidance that policies & labels should be used instead of MRM; however the question mentions Tags which is an MRM thing (and therefore follows the route for Managed Folder Assistant being used)!

Source (1) - Retention Policies: https://docs.microsoft.com/en-us/microsoft-365/compliance/retention-policies#use-a-retention-policy-instead-of-these-features
Source (2) - Retention Labels: https://docs.microsoft.com/en-us/microsoft-365/compliance/labels#use-retention-labels-instead-of-these-features
Source (3) - Classic MRM tags and policies: https://docs.microsoft.com/en-us/exchange/security-and-compliance/messaging-records-management/retention-tags-and-policies

upvoted 4 times

itmp Highly Voted 1 year, 3 months ago

Can't these answers be updated/corrected ?

upvoted 13 times

lime568 Most Recent 2 weeks, 1 day ago

a retension policy dont need a tag. the tag is necessary only for a tag policy. the first action is not related to the second so... the answer is good

upvoted 1 times

kiketxu 4 months, 3 weeks ago

I would select B. Use the Start-ManagedFolderAssistant cmdlet to immediately start messaging records management (MRM) processing of mailboxes that you specify.

https://docs.microsoft.com/es-es/powershell/module/exchange/start-managedfolderassistant?view=exchange-ps

upvoted 3 times

Sugar123 4 months, 3 weeks ago

The correct answer is D. " The question is asking how to assign a retention policy tags. Policy tags cannot be assigned without an actual policy. "To apply one or more retention tags to a mailbox, you must add them to a retention policy and then apply the policy to mailboxes. A mailbox can't have more than one retention policy. Retention tags can be linked to or unlinked from a retention policy at any time, and the changes automatically take effect for all mailboxes that have the policy applied." https://docs.microsoft.com/en-us/exchange/security-and-compliance/messaging-records-management/retention-tags-and-policies

Also, the Start-ManagedFolderAssistant cmdlet is specific to retention policies, not tags. "The Managed Folder Assistant uses the retention policy settings of users' mailboxes to process retention of items." https://docs.microsoft.com/en-us/powershell/module/exchange/start-managedfolderassistant?view=exchange-ps

upvoted 1 times

Sido1 5 months, 1 week ago

Unlike retention policies, retention settings from retention labels travel with the content if it's moved to a different location within your Microsoft 365 tenant. In addition, retention labels have the following capabilities that retention policies don't support:

Options to start the retention period from when the content was labeled or based on an event, in addition to the age of the content or when it was last modified.

Use trainable classifiers to identify content to label.

Apply a default label for SharePoint documents.

Support disposition review to review the content before it's permanently deleted.

Mark the content as a record as part of the label settings, and always have proof of disposition when content is deleted at the end of its retention period.

upvoted 1 times

lfecoded 6 months, 3 weeks ago

I think the right answer is B as many here as explained. Run the MFA powershell command.

upvoted 1 times

serget12 8 months ago

I'm thinking the answer is correct: " can be assigned to mailbox items as soon as possible." it is talking about being able to be assigned, not to "be assigned". Just my understanding of the question.

upvoted 1 times

TonySuccess 8 months ago

It's B. I've used this at work.

upvoted 2 times

Garmaxx 8 months, 1 week ago

The Managed Folder Assistant uses the retention policy settings of users' mailboxes to process retention of items. This mailbox processing occurs automatically. You can use the Start-ManagedFolderAssistant cmdlet to immediately start processing the specified mailbox.

upvoted 2 times

balajim212 8 months, 2 weeks ago

The question does say "You create a retention policy and apply the policy to Exchange Online mailboxes." No need to create a policy again, just manually start the managed folder assistant.

upvoted 1 times

FumerLaMoquette 9 months ago

This question appeared before in one of the earlier pages. Answer is B.

upvoted 1 times

Ashoky7 9 months, 3 weeks ago

I think this should be B. From Exchange Online PowerShell, run Start-ManagedFolderAssistant

upvoted 2 times

jack987 1 year, 1 month ago

The correct answer should be B. From Exchange Online PowerShell, run Start-ManagedFolderAssistant

upvoted 6 times

Soumia_Djenan 1 year, 2 months ago

The correct answer is B
The Managed Folder Assistant uses the retention policy settings of users' mailboxes to process retention of items. This mailbox processing occurs automatically. You can use the Start-ManagedFolderAssistant cmdlet to immediately start processing the specified mailbox.

https://docs.microsoft.com/en-us/powershell/module/exchange/policy-and-compliance-retention/start-managedfolderassistant?view=exchange-ps

upvoted 4 times

xofowi5140 1 year, 3 months ago

Almost identical to Exam MS-500 topic 4 question 10 discussion
https://www.examtopics.com/exams/microsoft/ms-500/view/17/

upvoted 8 times

jwhld 6 months, 3 weeks ago

Except their "you created retention labels" and publish them. Here you created a retention policy which cannot be assign to individual items, therefore you need to create a label policy. Answer D

upvoted 2 times

WoneSix 1 year, 6 months ago

Agreed with you all - the retention policy has already been assigned, but it won't automatically be available for up to one week. The Managed Folder Assistant is required to force it into use faster.

upvoted 3 times

WoneSix 1 year, 6 months ago

I'm adding to my note - the question specifically asks that the labels be available "as soon as possible". Creating a policy will allow the users to get to the policy, but within a week. You need to run the MFA to have it happen faster.

upvoted 2 times

krrunal 1 year, 7 months ago

Agree with Ronnie...

upvoted 3 times

Question #45 *Topic 4*

You have a Microsoft 365 subscription.

You need to ensure that users can manually designate which content will be subject to data loss prevention (DLP) policies.

What should you create first?

A. A retention label in Microsoft Office 365

B. A custom sensitive information type

C. A Data Subject Request (DSR)

D. A safe attachments policy in Microsoft Office 365

ChrisBr Highly Voted 1 year, 9 months ago

This question is about DLP not DSR.
You can use Retention Labels in a DLP Policy. Imho A should be the right answer.

upvoted 21 times

jack987 Highly Voted 1 year, 1 month ago

The correct answer is A. A retention label in Microsoft Office 365

Explanition:
Using a retention label as a condition in a DLP policy
Using a retention label in a policy is only supported for items in SharePoint Online and OneDrive for Business.

Support for sensitivity labels is coming
You can currently use only a retention label as a condition, not a sensitivity label. We're currently working on support for using a sensitivity label in this condition.

Types of sensitive information
A DLP policy can help protect sensitive information, which is defined as a sensitive information type. Microsoft 365 includes definitions for many common sensitive information types across many different regions that are ready for you to use, such as a credit card number, bank account numbers, national ID numbers, and passport numbers.

Source: https://docs.microsoft.com/en-us/microsoft-365/compliance/data-loss-prevention-policies?view=o365-worldwide

upvoted 19 times

Oz 11 months, 3 weeks ago

Agree. Explanation is here.
https://docs.microsoft.com/en-us/microsoft-365/compliance/retention?view=o365-worldwide#retention-policies-and-retention-labels
Section is named "Using a retention label as a condition in a DLP policy"

upvoted 2 times

mroczyslaw Most Recent 1 month, 3 weeks ago

Answer A.
We don't need automatically classify so don't need custom sensitive information type (ans.B). We make retention labels for using by users MANUALLY on docs - so Answer A.

upvoted 1 times

TimurKazan 3 months ago

seems like a question is a bit outdated. To use DLP, you will firstly need DLP policy, which can contain both sensitive information type or retention label as well (depending on what you choose).

upvoted 3 times

Neharsin 9 months, 1 week ago

B is the correct answer. Custom Sensitive Info Type allows DLP policy customization.
https://docs.microsoft.com/en-us/microsoft-365/compliance/data-loss-prevention-policies?view=o365-worldwide#using-a-retention-label-asa-condition-in-a-dlp-policy

upvoted 3 times

kiketxu 4 months, 3 weeks ago

Yes, B is the correct answer. I don't undertand why people mess this with DSR.
The question is "what should you create first? "
First of all if you want something "customized" for DLP is to create "Custom sensitivity infotype" to define what will included a condition. Then you can create a retention or sensitiviy label to include in the DLP condition. (Seems retention only applicable to Sharepoint and Onedrive but maybe this has already change as its article from 2019)
https://docs.microsoft.com/en-us/microsoft-365/compliance/data-loss-prevention-policies?view=o365-worldwide#using-a-retention-label-as-a-condition-in-a-dlp-policy

upvoted 3 times

itmaster 9 months, 3 weeks ago

Answer is A:
https://docs.microsoft.com/en-us/office365/securitycompliance/manage-gdpr-data-subject-requests-with-the-dsr-case-tool#more-information-about-using-the-dsr- case-tool

upvoted 5 times

itmaster 9 months, 3 weeks ago

This is the right reference:
https://docs.microsoft.com/en-us/microsoft-365/compliance/data-loss-prevention-policies?view=o365-worldwide#using-a-retention-label-as-a-condition-in-a-dlp-policy

upvoted 4 times

Dimonchik 5 months, 1 week ago

Why you gave a correct answer and a wrong link then?
https://docs.microsoft.com/en-us/microsoft-365/compliance/retention?view=o365-worldwide#using-a-retention-label-as-a-condition-in-a-dlp-policy

upvoted 2 times

Monsur 10 months, 1 week ago

The Answer C: is correct.
To manage investigations in response to a DSR submitted by a person in your organization, you can use the DSR case tool in the Security & Compliance Center to find content stored. If Admin did not first create a DSR case tool, he cannot respond or manage a DSR request from a user.
https://docs.microsoft.com/en-us/microsoft-365/compliance/manage-gdpr-data-subject-requests-with-the-dsr-case-tool?view=o365-worldwide#more-information-about-using-the-dsr-%20case-tool

upvoted 1 times

sourpuncher 10 months, 3 weeks ago

You need to ensure users can manually designate which content will be subject to DLP policies. a DSR is a report (will not help to apply a DLP) You are not going to create a DSR and assign permissions to view this for every user to apply a manual custom label to the content of their choice. You can create a retention label and users can apply that label when they want to retain that content. You dont need a custom one because the amount of work its going to take to create a custom info type for every single request from a community of users will lead you to insanity. My answer is A.

upvoted 3 times

mehnaz 1 year ago

Oh! this is really confusing. Option A and C are quite confusing.

upvoted 1 times

TaSpanja 1 year, 1 month ago

I dont get this isn't a data subject request just another dashboard for search request done by users to their companies Data Protection Officer to find out what data the company has about them, what does it have to do with DLP???

upvoted 1 times

xofowi5140 1 year, 3 months ago

What a sensitivity label can be customizable. You can create categories for different levels of sensitive content in your organization, such as Personal, Public, General, Confidential, and Highly Confidential.

And can be persistent. After you apply a sensitivity label to content, the label is stored in the metadata of that email or document. This means the label roams with the content, including the protection settings, and this data becomes the basis for applying and enforcing policies.

upvoted 1 times

xofowi5140 1 year, 3 months ago

A DLP policy can help protect sensitive information, which is defined as a sensitive information type.

You can currently use only a retention label as a condition, not a sensitivity label. Using a retention label in a policy is only supported for items in SharePoint Online and OneDrive for Business.

For me the correct answer is custom sensitive information type

upvoted 4 times

m2L 1 year, 6 months ago

I think the answer is correct DSR .A formal request by a person to their organization to take an action on their personal data is called a Data Subject Request or DSR.https://docs.microsoft.com/en-us/microsoft-365/compliance/manage-gdpr-data-subject-requests-with-the-dsr-case-tool#more-information-about-using-the-dsr-%20case-tool

upvoted 1 times

WoneSix 1 year, 6 months ago

m2L, none of the link you mention has anything to do with DLP. The question is specifically about DLP. DSRs are specifically used for locating and protecting personal information. If the user in the question wants to protect his project document that has nothing to do with personal information, he can't use a DSR.

upvoted 3 times

Zorag 1 year, 5 months ago

Both retention and sensitive info can be used to apply dlp policies

upvoted 3 times

alextt78 1 year, 8 months ago

Sorry, but I think that the question asking How a user can find by himself the right label/classification for a specific content. So DSR do the Job

upvoted 3 times

WoneSix 1 year, 6 months ago

DSRs only apply to personal information. The question doesn't say anything about what sensitive information. The end user can apply retention labels to data, and that retention label can be used as the basis for the DLP policy. So the Retention Label should be the answer.

upvoted 3 times

Ronnie123 1 year, 8 months ago

Correction, ChrisBr is right, see: https://docs.microsoft.com/en-us/microsoft-365/compliance/data-loss-prevention-policies#using-a-label-as-a-condition-in-a-dlp-policy

upvoted 12 times

Ronnie123 1 year, 8 months ago

Afaik retention labels have nothing to do with DLP's. But when you create a sensitivity label, you can assign DLP actions to it. So I think the anwser is:
B. A custom sensitive information type

upvoted 4 times

Question #46 *Topic 4*

You have an Azure Active Directory (Azure AD) tenant named contoso.com and a Microsoft 365 subscription.

All users in contoso.com use the Microsoft SharePoint Newsfeed.

You need to ensure that all the users use the Yammer.com service.

What should you do?

A. From the Yammer admin center, modify the Usage Policy settings

B. From the SharePoint admin center, modify the Enterprise Social Collaboration settings

C. From the SharePoint admin center, modify the Connected Services settings

D. From the Yammer admin center, modify the Configuration settings

Teesmd 6 months, 3 weeks ago

Answer B is correct according to the MS doc:
Office 365 includes two options for enterprise social features in SharePoint: Yammer and Newsfeed. The SharePoint administrator selects which option users see when they click Conversations in SharePoint. By default, users see Newsfeed.

You can turn Yammer off or on for conversations in SharePoint by using the SharePoint Online admin center. You must be a global administrator to make this change.

https://docs.microsoft.com/en-us/yammer/integrate-yammer-with-other-apps/yammer-and-newsfeed

upvoted 3 times

PattiD 7 months, 3 weeks ago

https://***YOURTENANT***-admin.sharepoint.com/_layouts/15/online/TenantSettings.aspx

upvoted 1 times

TrpOslik 9 months, 1 week ago

https://xxxxxx-admin.sharepoint.com/_layouts/15/online/TenantSettings.aspx

upvoted 3 times

Question #47 *Topic 4*

You have a Microsoft 365 E5 subscription.

A user reports that changes were made to several files in Microsoft OneDrive.

You need to identify which files were modified by which users in the userג€™s OneDrive.

What should you do?

A. From the Azure Active Directory admin center, open the audit log

B. From the OneDrive admin center, select Device access

C. From Security & Compliance, perform an eDiscovery search

D. From Microsoft Cloud App Security, open the activity log

sudoer Highly Voted 11 months ago

Cloud App Security - > Activity log , filtered by OneDrive

upvoted 8 times

Ashton_98 Most Recent 7 months, 2 weeks ago

It should be from Security & Compliance, view the audit logs. However, that is not an option. The reference link doesn't support D, and Cloud App Security serves a different purpose from my understanding.

upvoted 3 times

shanti0091 6 months, 2 weeks ago

I agree with your point. D is just a more justified answer in this context.

upvoted 1 times

kiketxu 4 months, 3 weeks ago

Agree too. It should be audit logs, but as they point to CAS, this is also valid.

upvoted 1 times

SUBZER0 11 months ago

Correct

upvoted 4 times

sudoer 11 months ago

Answer= D

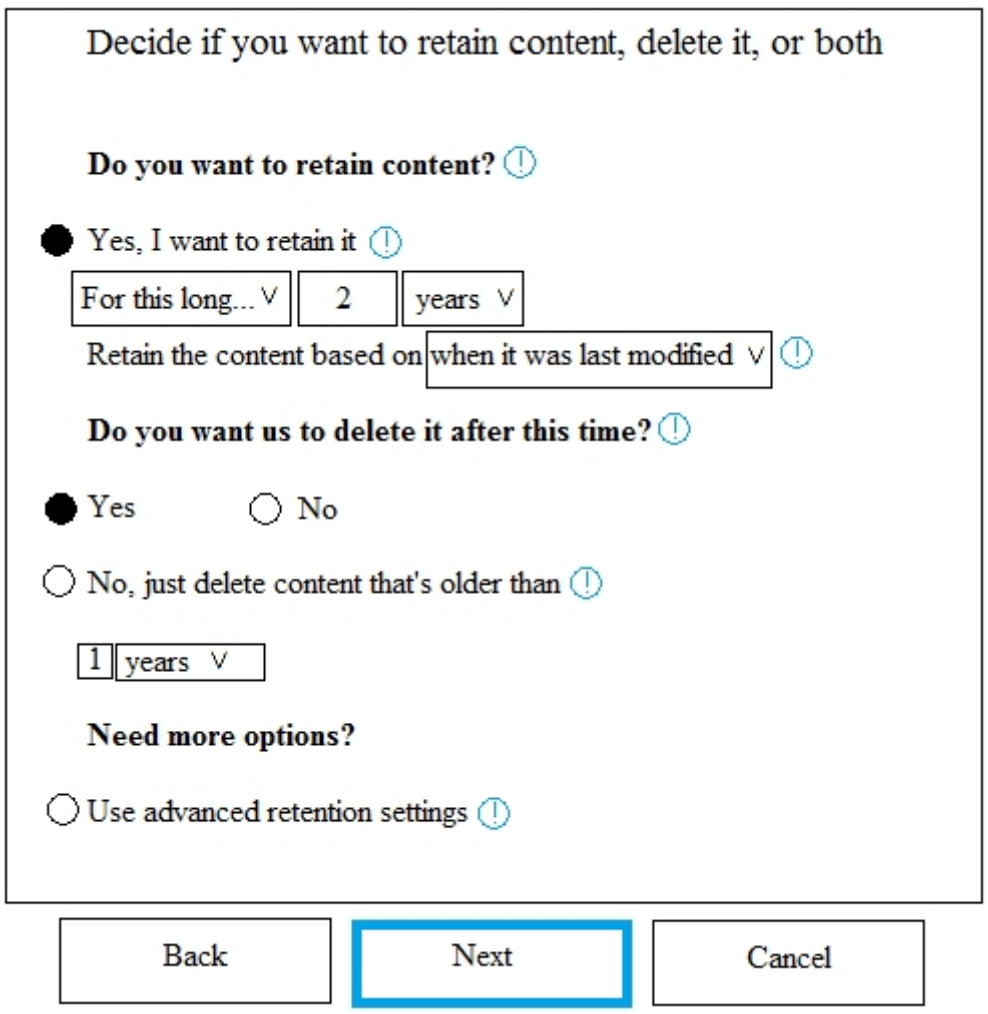
upvoted 2 times

Question #48 *Topic 4*

HOTSPOT -

You have a Microsoft 365 subscription.

You are creating a retention policy named Retention1 as shown in the following exhibit. (Click the Exhibit tab.)



You apply Retention1 to SharePoint sites and OneDrive accounts.

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

NOTE: Each correct selection is worth one point.

Hot Area:

Answer Area

If a user creates a file in a Microsoft SharePoint library on January 1, 2019, and modifies the file every six months, the file will be **[answer choice]**.

- retained
- deleted on January 1, 2021
- deleted on July 1, 2021

If a user creates a file in a Microsoft OneDrive on January 1, 2019, modifies the file on March 1, 2019, and deletes the file on May 1, 2019, the user **[answer choice]**.

- can recover the file until the Recycle Bin retention period expires
- can recover the file until January 1, 2021
- can recover the file until March 1, 2021
- can recover the file until May 1, 2021

kiketxu Highly Voted 4 months, 3 weeks ago

1.- Retained
2.- Can recover the file until the Recycle Bin retention period expired (93 days).
Because the question says "the user", so the user can't recover a file from the "Preservation hold library".
"If the content is modified or deleted during the retention period, a copy of the original content as it existed when the retention policy was assigned is created in the Preservation Hold library. There, the timer job identifies items whose retention period has expired. Those items are moved to the second-stage Recycle Bin, where they're permanently deleted at the end of 93 days. The second-stage Recycle Bin is not visible to end users (only the first-stage Recycle Bin is), but site collection admins can view and restore content from there."
https://docs.microsoft.com/en-us/microsoft-365/compliance/retention-policies-sharepoint?view=o365-worldwide

upvoted 15 times

chaoscreater 3 weeks, 3 days ago

Actually, I don't 100% agree with your explanations for the 2nd question. You are contradicting yourself. Content in a Sharepoint document library will be moved to the 1st-stage Recycle Bin within 7 days of disposition, and then after 7 days the content is moved to the 2nd-stage Recycle Bin and after 93 days it gets permanently deleted. "Users" can access the 1st-stage recycle bin, but only admins can access the 2nd-stage recycle bin.

So your answer "Can recover the file until the Recycle Bin retention period expired (93 days)" is wrong, because the question is asking about the user, not admin.

upvoted 1 times

chaoscreater 3 weeks, 3 days ago

I'm assuming that the question is talking about 1st stage recycle bin, in which case the answer would be correct, but your explanation for the answer is wrong.

upvoted 1 times

chaoscreater 3 weeks, 3 days ago

I wish there is an edit or delete button on this site...

I read the documentation again and the answer for the 2nd question just doesn't make sense at all.

Take a look at this image from the documentation closely:
https://docs.microsoft.com/en-us/microsoft-365/media/retention_diagram_of_retention_flow_in_sites.png?view=o365-worldwide

"If the content is NOT modified or deleted during the retention period, the timer job moves this content to the first-stage Recycle Bin at the end of the retention period."

Let's say a user creates a document today and the retention policy is applied to it. The retention policy says to retain for 2 years and delete the file after that point. If the user does NOT modify or create the file, then at the end of the 2 years, the file gets moved to the first stage recycle bin. A 93 day retention period is applied here (kinda like a grace period). Assuming the user does NOT delete the file from the first stage recycle bin, or empty the first-stage recycle bin, then the user has up to 93 days to recover the file from the first-stage recycle bin.

Based on the above, the answer WOULD be correct. HOWEVER, the question is saying that the user MODIFIES the file, so the above does NOT apply.

upvoted 1 times

chaoscreater 3 weeks, 3 days ago

Based on the above, the answer WOULD be correct. HOWEVER, the question is saying that the user MODIFIES the file, so the above does NOT apply.

In the documentation, it talks about:

"If the content IS MODIFIED OR DELETED during the retention period, a copy of the original content as it existed when the retention settings were assigned is created in the Preservation Hold library...."

In other words, the file does not even go into a first-stage recycle bin. Users do not have access to the Preservation Hold Library and they do not have access to the 2nd-stage recycle bin. So if the answer is that user can recover from the recycle bin, then it does not make sense...

upvoted 1 times

chaoscreater 1 month ago

Agreed. File will be deleted based on last modified date, so user won't be able to recover it on March 1st 2021. However, the file will be recoverable by admin.

upvoted 1 times

arunjana 2 months, 2 weeks ago

Awesome. Perfect explanation

upvoted 1 times

Question #49 *Topic 4*

DRAG DROP -

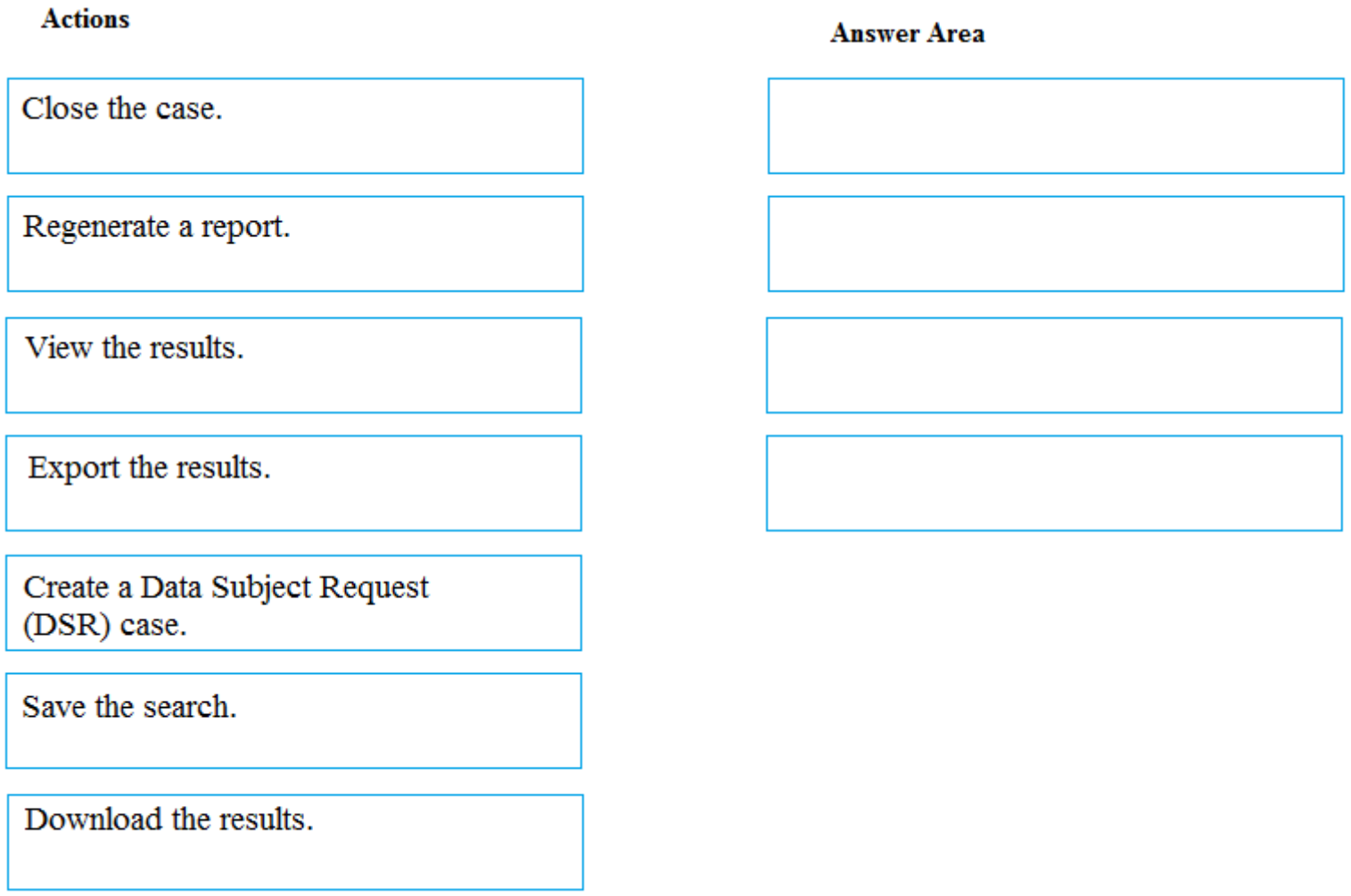
You have a Microsoft 365 subscription.

A customer requests that you provide her with all documents that reference her by name.

You need to provide the customer with a copy of the content.

Which four 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:



kiketxu Highly Voted 4 months, 3 weeks ago

I Imagine this question in the exam will have refined answers as the given ones are not exactly valid. You do not NEED to 'Save' as you can export and download without this.
So the answer should be:
Create DSR case
Export the results
Download the results
Close the case

https://www.examtopics.com/discussions/microsoft/view/6266-exam-ms-500-topic-4-question-27-discussion/

upvoted 5 times

chaoscreater 1 month ago

You didn't include view results, so how would you know exactly what the results looks like? You're exporting the result without checking it first?

upvoted 1 times

GevedeBe Most Recent 3 months, 2 weeks ago

As you have the query run - you Preview the results --> When the search is complete, click Preview results to preview the search results. For more information, see Preview search results. so, that is why View Results should be in it.

upvoted 1 times

GevedeBe 3 months, 2 weeks ago

Create DSR case
View results
Export the results
Download the results

upvoted 2 times

Question #50 *Topic 4*

You have a Microsoft 365 subscription. You need to ensure that users can apply retention labels to individual documents in their Microsoft SharePoint libraries.
Which two actions should you perform? Each correct answer presents part of the solution.
NOTE: Each correct selection is worth one point.

A. From the Cloud App Security admin center, create a file policy.

B. From the SharePoint admin center, modify the Site Settings.

C. From the Compliance admin center, create a label.

D. From the SharePoint admin center, modify the records management settings.

E. From the Compliance admin center, publish a label.

WoneSix Highly Voted 1 year, 6 months ago
Answer B does nothing with respect to the retention label. You can't publish a label until it's been created, and you can't apply a non-existent label to the site settings. It has to be a typo, and it has to be C and E.
upvoted 16 times

AB1 Highly Voted 1 year, 10 months ago
Where is SharePoint & Compliance Center? Never heard of it
upvoted 8 times

STFN2019 1 year, 1 month ago
just a typo mate
upvoted 6 times

kiketxu Most Recent 4 months, 3 weeks ago
Given answers C and E are correct. For sure!
upvoted 3 times

shanti0091 6 months, 1 week ago
agreed typo, its CE
upvoted 1 times

pdpduy 11 months, 3 weeks ago
https://docs.microsoft.com/en-us/microsoft-365/compliance/create-apply-retention-labels?view=o365-worldwide#applying-a-default-retention-label-to-all-content-in-a-sharepoint-library-folder-or-document-set
In addition to enabling people to apply a retention label to individual documents, you can also apply a default retention label to a SharePoint library, folder, or document set, so that all documents in that location get the default retention label.
Is it B, site settings?
upvoted 1 times

tintin_ 1 year, 2 months ago
It's C,E
upvoted 3 times

Ronnie123 1 year, 8 months ago
Should be B and E
upvoted 7 times

Exammiemie 1 year, 7 months ago
If it is a typo and it is SCC, then CE are correct. If not, BE as you mention.
upvoted 2 times

Sizz 1 year, 7 months ago
Looks like just a typo. C and E are correct (the SharePoint configuration is in the library, not site settings).
From the link provided:
1. *Create* the desired retention labels and *publish* these. It can take up to 12 hours for these to be published.
2. For the desired SharePoint sites, edit the document library settings to apply the desired retention labels to items in the library.
3. Create DLP policies to take action based on the retention labels.
upvoted 2 times

Question #51 *Topic 4*

You recently created and published several label policies in a Microsoft 365 subscription.

You need to view which labels were applied by users manually and which labels were applied automatically.

What should you do from the Security & Compliance admin center?

A. From Search & investigation, select Content search

B. From Alerts, select View alerts

C. From eDiscovery, view an eDiscovery case

D. From Reports, select Dashboard

ellik 3 months, 1 week ago

now it is also available from SCC> Infor governance > Lable activity explorer
https://docs.microsoft.com/en-us/microsoft-365/compliance/view-label-activity-for-documents?view=o365-worldwide

upvoted 2 times

kiketxu 4 months, 3 weeks ago

D for sure!

upvoted 3 times

Question #52 *Topic 4*

You have an Azure Active Directory (Azure AD) tenant named contoso.com and a Microsoft 365 subscription. Contoso.com contains the groups shown in the following table.

Name	Type
Group1	Office 365
Group2	Distribution list
Group3	Mail-enabled security
Group4	Security

You plan to create a supervision policy named Policy1.

You need to identify which groups can be supervised by using Policy1.

Which groups should you identify?

A. Group1 and Group4 only

B. Group1 only

C. Group1, Group3, and Group4 only

D. Group2 and Group3 only

E. Group1, Group2, and Group3 only

PeterC Highly Voted 4 months, 3 weeks ago

Only Group 1 and 2 are correct.

https://docs.microsoft.com/en-us/microsoft-365/compliance/communication-compliance-configure?view=o365-worldwide#step-3-optional-set-up-groups-for-communication-compliance

upvoted 10 times

arunjana 2 months, 2 weeks ago

Distribution & M365 groups are the only supported ones

upvoted 2 times

Sethoo 4 months, 1 week ago

That is not an option in the answer choices

upvoted 3 times

NikPat3125 Most Recent 1 week, 4 days ago

came in ms-101 exam on 27.07.2021

upvoted 1 times

SimoneV 2 months, 1 week ago

This one was in MS-101 on 14-05-2021.

upvoted 4 times

kiketxu 4 months, 3 weeks ago

as "Supervision policies" are moving to "Comunicacion compliance" not sure if there will be questions related in the exam.
Btw, based on the shared link by PeterC I would say the same, only group1 and 2 are valid for this.

upvoted 2 times

Question #53 *Topic 4*

Note: This question is part of a series of questions that present the same scenario. Each question in the series contains a unique solution that might meet the stated goals. Some question sets might have more than one correct solution, while others might not have a correct solution.
After you answer a question in this section, you will NOT be able to return to it. As a result, these questions will not appear in the review screen.
You have a Microsoft 365 subscription.
You have a user named User1. Several users have full access to the mailbox of User1.
Some email messages sent to User1 appear to have been read and deleted before the user viewed them.
When you search the audit log in Security & Compliance to identify who signed in to the mailbox of User1, the results are blank.
You need to ensure that you can view future sign-ins to the mailbox of User1.
You run the Set-MailboxFolderPermission ‎λ€"Identity "User1"
-User User1@contoso.com ‎λ€"AccessRights Owner command.
Does that meet the goal?

A. Yes

B. No

Mornay Highly Voted 10 months, 1 week ago

To enable auditing for a single mailbox (in this example, belonging to Holly Sharp), use this PowerShell command: Set-Mailbox -Identity "Holly Sharp" -AuditEnabled $true.

To enable auditing for all Office 365 mailboxes in your organization, use this PowerShell command: Get-Mailbox -ResultSize Unlimited -Filter{RecipientTypeDetails -eq "UserMailbox"} | Set-Mailbox -AuditEnabled$true.

https://support.microsoft.com/en-za/help/4026501/office-auditing-in-office-365-for-admins#:~:text=To%20enable%20auditing%20for%20all,%2DMailbox%20%2DAuditEnabled%24true.

upvoted 10 times

shanti0091 Highly Voted 6 months, 1 week ago

Answer = B. Right command Set-Mailbox -identity "User" -AuditEnabled $true

upvoted 5 times

PattiD Most Recent 7 months, 3 weeks ago

Set-Mailbox -Identity "User1" -AuditEnabled $true

upvoted 3 times

pmr123 10 months, 2 weeks ago

Oops!! Nobody here..Plz continue with option :)

upvoted 1 times

Question #54 *Topic 4*

Note: This question is part of a series of questions that present the same scenario. Each question in the series contains a unique solution that might meet the stated goals. Some question sets might have more than one correct solution, while others might not have a correct solution.
After you answer a question in this section, you will NOT be able to return to it. As a result, these questions will not appear in the review screen.
You have a Microsoft 365 subscription that contains the users shown in the following table.

Name	Role
User1	Compliance Manager Contributor
User2	Compliance Manager Assessor
User3	Compliance Manager Administrator
User4	Portal Admin

You discover that all the users in the subscription can access Compliance Manager reports.
The Compliance Manager Reader role is not assigned to any users.
You need to recommend a solution to prevent a user named User5 from accessing the Compliance Manager reports.
Solution: You recommend assigning the Compliance Manager Reader role to User1.
Does this meet the goal?

A. Yes
B. No

Rockalm Highly Voted 3 months, 2 weeks ago
Why should editing user1 have any impact on user5's access?
upvoted 8 times

Blue Highly Voted 11 months, 2 weeks ago
I tried to replicate this is my environment. But in the newest version of Compliance manager "there is no longer a default Guest access role." Which I Believe this question is refering to. "Now each user must be assigned a role in order to access and work within Compliance Manager." So logic says this series of questions is based off the older set up that allowed all users with an Azure AD account to access Compliance manager as a guest.

To me it does not make sense to apply lower permissions to another user to counteract no/derfault permissions because user1 already has contributor access and by default reader access so no changes would be made if you added this permission to this user.

Same with adding reader access to User5 themselves either way you either made no change at all or the opposite of what you wanted to achieve.

With that logic in mind I would say the both this answer and the following is No.

I would love to know what Microsoft believe the correct answer to be on this question as I would love to know.

https://docs.microsoft.com/en-us/microsoft-365/compliance/compliance-manager-overview?view=o365-worldwide
upvoted 5 times

VTHAR 10 months, 3 weeks ago
With this changes, this question series no longer make any sense and thus seem invalid in future exam.
upvoted 4 times

prats005 Most Recent 4 months ago
Role types
The table below shows the functions allowed by each role in Compliance Manager. The table also shows how each Azure AD role maps to Compliance Manager roles. Users will need at least the Compliance Manager reader role, or Azure AD global reader role, to access Compliance Manager.

ROLE TYPES
User can: Compliance Manager role Azure AD role
Read but not edit data Compliance Manager Reader Azure AD Global reader, Security reader
Edit data Compliance Manager Contribution Compliance Administrator
Edit test results Compliance Manager Assessor Compliance Administrator
Manage assessments, and template and tenant data Compliance Manager Administration Compliance Administrator, Compliance Data Administrator, Security Administrator
Assign users Global Administrator Global Administrator
upvoted 1 times

Gamer50 5 months, 3 weeks ago
The Compliance Manager Contributor, Compliance Manager Assessor, Compliance Manager Administrator all have the Compliance Manager Reader sub role defined under each assignment.

Reference : https://docs.microsoft.com/en-us/microsoft-365/security/office-365-security/permissions-in-the-security-and-compliance-center?view=o365-worldwide
upvoted 1 times

LuisLfr 6 months ago

The correct answer is b, because the user 1 assigment It has nothing to do with user 5 assigment
upvoted 1 times

Atanas 6 months, 3 weeks ago
Compliance Manager Reader can read but not edit data. But "read" means "access" as well in my opinion. Most of the questions and answers here are unclear.
upvoted 1 times

PattiD 7 months, 3 weeks ago
https://docs.microsoft.com/en-us/microsoft-365/compliance/meet-data-protection-and-regulatory-reqs-using-microsoft-cloud?view=o365-worldwide
upvoted 1 times

Learner7 9 months, 3 weeks ago
This question is on the default behaviour. See "By default, this role group may not appear to have any members. However, the Security Reader role from Azure Active Directory is assigned to this role group. Therefore, this role group inherits the capabilities and membership of the Security Reader role from Azure Active Directory.

To manage permissions centrally, add and remove group members in the Azure Active Directory admin center. For more information, see Administrator role permissions in Azure Active Directory. If you edit this role group in the Security & Compliance Center (membership or roles), those changes apply only to the Security & Compliance Center and not to any other services." https://docs.microsoft.com/en-us/microsoft-365/security/office-365-security/permissions-in-the-security-and-compliance-center?view=o365-worldwide
So, if no users are assigned with Compliance Manager Security Reader role, in fact by default, the Security Reader role from Azure Active Directory is used and User5 will have this role. If Compliance Manager Security Reader role is explicitly assigned to User1, all other users, including User5 will be spared this role.
upvoted 2 times

ExamStudy68 9 months, 1 week ago
I understand the Security Reader role default and then assigning it kills the default to everyone - where I get confused is it states "Compliance Manager Reader" NOT Security Reader role - are there two different roles are are those interchangeably the same?
upvoted 1 times

Matthias_privat 1 year, 1 month ago
Answer is No

Typo in text:
Solution: You recommend assigning the Compliance Manager Reader role to User5.
upvoted 2 times

Tayta 1 year, 1 month ago
It's not a typo. There is a question identical to this one (part of a series of questions) with the possible answer of "You recommend assigning the Compliance Manager Reader role to User5." And that answer is no. This answer suggesting if you add the role to User1, does that prevent User5 from accessing the reports, the answer is yes due to that fact that there is now a defined reader role assignment to another user account, this the default all user access allowance is now revoked and all users not granted this role can no longer access the reports.
upvoted 6 times

Tayta 1 year, 1 month ago
I.e if *no* assignment for the role...All users can access. If assignment *is* granted to a user account. All user no longer can access (except the one(s) granted the assignment)
upvoted 5 times

SUBZER0 11 months ago
And how that typo prevents user 5 from accessing to the reports that is the purpose of the question?
upvoted 1 times

mehnaz 1 year ago
This will give USER5 explicit access to reports but the question is about preventing user5 from accessing the reports. So "assign compliance manager reader role to user1" is correct.
upvoted 2 times

BobInTheMoon 1 year, 6 months ago
Answer should be = No.
Typo in the question, the solution should be: "Solution: You recommend assigning the Compliance Manager Reader role to User5."
This solution does not prevent User5 from accessing the Compliance Manager reports.
Notice that the question says "The Compliance Manager Reader role is not assigned to any users." That must mean that all users are accessing the compliance manager reports because they have assigned the "Azure AD Global Reader" permission which also gives read permission to Compliance Manager. I believe the correct solution is the one that mention to remove User5 license.
upvoted 3 times

WoneSix 1 year, 6 months ago
There is no typo in the question. originally, if you had no one in the Compliance Manager Reader group, everyone had access. Adding a single person blocked everyone else.
upvoted 52 times

mehnaz 1 year ago
Perfect answer.
upvoted 1 times

mehnaz 1 year ago

Correction. The questions asks us to PREVENT user5 from accessing the compliance manager reports.And, n order to do so, assigning Compliance manager reader role to USER1 will prevent the USER5 from accessing the reports.

upvoted 4 times

jack987 1 year, 1 month ago

I agree with WoneSix. Answer is correct. There is no typo.

upvoted 3 times

jwkin 1 year, 2 months ago

Do you have anything to back that up? I cannot find anything on what you just said.

upvoted 3 times

krrunal 1 year, 7 months ago

I think in the question where it says "Solution: You recommend assigning the Compliance Manager Reader role to User1." , its a typo.It should be User5 instead of User1 and thats why answer is YES.

upvoted 1 times

Wallace44 1 year, 6 months ago

I'm trying to prevent User5 from seeing reports. Assuming it is a typo, how does assigning USER5 the Reader Role prevent that? Is it not literally granting him read access?

upvoted 7 times

Sizz 1 year, 7 months ago

Would make sense; also here's the correct source reference: https://docs.microsoft.com/en-us/microsoft-365/compliance/meet-data-protection-and-regulatory-reqs-using-microsoft-cloud#permissions-and-role-based-access-control

upvoted 1 times

Sizz 1 year, 7 months ago

I expect the key part of the documentation is actually this: "Note that there is no longer a default Guest access role.". This change was made to the docs in October 2019 (from GitHub history for that article).
It's also mentioned in a blog: "Once role-based access is enabled, all new users have guest access unless assigned more than that." (Source: https://www.agileit.com/news/understanding-microsoft-compliance-manager/)

upvoted 3 times

nitram 1 year, 8 months ago

The link points to a preview. Preview is not valid and the document does not answer the question. It must be the answer No

upvoted 3 times

ChrisBr 1 year, 9 months ago

This makes no sense...
How can I prevent User 5 to see a report by changing the role assignment for User 1?

upvoted 2 times

Niro 1 year, 9 months ago

Read reference for explanation

upvoted 2 times

Question #55 *Topic 4*

HOTSPOT -

You have a Microsoft 365 tenant.

You need to retain Azure Active Directory (Azure AD) audit logs for two years. Administrators must be able to query the audit log information by using the Azure

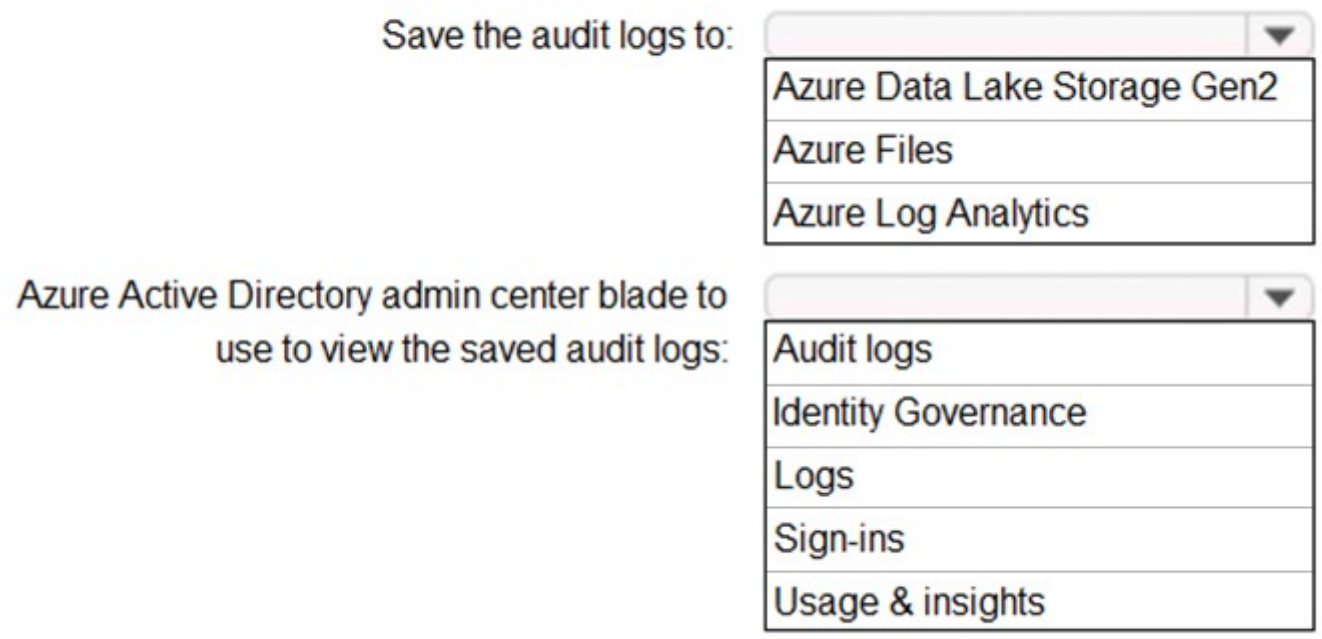
Active Directory admin center.

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

NOTE: Each correct selection is worth one point.

Hot Area:

Answer Area



kiketxu 4 months, 3 weeks ago

I would say given answers are correct.
To the first, is a clear and common procedure. https://docs.microsoft.com/en-gb/azure/active-directory/reports-monitoring/howto-integrate-activity-logs-with-log-analytics

For the second is a bit tricky question as you can continue seeing the "audit logs" in the AAD blade, but the point of the question is "...to view the saved audit logs". AFAIK you need to use "logs" for this.

upvoted 1 times

Question #56 *Topic 4*

Note: This question is part of a series of questions that present the same scenario. Each question in the series contains a unique solution that might meet the stated goals. Some question sets might have more than one correct solution, while others might not have a correct solution.
After you answer a question in this section, you will NOT be able to return to it. As a result, these questions will not appear in the review screen.
You have a Microsoft 365 subscription that contains the users shown in the following table.

Name	Role
User1	Compliance Manager Contributor
User2	Compliance Manager Assessor
User3	Compliance Manager Administrator
User4	Portal Admin

You discover that all the users in the subscription can access Compliance Manager reports.
The Compliance Manager Reader role is not assigned to any users.
You need to recommend a solution to prevent a user named User5 from accessing the Compliance Manager reports.
Solution: You recommend modifying the licenses assigned to User5.
Does this meet the goal?

A. Yes
B. No

mnak Highly Voted 7 months, 3 weeks ago
Just an FYI, while this is correct for when the test was created, it is not correct anymore today. You no longer have to have at least one member in each compliance manager role to disable access to all users. MS finally decided in their infinite wisdom that it was a bad idea to have all your users be able to perform actions in compliance manager.... Reference: https://docs.microsoft.com/en-us/microsoft-365/compliance/meet-data-protection-and-regulatory-reqs-using-microsoft-cloud?view=o365-worldwide#permissions-and-role-based-access-control
upvoted 7 times

Tom993 Highly Voted 8 months, 3 weeks ago
Outdated: https://docs.microsoft.com/en-us/microsoft-365/compliance/meet-data-protection-and-regulatory-reqs-using-microsoft-cloud?view=o365-worldwide

"Note that there is no longer a default Guest access role. Each user must be assigned a role in order to access and work within Compliance Manager."
upvoted 6 times

Gamer50 Most Recent 5 months, 3 weeks ago
Answer is YES.
https://docs.microsoft.com/en-us/office365/servicedescriptions/microsoft-365-service-descriptions/microsoft-365-tenantlevel-services-licensing-guidance/microsoft-365-security-compliance-licensing-guidance#which-licenses-provide-the-rights-for-a-user-to-benefit-from-the-service-6
upvoted 2 times

The_Shepherd 8 months, 2 weeks ago
The given answer is correct :The answer is to assign the compliance manager reader role to user 1. Since no one was assigned this role, means every one have access. So when the role is assigned to User 1, User 5 loses access
upvoted 2 times

gills 1 year, 3 months ago
The answer is to assign the compliance manager reader role to user 1. Since no one was assigned this role, means every one have access. So when the role is assigned to User 1, User 5 loses access.
upvoted 1 times

jwkin 1 year, 2 months ago
Can you provide a link that states that? I cannot find anything about assigning the reader role to prevent other users access.
upvoted 1 times

BobInTheMoon 1 year, 6 months ago
If the User5 license is modified (maybe removed) this should prevent User5 from access to the Compliance Manager right? (not tested).
upvoted 1 times

Akc0 4 months, 2 weeks ago
AFAIK unlicensed users can still be compliance managers and do stuff in compliance/admin portals so answer should be No
upvoted 1 times

ifex380 1 year, 7 months ago
This should be a big YES
upvoted 3 times

ifex380 1 year, 6 months ago
sorry. No.. The answer should be assigning the compliance manager reader role to user5

upvoted 4 times

AlistairMarini 1 year, 2 months ago

Exactly. read the question again. Role and Licenses are different. in the question the proposed solution talks about licenses.

upvoted 3 times

Wallace44 1 year, 6 months ago

but we are trying to prevent user5 from accessing the compliance manager reports. How does assigning him the reader role prevent that?

upvoted 4 times

Question #57 *Topic 4*

Note: This question is part of a series of questions that present the same scenario. Each question in the series contains a unique solution that might meet the stated goals. Some question sets might have more than one correct solution, while others might not have a correct solution.
After you answer a question in this section, you will NOT be able to return to it. As a result, these questions will not appear in the review screen.
You have a Microsoft 365 subscription that contains the users shown in the following table.

Name	Role
User1	Compliance Manager Contributor
User2	Compliance Manager Assessor
User3	Compliance Manager Administrator
User4	Portal Admin

You discover that all the users in the subscription can access Compliance Manager reports.
The Compliance Manager Reader role is not assigned to any users.
You need to recommend a solution to prevent a user named User5 from accessing the Compliance Manager reports.
Solution: You recommend assigning the Compliance Manager Reader role to User5.
Does this meet the goal?

A. Yes

B. No

BobInTheMoon Highly Voted 1 year, 6 months ago

Answer should be = No.
Typo in the question, the solution should be: "Solution: You recommend assigning the Compliance Manager Reader role to User5."
This solution does not prevent User5 from accessing the Compliance Manager reports.
Notice that the question says "The Compliance Manager Reader role is not assigned to any users." That must mean that all users are accessing the compliance manager reports because they have assigned the "Azure AD Global Reader" permission which also gives read permission to Compliance Manager. I believe the correct solution is the one that mention to modify User5 license.

upvoted 7 times

Soumia_Djenan 1 year, 2 months ago

Tested unlicensing a user and then giving him admin roles including the compliance manager and it worked so the type of the license or whether there's any licenses at all doesn't make any difference

upvoted 8 times

Gamer50 Most Recent 5 months, 3 weeks ago

Answers should be NO. Assigning the Compliance Manager Reader Role will grant acess to reports.

https://docs.microsoft.com/en-us/microsoft-365/compliance/compliance-manager-setup?view=o365-worldwide#role-types

upvoted 1 times

ifex380 1 year, 6 months ago

should be yes

upvoted 2 times

Wallace44 1 year, 6 months ago

Disagree. Assigning User 5 the compliance manager reader role is granting read rights to Compliance Manager. The question asks to prevent User5 from accessing the reports.

upvoted 16 times

mehnaz 1 year ago

the answer is correct.Its NO.

upvoted 1 times

STFN2019 1 year, 1 month ago

that's the thing, all the previous related qs should be no. If we wanna prevent access we wouldn't assign the permission to view it. It just contradicts

upvoted 1 times

Question #58 *Topic 4*

You have a Microsoft 365 subscription.

You enable auditing for the subscription.

You plan to provide a user named Auditor with the ability to review audit logs.

You add Auditor to the Global administrator role group.

Several days later, you discover that Auditor disabled auditing.

You remove Auditor from the Global administrator role group and enable auditing.

You need to modify Auditor to meet the following requirements:

- Be prevented from disabling auditing
- Use the principle of least privilege
- Be able to review the audit log

To which role group should you add Auditor?

A. Security reader

B. Compliance administrator

C. Security operator

D. Security administrator

itmp Highly Voted 1 year, 3 months ago

Answer is correct - Security Reader does NOT have the "View-Only Audit Logs".
https://docs.microsoft.com/en-us/microsoft-365/security/office-365-security/permissions-in-the-security-and-compliance-center?view=o365-worldwide

upvoted 23 times

TDAC 10 months, 1 week ago

itmp is correct. This person speaks the gospel.

upvoted 4 times

jack987 1 year, 1 month ago

I agree with itmp. The answer is correct - Security Operator - has the View-Only Audit Log

upvoted 3 times

gills 1 year, 3 months ago

This is correct as listed in the URL https://docs.microsoft.com/en-us/microsoft-365/security/office-365-security/permissions-in-the-security-and-compliance-center?view=o365-worldwide

upvoted 2 times

BobInTheMoon Highly Voted 1 year, 6 months ago

Security reader Read-only access to security features, sign-in reports, and audit logs.
https://docs.microsoft.com/en-us/office365/admin/add-users/about-admin-roles?redirectSourcePath=%252farticle%252fAbout-Office-365-admin-roles-da585eea-f576-4f55-a1e0-87090b6aaa9d&view=o365-worldwide

upvoted 11 times

weabey Most Recent 2 months, 3 weeks ago

View-Only Audit Logs is a separate ROLE. This can be only performed by Compliance Administrator, Compliance Data Administrator, Global Reader, Organization Management, Security Administrator, Security Operator

So the least privilege role which allows to view-only audit logs is Security Operator
So Answer is correct

upvoted 1 times

GevedeBe 3 months, 1 week ago

Azure Active Directory roles in the Microsoft 365 admin center , updated 14-4-2021 shows the following " Security reader: Read-only access to security features, sign-in reports, and audit logs."

upvoted 4 times

Johnny1980 2 months, 3 weeks ago

Name:Security reader
Description:Users with this role have global read-only access, including all information in Azure Active Directory, Identity Protection, Privileged Identity Management, as well as the ability to read Azure Active Directory sign-in reports and audit logs. The role also grants read-only permission in Office 365 Security & Compliance Center

upvoted 2 times

kiketxu 4 months, 3 weeks ago

What a mess of discussion, Security Reader doesn't have the View-Only Audit Logs role. So, its SECURITY OPERATOR.

upvoted 2 times

arunjana 2 months, 2 weeks ago

5/20/2021 - Security reader has the permissions

microsoft.directory/auditLogs/allProperties/read
Read audit logs.

upvoted 1 times

arunjana 2 months, 2 weeks ago

Ouch. MS article (4.17.2021) says this can only be done with a 'Security Operator' role:
https://docs.microsoft.com/en-us/microsoft-365/security/office-365-security/permissions-in-the-security-and-compliance-center?view=o365-worldwide#permissions-needed-to-use-features-in-the-security--compliance-center:~:text=features.-,Compliance%20Search,View%2DOnly%20Manage%20Alerts

upvoted 1 times

itstudy369 6 months, 2 weeks ago

Security Operator 100%

upvoted 3 times

Martyvdb 6 months, 2 weeks ago

https://docs.microsoft.com/en-us/azure/active-directory/roles/permissions-reference#security-operator

Security Reader
Users with this role have global read-only access on security-related feature, including all information in Microsoft 365 security center, Azure Active Directory, Identity Protection, Privileged Identity Management, as well as the ability to read Azure Active Directory sign-in reports and audit logs, and in Office 365 Security & Compliance Center.

upvoted 3 times

Mary_Yvette 6 months, 4 weeks ago

Tested this, only COmpliance Admin will allow the user to access the Audit Logs.

upvoted 1 times

ash4rose 7 months, 1 week ago

Correct Answer is "Security Reader Role" Please refer this Ms Article, Security Operator role has no permission with Review audit logs.

https://docs.microsoft.com/en-us/azure/active-directory/roles/permissions-reference#security-operator

upvoted 2 times

TonySuccess 8 months, 1 week ago

Security Reader:

Assigned roles
View-Only Manage Alerts
View-Only Device Management
View-Only IB Compliance Management
View-Only DLP Compliance Management
Security Reader
Sensitivity Label Reader

Security Operator:

Assigned roles
Manage Alerts
View-Only Manage Alerts
View-Only Device Management
View-Only IB Compliance Management
View-Only DLP Compliance Management
Security Reader
>>>>>>>>>>>>>>>>>>>>View-Only Audit Logs <<<<<<<<<<<<<<<<<<<<<<<<<<<<
Compliance Search

upvoted 3 times

sathya69 8 months, 3 weeks ago

Security reader.
Who can access the data?
Users in the Security Administrator, Security Reader, Report Reader , Global Reader or Global Administrator roles

upvoted 2 times

Ashton_98 7 months, 2 weeks ago

Permissions are detailed clearly here - https://docs.microsoft.com/en-us/microsoft-365/security/office-365-security/permissions-in-the-security-and-compliance-center?view=o365-worldwide

Sadly, the documentation still says Security Operator so that's what I would answer with until it is changed / updated.

upvoted 1 times

DrMe 7 months, 2 weeks ago

Agreed, it doesn't list audit for security reader:
https://docs.microsoft.com/en-us/microsoft-365/security/office-365-security/permissions-in-the-security-and-compliance-center?view=o365-worldwide#permissions-needed-to-use-features-in-the-security--compliance-center:~:text=services.-,Security%20Reader,View%2DOnly%20Manage%20Alerts

But it does for Security Operator:
https://docs.microsoft.com/en-us/microsoft-365/security/office-365-security/permissions-in-the-security-and-compliance-center?view=o365-worldwide#permissions-needed-to-use-features-in-the-security--compliance-center:~:text=features.-,Compliance%20Search,View%2DOnly%20Manage%20Alerts

upvoted 1 times

Alvaroll 9 months ago

Security Reader
"Users with this role have global read-only access on security-related feature, including all information in Microsoft 365 security center, Azure Active Directory, Identity Protection, Privileged Identity Management, as well as the ability to read Azure Active Directory sign-in reports and audit logs, and in Office 365 Security & Compliance Center. More information about Office 365 permissions is available at Permissions in the Security & Compliance Center."
https://docs.microsoft.com/en-us/azure/active-directory/roles/permissions-reference#security-reader

upvoted 1 times

Alvaroll 9 months ago

I've just tried on my LAB, and Security Reader can't access to Audit log search, so I'm with Security Operator.

upvoted 2 times

Saavugrakki99 10 months, 1 week ago

Security Operator

upvoted 1 times

Morne 10 months, 3 weeks ago

Security Operator Members can manage security alerts, and also view reports and settings of security features.
View-Only Audit Logs

https://docs.microsoft.com/en-us/microsoft-365/security/office-365-security/permissions-in-the-security-and-compliance-center?view=o365-worldwide

upvoted 1 times

Hisagenda 11 months ago

Answer is security reader, using the principle of least privilege.Security op can can view, investigate, and respond to active threats to your Microsoft 365 users, devices, and content. while security reader cannot respond!!!

upvoted 1 times

junkz 1 year ago

it's a bit weird. i tested this with fresh user and gave the 4 options as role groups for this user:
security operator- no audit menu in search
security reader - missing entire search menu
compliance admin - missing entire search menu
security admin -missing entire search menu
if i tried to go to the page explicitly, i got "You don't have the required permission. Check your permission and try again" though checking turned out fine. Not sure what to make of this but based on "https://docs.microsoft.com/en-us/microsoft-365/security/office-365-security/permissions-in-the-security-and-compliance-center?view=o365-worldwide#roles-in-the-security--compliance-center" i would go with security administrator as option
Audit Logs Turn on and configure auditing for the organization, view the organization's audit reports, and then export these reports to a file. Organization Management|Security Administrator

upvoted 1 times

junkz 1 year ago

correction, security operator , because that gives least priviledged while allowing RO auditing
View-Only Audit Logs View and export audit reports. Because these reports might contain sensitive information, you should only assign this role to people with an explicit need to view this information.
Compliance Administrator
Compliance Data Administrator
Organization Management
Security Administrator
Security Operator

upvoted 8 times

mariansdj 1 year ago

Copy/paste from my tenant:

Assign the Security reader role to users who need to do the following:

-View security-related features in the Microsoft 365 Security center, Azure AD Identity Protection, Privileged Identity Management, but not edit any settings
-View Azure AD sign-in reports and audit logs

upvoted 2 times

Question #59

Topic 4

You have a Microsoft 365 E3 subscription.

You plan to audit all Microsoft Exchange Online user and admin activities.

You need to ensure that all the Exchange audit log records are retained for one year.

What should you do?

A. Modify the retention period of the default audit retention policy.

B. Create a custom audit retention policy.

C. Assign Microsoft 365 Enterprise E5 licenses to all users.

D. Modify the record type of the default audit retention policy.

Davemarshal 1 day, 14 hours ago

Answer is C

upvoted 1 times

SerhioG 4 months, 1 week ago

Before you create an audit log retention policy

You have to be assigned the Organization Configuration role in the Security & Compliance Center to create or modify an audit retention policy.

You can have a maximum of 50 audit log retention policies in your organization.

To retain an audit log for longer than 90 days (and up to 1 year), the user who generates the audit log (by performing an audited activity) must be assigned an Office 365 E5 or Microsoft 365 E5 license or have a Microsoft 365 E5 Compliance or E5 eDiscovery and Audit add-on license. To retain audit logs for 10 years, the user who generates the audit log must also be assigned a 10-year audit log retention add-on license in addition to an E5 license.

All custom audit log retention policies (created by your organization) take priority over the default retention policy. For example, if you create an audit log retention policy for Exchange mailbox activity that has a retention period that's shorter than one year, audit records for Exchange mailbox activities will be retained for the shorter duration specified by the custom policy.
https://docs.microsoft.com/en-us/microsoft-365/compliance/audit-log-retention-policies?view=o365-worldwide

upvoted 3 times

kiketxu 4 months, 3 weeks ago

C for sure!

upvoted 3 times

Question #60 *Topic 4*

You have a Microsoft 365 subscription.

You have a team named Team1 in Microsoft Teams.

You plan to place all the content in Team1 on hold.

You need to identify which mailbox and which Microsoft SharePoint site collection are associated to Team1.

Which cmdlet should you use?

A. Get-UnifiedGroup

B. Get-MailUser

C. Get-Team

D. Get-TeamChannel

kiketxu Highly Voted 4 months, 3 weeks ago

Correct.
https://docs.microsoft.com/en-us/powershell/module/exchange/get-unifiedgroup?view=exchange-ps

upvoted 5 times

AjayGadge Most Recent 3 weeks, 1 day ago

Get-UnifiedGroup -Identity "*Team1*" | Select -ExpandProperty SharePointSiteURL

Get-UnifiedGroup -Identity "*Team1*" -ResultSize Unlimited | Select DisplayName,EmailAddresses,Notes,ManagedBy,AccessType

upvoted 1 times

Question #61 *Topic 4*

Note: This question is part of a series of questions that present the same scenario. Each question in the series contains a unique solution that might meet the stated goals. Some question sets might have more than one correct solution, while others might not have a correct solution.
After you answer a question in this section, you will NOT be able to return to it. As a result, these questions will not appear in the review screen.
You have a Microsoft 365 subscription that contains the users shown in the following table.

Name	Role
User1	Compliance Manager Contributor
User2	Compliance Manager Assessor
User3	Compliance Manager Administrator
User4	Portal Admin

You discover that all the users in the subscription can access Compliance Manager reports.

The Compliance Manager Reader role is not assigned to any users.

You need to recommend a solution to prevent a user named User5 from accessing the Compliance Manager reports.

Solution: You recommend removing User1 from the Compliance Manager Contributor role.

Does this meet the goal?

A. Yes

B. No

Currently there are no comments in this discussion, be the first to comment!

Topic 5 - Question Set 5

Question #1 *Topic 5*

NOTE: This question is a part of a series of questions that present the same scenario. For each of the following statements, select the best response
(s) to the question or statement below. Each answer is worth one point.
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.
Your company's head of IT Security has instructed you to put a continual privileged access review system in place. He requires that all privileged accounts be reviewed every seven days. Users with administrative privileges must self-assess their access, however, if an administrator doesn't respond within three days of receiving such a request, privileged access must be removed.
What tool will you use to implement his requirements?

A. Azure Active Directory

B. Azure AD Privileged Identity Management

C. Identity Governance

D. Activity Log

Sorrynotsorry 2 weeks, 1 day ago

Why not Identity Governance? it has Access Reviews

upvoted 1 times

ThBEST 1 month ago

I agree with the answer and I would like to add that this question has been updated. There is a similar question within these practice questions that is worded slightly different but has the exact same answer.

upvoted 2 times

Question #2 *Topic 5*

NOTE: This question is a part of a series of questions that present the same scenario. For each of the following statements, select the best response
(s) to the question or statement below. Each answer is worth one point.
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.
Your company's head of IT Security has instructed you to put a continual privileged access review system in place. He requires that all privileged accounts be reviewed every seven days. Users with administrative privileges must self-assess their access, however, if an administrator doesn't respond within three days of receiving such a request, privileged access must be removed.
What will you configure as the frequency on the access review?

A. One time

B. Weekly

C. Monthly

D. Quarterly

E. Annually

Question #3 *Topic 5*

NOTE: This question is a part of a series of questions that present the same scenario. For each of the following statements, select the best response
(s) to the question or statement below. Each answer is worth one point.
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.
Your company's head of IT Security has instructed you to put a continual privileged access review system in place. He requires that all privileged accounts be reviewed every seven days. Users with administrative privileges must self-assess their access, however, if an administrator doesn't respond within three days of receiving such a request, privileged access must be removed.
What will you select for the Reviewers option of the access review?

A. Selected users

B. Members

C. Administrators

D. Privileged users

Question #4 *Topic 5*

NOTE: This question is a part of a series of questions that present the same scenario. For each of the following statements, select the best response
(s) to the question or statement below. Each answer is worth one point.
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.
Your company's head of IT Security has instructed you to put a continual privileged access review system in place. He requires that all privileged accounts be reviewed every seven days. Users with administrative privileges must self-assess their access, however, if an administrator doesn't respond within three days of receiving such a request, privileged access must be removed.
Where would you configure what happens if a reviewer doesn't respond to the request?

A. Upon completion settings

B. Advanced settings

C. Duration

D. Review role membership

Question #5 *Topic 5*

NOTE: This question is a part of a series of questions that present the same scenario. For each of the following statements, select the best response
(s) to the question or statement below. Each answer is worth one point.
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.
Your company's head of IT Security has instructed you to put a continual privileged access review system in place. He requires that all privileged accounts be reviewed every seven days. Users with administrative privileges must self-assess their access, however, if an administrator doesn't respond within three days of receiving such a request, privileged access must be removed.
What would you select for the ز€If reviewers don't respondز€ option?

A. No change

B. Remove access

C. Approve access

D. Take recommendations

Question #6 *Topic 5*

NOTE: This question is a part of a series of questions that present the same scenario. For each of the following statements, select the best response
(s) to the question or statement below. Each answer is worth one point.
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 Windows Server 2016 server in your environment that will be a domain controller. You want to enable the following security products on the new server:

Azure ATP -

Defender ATP -

Azure Sentinel -
Which of the following will you download and install on the server? Each answer is part of the complete solution. (Choose two.)

A. Microsoft Management Agent

B. Local script

C. Sensor setup package

D. Azure Management Agent

JoelB 4 weeks, 1 day ago
Answer A. should say "Microsoft Monitoring Agent", not management agent.
upvoted 1 times

Question #7 *Topic 5*

NOTE: This question is a part of a series of questions that present the same scenario. For each of the following statements, select the best response
(s) to the question or statement below. Each answer is worth one point.
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 Windows Server 2016 server in your environment that will be a domain controller. You want to enable the following security products on the new server:

Azure ATP -

Defender ATP -

Azure Sentinel -
Which of the following items will you require for the configuration on the server? (Choose all that apply.)

A. Workspace ID from Azure ATP console

B. Workspace key from Azure ATP console

C. Workspace ID from Defender ATP console

D. Workspace key from Defender ATP console

E. Workspace ID from Sentinel console

F. Workspace key from Sentinel console

Question #8 *Topic 5*

NOTE: This question is a part of a series of questions that present the same scenario. For each of the following statements, select the best response
(s) to the question or statement below. Each answer is worth one point.
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 Windows Server 2016 server in your environment that will be a domain controller. You want to enable the following security products on the new server:

Azure ATP -

Defender ATP -

Azure Sentinel -
How will you configure the Microsoft Management Agent on the server? (Choose all that apply.)

A. Workspace ID from Azure ATP console

B. Workspace key from Azure ATP console

C. Workspace ID from Defender ATP console

D. Workspace key from Defender ATP console

E. Workspace ID from Sentinel console

F. Workspace key from Sentinel console

Question #9 *Topic 5*

You are configuring Azure Active Directory and need to synchronize on-premises Active Directory user accounts, but your security officer does not want passwords or their derivatives to be stored in the cloud at all.
Which options are available to you? (Choose two.)

A. AAD Connect with Azure Active Directory Domain Services

B. AAD Connect with pass-through authentication (PTA)

C. AAD Connect with password hash-sync (PHS)

D. AAD Connect with AD federation (AD FS)

Question #10 *Topic 5*

Which of the following Windows 10 Enterprise features provides biometric identity access control?

A. Windows Hello

B. Credential Guard

C. Device Guard

D. Defender Antivirus

E. Defender ATP

JakubK64 2 weeks, 2 days ago
Definetly
upvoted 1 times

Question #11 *Topic 5*

You have deployed AIP in your organization. You are trying to discover, classify and protect existing data in your organization. You have deployed AIP scanner to a server named Bigbrother1.
Which of the following are valid targets in for your AIP Scanner deployment? (Choose two.)

A. UNC path over SMB protocol

B. Local storage on BigBrother1

C. OneDrive

D. Windows Server 2012 and above

E. SharePoint Server 2013 and above

F. Exchange Server 2013 and above

JamieWilson 1 month, 1 week ago

SharePoint is now supported:
The AIP scanner runs as a service on Windows Server and lets you discover, classify, and protect files on the following data stores:

UNC paths for network shares that use the SMB or NFS (Preview) protocols.

SharePoint document libraries and folder for SharePoint Server 2019 through SharePoint Server 2013. SharePoint 2010 is also supported for customers who have extended support for this version of SharePoint.

upvoted 4 times

Question #12 *Topic 5*

You are the global administrator of your organizationâ€™s M365 subscription. You have created a data subject request case and you are reviewing the search results, but you see the following message in place of the expected results:
You don't have permissions to preview, ask the administrator to assign them.
Where would you assign yourself the appropriate permissions?

A. Azure portal

B. M365 admin portal

C. Office 365 Security & Compliance Center

D. Microsoft Cloud App Security

E. M365 Compliance Center

PeterDad 3 weeks ago

You can actually do it from both M 365 Compliance center (https://compliance.microsoft.com/) and Office365 Security & Compliance Center (https://protection.office.com/permissions) from Permissions option!
Not sure if the question is outdated??
upvoted 3 times

oscargtech 3 weeks, 1 day ago

I think the correct answer should be E.

"Assign eDiscovery permissions
Go to https://compliance.microsoft.com and sign in using an account that can assign permissions.

In the left pane of the Microsoft 365 compliance center, select Permissions.

On the Permissions & Roles page, under Compliance center, click Roles.

On the Compliance center roles page, select eDiscovery Manager.

On the eDiscovery Manager flyout page, do one of the following based on the eDiscovery permissions that you want to assign."

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

Question #13 *Topic 5*

What is the maximum number of days you can allow users to remember their MFA sessions?

A. 15 days

B. 30 days

C. 60 days

D. 120 days

JamieWilson Highly Voted 1 month, 1 week ago

This is now 365 Days:

"Allow users to remember multi-factor authentication on devices they trust (between one to 365 days)"
upvoted 9 times

oscargtech 3 weeks, 1 day ago

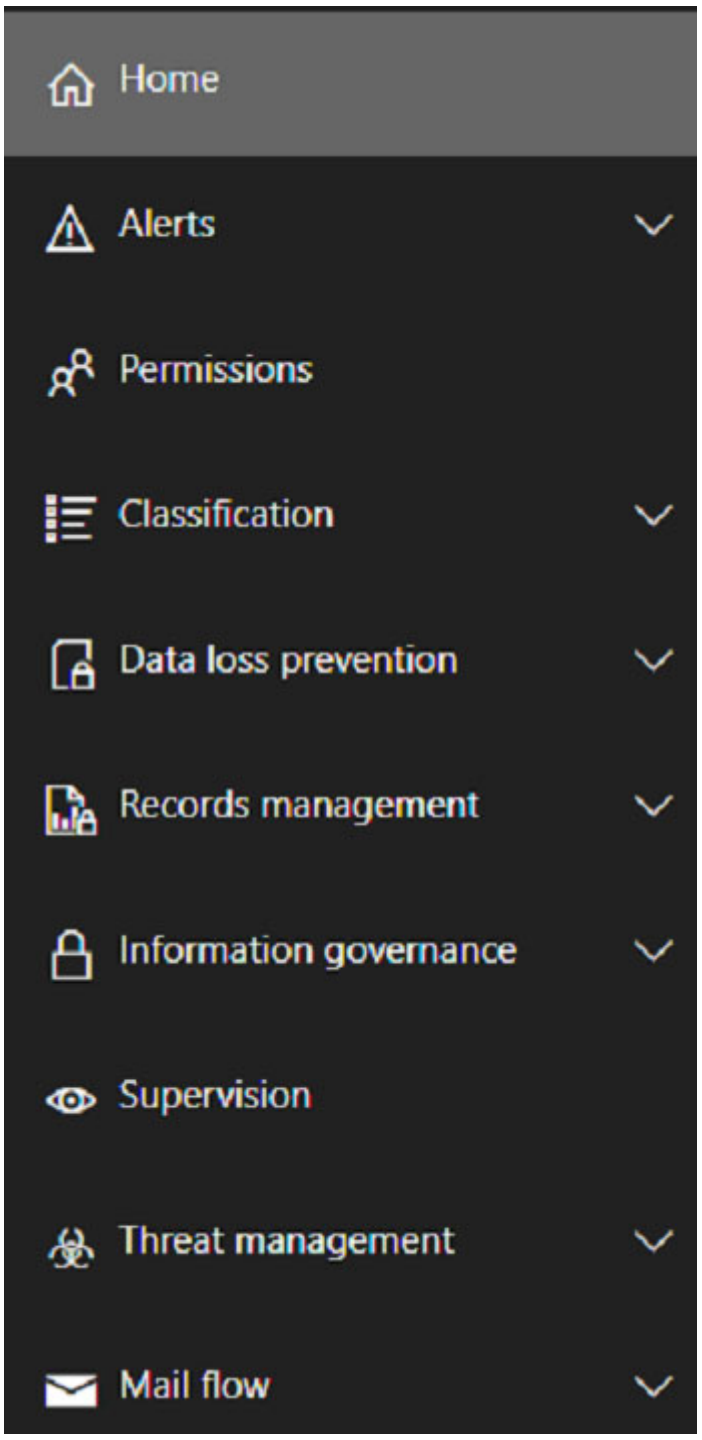
Just tested and confirmed this change
upvoted 3 times

Question #14

Topic 5

The exhibit shows the O365 Security & Compliance Center interface.

Where would you start a Data Subject Request (DSR) search?



A. Data loss prevention

B. Records management

C. Information governance

D. Data privacy

E. Search

F. eDiscovery

Fala_Fel 2 weeks, 5 days ago

July 2021 this is now in
- M365 Compliance > Solutions > Data Subject Requests.
(Data Privacy isn't on the current menu)

upvoted 3 times

Fala_Fel 2 weeks, 5 days ago

Answer is still correct. Data Subject Requests are also found in "Office 365 Security & Compliance" > Data Privacy
Apologies for any confusion. Two different consoles doing similar things.

upvoted 3 times

Question #15 *Topic 5*

You've deployed WIP in silent mode, what is the user experience?

A. Sensitive content is blocked without user intervention

B. User is warned not to share sensitive data, but can override the warning

C. User is warned not to share sensitive data, and the action is blocked

D. Sensitive data is not blocked

Fala_Fel 2 weeks, 5 days ago

Ans is correct = D
Silent mode does not stop sharing sensitive data, does not prompt user (but does log it)
"WIP runs silently, logging inappropriate data sharing, without blocking anything that would have been prompted for employee interaction while in Allow Override mode. "
https://docs.microsoft.com/en-us/mem/intune/apps/windows-information-protection-policy-create

upvoted 1 times

Question #16 *Topic 5*

You are configuring Conditional Access App Control (CAAC) for SharePoint Online to prevent printing and downloading of content when the sire is accessed from unmanaged devices. You start by configuring the appropriate conditional access policy in Azure Active Directory. You also need to configure the correct policy in
Microsoft Cloud App Security.
Which CAS policy do you create?

A. Activity policy

B. File policy

C. Access policy

D. Session policy

Question #17 *Topic 5*

The Customer lockbox feature helps you control how an administrator can access customer data.
NOTE: Change (or not) the highlighted section of the following statement to make it true.

A. Leave unchanged

B. a Microsoft support engineer

C. an Azure Active Directory B2B user

D. an Azure Active Directory authenticated user

Question #18 *Topic 5*

Who participates in the shared responsibility model in the compliance manager? (Choose two.)

A. Microsoft

B. Azure

C. Customer

D. Partner

E. Vendor

F. Standards organization

Question #19 *Topic 5*

When you enable in-place archiving for a user's mailbox in O365, which of the following will happen for the user's mailbox?

A. When the user's mailbox exceeds the maximum mailbox size by 50%, Outlook will prompt the user to move email to the archive mailbox.

B. When the user's mailbox exceeds the maximum mailbox size by 20%, Outlook will prompt the user to move email to the archive mailbox.

C. All email older than 2 years will be immediately moved to the archive mailbox.

D. All email older than 3 years will be immediately moved to the archive mailbox.

Fala_Fel 2 weeks, 5 days ago

Correct = C
"When an archive mailbox is enabled, the default Exchange retention policy automatically does the following:
Moves items that are two years or older from a user's primary mailbox to their archive mailbox."
https://docs.microsoft.com/en-us/microsoft-365/compliance/enable-archive-mailboxes?view=o365-worldwide

upvoted 1 times

oscargtech 3 weeks, 1 day ago

Correct.

" The default archive policy that is part of the retention policy assigned to Exchange Online mailboxes moves items to the archive mailbox two years after the date the item was delivered to the mailbox or created by the user." From the linked source

upvoted 3 times

Question #20 *Topic 5*

Your organization has decided that user's personal mobile devices are not to be enrolled or managed by your organizationλ€™s Intune Mobile Device Management
(MDM) solution. Furthermore, your organization requires you to protect the organizationλ€™s data, including data on users' personal mobile devices.
Which of the following is the best course of action in this scenario?

A. Deploy Azure Information Protection (AIP) to classify, label and protect corporate data on users' devices

B. Deploy Azure Active Directory Identity Protection to provide access control to corporate data on users' devices

C. Enroll devices in Intune MDM and deploy device configuration policies to protect corporate data on users' devices

D. Deploy Intune Mobile Application Management policies to protect corporate data on users' devices

E. None of the options meet the objectives.

Fala_Fel 2 weeks, 5 days ago

Agree Ans = D
"Mobile Application Management (MAM) app protection policies allows you to manage and protect your organization's data within an application. With MAM without enrollment (MAM-WE), a work or school-related app that contains sensitive data can be managed on almost any device, including personal devices in bring-your-own-device (BYOD) scenarios"
https://docs.microsoft.com/en-us/mem/intune/apps/app-protection-policy

upvoted 1 times

Question #21 *Topic 5*

How long are messages sent to Office 365 Quarantine retained before being purged?

A. 15 days

B. 30 days

C. 90 days

D. 24 hours

E. 48 hours

oscargtech 3 weeks, 1 day ago

Correct. From the source: Retain spam in quarantine for this many days: Specifies how long to keep the message in quarantine if you selected Quarantine message as the action for a spam filtering verdict. After the time period expires, the message is deleted. The default value is 30 days. A valid value is from 1 to 30 days.

upvoted 1 times

Question #22 *Topic 5*

You're looking for information regarding Microsoft security, privacy and compliance practices relevant to your M365 subscription.
Which of the following resources will you consult?

A. Service Trust Portal

B. Compliance Manager

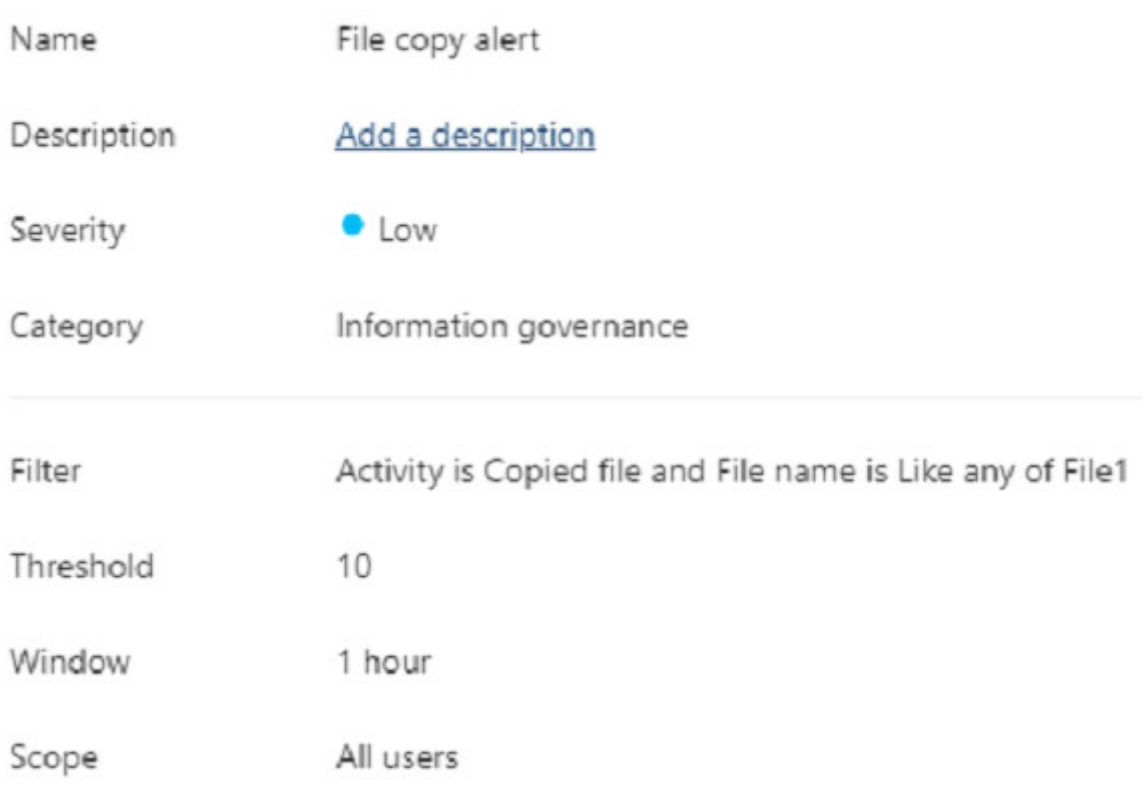
C. Trust Center

D. Azure Security Center

E. Microsoft Compliance Portal

Question #23

Topic 5



You create an alert policy as in the exhibit. (Choose all that apply.)

A. User1 copies File1 every 5 minutes. An alert is triggered after 10 minutes.

B. User1 copies File1 every 5 minutes. An alert is triggered after 50 minutes.

C. User1 copies File1 every 5 minutes. An alert is triggered after 60 minutes.

D. Five users all copy File1 every 5 minutes. An alert is triggered after 10 minutes.

E. Five users all copy File1 every 5 minutes. An alert is triggered after 50 minutes.

F. Five users all copy File1 every 5 minutes. An alert is triggered after 60 minutes.

chaoscreater 1 month ago

Alert should be triggered immediately, that's the whole point of an "alert". The threshold is set to 10, so if user1 copies file1 every 5 minutes, then in 50 minutes the threshold would be met. So B is definitely one of the answers. Same goes with D and E. The reason why E is also correct is because the threshold would be met by 5 users copying every 10 minutes. So at each 10 minute mark, there should be an alert generated.

upvoted 1 times

JoelB 4 weeks, 1 day ago

With regards to your last sentence - it depends on the tenant subscription, which is not specified in the question. Alerts are aggregated so in the case of E3 subscription a new alert will not be generated every 10 minutes, the new event is added to the existing alert.

upvoted 2 times

Nasser 1 month ago

I say that the correct answers are B & D.
- Due to B the same as you said.
- Due to D: when five users copy the file every 5 minutes, then the policy would be triggered after 10 minutes, not after 50 or 60 minutes.
within 5 minutes ---> 5 actions happen
so the limit will be reached after the 2nd 5 minutes (after 10 minutes)

upvoted 2 times

Fala_Fel 2 weeks, 5 days ago

@JoelB yes the answer depends on the aggregation interval, which is different depending on your subscription. B & D are def correct answers. Aggregation interval for E5 is 1 min, for E3 is 15 min.
Assuming they have an E5 license then the correct answer is B-D-E-F
Which is the answer I will be giving in the exam, as most of the questions require an E5 license.
https://docs.microsoft.com/en-us/microsoft-365/compliance/alert-policies?view=o365-worldwide#alert-aggregation

upvoted 1 times

Question #24

Topic 5

How do you require MFA for all users while keeping productivity disruptions to a minimum?

A. Enable MFA for all users using the MFA console

B. Enable a conditional access policy

C. Enable Azure AD Privileged Identity management

D. Enable Azure Role Based Access Control

Fala_Fel 2 weeks, 5 days ago

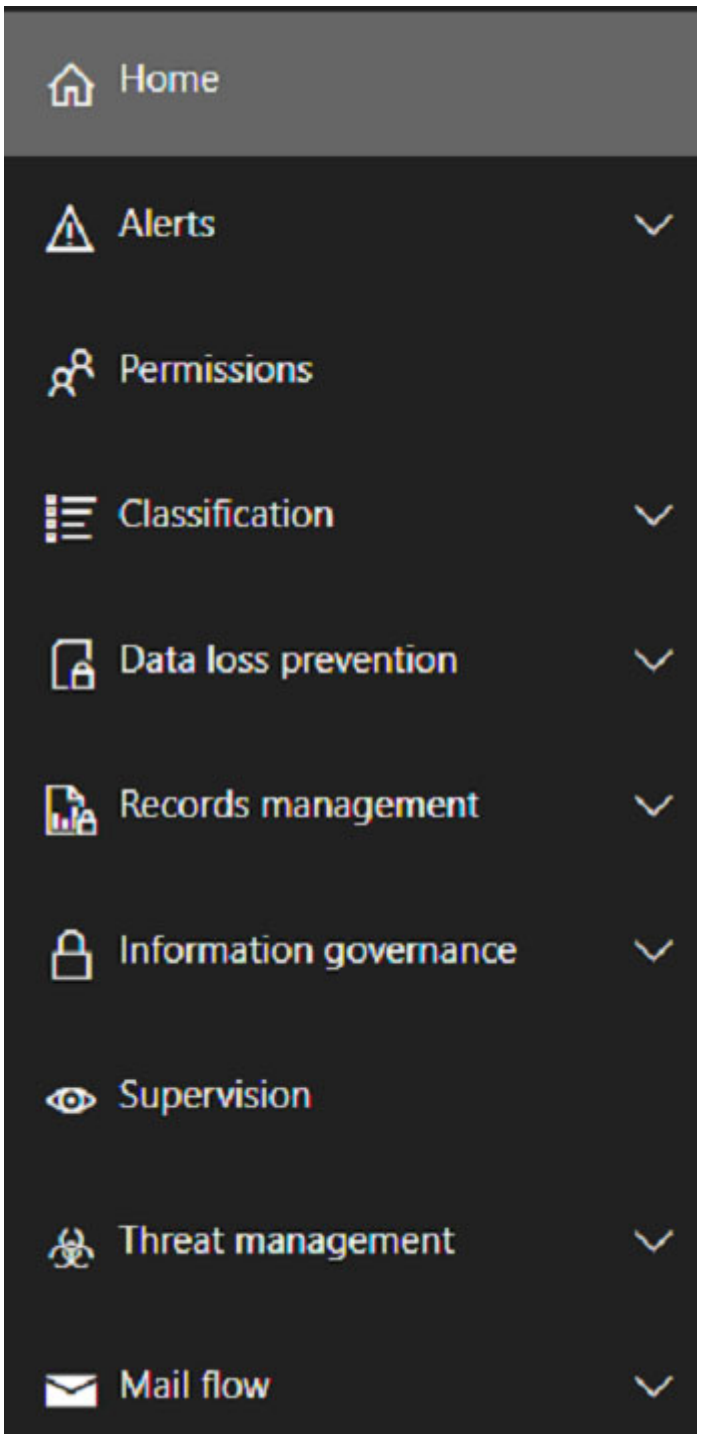
Agreed - B

upvoted 3 times

Question #25

Topic 5

The exhibit shows the O365 Security & Compliance Center interface.



Where would you configure data retention labels?

A. Data loss prevention

B. Records management

C. Information governance

D. Data privacy

E. Search

F. eDiscovery

G. Classification

Fala_Fel 2 weeks, 5 days ago

Maybe old question. July 2021 In Microsoft 365 Compliance (not Office 365) Retention & Labels are configured in Solutions > Information Governance

upvoted 1 times

Fala_Fel 2 weeks, 5 days ago

But answer is still correct = Classification
Just found "Office 365 Security & Compliance" and Retention Labels are under Classification.

upvoted 2 times

Question #26 *Topic 5*

You create a sensitivity label named secret and enable encryption. On the assign permission page, you select all tenant members. A user ز€" Sally ز€" creates a team in Teams and invites a guest user ز€" Kevin. Sally creates a document in Word and applies the secret label. She uploads to document to the Teams file library.
Select which items are true. (Choose three.)

A. Sally successfully uploads the document to Teams

B. Kevin can see the document listed in the Teams files library

C. Kevin can download the document from the Teams files library

D. Kevin can open the document and view the content

Question #27 *Topic 5*

You are the administrator of your organizationز€™s Office 365 ATP anti-phishing policies.
What is the default location for delivering email messages identified as phishing?

A. Phishing emails are blocked (deleted)

B. Phishing emails are delivered to users' inbox

C. Phishing emails are delivered to O365 quarantine

D. Phishing emails are delivered to users' junk email folder

VMS 1 week, 2 days ago

By default goes to user's Junk Email folder
https://docs.microsoft.com/en-us/microsoft-365/security/office-365-security/set-up-anti-phishing-policies?view=o365-worldwide#impersonation-settings-in-atp-anti-%20phishing-policies

upvoted 3 times

zafra2020 2 weeks, 1 day ago

https://docs.microsoft.com/en-us/microsoft-365/security/office-365-security/quarantine-email-messages?view=o365-worldwide#:~:text=By%20default%2C%20anti-spam%20polices%20quarantine%20phishing%20messages%2C%20and%20deliver%20spam%20and%20bulk%20email%20messages%20to%20the%20user%27s%20Junk%20Email%20folder.%20But%2C%20you%20can%20also%20create%20and%20customize%20anti-spam%20policies%20to%20quarantine%20spam%20and%20bulk-email%20messages.%20For%20more%20information%2C%20see%20Configure%20anti-spam%20policies%20in%20EOP.

upvoted 1 times

Question #28 *Topic 5*

You configure AAD Connect to synchronize your OPE AD with AAD. You choose express settings.
Which of the following features are configured?

A. Password hash synchronization (PHS)

B. Password writeback

C. Group writeback

D. Device writeback

E. All of the options

F. None of the options

Question #29 *Topic 5*

Which of the following regulatory standards are supported as part of the compliance manager? (Choose all that apply.)

A. NIST 800-53

B. ISO27001

C. GDPR

D. ISO27002

E. ISO27018

F. Sarbanes-Oxley

JoelB 4 weeks, 1 day ago

The provided link shows an example of assessment groups, however the assessment templates included in Compliance Manager are available here: https://docs.microsoft.com/en-gb/microsoft-365/compliance/compliance-manager-templates-list?view=o365-worldwide#included-templates
Some of the choices in the answers are premium options, yet still supported. Not sure MS would want us to memorize 300+ templates, but the base templates is a good start

upvoted 1 times

Question #30 *Topic 5*

What license level is needed for AAD Connect with pass-through authentication?

A. AAD P1

B. AAD P2

C. O365 Apps

D. AAD free

oscargtech 3 weeks, 1 day ago

"Is Pass-through Authentication a free feature?
Pass-through Authentication is a free feature. You don't need any paid editions of Azure AD to use it."

https://docs.microsoft.com/en-us/azure/active-directory/hybrid/how-to-connect-pta-faq

upvoted 2 times

Question #31 *Topic 5*

What content marking options are available when creating classification labels in O365? (Choose three.)

A. Header

B. Footer

C. Watermark

D. Steganography

E. Hidden text

Question #32 *Topic 5*

Which of the following URLs provides access to the compliance manger?

A. security.microsoft.com

B. compliance.microsoft.com

C. servicetrust.microsoft.com

D. protection.office.com

E. securitycenter.windows.com

chaoscreater Highly Voted 1 month ago

Anwer is wrong. B is correct. The link in servicetrust.microsoft.com simply takes you to B. From B, you can definitely access Compliance Manager.

upvoted 8 times

AnonymousUser1029 1 month ago

Agreed, although you can access from servicetrust.microsoft.com, compliance.microsoft.com is more direct and accurate way to access it.

upvoted 2 times

Nasser 1 month ago

Totally agree

upvoted 2 times

Fala_Fel 2 weeks, 5 days ago

Yes answer should be B
"Microsoft Compliance Manager is a feature in the Microsoft 365 compliance center "
I access Compliance Manager from M365 Compliance Center https://compliance.microsoft.com/ and when I'm in it the URL is https://compliance.microsoft.com/compliancemanager

upvoted 1 times

Question #33 *Topic 5*

You use the content search tool in O365 Security & Compliance Center as part of an eDiscovery project.

Which of the following search types are available to you? (Choose three.)

A. Content search

B. Saved search

C. New search

D. Guided search

E. Search by ID list

chaoscreater 1 month ago

Should be B, C, E. When you click on "New search", it's just a guided search. Once you've searched for something, it gets saved and you can re-use the saved search.

upvoted 2 times

The_Dude 1 month ago

Given answer is correct but since June outdated, https://www.nucleustechnologies.com/blog/how-to-search-for-content-in-office-365/ you can't now select search type

upvoted 3 times

Fala_Fel 2 weeks, 5 days ago

Searches options I get are 'New Search' & 'Search by ID List'
I can open an old search and rerun search but don't consider that a search type.
So my answer will be C & E

upvoted 1 times

lime568 2 weeks ago

You have 'Copy Search'

upvoted 1 times

Question #34 *Topic 5*

Which of the following components are required for Azure AD Hybrid Identity with Password Hash Sync? (Choose two.)

A. Azure AD Connect

B. Federation Proxy

C. Federation Server

D. Authentication Agent

E. Active Directory

Fala_Fel 2 weeks, 5 days ago

Correct A & E
Federation Proxy / Server is only required for ADFS
An Authentication Agent is only required for Pass Thru Auth (PTA)
So all you need for Password Hash Sync is AAD Connect & of course an on prem AD

upvoted 3 times

Question #35 *Topic 5*

Which of the following classification labels are configurable in O365? (Choose two.)

A. Encryption label

B. Protection label

C. Sensitivity label

D. Compliance label

E. Retention label

F. Policy label

Question #36 *Topic 5*

Which feature do you configure to ensure that password changes comply with Active Directory password policy?

A. Password Protection

B. Identity Protection

C. Password writeback

D. Privileged Identity Management

E. Password hash sync (PHS)

maxustermann 3 days, 20 hours ago

Correct: C

upvoted 1 times

Question #37 *Topic 5*

In O365 ATP Safe Attachments, what happens when you select Dynamic Delivery?

A. The message is delivered, but attachments containing malware is blocked

B. The message is not delivered until attachments have been confirmed safe

C. The message is delivered, but attachments containing malware is replaced by a message informing the user that the missing attachment contained malware and was blocked

D. The message and attachments are quarantined if malware is detected in any of the attachments

E. The message is delivered without attachments. When the attachments are confirmed safe, the message is updated with the attachments

JakubK64 2 weeks, 2 days ago

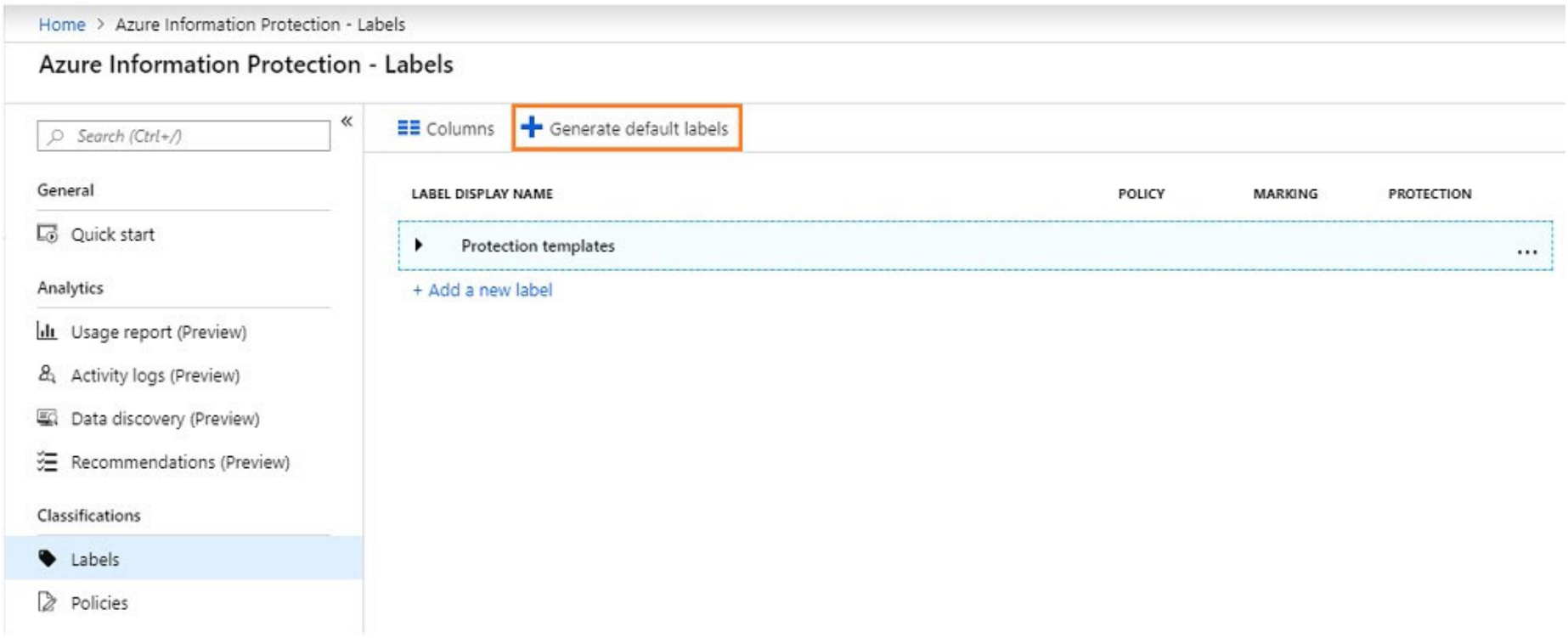
E is correct

upvoted 3 times

Question #38

Topic 5

You click on the button as indicated in the exhibit.



Select all of the sensitivity labels that are generated by AIP. (Choose five.)

A. Personal

B. Non-Business

C. Private

D. Public

E. General

F. Business General

G. Sensitive

H. Confidential

I. Secret

J. Highly Confidential K. Top Secret

Mahoni 3 weeks, 6 days ago

non business- public - general -confidential- Highly confidential

upvoted 1 times

The_Dude 4 weeks, 1 day ago

Given answer is correct, on https://docs.microsoft.com/en-us/microsoft-365/compliance/create-sensitivity-labels?view=o365-worldwide, there is screenshot where yo can see 5 labels:
Personal
Public
General
Confidential
Highly Confidential

upvoted 3 times

Fala_Fel 2 weeks, 5 days ago

Default labels don't seem to exist anymore in M365 Compliance, so not possible to test, but from The_Dude link I will go with that. A-D-E-H-J
Personal, Public, General, Confidential, Highly Confidential

upvoted 1 times

chaoscreater 1 month ago

The link in the answer shows only these 4 labels and not Public?

The default Azure Information Protection classification labels are:

Personal
General
Confidential
Highly Confidential

upvoted 1 times

chaoscreater 1 month ago

But I also found this - https://docs.microsoft.com/en-us/azure/information-protection/configure-policy-migrate-labels

upvoted 1 times

Question #39 *Topic 5*

A user phones you complaining that a set of work documents he shared from his OneDrive for business has disappeared. He wants to know who deleted the documents.
Which M365 security tool would you use to discover who deleted the documents?

A. OneDrive for business administration console

B. Office 365 admin portal

C. Azure security center

D. Cloud App Security

Question #40 *Topic 5*

You are configuring O365 security. You notice that URLs in O365 are being rewritten in order to prevent users clicking on malicious URLs. However, you want to prevent certain URLs that you trust from being rewritten in this way and apply it to the entire organization.
How would you configure this exclusion?

A. Create a conditional access policy

B. Edit the default conditional access policy

C. Create a safe links policy

D. Edit the default safe links policy

E. Create a O365 ATP security policy

F. Edit the default O365 ATP security policy

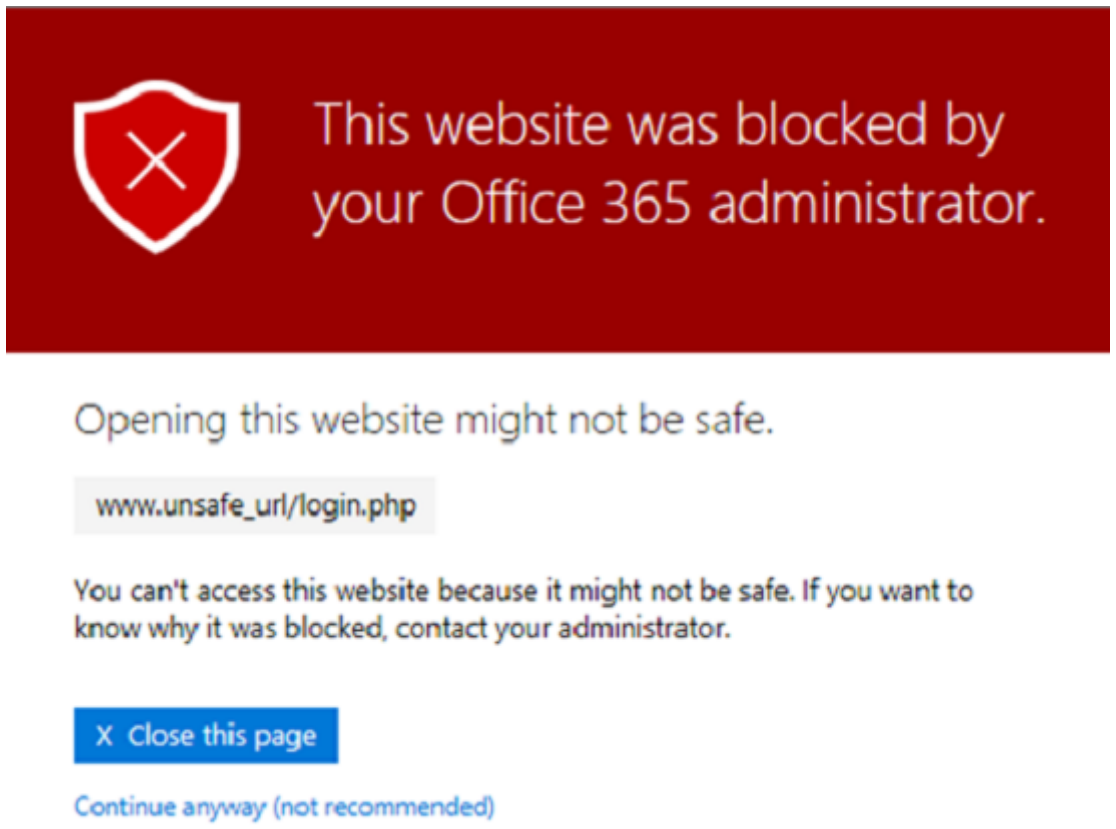
Fala_Fel 2 weeks, 5 days ago

Correct and verified in test lab

upvoted 3 times

Question #41 *Topic 5*

A user phones to complain that his browser is not allowing him to visit a URL that is normally used for business saying that "This website was blocked by your
Office 365 administrator." as in the exhibit.



You know that your M365 security policies was recently updated.
Where would you start your investigation?

A. Microsoft Defender ATP

B. Azure ATP

C. Office ATP

D. Microsoft Secure Score

VMS 1 week, 2 days ago
Office 365 Advanced Threat Protection is now Microsoft Defender for Office 365, hence the confusion, "Safe Links is a feature in Defender for Office 365"
C is correct
https://docs.microsoft.com/en-us/microsoft-365/security/office-365-security/safe-links?view=o365-worldwide#warning-pages-from-safe-links
upvoted 1 times

kcezeh 2 weeks, 2 days ago
I think the answer is A. Microsoft Defender ATP
upvoted 1 times

nidentify 3 weeks, 1 day ago
Defender ATP also does url filtering https://techcommunity.microsoft.com/t5/core-infrastructure-and-security/microsoft-defender-atp-web-content-filtering/ba-p/1550096
upvoted 2 times

Fala_Fel 2 weeks, 5 days ago
IMO Ans is also A = Microsoft Defender ATP
upvoted 1 times

Fala_Fel 2 weeks, 5 days ago
Actual name - Microsoft 365 Defender found here https://security.microsoft.com/safelinksv2
https://docs.microsoft.com/en-us/microsoft-365/security/office-365-security/atp-safe-links-warning-pages
upvoted 1 times

Question #42 *Topic 5*

What license do you require to enable password writeback in Azure AD Connect?
You must minimize costs.

A. M365-E5

B. M365-E3

C. EMS-E5

D. EMS-E3

E. O365-E3

F. O365-E5

G. Azure AD Premium P1

H. Azure AD Premium P2

Question #43 *Topic 5*

How long after you've deleted a user account in AAD can the account be recovered?

A. The account cannot be recovered ג€" user account deletions in ADD is permanent

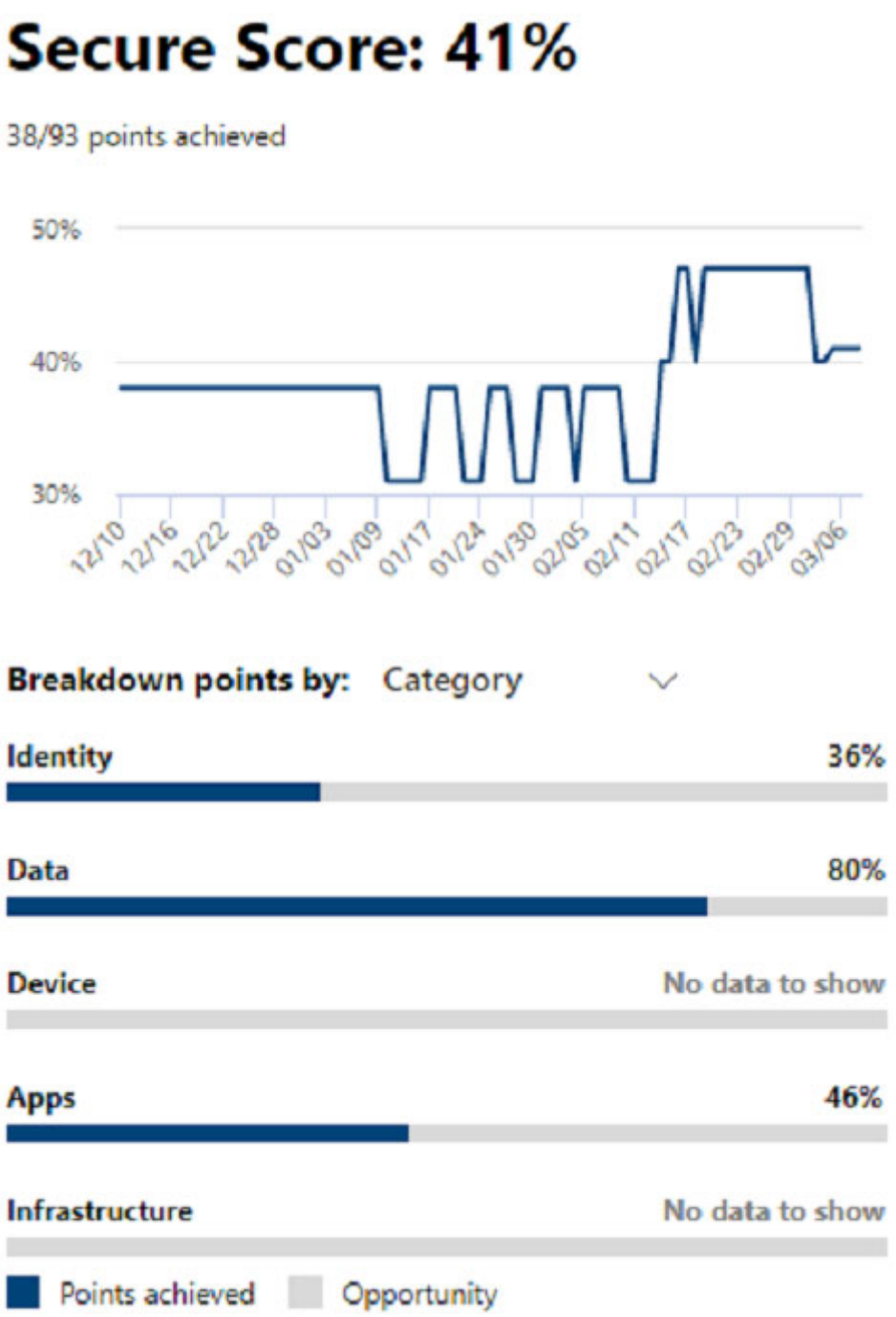
B. 15 days

C. 30 days

D. 90 days

E. For ever

Question #44 *Topic 5*



You are using Microsoft Secure Score to improve the posture of the security in your organization. The Secure Score overview page reports your secure score by category as in the exhibit. You notice the secure score for Devices reports No data to show.

Which of the following would you choose to correct the situation?

A. Implement and configure Microsoft Defender Advanced Threat Protection

B. Implement and configure Microsoft Cloud App Security

C. Implement and configure Azure Information Protection

D. Implement and configure Azure Advanced Threat Protection

E. Purchase and assign M365-E5 licenses to users

Question #45 *Topic 5*

You configure AD Connect group writeback. This causes M365 groups to be created in on-premises AD.
What type of groups are created?

A. Security group

B. Mail-enabled security group

C. Distribution list

D. Dynamic user group

Question #46 *Topic 5*

Which of the following authentication methods are available for SSPR? (Choose all that apply.)

A. Password

B. Security questions

C. Email address

D. Authentication app

E. OATH token

F. SMS

G. Voice call

H. App password

Nasser Highly Voted 1 month ago

The following authentication methods are available for SSPR:
Mobile app notification
Mobile app code
Email
Mobile phone
Office phone (available only for tenants with paid subscriptions)
Security questions
https://docs.microsoft.com/en-us/azure/active-directory/authentication/concept-sspr-howitworks

upvoted 5 times

Nasser 1 month ago

So the possible answers are: B C D F G

upvoted 3 times

Robert__Susin 4 days, 12 hours ago

Mobile app code is the same as OATH token so is B C D E F G

upvoted 2 times

Drewbinski 4 weeks, 1 day ago

another link that looks to support this:
https://docs.microsoft.com/en-us/azure/active-directory/authentication/tutorial-enable-sspr

upvoted 1 times

Question #47 *Topic 5*

How do you integrate O365 ATP with MD-ATP? Each option is a complete solution. (Choose two.)

A. There is no integration between 0365 ATP and MD-ATP

B. Go to protection.office.com, threat management, explorer, WDATP settings, enable

C. Go to securitycenter.windows.com, settings, advanced features, Office 365 threat intelligence connection, enable

D. Go to security.microsoft.com, threat management, explorer, WDATP settings, enable

Question #48 *Topic 5*

In what format is Azure ATP downloadable reports available?

A. PDF

B. XLSX

C. DOCX

D. CSV

E. All of the above

Question #49 *Topic 5*

Sensitivity labels added to the metadata of documents that are labelled highly confidential and protected by AIP are encrypted.

A. True

B. False

Question #50 *Topic 5*

Select the appropriate AIP usage rights for the built-in role of Reviewer. (Choose all that apply.)

A. View

B. Reply

C. Reply all

D. Edit

E. Forward

F. Copy

G. Print

H. Change Rights

Question #51 *Topic 5*

Which of the following tools will you use to manage regulatory compliance within the shared responsibility model of the cloud?

A. Service Trust Portal

B. Compliance Manager

C. Trust Center

D. Azure Security Center

E. Microsoft Compliance Portal

oscargtech 3 weeks, 1 day ago

Based off of the given answer, shouldn't it be A then?

upvoted 2 times

masger 1 week, 5 days ago

According to the information provided in the response link. "Compliance Manager has moved from the Service Trust Portal to its new location in the Microsoft 365 compliance center (https://compliance.microsoft.com/)".

upvoted 1 times

Question #52 *Topic 5*

Which of the following are Azure AD Conditional Access assignments or conditions? (Choose all that apply.)

A. Group

B. Device

C. Location

D. Require MFA

E. Require compliant device

F. Require hybrid AAD domain join

G. Client app

H. Cloud app

I. Sign-in risk

J. Block

Robert__Susin 3 days, 14 hours ago

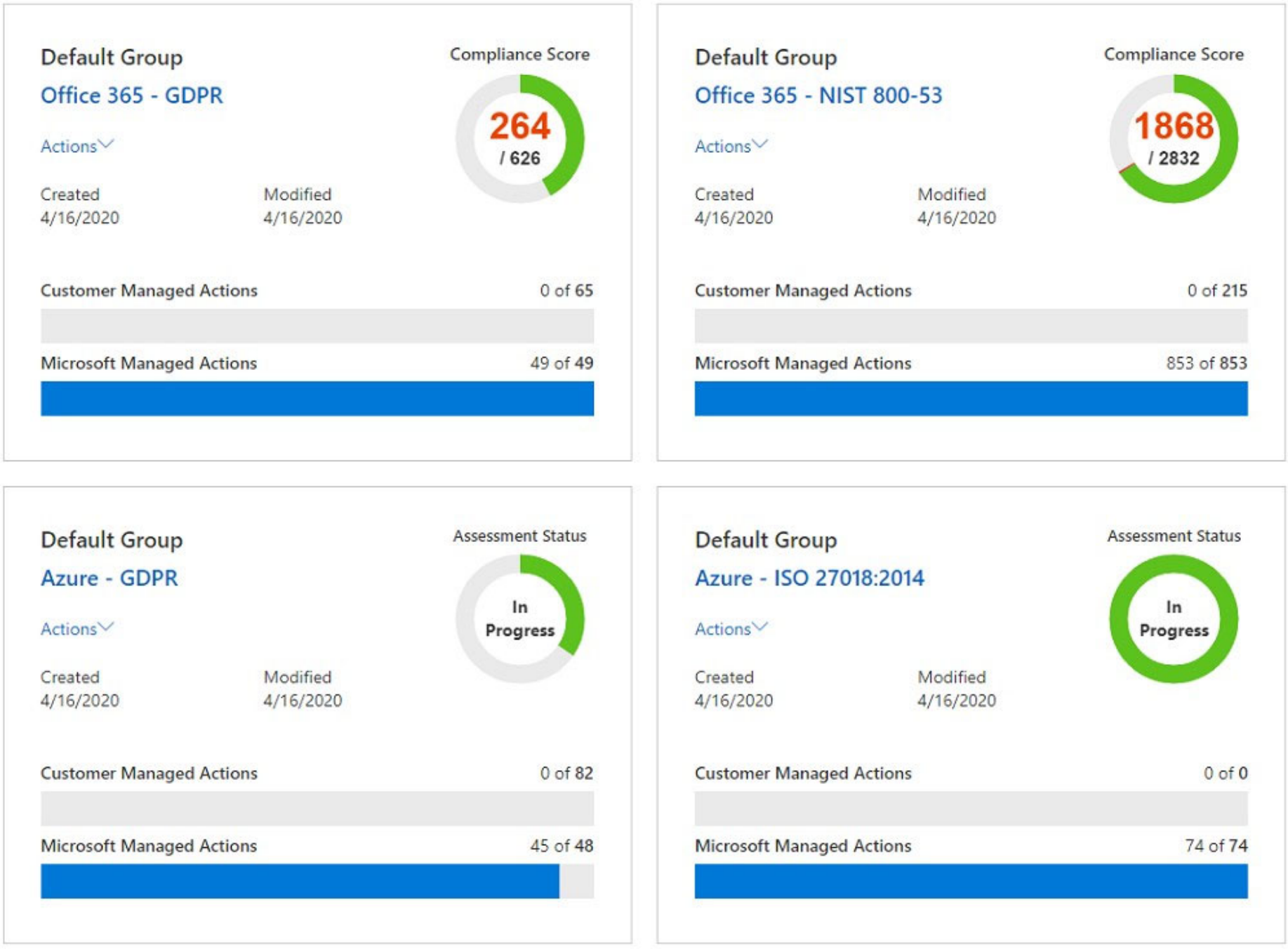
Both Require compliant device and Require hybrid AAD are Device State (Preview) condition, so the given answer should include E and F as well

upvoted 1 times

Question #53

Topic 5

NOTE: This question is a part of a series of questions that present the same scenario. For each of the following statements, select the best response
(s) to the question or statement below. Each answer is worth one point.
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 responsible for your organizationλ€™s regulatory compliance as evidenced by the compliance report as in the exhibit.



Your organization is GDPR compliant for M365 and Azure.
NOTE: Change (or not) the highlighted section of the following statement to make it true.

A. Leave unchanged

B. M365 only

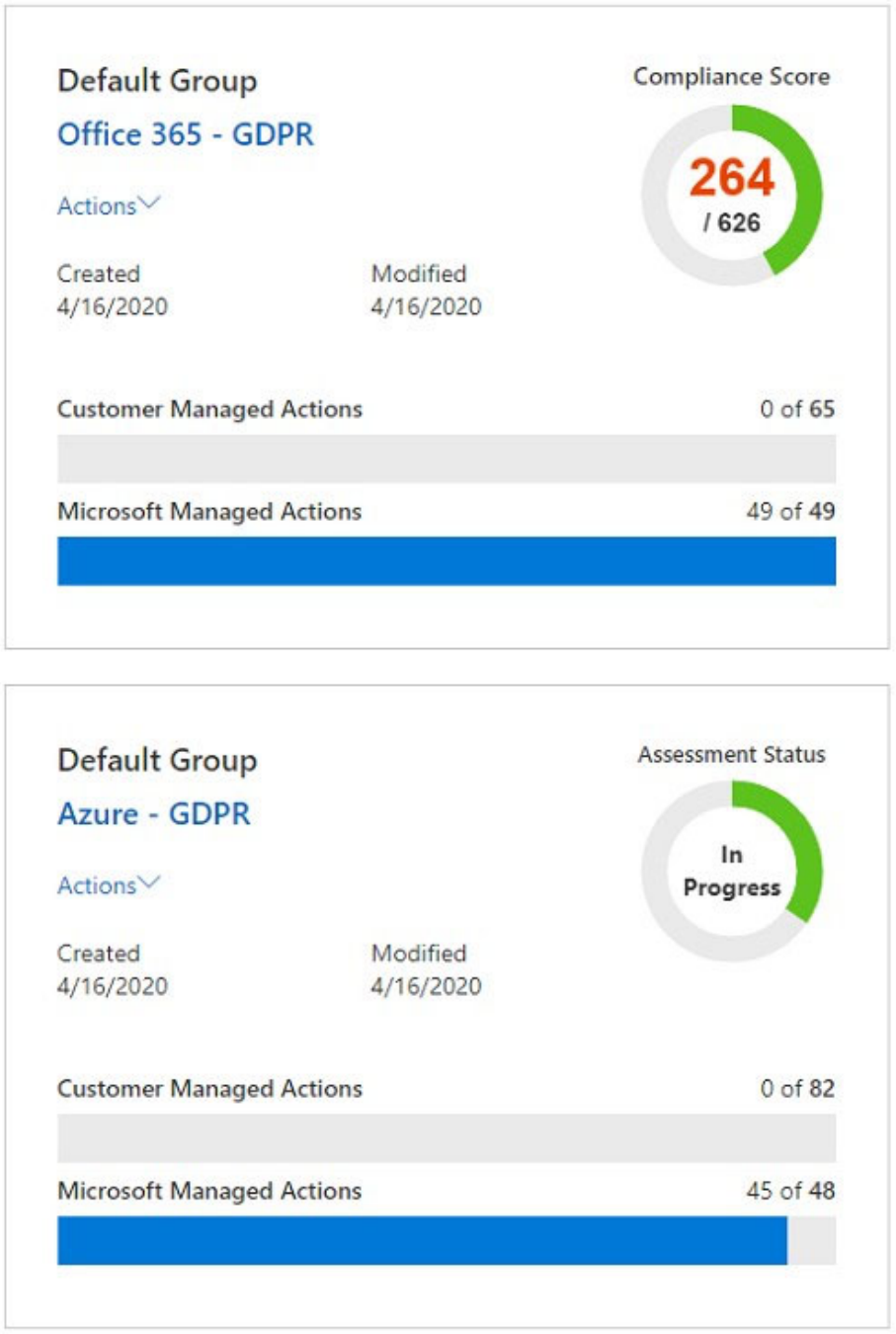
C. Azure only

D. neither M365 or Azure

Question #54

Topic 5

NOTE: This question is a part of a series of questions that present the same scenario. For each of the following statements, select the best response
(s) to the question or statement below. Each answer is worth one point.
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 responsible for your organizationλ€™s regulatory compliance as evidenced by the compliance report as in the exhibit.



In order for you to address customer managed actions you must assign, implement, and test controls.
NOTE: Change (or not) the highlighted section of the following statement to make it true.

A. Leave unchanged

B. assign

C. assign and implement

D. implement and test

The_Poet 6 days, 9 hours ago
Confirm the correct answer plz
upvoted 1 times

The_Dude 4 weeks, 1 day ago
Agree with chaoseater, it should be B (assign)
upvoted 1 times

chaoscreater 1 month ago
The link in the answer points to D? - "As the customer implements and tests each of the customer Actions, the Compliance Score for the Assessment will increase by the value assigned to the control."
upvoted 1 times

Robert__Susin 3 days, 13 hours ago
Shouldnt be D cuz the question isnt asking how to solely pump the score like the past question you linked
upvoted 1 times

chaoscreater 1 month ago

Also, why is it not B? In a separate question, it talks about assigning action items to improve the score - https://www.examtopics.com/exams/microsoft/ms-500/view/13/

upvoted 2 times

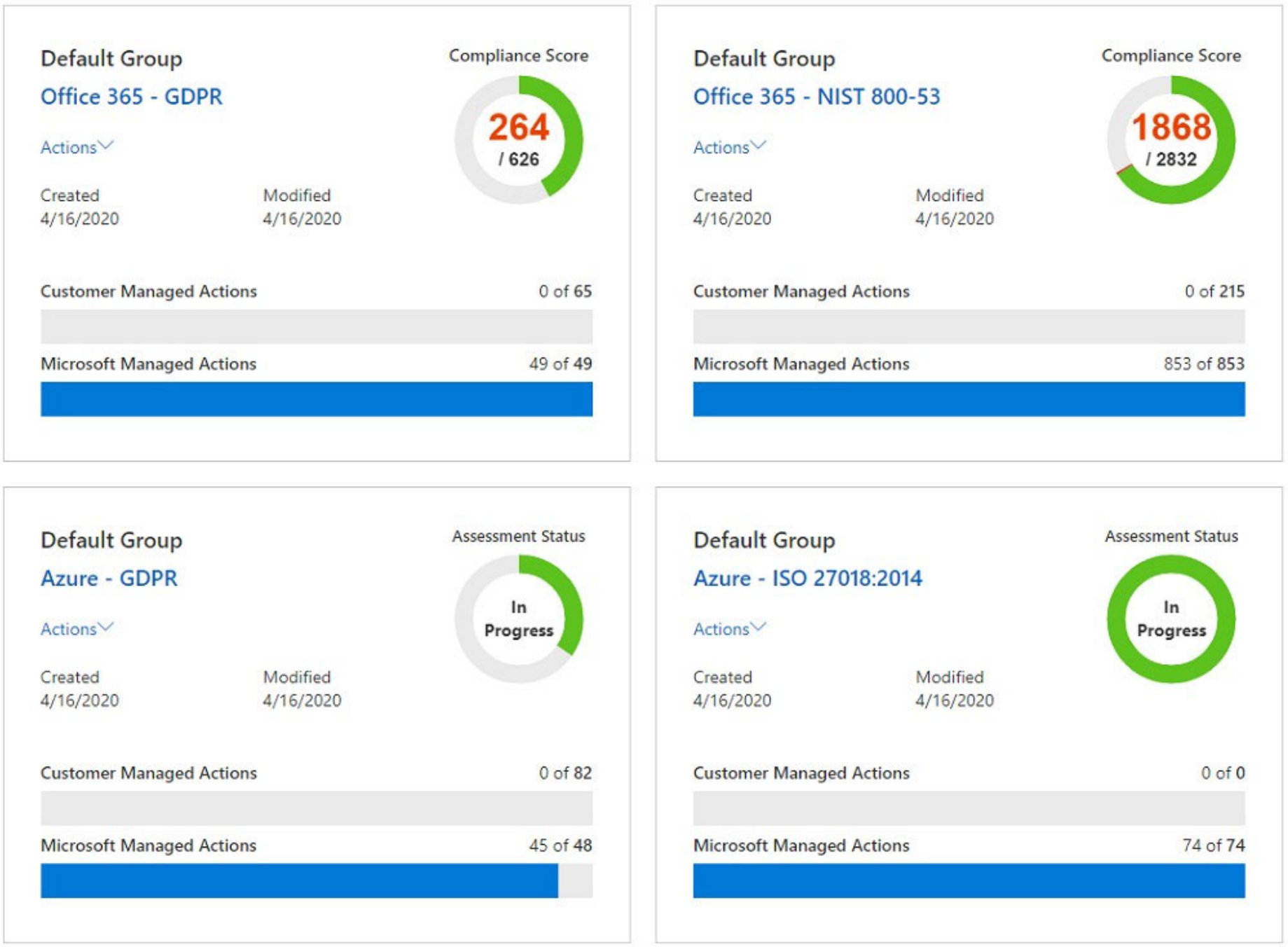
Question #55 *Topic 5*

NOTE: This question is a part of a series of questions that present the same scenario. For each of the following statements, select the best response

(s) to the question or statement below. Each answer is worth one point.

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 responsible for your organizationλ€™s regulatory compliance as evidenced by the compliance report as in the exhibit.



Customer managed actions are assessed manually; Microsoft managed actions are assessed manually.

NOTE: Change (or not) the highlighted section of the following statement to make it true.

A. Leave unchanged

B. manually; automatically

C. automatically; manually

D. automatically; automatically

Question #56 *Topic 5*

NOTE: This question is a part of a series of questions that present the same scenario. For each of the following statements, select the best response
(s) to the question or statement below. Each answer is worth one point.
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.
Your organization has a single-domain, single-forest Active Directory. You have installed Azure AD Connect with express settings. You need a new group that you want to use to manage access to a cloud application you have registered with Azure Active Directory.
Where would you create the group from?

A. M365 Admin Center

B. Azure AD Admin Center

C. Active Directory Users and Computers

D. Any of the above

E. None of the above

Fala_Fel 2 weeks, 4 days ago

I think answer is correct - Any of the above. A group could be created on prem or Azure to manage the app. No need for Group Write back
upvoted 2 times

chaoscreater 1 month ago

AD Connect is installed with express settings, which means group writeback is not enabled.
upvoted 3 times

MQH 1 month ago

good point, but it's a cloud app and already registered with AAD, why we need the access group to be written back to on-prem?
upvoted 1 times

chaoscreater 1 month ago

In fact, the next question #57 asks which type of group should you create and it only mentions security group, which tells me it's just a one-way sync from onprem AD to AAD. If both AAD and AD are answers here, then why wouldn't a O365 Group be an answer? These questions and answers are so inconsistent.
upvoted 2 times

Question #57 *Topic 5*

NOTE: This question is a part of a series of questions that present the same scenario. For each of the following statements, select the best response
(s) to the question or statement below. Each answer is worth one point.
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.
Your organization has a single-domain, single-forest Active Directory. You have installed Azure AD Connect with express settings. You need a new group that you want to use to manage access to a cloud application you have registered with Azure Active Directory.
What type of group will you create?

A. Security Group

B. Mail-enabled security group

C. Distribution list

D. Office 365 group

E. Any of the above

F. None of the above

Fala_Fel 2 weeks, 4 days ago

Confusing answers. Looks like it needs to be a security group and there would be no requirement to mail enable it. So best answer is A = Security Group
" Group-based assignment is supported for Security groups only. ...Microsoft 365 groups are not currently supported. "
https://docs.microsoft.com/en-us/azure/active-directory/manage-apps/add-application-portal-assign-users
upvoted 2 times

maxustermann 3 days, 20 hours ago

Agree with your answer
upvoted 1 times

Question #58 *Topic 5*

NOTE: This question is a part of a series of questions that present the same scenario. For each of the following statements, select the best response
(s) to the question or statement below. Each answer is worth one point.
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.
Your organization has a single-domain, single-forest Active Directory. You have installed Azure AD Connect with express settings. You need a new group that you want to use to manage access to a cloud application you have registered with Azure Active Directory.
What is the maximum number of members the group can have if you create the group on Active Directory?

A. Unlimited

B. 5,000

C. 50,000

D. 500,000

Question #59 *Topic 5*

NOTE: This question is a part of a series of questions that present the same scenario. For each of the following statements, select the best response
(s) to the question or statement below. Each answer is worth one point.
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.
A user with the UPN of user1@company.com leaves your organization and his user account is deleted. 40 days later you are asked to recover a large volume of data from the user's OneDrive. Your administrator user account is admin1@company.com. From the OneDrive admin center, you verify that the days to retain files in OneDrive after a user account is marked for deletion is set to 60 days.
What do you do first?

A. From M365 admin center, choose user1 from the deleted users panel, choose restore user

B. Issue the following PowerShell: Restore-MsolUser -UserPrincipalName user1@company.com

C. Issue the following PowerShell: Get-SPODeletedSite -Identity https://company-my.sharepoint.com/personal/user1_company_com

D. Issue the following PowerShell: Get-SPODeletedSite -Identity user1@company.com

Fala_Fel 2 weeks, 4 days ago
C best answer. Deleted users cannot be restored after 30 days in Azure AD. But can restore their OneDrive
upvoted 4 times

Drewbinski 4 weeks, 1 day ago
Udemy exam system?
upvoted 3 times

Question #60 *Topic 5*

NOTE: This question is a part of a series of questions that present the same scenario. For each of the following statements, select the best response
(s) to the question or statement below. Each answer is worth one point.
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.
A user with the UPN of user1@company.com leaves your organization and his user account is deleted. 40 days later you are asked to recover a large volume of data from the user's OneDrive. Your administrator user account is admin1@company.com. From the OneDrive admin center, you verify that the days to retain files in OneDrive after a user account is marked for deletion is set to 60 days.
What do you do second?

A. From the M365 admin center, choose deleted sites, select user1@company.com, choose Restore

B. From the SharePoint admin center, choose deleted sites, select user1@company.com, choose Restore

C. Issue the following PowerShell: Restore-SPODeletedSite -Identity user1@company.com

D. Issue the following PowerShell: Restore-SPODeletedSite -Identity https://company-my.sharepoint.com/personal/user1_company_com

Question #61 *Topic 5*

NOTE: This question is a part of a series of questions that present the same scenario. For each of the following statements, select the best response
(s) to the question or statement below. Each answer is worth one point.
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.
A user with the UPN of user1@company.com leaves your organization and his user account is deleted. 40 days later you are asked to recover a large volume of data from the user's OneDrive. Your administrator user account is admin1@company.com. From the OneDrive admin center, you verify that the days to retain files in OneDrive after a user account is marked for deletion is set to 60 days.
What do you do third?

A. From the SharePoint admin center, choose active sites, select user1@company.com, choose manage admins, add admin1@company.com

B. From the OneDrive admin center, choose Storage, select user1@company.com, choose manage admins, add admin1@company.com

C. Issue the following PowerShell: Set-SPOUser -Site https://company-my.sharepoint.com/personal/user1_company_com -LoginName user1@company.com -IsSiteCollectionAdmin $True

D. Issue the following PowerShell: Set -SPOUser -Site https://company-my.sharepoint.com/personal/user1_company_com -LoginName admin1@company.com -IsSiteCollectionAdmin $True

Fala_Fel 2 weeks, 4 days ago
Is this really MS-500?
upvoted 1 times

Question #62 *Topic 5*

You have been appointed as the new IT manager at your organization after the previous manager was fired. One of the other administrators assigns you the
Global Administrator role in Azure AD. You, however find out that the previous manager (the one that was fired) was the only one with access to your organizationג€™s Azure subscription that contains all of your organizationג€™s workloads. The workload is still on, but nobody can administer it.
What should you do to assign yourself the owner role in Azure?

A. Log in to the Azure portal, click on Azure Active Directory, then properties and switch on access management

B. Log in to the Azure portal, click on subscriptions, then Identity and Access Management then assign yourself the owner role

C. Log in to the Azure portal, click on Azure Active Directory, then open your user account from users, then configure Azure role assignments

D. Log in to the Azure portal, click on Privileged Identity Management, then permanently assign yourself the owner role

hellpp 1 week, 5 days ago
The correct answer is B
https://docs.microsoft.com/en-us/azure/role-based-access-control/role-assignments-portal?tabs=current
upvoted 2 times

The_Poet 6 days, 8 hours ago
A is correct
https://docs.microsoft.com/en-us/azure/role-based-access-control/elevate-access-global-admin
upvoted 1 times

nidentify 3 weeks, 1 day ago
The answer is incorrect, only global admin can do that
upvoted 1 times

The_Poet 6 days, 8 hours ago
The new manager is a Global Admin
upvoted 1 times

Question #63 *Topic 5*

Jeff is an entity covered under the GDPR to which your company. Jeff has requested ג€" as is his right under GDPR ג€" a report of his personally identifiable data held by your company.
What do you configure?

A. Content search

B. eDiscovery case

C. Advanced eDiscovery case

D. Data subject request

E. Litigation hold

Question #64 *Topic 5*

NOTE: This question is a part of a series of questions that present the same scenario. For each of the following questions, select the best answer. Each answer is worth one point.
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 RBAC in Azure. You need to give a user named Ted contributor access to the Marketing resource group. Match the RBAC property with the details in the scenario.
What does Ted represent in the RBAC configuration?

A. Role definition

B. Security principle

C. Role assignment

D. Scope

Question #65 *Topic 5*

NOTE: This question is a part of a series of questions that present the same scenario. For each of the following questions, select the best answer. Each answer is worth one point.
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 RBAC in Azure. You need to give a user named Ted contributor access to the Marketing resource group. Match the RBAC property with the details in the scenario.
What does Contributor represent in the RBAC configuration?

A. Role definition

B. Security principle

C. Role assignment

D. Scope

someOnePlus 1 week ago
Is this part of MS-500?
upvoted 2 times

Question #66 *Topic 5*

NOTE: This question is a part of a series of questions that present the same scenario. For each of the following questions, select the best answer. Each answer is worth one point.
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 RBAC in Azure. You need to give a user named Ted contributor access to the Marketing resource group. Match the RBAC property with the details in the scenario.
What does Marketing represent in the RBAC configuration?

A. Role definition

B. Security principle

C. Role assignment

D. Scope

Question #67 *Topic 5*

Select the appropriate AIP usage rights for the built-in role of Co-Author. (Choose all the apply.)

A. View

B. Reply

C. Reply all

D. Edit

E. Forward

F. Copy

G. Print

H. Change Rights

oscargtech 3 weeks, 1 day ago
ABCDEFG based off of linked source
upvoted 1 times

Question #68 *Topic 5*

You have just deployed MCAS and have successfully connected the Office 365 app connector. You want to create a policy that will create an alert when a user logs in from your honeynet network.
Which of the following policies would you create?

A. Access policy

B. Activity policy

C. Anomaly detection policy

D. File policy

E. Session policy

Question #69 *Topic 5*

You are investigating an incident reported by a user where several files were deleted from his shared OneDrive folders. You need to find out who deleted the files.
Which is the most appropriate course of action?

A. From the OneDrive admin center, open Storage

B. From Security and Compliance Center, open eDiscovery

C. From Security and Compliance Center, open Content search

D. From Security and Compliance Center, open

E. From MCAS, open activity log

Question #70 *Topic 5*

Which of the following threat protection components are offered by Windows 10? (Choose all that apply.)

A. Device Guard

B. App Locker

C. Secure Boot

D. Credential Guard

E. Controlled Folder Access

F. Azure Information Protection

G. Azure ATP

H. O365 ATP

Question #71 *Topic 5*

Which of these are O365 ATP attack simulator capabilities? (Choose three.)

A. Malware outbreak

B. Spam overrun

C. Spear phishing

D. Brute force password

E. Rainbow table password

F. Password spray

Question #72 *Topic 5*

Which of the following role definitions are available for assignment to resources in Azure?

A. User Access Administrator

B. Global Administrator

C. User Administrator

D. Billing Administrator

E. All of the options

F. None of the options

Question #73 *Topic 5*

Which of the following response options are available in Azure ATP? (Choose three.)

A. Protection policy

B. Alert notification

C. Syslog notification

D. Microsoft Flow automation playbook

Question #74 *Topic 5*

You have to review messages that have been quarantined by your organizationג€™s O365 ATP security.
Where would you go to do this?

A. Protection.office.com, threat management, review, quarantine

B. Securitycenter.windows.com, incidents, filter detection sources to Office ATP

C. Portal.cloudappsecurity.com, investigate, files, filter app to Microsoft Exchange Online

D. Use the Preview-QuarantineMessage PowerShell cmdlet

Question #75 *Topic 5*

Sensitivity labels can enforce information protection policies if the file was created in SharePoint Online.
NOTE: Change (or not) the highlighted section of the following statement to make it true.

A. Leave unchanged

B. in OneDrive

C. in Dropbox

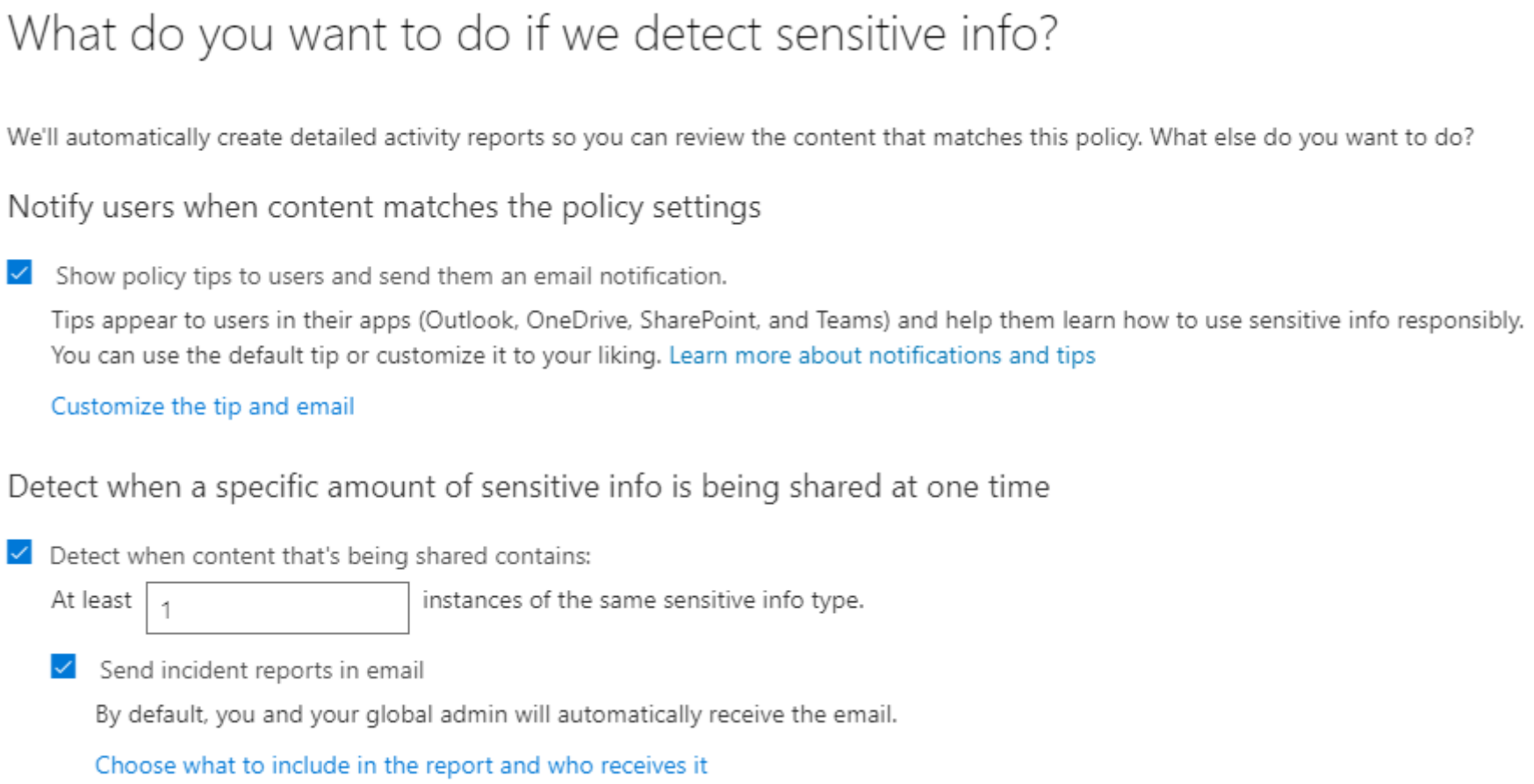
D. in an Office 365 app

E. anywhere

F. in any app integrated with Azure Active Directory

Question #76 *Topic 5*

You have created a DLP policy as in the exhibit.



What happens when a user attempts to send an email message that contains sensitive information?

A. The message is delivered and the user receives a notification

B. The message is blocked and the user receives a notification

C. The message is blocked and the administrator is notified

D. The message is blocked; both the user and the administrator receives a notification

E. None of the options are correct

oscargtech Highly Voted 3 weeks, 1 day ago

So wouldnt this be E? Since A is not 100% correct. It would be: The Message is delivered; both the user and the administrator receive a notification

upvoted 6 times

masger 1 week, 4 days ago

The email is delivered according to the DLP policy, so A is the only possible answer. But I agree that admin will also receive the notification.

upvoted 1 times

Question #77 *Topic 5*

Which of these are components provisioned during an Azure ATP installation? (Choose three.)

A. Portal

B. Sensor

C. Cloud service

D. Appliance

E. Agent

Question #78 *Topic 5*

Which of the following attacks are prevented by Windows 10 secure boot?

A. Bootkit

B. Rootkit

C. Malware

D. Trojan

The_Poet 6 days, 7 hours ago

Secure Boot, Trusted Boot, and Measured Boot create an architecture that is fundamentally resistant to bootkits and rootkits. In Windows 10, these features have the potential to eliminate kernel-level malware from your network. This is the most ground-breaking anti-malware solution that Windows has ever had; it's leaps and bounds ahead of everything else. With Windows 10, you can truly trust the integrity of your operating system.

What does that mean? Correct answers ABC?

upvoted 1 times

chaoscreater 1 month ago

Should be A and B. --> "Secure Boot is a mechanism that uses cryptography to ensure you're booting an operating system that hasn't been secretly meddled with; any addition of a bootkit or rootkit should be caught by Secure Boot."

upvoted 4 times

The_Poet 6 days, 7 hours ago

and C?

upvoted 1 times

Question #79 *Topic 5*

Which of the following are Azure AD Conditional Access controls? (Choose three.)

A. Group

B. Device

C. Location

D. Require MFA

E. Require compliant device

F. Require hybrid AAD domain join

G. Client app

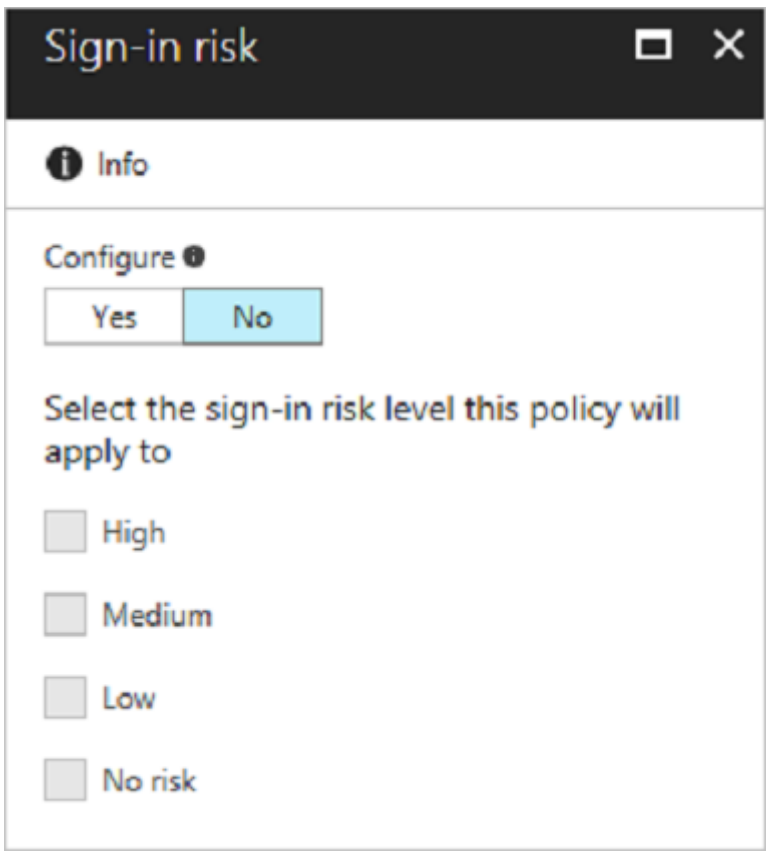
H. Cloud app

I. Sign-in risk

Question #80

Topic 5

You are configuring AAD Conditional Access as in the exhibit.



What level of licensing is required for enabling conditional access in this scenario?

A. O365-E3

B. O365-E5

C. EMS-E3

D. EMS-E5

E. AAD-P1

someOnePlus 1 week ago

do you really need this licence if the conditional access isn't set to "yes"?

upvoted 1 times

Kurujis 3 weeks, 4 days ago

Is this question will appear on the real exam?

upvoted 2 times

The_Poet 6 days, 7 hours ago

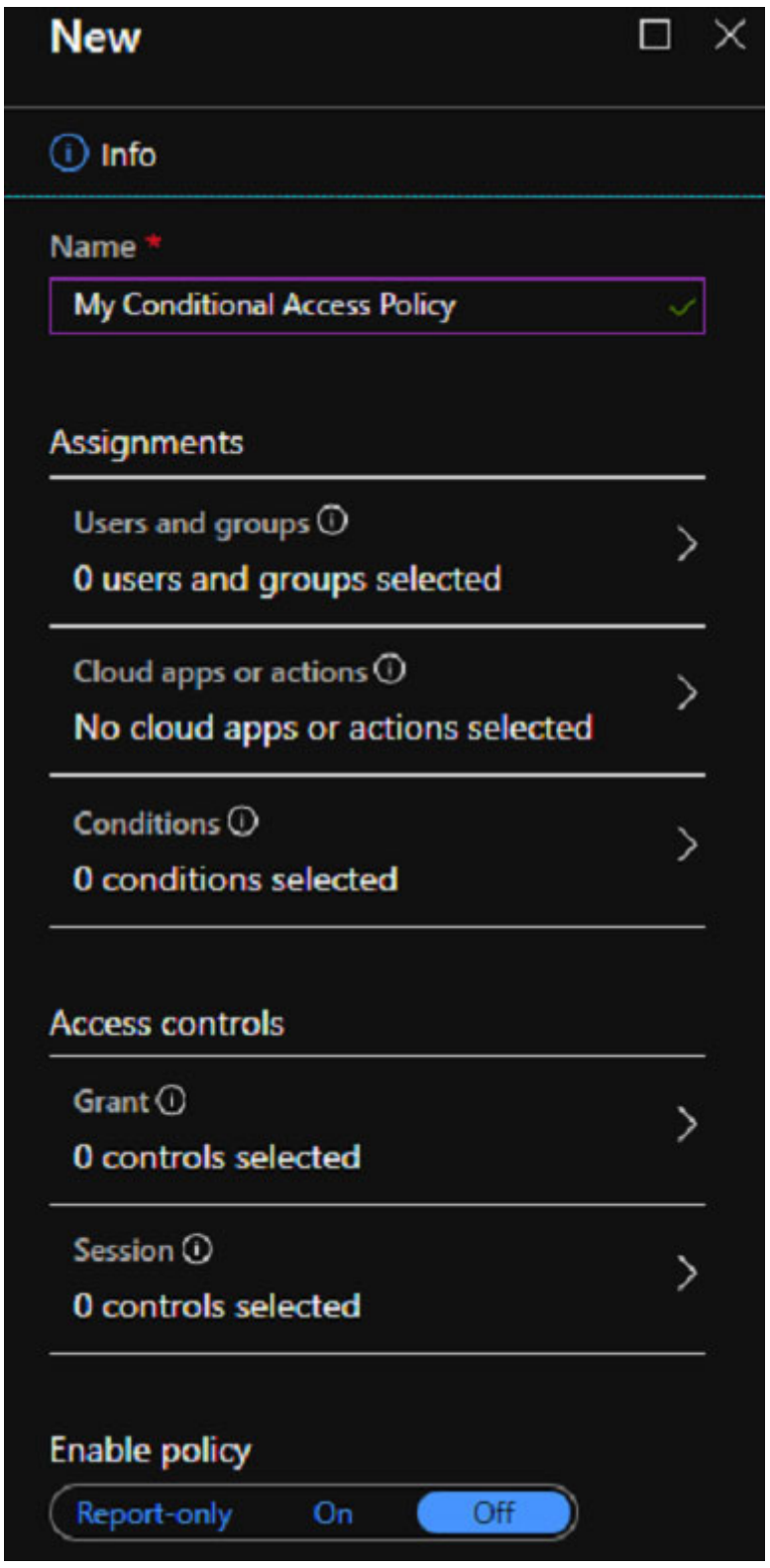
Why not

upvoted 1 times

Question #81

Topic 5

You are configuring Azure AD conditional access. You want to prevent users from accessing O365 cloud services on mobile devices' built-in applications; users must use only approved mobile applications or any desktop application.



Which section of the exhibit would you use to specify the application restriction?

A. Users and groups

B. Cloud apps and actions

C. Conditions

D. Grant

E. Session

Question #82 *Topic 5*

Which M365 threat protection feature will remove malicious email attachment after the email has been delivered?

A. Defender ATP

B. O365 ATP

C. Azure ATP

D. Exchange Online Protection (EOP)

E. Zero-hour Auto Purge (ZAP)

Question #83 *Topic 5*

You have an M365 subscription and you are using Azure Information Protection to classify, label and protect documents in your organization. Your on-premises
Active Directory is being synced to Azure AD. You have both on-premises groups and Azure AD groups. You want to assign your policy to these groups.
What are the requirements for these groups to be selected for AIP assignment? (Choose all that apply.)

A. The AD groups must have email addresses assigned

B. The AAD groups must have email addresses assigned

C. The AD groups can be universal

D. The AD groups can be domain local

E. The AAD groups can be O365 groups

F. The AAD groups can be security groups

Question #84 *Topic 5*

You have the following O365 DLP rules defined in priority order. You have a file that is uploaded to OneDrive that matches all of the rules in the list below.
Rule 1: only notifies users, policy tip 1
Rule 2: notifies users, restricts access, and allows user overrides, policy tip 2
Rule 3: notifies users, restricts access, and does not allow user overrides, policy tip 3
Rule 4: only notifies users, policy tip 4
Rule 5: restricts access, policy tip 5
Rule 6: notifies users, restricts access, and does not allow user overrides, policy tip 6
What is the effective policy tip that will be displayed?

A. Policy tip 1

B. Policy tip 2

C. Policy tip 3

D. Policy tip 4

E. Policy tip 5

F. Policy tip 6

Question #85 *Topic 5*

Which of these measures would lower the risk of having too many user accounts with the security administrator role in Azure AD?

A. Configure single sign on

B. Configure Intune

C. Configure conditional access

D. Configure privileged identity management

E. Configure identity protection

Question #86 *Topic 5*

Your organization strictly follows the principle of least privilege.
Which of the following roles do you require in order to implement privileged identity management?

A. Global Administrator

B. Azure Subscription Owner

C. Azure Subscription Contributor

D. Security Administrator

E. Privileged Role Administrator

Question #87 *Topic 5*

You are the security administrator of your organizations M365 environment. You have configured O365-ATP safe attachments policy with dynamic delivery. Your users complain that the system takes too long to scan and deliver attachments after messages have been delivered. You don't want to reduce your security posture.
Which course of action should you take?

A. Log a support ticket with Microsoft

B. Change the safe attachments policy to Monitor

C. Change the safe attachments policy to Replace

D. Change the safe attachments policy to Off

E. Sell the company's admin credentials at an underground web site and resign

masger Highly Voted 1 week, 4 days ago

Using the replace will cause that emails are quarantined until the antimalware scan is passed, so it won't improve the delivery time. But maybe the users perception will be better since they will receive the email (body + attachments) at once.

Btw, option E is amazing! :D

upvoted 5 times

Davemarshal Most Recent 1 day, 1 hour ago

Option E is very funny!
Correct Answer is C

upvoted 1 times

Question #88 *Topic 5*

Your company has a M365 subscription and is using Intune to manage endpoints and mobile devices. Your company, however, does not allow the enrolment of personally owned devices in MDM, but allows the use of these devices to access corporate data. The policy further states that all devices, whether personally owned or corporate owned must be prevented from accessing corporate data if the device is jailbroken or rooted. Which of the following would you deploy to achieve your goal?

A. A conditional access policy that uses a device access control

B. A conditional access policy that uses a device condition

C. A device compliance policy

D. A device configuration profile

E. An app protection policy

Question #89 *Topic 5*

Which of the following would you create in order to prevent deletion of all mailbox content in the course of a compliance investigation?

A. eDiscovery

B. Litigation hold

C. Retention label and policy

D. Preservation hold library

Question #90 *Topic 5*

Which of the following O365-ATP safe attachment policies does not cause a message delivery delay? (Choose two.)

A. Off

B. Monitor

C. Replace

D. Block

E. Dynamic Delivery

zafra2020 2 weeks, 3 days ago

https://docs.microsoft.com/en-us/microsoft-365/security/office-365-security/safe-attachments?view=o365-worldwide

upvoted 1 times

Question #91 *Topic 5*

Which license bundles include threat intelligence? (Choose two.)

A. M365-E3

B. M365-E5

C. O365-E3

D. O365-E5

E. EMS-E3

F. EMS-E5

Question #92 *Topic 5*

You assign the Security Reader role to user1 using the M365 admin portal. You want to verify what permissions user1 has.
Where do you go to look?

A. Roles and administrators from AAD in the Azure portal

B. Azure AD Roles from PIM in the Azure portal

C. Identity protection from AAD in the Azure portal

D. Manage roles from M365 admin portal

E. Manage groups from the M365 admin portal

F. Conditional access from AAD in the Azure portal

Question #93 *Topic 5*

Your setting up DLP policies in O365 Security & Compliance Center.
Which of the options can you choose to apply your DLP policy to? (Choose all that apply.)

A. Exchange Online

B. SharePoint Online

C. Teams chat

D. SharePoint

E. OneDrive

F. Teams Channel messages

G. Teams file libraries

Question #94 *Topic 5*

Which of the following role assignments can approve a valid Azure Privileged Identity Management request? (Choose two.)

A. Global administrator

B. Privileged Role Administrator

C. Security Administrator

D. Privileged Authentication Administrator

E. Owner

Question #95 *Topic 5*

By default, who can invite B2B guests to your Azure AD?

A. All members and existing guests

B. Members with the Guest inviter role

C. All members, but not existing guests

D. None of the above

MQH 1 month ago

IMO it should be C.
https://docs.microsoft.com/en-us/azure/active-directory/external-identities/add-users-administrator#:~:text=to%20invite%20guests.-,By%20default%2C%20all%20users%20and%20admins%20can%20invite%20guests.,-But%20your%20organization%27s

upvoted 1 times

Fala_Fel 2 weeks, 4 days ago

I think the answer is still correct. The link here is talking about adding guests using the Azure Portal, which is more restricted by default.

upvoted 1 times

Question #96 *Topic 5*

You are the administrator of your organizaтЂ™s M365 subscription. You are managing your users' existing Windows 10 workstations using Intune. You want to configure the telemetry settings to only send security-related information to Microsoft.

Which of the following do you configure?

A. Device configuration profile

B. Device configuration policy

C. Device compliance policy

D. Device deployment profile

E. MDM Security Baseline profile

Question #97 *Topic 5*

You need to download the exported results from a content search.
What security mechanism do you need to access the download location?

A. The password

B. The export key

C. The administrator credentials

D. The certificate

E. The PIN code

Question #98 *Topic 5*

How long is auditing data retained for in M365?

A. 15 days

B. 30 days

C. 90 days

D. 120 days

E. For ever

Question #99 *Topic 5*

Which of the following types of groups can you assign an AIP policy to? (Choose three.)

A. Office 365

B. Distribution

C. Security

D. Mail-enabled security

Question #100 *Topic 5*

You have a M365-E5 subscription. You have deployed Microsoft Defender ATP. You want to run a phishing campaign in your organization using the Attack
Simulator.
Which of the following options must you do?

A. Switch on Microsoft Cloud App Security in Defender ATP settings

B. Switch on Office 365 Threat Intelligence connection in Defender ATP settings

C. Enable your account for MFA

D. Deploy and configure Microsoft Cloud App Security

E. Create a user account from where attack simulator will send out the phishing emails

Question #101

Topic 5

You are configuring Azure ATP and have switched on delayed deployment for all sensors.
How long after the release of a service update will the sensors update?

A. 12 hours

B. 72 hours

C. 14 days

D. 30 days

E. 12 months

Question #102

Topic 5

NOTE: This question is a part of a series of questions that present the same scenario. For each of the following statements, select the best response
(s) to the question or statement below. Each answer is worth one point.
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.
Your organization uses SharePoint Online to share files with internal team members as well as occasionally share files with external users. Your CISO is concerned that users in the Retail department is could potentially share files that contain credit card numbers with external recipients from their SharePoint online site. You are tasked to remove external sharing for files where this is already happening, and also prevent it from happening in future. You decide to use Microsoft
Cloud App Security to accomplish the task.
What type of policy would you create to accomplish your task?

A. Session Policy

B. Access Policy

C. File Policy

D. Activity Policy

Question #103 *Topic 5*

NOTE: This question is a part of a series of questions that present the same scenario. For each of the following statements, select the best response
(s) to the question or statement below. Each answer is worth one point.
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.
Your organization uses SharePoint Online to share files with internal team members as well as occasionally share files with external users. Your CISO is concerned that users in the Retail department is could potentially share files that contain credit card numbers with external recipients from their SharePoint online site. You are tasked to remove external sharing for files where this is already happening, and also prevent it from happening in future. You decide to use Microsoft
Cloud App Security to accomplish the task.
Which of the following file filters will you specify? You have to minimize the number of filter conditions you apply. (Choose two.)

A. Access level

B. Parent folder

C. App

D. Classification label

E. Collaborators

Question #104 *Topic 5*

NOTE: This question is a part of a series of questions that present the same scenario. For each of the following statements, select the best response
(s) to the question or statement below. Each answer is worth one point.
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.
Your organization uses SharePoint Online to share files with internal team members as well as occasionally share files with external users. Your CISO is concerned that users in the Retail department is could potentially share files that contain credit card numbers with external recipients from their SharePoint online site. You are tasked to remove external sharing for files where this is already happening, and also prevent it from happening in future. You decide to use Microsoft
Cloud App Security to accomplish the task.
Which section of the policy would you use to configure only files that contain credit card numbers should be matched with this policy?

A. Create a filter

B. Apply to

C. Inspection method

D. Governance actions

Question #105 *Topic 5*

NOTE: This question is a part of a series of questions that present the same scenario. For each of the following statements, select the best response
(s) to the question or statement below. Each answer is worth one point.
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 multi-domain single-forest Active Directory that contains 100 users. 10 of your users belong to the Executives group. You have a M365-E5 subscription and would like to synchronize your on-premises identities with Azure AD. You have to minimize costs and administrative effort.
What do you install to implement directory synchronization?

A. DirSync

B. Azure AD Connect using express settings

C. Azure AD Connect using custom settings

D. Active Directory Federation Services (ADFS)

Question #106 *Topic 5*

NOTE: This question is a part of a series of questions that present the same scenario. For each of the following statements, select the best response
(s) to the question or statement below. Each answer is worth one point.
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 multi-domain single-forest Active Directory that contains 100 users. 10 of your users belong to the Executives group. You have a M365-E5 subscription and would like to synchronize your on-premises identities with Azure AD. You have to minimize costs and administrative effort.
You install AD Connect using express settings and successfully complete a full synchronization of all 100 user accounts.
Subsequently, you configure a filter in AD Connect to only synchronize members of the Executives group.
What happens to the accounts in Azure AD that was synchronized before you applied the filer?

A. The Azure AD user accounts in the Executives group are deleted

B. The Azure AD user accounts that are not in the Executives group are deleted

C. The Azure AD user accounts that are not in the Executives group are retained, but no longer synchronized

D. The AD user accounts that are not in the Executives group are deleted

Question #107 *Topic 5*

NOTE: This question is a part of a series of questions that present the same scenario. For each of the following statements, select the best response
(s) to the question or statement below. Each answer is worth one point.
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 multi-domain single-forest Active Directory that contains 100 users. 10 of your users belong to the Executives group. You have a M365-E5 subscription and would like to synchronize your on-premises identities with Azure AD. You have to minimize costs and administrative effort.
After installing AD Connect using express settings, you successfully complete a full synchronization of all 100 user accounts. Your users O365 services including extensive use of OneDrive for about a month.
You configure a filter in AD Connect to only synchronize members of the Executives group. You discover after your configuration that all user accounts (other than members of the Executives group) have been deleted along with OneDrive data.
How do you recover the user accounts and restore the data of the deleted user accounts?

A. Resynchronize the user accounts to Azure AD by removing the filter condition from AD Connect. User data is automatically restored.

B. You can only restore the user accounts using the O365 admin center. Restore user data using PowerShell.

C. You can only restore the user accounts using PowerShell. Restore user data using PowerShell.

D. Stop synchronization by uninstalling AD Connect. Delete all user accounts in Azure AD. Reinstall AD Connect and configure the appropriate filter conditions. Restore user data using PowerShell.

Sorrynotsorry 1 week, 5 days ago

Answer is correct
If user objects were inadvertently deleted in Azure AD because of a filtering error, you can recreate the user objects in Azure AD by removing your filtering configurations. Then you can synchronize your directories again. This action restores the users from the recycle bin in Azure AD. However, you can't undelete other object types. For example, if you accidentally delete a security group and it was used to ACL a resource, the group and its ACLs can't be recovered.
https://docs.microsoft.com/en-us/azure/active-directory/hybrid/how-to-connect-sync-configure-filtering

upvoted 1 times

chaoscreater 1 month ago

This answer sucks. Technically it should be both A and B. The deleted AAD accounts will still need to be recovered from the AAD Recycle Bin, otherwise a new AAD user object gets created. You can also restore Sharepoint (i.e OneDrive) data from Powershell as well and there are 2 questions about this already - https://www.examtopics.com/exams/microsoft/ms-500/view/23/ and https://www.examtopics.com/exams/microsoft/ms-500/view/24/.

Furthermore, even when you restore the AAD account, you still need to make sure the AD account is synced, otherwise they will just be deleted again on the next sync. So both answers are required to be correct.

upvoted 1 times

Question #108 *Topic 5*

NOTE: This question is a part of a series of questions that present the same scenario. For each of the following statements, select the best response
(s) to the question or statement below. Each answer is worth one point.
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 the administrator ג€" admin@company.com ג€" of your organizationג€™s M365-E5 environment. You have deployed AIP and you've seen major adoption of the technology over the past few months ג€" many of your labels have been configured to protect documents with encryption.
One of your users ג€" pebbles@company.com ג€" leaves the organization and you are tasked with handing over the documents to a new owner ג€" bambam@company.com.
You decide to relabel the files, what is the best course of action to allow Bambam to access the content?

A. Reset Pebbles' password, sign-in as Pebbles, relabel the files using PowerShell

B. Assign the AIP super users feature to user BamBam

C. Assign the AIP super users feature to yourself

D. Reset Pebbles' password, sign-in as Pebbles, relabel the files using Windows Explorer

Question #109 *Topic 5*

NOTE: This question is a part of a series of questions that present the same scenario. For each of the following statements, select the best response
(s) to the question or statement below. Each answer is worth one point.
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 the administrator ג€" admin@company.com ג€" of your organizationג€™s M365-E5 environment. You have deployed AIP and you've seen major adoption of the technology over the past few months ג€" many of your labels have been configured to protect documents with encryption.
One of your users ג€" pebbles@company.com ג€" leaves the organization and you are tasked with handing over the documents to a new owner ג€" bambam@company.com.
You decide to use the AIP superuser feature to achieve your goal.
Select the correct PowerShell cmdlets in the script below to achieve the above plan. (Choose three.)

XXX -

YYY -EmailAddress ZZZ -

A. XXX = Enable-AipService

B. XXX = Enable-AipService -SuperUserFeature $True

C. XXX = Enable-AipServiceSuperUserFeature

D. YYY = Add-AipServiceSuperUser

E. YYY = Set-AipServiceSuperUserGroup

F. YYY = Enable-AipServiceSuperUserFeature

G. ZZZ = pebbles@company.com

H. ZZZ = admin@company.com

I. ZZZ = bambam@company.com

Question #110 *Topic 5*

NOTE: This question is a part of a series of questions that present the same scenario. For each of the following statements, select the best response
(s) to the question or statement below. Each answer is worth one point.
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 the administrator ג€" admin@company.com ג€" of your organizationג€™s M365-E5 environment. You have deployed AIP and you've seen major adoption of the technology over the past few months ג€" many of your labels have been configured to protect documents with encryption.
One of your users ג€" pebbles@company.com ג€" leaves the organization and you are tasked with handing over the documents to a new owner ג€" bambam@company.com.
Select the correct PowerShell to verify that you have completed the AIP superuser feature configuration correctly.

A. Get-AipServiceSuperUser

B. Get-AipServiceSuperUserGroup

C. Get-AipServiceAdminLog

Question #111 *Topic 5*

NOTE: This question is a part of a series of questions that present the same scenario. For each of the following statements, select the best response
(s) to the question or statement below. Each answer is worth one point.
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 user accounts configured as in the exhibit. You've configured an Azure AD Identity Protection risk policy as in the second exhibit. Azure AD Identity
Protection determines that all instances in this case represents a high risk.

User	Group membership	User type	SSPR/MFA status
User1	Sales	Member	Registered
User2	Sales, R&D	Member	Registered
User3	Sales	Member	Not registered
User4	Sales	Guest	Registered

Include	Sales
Exclude	R&D
Conditions	Sign-in risk: High
Access	Allow, require password change

Which of the actions below will be performed on User1's account? (Choose three.)

A. User account will be blocked

B. User account will be allowed access

C. User account will be required to change password

D. User account will be prompted for MFA

Question #112

Topic 5

NOTE: This question is a part of a series of questions that present the same scenario. For each of the following statements, select the best response
(s) to the question or statement below. Each answer is worth one point.
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 user accounts configured as in the exhibit. You've configured an Azure AD Identity Protection risk policy as in the second exhibit. Azure AD Identity
Protection determines that all instances in this case represents a high risk.

User	Group membership	User type	SSPR/MFA status
User1	Sales	Member	Registered
User2	Sales, R&D	Member	Registered
User3	Sales	Member	Not registered
User4	Sales	Guest	Registered

Include	Sales
Exclude	R&D
Conditions	Sign-in risk: High
Access	Allow, require password change

Which of the actions below will be performed on User2's account?

A. User account will be blocked

B. User account will be allowed access

C. User account will be required to change password

D. User account will be prompted for MFA

chaoscreater 1 month ago

B is definitely correct, but I don't quite understand why D isn't also correction. Question asks which "actions" and that implies more than 1 correct answer here. More importantly, even if the condition access policy doesn't apply, it shows that User2 has already been MFA registered. Regardless of conditional access policy, the normal user MFA should still kick in.

upvoted 4 times

masger 1 week, 4 days ago

The MFA concept in the exhibit refers the SSPR (Self Service Password Reset). As the user is not prompted to reset his password the MFA is neither requested.

upvoted 1 times

Fala_Fel 2 weeks, 4 days ago

Maybe although User2 is registered for MFA & has enrolled, there isn't a policy set up that enforces MFA for this user for each log in. So I'm sticking with just B.

upvoted 1 times

Question #113 *Topic 5*

NOTE: This question is a part of a series of questions that present the same scenario. For each of the following statements, select the best response
(s) to the question or statement below. Each answer is worth one point.
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 user accounts configured as in the exhibit. You've configured an Azure AD Identity Protection risk policy as in the second exhibit. Azure AD Identity
Protection determines that all instances in this case represents a high risk.

User	Group membership	User type	SSPR/MFA status
User1	Sales	Member	Registered
User2	Sales, R&D	Member	Registered
User3	Sales	Member	Not registered
User4	Sales	Guest	Registered

Include	Sales
Exclude	R&D
Conditions	Sign-in risk: High
Access	Allow, require password change

Which of the actions below will be performed on User3's account?

A. User account will be blocked

B. User account will be allowed access

C. User account will be required to change password

D. User account will be prompted for MFA

Question #114 *Topic 5*

NOTE: This question is a part of a series of questions that present the same scenario. For each of the following statements, select the best response
(s) to the question or statement below. Each answer is worth one point.
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 user accounts configured as in the exhibit. You've configured an Azure AD Identity Protection risk policy as in the second exhibit. Azure AD Identity
Protection determines that all instances in this case represents a high risk.

User	Group membership	User type	SSPR/MFA status
User1	Sales	Member	Registered
User2	Sales, R&D	Member	Registered
User3	Sales	Member	Not registered
User4	Sales	Guest	Registered

Include	Sales
Exclude	R&D
Conditions	Sign-in risk: High
Access	Allow, require password change

Which of the actions below will be performed on User4's account?

A. User account will be blocked

B. User account will be allowed access

C. User account will be required to change password

D. User account will be prompted for MFA

Mahoni 3 weeks, 5 days ago
Why not allowed, required to change pW, ask MFA ?
upvoted 1 times

Fala_Fel 2 weeks, 4 days ago
User 4 is a guest user so a password change cannot be enforced "If a guest user triggers the Identity Protection user risk policy to force password reset, they will be blocked. This block is due to the inability to reset passwords in the resource directory."
https://docs.microsoft.com/en-us/azure/active-directory/identity-protection/concept-identity-protection-b2b#what-do-i-do-if-a-b2b-collaboration-user-was-blocked-due-to-a-risk-based-policy-in-my-organization
upvoted 1 times

Question #115 *Topic 5*

Which of the following O365 ATP Safe Attachment options delivers the message to the user, regardless whether or not malware was detected in the attachments?
(Choose four.)

A. Off

B. Monitor

C. Block

D. Allow

E. Replace

F. Dynamic Delivery

Mahoni 3 weeks, 5 days ago
So replace and dynamic does not deliver the message if there is a malware.
upvoted 1 times

Fala_Fel 2 weeks, 4 days ago
The message is delivered, the attachment is not
upvoted 1 times

Question #116 *Topic 5*

Which three technologies is used by O365 ATP to implement anti-spoofing? (Choose three.)

A. SPF

B. DKIM

C. DMARC

D. DNSSEC

E. Azure Information Protection

Question #117 *Topic 5*

What are the installation steps in the correct order for deploying Azure ATP? a) Create Azure ATP instance b) Create an Azure AD service account c) Connect to Active Directory d) Download Azure ATP Sensor package e) Install Azure ATP Sensor

A. a, b, c, d, e

B. b, a, d, e, c

C. b, a, c, d, e

D. a, c, d, e

E. a, b, d, e

Fala_Fel 2 weeks, 3 days ago
The options given misses out "Create a group Managed Service Account in On Prem AD" step
But apart from that the answer given is correct.
b) Create an Azure AD service account - is not part of the set up
Note the change of name: "Microsoft Defender for Identity (formerly Azure Advanced Threat Protection, also known as Azure ATP)"
upvoted 2 times

Question #118 *Topic 5*

Which of the following tools are available from the service trust portal? (Choose two.)

A. Compliance Manager

B. Trust Center

C. Azure Security Center

D. Microsoft Compliance Portal

E. O365 Security & Compliance Center

Question #119 *Topic 5*

Which of the following tools will you use to action a GDPR Data Subject Request?

A. Service Trust Portal

B. Compliance Manager

C. Trust Center

D. Azure Security Center

E. Microsoft Compliance Portal

F. O365 Security & Compliance Center

Fala_Fel 2 weeks, 3 days ago

Can also do it in Microsoft 365 Compliance - but not an option in the question.

upvoted 2 times

Question #120 *Topic 5*

You are implementing MCAS.

Which of the following data sources can be used for discovery of Shadow IT? (Choose three.)

A. Log collector

B. Data Gateway

C. Secure Web Gateway

D. Defender ATP

E. Azure Sentinel

Question #121 *Topic 5*

What license level is needed for AAD Connect with password hash sync (PHS) and password write-back?

A. AAD P1

B. AAD P2

C. O365 Apps

D. AAD free

Question #122 *Topic 5*

You have implemented Azure AD Connect for your organization. You have made some changes to user accounts in your local Active Directory and notice that these changes have not yet synchronized to Azure.
What is the PS command to force an Azure AD Connect sync?

A. Start-ADSyncSyncCycle -PolicyType Delta

B. Start-ADSyncSyncCycle -PolicyType Initial

C. Get-ADSyncScheduler

D. Set-MsolDirSyncFeature -Feature SynchronizeUpnForManagedUsers -Enable $true

Question #123 *Topic 5*

Which of the following components are required for Azure AD Hybrid Identity with Passthrough Authentication? (Choose three.)

A. Azure AD Connect

B. Federation Proxy

C. Federation Server

D. Authentication Agent

E. Active Directory

Question #124 *Topic 5*

You want to detect and respond to possible attacks on the Kerberos protocol.
Which M365 security solution would you implement?

A. Network Security Group

B. Intrusion Detection System (IDS)

C. Microsoft Defender ATP

D. O365 ATP

E. Azure ATP

F. Microsoft Threat Prevention (MTP)

The_Dude 4 weeks, 1 day ago

Correction: Azure ATP is now Microsoft Defender for Identity

upvoted 2 times

The_Dude 4 weeks, 1 day ago

uh!. this is badly formed question, Microsoft Defender ATP is now Microsoft Defender for Identity - https://docs.microsoft.com/en-us/defender-for-identity/whats-new
Technically, both answers are correct

upvoted 1 times

chaoscreater 1 month ago

The link in the answer points to C - Microsoft Defender ATP?

upvoted 4 times

Question #125 *Topic 5*

Which of these are capabilities provided by Microsoft Defender ATP? (Choose all that apply.)

A. Attack surface reduction

B. Next Generation Protection

C. Endpoint Detection and Response

D. Auto Investigation and Remediation

E. Security Posture

F. Anti-malware

G. Security Management

Question #126 *Topic 5*

You are implementing compliance management for your organization.
How do you enable O365 in-place archiving?

A. Admin.microsoft.com; Exchange; Compliance management; archive

B. Protection.office.com; information governance; archive

C. servicetrust.microsoft.com; Compliance manager, archiving

D. servicetrust.microsoft.com; Trust center; archiving

maxustermann 3 days, 3 hours ago
Compliance Admin Center; information governance; archive
upvoted 1 times

Question #127 *Topic 5*

You are adjusting data retention policies in O365. A colleague has set up a data retention policy that retains certain sensitive information types for 7 years. As part of your corporate data governance policies you are required to allow users to manually tag items for retention for up to 3 years.
You open the SCC and create a data retention label with data retention of 3 years. A user creates an email that contains a GDPR-related sensitive information type. The user tags the item with the 3-year retention label.
How long will Exchange retain the email item for?

A. The item will be retained for 7 years

B. The item will be retained for 3 years

C. The item will be retained for 10 years

D. The item will be retained for 4 years

Question #128 *Topic 5*

You've deployed AIP and need to choose the appropriate AIP client.
You have the following requirements, which AIP client will you choose?
Your organization requires a HYOK deployment
Your organization requires that you install the client on Windows and MacOS

Label with file explorer -

A. Classic

B. Unified

C. Office

chaoscreater 1 month ago
According to documentation provided in the answer, both A and B are correct? Label with file explorer is supported with Unified client as well...
upvoted 2 times

The_Dude 4 weeks, 1 day ago
Question asks for HYOK, that's why Classic is answer: from the same link:
"For a subset of users, you deploy the classic client because these users require labels that apply hold your own key (HYOK) protection."

On the same link, you can see a table where you can see HYOK supports classic client
upvoted 2 times

Question #129 *Topic 5*

Which of the following attacks are prevented by trusted boot?

A. Bootkit

B. Rootkit

C. Malware

D. Trojan

Question #130 *Topic 5*

What sign-in methods do AD Connect Seamless SSO work with? (Choose two.)

A. PHS

B. PTA

C. ADFS

D. AD Trust

Question #131 *Topic 5*

If you deploy more than one AAD Connect server, what are the non-primary servers referred to as?

A. Backup servers

B. Standby servers

C. Cluster servers

D. Staging servers

E. Fail-over servers

Question #132 *Topic 5*

Your organization has AD DS and on premises Exchange server. Users log in using their email addresses. Their email addresses are standardized using the following naming convention: firstname.surname@contoso.com. You are performing a cloud migration of your users to M365. As one of your initial steps of the migration you are configuring AAD Connect in line with the detailed planning you've already completed.
Which of the following must you do in preparation for the deployment of AAD Connect? (Choose all that apply.)

A. Perform a domain registration on Azure AD

B. Run the IDFIX tool

C. Prepare the AD Connect server

D. Assign user licenses

E. Obtain AAD global administrator account

F. Obtain AD enterprise administrator account

Question #133 *Topic 5*

Your Azure AD Connect is configured with Passthrough Authentication. You want to ensure reliable authentication for users.
What should you deploy in addition to your already deployed Azure AD Connect server?

A. Azure AD Connect Staging Server

B. Azure AD Connect Failover Server

C. Azure AD Connect Authentication Agent

D. Azure AD Connect Federation Server

E. Federation Proxy Server

Question #134 *Topic 5*

You're deploying Defender ATP. You want it to apply automatic remediation to all users, except for executives who must be manually remediated.
What do you configure to achieve this?

A. Two alerts

B. Two Defender roles

C. Two machine groups

D. Two dynamic groups

E. Two device configuration profiles

Question #135 *Topic 5*

You need to configure Microsoft Defender Exploit Guard on all your Intune-managed Windows 10 devices.
What type of device configuration profile would you configure?

A. Device restrictions

B. Endpoint protection

C. Microsoft Defender ATP (Windows 10 Desktop)

D. Custom

Question #136 *Topic 5*

The My Library feature of the service trust portal lets you save your own documents so that you can quickly access them on your My Library page.

A. True

B. False

masger 1 week, 4 days ago

It should be 'True' according to the response link:
My Library
This new feature lets you save (or pin) documents so that you can quickly access them on your My Library page.
upvoted 4 times

Question #137 *Topic 5*

Which of the below roles do you need if you want to use O365 ATP Attack Simulator? (Choose three.)

A. Global Administrator

B. Security Administrator

C. Organizational Management

D. Compliance Administrator

E. Security Operator

Question #138 *Topic 5*

You need to check your organizationג€™s compliance levels against regulatory requirements.
Which tool do you use?

A. Azure Monitor

B. Office 365 Security & Compliance Center

C. M365 Admin Center

D. Service Trust Portal

E. Trust Center

Question #139 *Topic 5*

How do you force newly created retention labels to be uploaded to Exchange Online?

A. Validate-RetentionRuleQuery

B. Enable-ComplianceTagStorage

C. New-ComplianceRetentionEvent

D. Start-ManagedFolderAssistant

Question #140 *Topic 5*

Which AD Connect-related PowerShell cmdlet causes an immediate full directory synchronization?

A. Start-AdSynchronization -Now

B. Start-AdSynchronization -Immediate

C. Start-AdSyncSyncCycle -PolicyType Delta

D. Start-AdSyncSyncCycle -PolicyType Initial

Question #141 *Topic 5*

You are configuring Intune device configuration profiles. You need to adjust the BitLocker settings.
Which profile type would you configure?

A. Device restrictions

B. Endpoint protection

C. Microsoft Defender ATP (Windows 10 Desktop)

D. Custom

Question #142 *Topic 5*

You are using Attack Surface Reduction (ASR) in Microsoft 365 security center to help reduce your Windows 10 attack surfaces.
Which of the following is a prerequisite requirement for deploying ASR to Windows 10 devices?

A. Intune

B. Configuration Manager

C. Defender ATP

D. M365 license assignment

E. Device Guard

Question #143 *Topic 5*

You are configuring a 3rd party DLP solution for your organization. You need to give the DLP system the ability to decrypt any data item that has been protected by a AIP label. You want to solution to be operational immediately.
What should you do? (Choose three.)

A. Run the Enable-AipServiceSuperUserFeature PowerShell cmdlet

B. Run the Add-AipServiceSuperUser PowerShell cmdlet

C. Run the Set-AipServiceSuperUserGroup PowerShell cmdlet

D. Run the New-AzureADUser PowerShell cmdlet

E. Run the Add-AzureADGroupMember PowerShell cmdlet

Question #144 *Topic 5*

Where do you configure W10 telemetry settings in Intune?

A. Device configuration profile --> Device restrictions

B. Endpoint security --> Security baselines

C. Compliance policy --> Conditional access

D. Device configuration profile --> Endpoint protection

Question #145 *Topic 5*

How often are newly created retention labels published to Exchange Online?

A. Immediately

B. Every 4 hours

C. Every day

D. Every 7 days

Creature Highly Voted 3 weeks, 2 days ago

Didn't find answer in referenced document.

Found better document.

Link goes directly to the relevant section:

https://docs.microsoft.com/en-us/microsoft-365/compliance/create-apply-retention-labels?view=o365-worldwide#when-retention-labels-become-available-to-apply

Answer appears to be correct.

upvoted 6 times

Question #146 *Topic 5*

What is the default retention period if you quarantine email messages that contain malware?

A. 7 days

B. 15 days

C. 30 days

D. 90 days

Question #147 *Topic 5*

NOTE: This question is a part of a series of questions that present the same scenario. For each of the following statements, select the best response
(s) to the question or statement below. Each answer is worth one point.
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 configure Azure Information Protection (AIP) for your organization. You have deployed the unified labelling client to your endpoints, who all run Windows 10.
Your users have been using AIP for a few months, but your organizationא€™s privacy department have decided to change their classification naming convention and as a result you also had to change one of your AIP label's name, but no other settings had changed.
You notice that the updated label has not yet synchronized to your local machine. You want to start testing the updated label.
What PowerShell cmdlet can you run in order to reset the settings of your locally installed AIP client?

A. Get-AipServiceTemplate

B. Add-AipServiceTemplate

C. Clear-AipAuthentication

D. Connect-AipService

Question #148 *Topic 5*

NOTE: This question is a part of a series of questions that present the same scenario. For each of the following statements, select the best response
(s) to the question or statement below. Each answer is worth one point.
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 configure Azure Information Protection (AIP) for your organization. You have deployed the unified labelling client to your endpoints, who all run Windows 10.
Your users have been using AIP for a few months, but your organizationא€™s privacy department have decided to change their classification naming convention and as a result you also had to change one of your AIP label's name, but no other settings had changed.
What PowerShell cmdlet can you use to scan and reapply the updated label to the My Documents folder on your computer?

A. Set-AIPFileClassification

B. Set-AIPFileLabel

C. Set-AIPScanner

D. Set-AIPScannerScannedFileTypes

Question #149 *Topic 5*

NOTE: This question is a part of a series of questions that present the same scenario. For each of the following statements, select the best response
(s) to the question or statement below. Each answer is worth one point.
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 a junior security administrator for your organizationא€™s M365 implementation. All users are assigned a M365-E5 license and your senior colleagues have deployed full-stack ATP. You are requested to present a report on malware detected in email every Monday at your company's internal security meeting. Your current role does not afford you global administrator privileges and your organization has a strict least privilege policy.
You need security administrator privilege in order to access reports in the Security & Compliance Center.
NOTE: Change (or not) the highlighted section of the following statement to make it true.

A. Leave unchanged

B. Security Reader

C. Reviewer

D. Supervisory Review

Question #150 *Topic 5*

NOTE: This question is a part of a series of questions that present the same scenario. For each of the following statements, select the best response
(s) to the question or statement below. Each answer is worth one point.
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 a junior security administrator for your organizationλ€™s M365 implementation. All users are assigned a M365-E5 license and your senior colleagues have deployed full-stack ATP. You are requested to present a report on malware detected in email every Monday at your company's internal security meeting. Your current role does not afford you global administrator privileges and your organization has a strict least privilege policy.
In the Security & Compliance Center, go to Reports > Dashboard
NOTE: Change (or not) the highlighted section of the following statement to make it true.

A. Leave unchanged

B. Reports > Manage schedules

C. Reports > Reports for download

D. Home > Microsoft Secure Score

Question #151 *Topic 5*

NOTE: This question is a part of a series of questions that present the same scenario. For each of the following statements, select the best response
(s) to the question or statement below. Each answer is worth one point.
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 a junior security administrator for your organizationλ€™s M365 implementation. All users are assigned a M365-E5 license and your senior colleagues have deployed full-stack ATP. You are requested to present a report on malware detected in email every Monday at your company's internal security meeting. Your current role does not afford you global administrator privileges and your organization has a strict least privilege policy.
In the Security & Compliance Center, you navigate to the appropriate screen and choose + Create schedule
NOTE: Change (or not) the highlighted section of the following statement to make it true.

A. Leave unchanged

B. Malware detected in email

C. Metrics and trends

D. Office 365 ATP

Question #152

Topic 5

NOTE: This question is a part of a series of questions that present the same scenario. For each of the following statements, select the best response
(s) to the question or statement below. Each answer is worth one point.
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 user accounts as in the exhibit.

Name	User Type	Role Assignment
User1	Member	Helpdesk Administrator
User2	Guest	None
User3	Member	User Administrator
User4	Member	None
User5	Member	Guest Inviter

Which users can reset passwords of other users? (Choose two.)

A. User1

B. User2

C. User3

D. User4

E. User5

Question #153

Topic 5

NOTE: This question is a part of a series of questions that present the same scenario. For each of the following statements, select the best response
(s) to the question or statement below. Each answer is worth one point.
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 user accounts as in the exhibit.

Name	User Type	Role Assignment
User1	Member	Helpdesk Administrator
User2	Guest	None
User3	Member	User Administrator
User4	Member	None
User5	Member	Guest Inviter

Which usersא€™ passwords can be reset by User1? (Choose three.)

A. User1

B. User2

C. User3

D. User4

E. User5

Question #154

Topic 5

NOTE: This question is a part of a series of questions that present the same scenario. For each of the following statements, select the best response
(s) to the question or statement below. Each answer is worth one point.
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 user accounts as in the exhibit.

Name	User Type	Role Assignment
User1	Member	Helpdesk Administrator
User2	Guest	None
User3	Member	User Administrator
User4	Member	None
User5	Member	Guest Inviter

Which usersג€™ passwords can be reset by User3? (Choose three.)

A. User1

B. User2

C. User3

D. User4

E. User5

Question #155

Topic 5

NOTE: This question is a part of a series of questions that present the same scenario. For each of the following statements, select the best response
(s) to the question or statement below. Each answer is worth one point.
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 devices organized in groups as in the exhibit. You also have Intune device configuration profiles assigned to groups as in the second exhibit. You want to determine which policies will be applied to which devices.

Name	Group Membership
Device1	GroupA, GroupC
Device2	GroupB, GroupC
Device3	GroupA, GroupB
Device4	GroupB
Device5	GroupC

Name	Include	Exclude
Policy1	GroupC	None
Policy2	GroupB	GroupC

Select all devices on which Policy1 will be applied. (Choose three.)

A. Device1

B. Device2

C. Device3

D. Device4

E. Device5

Question #156 *Topic 5*

NOTE: This question is a part of a series of questions that present the same scenario. For each of the following statements, select the best response
(s) to the question or statement below. Each answer is worth one point.
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 devices organized in groups as in the exhibit. You also have Intune device configuration profiles assigned to groups as in the second exhibit. You want to determine which policies will be applied to which devices.

Name	Group Membership
Device1	GroupA, GroupC
Device2	GroupB, GroupC
Device3	GroupA, GroupB
Device4	GroupB
Device5	GroupC

Name	Include	Exclude
Policy1	GroupC	None
Policy2	GroupB	GroupC

Select all devices on which Policy2 will be applied. (Choose two.)

A. Device1

B. Device2

C. Device3

D. Device4

E. Device5

Question #157 *Topic 5*

Using minimum effort, how would you enforce Safe Boot on your Windows 10 computers?

A. Run Msinfo32

B. Deploy AD Group Policy

C. Modify BIOS settings

D. Deploy an Intune configuration profile

Mahoni 3 weeks, 5 days ago
or use group policy, need to research which one is easier/doable.
upvoted 1 times

Mahoni 3 weeks, 5 days ago
secure boot and safe boot are different things. Safe boot can be initialized from windows interface so it can be done using intune, just logic.
upvoted 1 times

Question #158 *Topic 5*

Which two do you need to configure to allow access to your company's Exchange online service from Outlook on mobile devices, but only if the corporate data on the mobile device is encrypted? (Choose two.)

A. Cloud App Security access policy

B. Information Protection policy

C. Intune App Protection policy

D. Conditional Access policy

E. Intune Device Compliance policy

Question #159 *Topic 5*

Your organization has several conditional access policies for various purposes. One of these policies requires users to provide MFA when they access Teams.
However, you're uncertain that all users are being prompted for MFA and you want to verify this.
Where would you obtain information to help you reach your goal?

A. O365 Security & Compliance Center, Reports

B. M365 Security Center, Reports

C. M365 Admin Center, Reports

D. Azure AD portal, Enterprise applications

E. Azure AD portal, Conditional access

Question #160 *Topic 5*

You are configuring Intune Mobile Application Management policies.
Which of the following restrictions would require your devices to be enrolled in Mobile Device Management?

A. Prevent Save-As

B. Restrict Cut, copy and paste

C. Require simple PIN for access

D. Block managed apps from running on jailbroken or rooted devices

E. All of the options

F. None of the options

Question #161 *Topic 5*

You create a new user using the M365 admin center. You plan to assign the new user the Security Reader role, but you first want to confirm what permissions will be made available to the user if you do so.
Which interface will you use to accomplish your task?

A. MCAS

B. Office 365 Security & Compliance Center

C. Azure Portal

D. M365 Security Center

E. M365 Compliance Center

Question #162 *Topic 5*

You want to prevent users from accessing cloud applications which your organization has determined to be unsanctioned apps. You mark the identified apps as unsanctioned in MCAS.
What else is required to enforce the policy? (Choose two.)

A. Integrate with Azure ATP

B. Integrate with Defender ATP

C. Integrate with the firewall

D. Integrate with Intune

E. Integrate with Office ATP

Question #163 *Topic 5*

You are the M365 administrator for your organization. Your company has created a policy that requires that the mailboxes of employees that have left the organization be retained for content searches for three years and then be automatically deleted. You also need the licenses assigned to the users to be available for reassignment to new employees.
Select all the actions that will accomplish this task. Every selection is part of the overall solution. (Choose two.)

A. Delete the user account

B. Block the user account

C. Assign an AIP policy

D. Assign a retention policy

E. Create an eDiscovery case

Question #164 *Topic 5*

Which of the following Windows 10 Enterprise features provides identity protection?

A. Windows Hello

B. Credential Guard

C. Device Guard

D. Defender Antivirus

E. Defender ATP

Question #165 *Topic 5*

Which of the following device platforms can be enrolled through the Device Enrolment Program (DEP)?

A. Android

B. Android for Work

C. iOS

D. Windows 8.1

E. Windows 10

Question #166 *Topic 5*

Which role do you need if you want to view alerts in the data governance and DLP categories? You must implement the principle of least privilege.

A. Record Management

B. Compliance Administrator

C. Global Administrator

D. Security Reader

E. Security Administrator

Question #167 *Topic 5*

As part of your GDPR responsibilities, a user makes a formal request for you to provide a copy of all personal data held in Office 365. You're enlisting the help of your compliance team and you are planning to minimize the number of actions.
Which of these actions do you take? (Choose all that apply.)

A. Assign eDiscovery permissions to case members

B. Create a Data Subject Request (DSR)

C. Create an eDiscovery case

D. Add members to the case

E. Modify search query

F. Save search query

G. Run search query

H. Place data sources on hold

I. Create a report

J. Export the data

Question #168 *Topic 5*

You are testing the impact of Windows diagnostic data sent to Microsoft at different levels by changing the registry on your own computer.
What elements do you configure? (Choose all that apply.)

A. Registry key: HKEY_LOCAL_MACHINE\Software\Policies\Microsoft\Windows\Data Collection

B. Registry key: HKEY_LOCAL_MACHINE\Software\Policies\Microsoft\Windows\EventLog

C. Registry key: HKEY_LOCAL_MACHINE\Software\Policies\Microsoft\Windows\SettingSync

D. Value Name: (Default)

E. Value Name: EnablePeerCaching

F. Value Name: AllowTelemetry

G. Value Type: String

H. Value Type: Binary

I. Value Type: DWORD (32-bit) Value

J. Value Data: "Enhanced" K. Value Data: 2 L. Value Data: 1

someOnePlus 1 week ago
Someone has found this cuestion in the exam?
upvoted 1 times

chaoscreater 3 weeks, 6 days ago
Answer says AFIK and there is no option K...
upvoted 1 times

hellpp 1 week, 5 days ago
There is along the same line with J
upvoted 2 times

Question #169 *Topic 5*

You are receiving email messages with "Unhealthy Identity Synchronization Notification" in the subject line.
Which of the following tools would you use to investigate this issue by first reviewing the DirSync status?

A. IdFix

B. Office 354 Admin Center

C. Azure AD Connect wizard

D. Active Directory Users and Computers

E. Azure portal

AnonymousUser1029 Highly Voted 4 weeks, 1 day ago
354 LOL!
upvoted 5 times

nerflan Most Recent 2 weeks ago
Also not called dirsync any more, old question, badly typed
upvoted 1 times

chaoscreater 3 weeks, 6 days ago
Can't you also view this in Azure Portal as well?
upvoted 1 times

nidentify 2 weeks, 5 days ago
yes you can
upvoted 1 times

Question #170 *Topic 5*

How many retention and sensitivity labels can be applied to an O365 item?

A. One retention; one sensitivity

B. Up to 15 retention; up to 15 sensitivity

C. Unlimited retention; unlimited sensitivity

D. One label only ג€" either sensitivity or retention

E. One auto-applied retention label; one auto-applied sensitivity; one manually-applied retention; one manually applied sensitivity ג€" effectively 4 in total

Question #171 *Topic 5*

You need to create a group that will be used to provide limited access to SharePoint resources for users.
Which of the following options are available to you to create the group? (Choose two.)

A. Using the M365 admin center, create an O365 group

B. Using the M365 admin center, create a security group

C. Using the M365 admin center, create a distribution list

D. Using Azure AD admin center, create a security group

E. Using Azure AD admin center, create an O365 group

Question #172 *Topic 5*

Which of the following sign-in risks are considered medium risks by AAD Identity Protection? (Choose three.)

A. Users with leaked credentials

B. Sign-ins from anonymous IP addresses

C. Impossible travels to atypical locations

D. Sing-ins from an unfamiliar location

E. Sign-ins from infected devices

Question #173 *Topic 5*

Which of the following items are considered mandatory AAD conditional access conditions? (Choose two.)

A. User / group

B. Locations

C. MFA

D. Grant access

E. Block access

F. Cloud apps

G. Client apps

Question #174 *Topic 5*

Which of the following components are not required for Azure AD Hybrid Identity with Federated authentication?

A. Azure AD Connect

B. Federation Proxy

C. Federation Server

D. Authentication Agent

E. Active Directory

Question #175 *Topic 5*

What is the default retention period if you quarantine spam and bulk email messages?

A. 7 days

B. 15 days

C. 30 days

D. 90 days

Question #176 *Topic 5*

You configure a user to authorize Customer LockBox requests.
Which of the following does the user use?

A. O365 Security & Compliance center: Supervision

B. M365 Admin Center: View service requests

C. M365 Admin Center: Security & compliance

D. O365 Security & Compliance center: Data subject requests

E. Azure Portal: Key Vault

Question #177 *Topic 5*

You create a retention label as in the exhibit and publish the label to SharePoint sites. A file is created in SharePoint on 1 January 2019. Select the best answer.

A. A user can delete the file after 1 January 2019

B. A user can delete the file after 1 January 2021

C. A user can never delete the file

D. The file will be deleted automatically after 1 January 2019

E. The file will be deleted automatically after 1 January 2021

F. The file will never be automatically deleted

masger 1 week, 3 days ago
The question is missing the mentioned exhibit...
upvoted 4 times

Topic 6 - Testlet 1

Question #1 *Topic 6*

Introductory Info

This is a case study. Case studies are not timed separately. You can use as much exam time as you would like to complete each case. However, there may be additional case studies and sections on this exam. You must manage your time to ensure that you are able to complete all questions included on this exam in the time provided.

To answer the questions included in a case study, you will need to reference information that is provided in the case study. Case studies might contain exhibits and other resources that provide more information about the scenario that is described in the case study. Each question is independent of the other questions in this case study.

At the end of this case study, a review screen will appear. This screen allows you to review your answers and to make changes before you move to the next section of the exam. After you begin a new section, you cannot return to this section.

To start the case study -

To display the first question in this case study, click the Next button. Use the buttons in the left pane to explore the content of the case study before you answer the questions. Clicking these buttons displays information such as business requirements, existing environment, and problem statements. If the case study has an All Information tab, note that the information displayed is identical to the information displayed on the subsequent tabs. When you are ready to answer a question, click the Question button to return to the question.

Overview -

Fabrikam, Inc. is manufacturing company that sells products through partner retail stores. Fabrikam has 5,000 employees located in offices throughout Europe.

Existing Environment -

Network Infrastructure -

The network contains an Active Directory forest named fabrikam.com. Fabrikam has a hybrid Microsoft Azure Active Directory (Azure AD) environment.

The company maintains some on-premises servers for specific applications, but most end-user applications are provided by a Microsoft 365 E5 subscription.

Problem Statements -

Fabrikam identifies the following issues:

Since last Friday, the IT team has been receiving automated email messages that contain "Unhealthy Identity Synchronization Notification" in the subject line.

Several users recently opened email attachments that contained malware. The process to remove the malware was time consuming.

Requirements -

Planned Changes -

Fabrikam plans to implement the following changes:

Fabrikam plans to monitor and investigate suspicious sign-ins to Active Directory

Fabrikam plans to provide partners with access to some of the data stored in Microsoft 365

Application Administration -

Fabrikam identifies the following application requirements for managing workload applications:

User administrators will work from different countries

User administrators will use the Azure Active Directory admin center

Two new administrators named Admin1 and Admin2 will be responsible for managing Microsoft Exchange Online only

Security Requirements -

Fabrikam identifies the following security requirements:

Access to the Azure Active Directory admin center by the user administrators must be reviewed every seven days. If an administrator fails to respond to an access request within three days, access must be removed

Users who manage Microsoft 365 workloads must only be allowed to perform administrative tasks for up to three hours at a time. Global administrators must be exempt from this requirement

Users must be prevented from inviting external users to view company data. Only global administrators and a user named User1 must be able to

send invitations

Azure Advanced Threat Protection (ATP) must capture security group modifications for sensitive groups, such as Domain Admins in Active Directory

Workload administrators must use multi-factor authentication (MFA) when signing in from an anonymous or an unfamiliar location

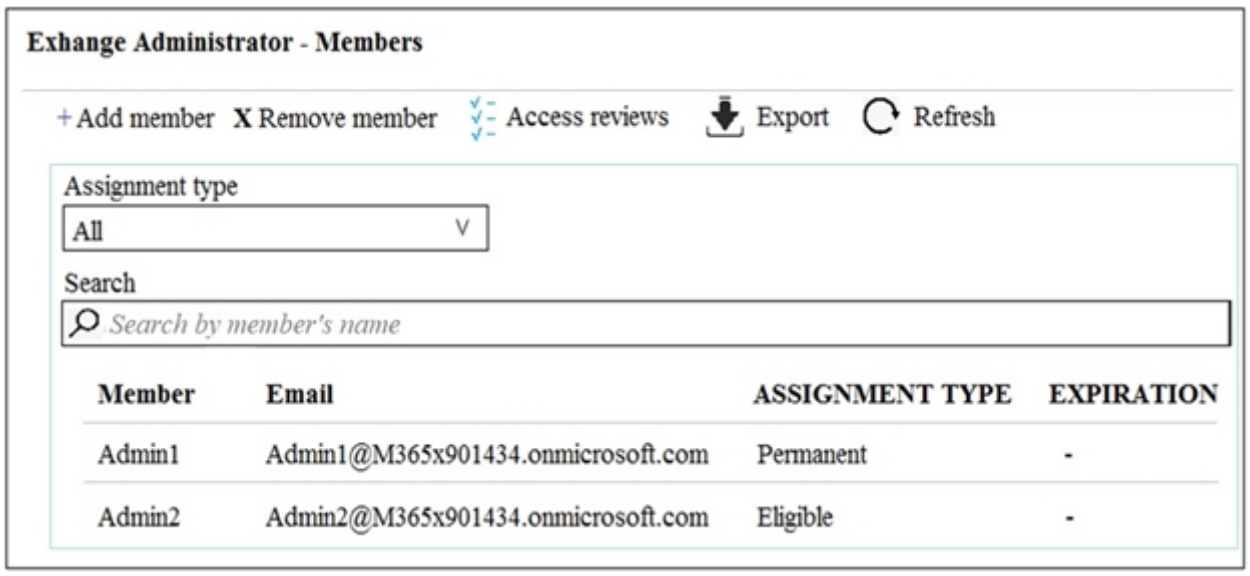
The location of the user administrators must be audited when the administrators authenticate to Azure AD

Email messages that include attachments containing malware must be delivered without the attachment

The principle of least privilege must be used whenever possible

Question

An administrator configures Azure AD Privileged Identity Management as shown in the following exhibit.



What should you do to meet the security requirements?

A. Change the Assignment Type for Admin2 to Permanent

B. From the Azure Active Directory admin center, assign the Exchange administrator role to Admin2

C. From the Azure Active Directory admin center, remove the Exchange administrator role to Admin1

D. Change the Assignment Type for Admin1 to Eligible

JakubK64 2 weeks, 2 days ago

D looks correct

upvoted 1 times

Question #2 *Topic 6*

Introductory Info

This is a case study. Case studies are not timed separately. You can use as much exam time as you would like to complete each case. However, there may be additional case studies and sections on this exam. You must manage your time to ensure that you are able to complete all questions included on this exam in the time provided.

To answer the questions included in a case study, you will need to reference information that is provided in the case study. Case studies might contain exhibits and other resources that provide more information about the scenario that is described in the case study. Each question is independent of the other questions in this case study.

At the end of this case study, a review screen will appear. This screen allows you to review your answers and to make changes before you move to the next section of the exam. After you begin a new section, you cannot return to this section.

To start the case study -

To display the first question in this case study, click the Next button. Use the buttons in the left pane to explore the content of the case study before you answer the questions. Clicking these buttons displays information such as business requirements, existing environment, and problem statements. If the case study has an All Information tab, note that the information displayed is identical to the information displayed on the subsequent tabs. When you are ready to answer a question, click the Question button to return to the question.

Overview -

Fabrikam, Inc. is manufacturing company that sells products through partner retail stores. Fabrikam has 5,000 employees located in offices throughout Europe.

Existing Environment -

Network Infrastructure -

The network contains an Active Directory forest named fabrikam.com. Fabrikam has a hybrid Microsoft Azure Active Directory (Azure AD) environment.

The company maintains some on-premises servers for specific applications, but most end-user applications are provided by a Microsoft 365 E5 subscription.

Problem Statements -

Fabrikam identifies the following issues:

Since last Friday, the IT team has been receiving automated email messages that contain "Unhealthy Identity Synchronization Notification" in the subject line.

Several users recently opened email attachments that contained malware. The process to remove the malware was time consuming.

Requirements -

Planned Changes -

Fabrikam plans to implement the following changes:

Fabrikam plans to monitor and investigate suspicious sign-ins to Active Directory

Fabrikam plans to provide partners with access to some of the data stored in Microsoft 365

Application Administration -

Fabrikam identifies the following application requirements for managing workload applications:

User administrators will work from different countries

User administrators will use the Azure Active Directory admin center

Two new administrators named Admin1 and Admin2 will be responsible for managing Microsoft Exchange Online only

Security Requirements -

Fabrikam identifies the following security requirements:

Access to the Azure Active Directory admin center by the user administrators must be reviewed every seven days. If an administrator fails to respond to an access request within three days, access must be removed

Users who manage Microsoft 365 workloads must only be allowed to perform administrative tasks for up to three hours at a time. Global administrators must be exempt from this requirement

Users must be prevented from inviting external users to view company data. Only global administrators and a user named User1 must be able to

send invitations

Azure Advanced Threat Protection (ATP) must capture security group modifications for sensitive groups, such as Domain Admins in Active Directory

Workload administrators must use multi-factor authentication (MFA) when signing in from an anonymous or an unfamiliar location

The location of the user administrators must be audited when the administrators authenticate to Azure AD

Email messages that include attachments containing malware must be delivered without the attachment

The principle of least privilege must be used whenever possible

Question

You need to recommend a solution for the user administrators that meets the security requirements for auditing.

Which blade should you recommend using from the Azure Active Directory admin center?

A. Sign-ins

B. Azure AD Identity Protection

C. Authentication methods

D. Access review

Question #3 *Topic 6*

Introductory Info

This is a case study. Case studies are not timed separately. You can use as much exam time as you would like to complete each case. However, there may be additional case studies and sections on this exam. You must manage your time to ensure that you are able to complete all questions included on this exam in the time provided.

To answer the questions included in a case study, you will need to reference information that is provided in the case study. Case studies might contain exhibits and other resources that provide more information about the scenario that is described in the case study. Each question is independent of the other questions in this case study.

At the end of this case study, a review screen will appear. This screen allows you to review your answers and to make changes before you move to the next section of the exam. After you begin a new section, you cannot return to this section.

To start the case study -

To display the first question in this case study, click the Next button. Use the buttons in the left pane to explore the content of the case study before you answer the questions. Clicking these buttons displays information such as business requirements, existing environment, and problem statements. If the case study has an All Information tab, note that the information displayed is identical to the information displayed on the subsequent tabs. When you are ready to answer a question, click the Question button to return to the question.

Overview -

Fabrikam, Inc. is manufacturing company that sells products through partner retail stores. Fabrikam has 5,000 employees located in offices throughout Europe.

Existing Environment -

Network Infrastructure -

The network contains an Active Directory forest named fabrikam.com. Fabrikam has a hybrid Microsoft Azure Active Directory (Azure AD) environment.

The company maintains some on-premises servers for specific applications, but most end-user applications are provided by a Microsoft 365 E5 subscription.

Problem Statements -

Fabrikam identifies the following issues:

Since last Friday, the IT team has been receiving automated email messages that contain "Unhealthy Identity Synchronization Notification" in the subject line.

Several users recently opened email attachments that contained malware. The process to remove the malware was time consuming.

Requirements -

Planned Changes -

Fabrikam plans to implement the following changes:

Fabrikam plans to monitor and investigate suspicious sign-ins to Active Directory

Fabrikam plans to provide partners with access to some of the data stored in Microsoft 365

Application Administration -

Fabrikam identifies the following application requirements for managing workload applications:

User administrators will work from different countries

User administrators will use the Azure Active Directory admin center

Two new administrators named Admin1 and Admin2 will be responsible for managing Microsoft Exchange Online only

Security Requirements -

Fabrikam identifies the following security requirements:

Access to the Azure Active Directory admin center by the user administrators must be reviewed every seven days. If an administrator fails to respond to an access request within three days, access must be removed

Users who manage Microsoft 365 workloads must only be allowed to perform administrative tasks for up to three hours at a time. Global administrators must be exempt from this requirement

Users must be prevented from inviting external users to view company data. Only global administrators and a user named User1 must be able to

send invitations

Azure Advanced Threat Protection (ATP) must capture security group modifications for sensitive groups, such as Domain Admins in Active Directory

Workload administrators must use multi-factor authentication (MFA) when signing in from an anonymous or an unfamiliar location

The location of the user administrators must be audited when the administrators authenticate to Azure AD

Email messages that include attachments containing malware must be delivered without the attachment

The principle of least privilege must be used whenever possible

Question

HOTSPOT -

You plan to configure an access review to meet the security requirements for the workload administrators. You create an access review policy and specify the scope and a group.

Which other settings should you configure? To answer, select the appropriate options in the answer area.

NOTE: Each correct selection is worth one point.

Hot Area:

Set the frequency to:

One time	∨
Weekly	
Monthly	

To ensure that access is removed if an administrator fails to respond, configure the:

Upon completion settings	∨
Advanced settings	
Programs	
Reviewers	

JakubK64 2 weeks, 2 days ago

Weekly & Uppon completion settings. Correct

upvoted 2 times

Question #4 *Topic 6*

Introductory Info

This is a case study. Case studies are not timed separately. You can use as much exam time as you would like to complete each case. However, there may be additional case studies and sections on this exam. You must manage your time to ensure that you are able to complete all questions included on this exam in the time provided.

To answer the questions included in a case study, you will need to reference information that is provided in the case study. Case studies might contain exhibits and other resources that provide more information about the scenario that is described in the case study. Each question is independent of the other questions in this case study.

At the end of this case study, a review screen will appear. This screen allows you to review your answers and to make changes before you move to the next section of the exam. After you begin a new section, you cannot return to this section.

To start the case study -

To display the first question in this case study, click the Next button. Use the buttons in the left pane to explore the content of the case study before you answer the questions. Clicking these buttons displays information such as business requirements, existing environment, and problem statements. If the case study has an All Information tab, note that the information displayed is identical to the information displayed on the subsequent tabs. When you are ready to answer a question, click the Question button to return to the question.

Overview -

Fabrikam, Inc. is manufacturing company that sells products through partner retail stores. Fabrikam has 5,000 employees located in offices throughout Europe.

Existing Environment -

Network Infrastructure -

The network contains an Active Directory forest named fabrikam.com. Fabrikam has a hybrid Microsoft Azure Active Directory (Azure AD) environment.

The company maintains some on-premises servers for specific applications, but most end-user applications are provided by a Microsoft 365 E5 subscription.

Problem Statements -

Fabrikam identifies the following issues:

Since last Friday, the IT team has been receiving automated email messages that contain "Unhealthy Identity Synchronization Notification" in the subject line.

Several users recently opened email attachments that contained malware. The process to remove the malware was time consuming.

Requirements -

Planned Changes -

Fabrikam plans to implement the following changes:

Fabrikam plans to monitor and investigate suspicious sign-ins to Active Directory

Fabrikam plans to provide partners with access to some of the data stored in Microsoft 365

Application Administration -

Fabrikam identifies the following application requirements for managing workload applications:

User administrators will work from different countries

User administrators will use the Azure Active Directory admin center

Two new administrators named Admin1 and Admin2 will be responsible for managing Microsoft Exchange Online only

Security Requirements -

Fabrikam identifies the following security requirements:

Access to the Azure Active Directory admin center by the user administrators must be reviewed every seven days. If an administrator fails to respond to an access request within three days, access must be removed

Users who manage Microsoft 365 workloads must only be allowed to perform administrative tasks for up to three hours at a time. Global administrators must be exempt from this requirement

Users must be prevented from inviting external users to view company data. Only global administrators and a user named User1 must be able to

send invitations

Azure Advanced Threat Protection (ATP) must capture security group modifications for sensitive groups, such as Domain Admins in Active Directory

Workload administrators must use multi-factor authentication (MFA) when signing in from an anonymous or an unfamiliar location

The location of the user administrators must be audited when the administrators authenticate to Azure AD

Email messages that include attachments containing malware must be delivered without the attachment

The principle of least privilege must be used whenever possible

Question

You need to recommend a solution to protect the sign-ins of Admin1 and Admin2.

What should you include in the recommendation?

A. a device compliance policy

B. an access review

C. a user risk policy

D. a sign-in risk policy

JakubK64 2 weeks, 2 days ago

The only possible answer

upvoted 1 times

Question #5 *Topic 6*

Introductory Info

This is a case study. Case studies are not timed separately. You can use as much exam time as you would like to complete each case. However, there may be additional case studies and sections on this exam. You must manage your time to ensure that you are able to complete all questions included on this exam in the time provided.

To answer the questions included in a case study, you will need to reference information that is provided in the case study. Case studies might contain exhibits and other resources that provide more information about the scenario that is described in the case study. Each question is independent of the other questions in this case study.

At the end of this case study, a review screen will appear. This screen allows you to review your answers and to make changes before you move to the next section of the exam. After you begin a new section, you cannot return to this section.

To start the case study -

To display the first question in this case study, click the Next button. Use the buttons in the left pane to explore the content of the case study before you answer the questions. Clicking these buttons displays information such as business requirements, existing environment, and problem statements. If the case study has an All Information tab, note that the information displayed is identical to the information displayed on the subsequent tabs. When you are ready to answer a question, click the Question button to return to the question.

Overview -

Fabrikam, Inc. is manufacturing company that sells products through partner retail stores. Fabrikam has 5,000 employees located in offices throughout Europe.

Existing Environment -

Network Infrastructure -

The network contains an Active Directory forest named fabrikam.com. Fabrikam has a hybrid Microsoft Azure Active Directory (Azure AD) environment.

The company maintains some on-premises servers for specific applications, but most end-user applications are provided by a Microsoft 365 E5 subscription.

Problem Statements -

Fabrikam identifies the following issues:

Since last Friday, the IT team has been receiving automated email messages that contain "Unhealthy Identity Synchronization Notification" in the subject line.

Several users recently opened email attachments that contained malware. The process to remove the malware was time consuming.

Requirements -

Planned Changes -

Fabrikam plans to implement the following changes:

Fabrikam plans to monitor and investigate suspicious sign-ins to Active Directory

Fabrikam plans to provide partners with access to some of the data stored in Microsoft 365

Application Administration -

Fabrikam identifies the following application requirements for managing workload applications:

User administrators will work from different countries

User administrators will use the Azure Active Directory admin center

Two new administrators named Admin1 and Admin2 will be responsible for managing Microsoft Exchange Online only

Security Requirements -

Fabrikam identifies the following security requirements:

Access to the Azure Active Directory admin center by the user administrators must be reviewed every seven days. If an administrator fails to respond to an access request within three days, access must be removed

Users who manage Microsoft 365 workloads must only be allowed to perform administrative tasks for up to three hours at a time. Global administrators must be exempt from this requirement

Users must be prevented from inviting external users to view company data. Only global administrators and a user named User1 must be able to

send invitations

Azure Advanced Threat Protection (ATP) must capture security group modifications for sensitive groups, such as Domain Admins in Active Directory

Workload administrators must use multi-factor authentication (MFA) when signing in from an anonymous or an unfamiliar location

The location of the user administrators must be audited when the administrators authenticate to Azure AD

Email messages that include attachments containing malware must be delivered without the attachment

The principle of least privilege must be used whenever possible

Question

You need to resolve the issue that generates the automated email messages to the IT team.

Which tool should you run first?

A. Synchronization Service Manager

B. Azure AD Connect wizard

C. Synchronization Rules Editor

D. IdFix

Topic 7 - Testlet 2

Question #1 *Topic 7*

Introductory Info

This is a case study. Case studies are not timed separately. You can use as much exam time as you would like to complete each case. However, there may be additional case studies and sections on this exam. You must manage your time to ensure that you are able to complete all questions included on this exam in the time provided.

To answer the questions included in a case study, you will need to reference information that is provided in the case study. Case studies might contain exhibits and other resources that provide more information about the scenario that is described in the case study. Each question is independent of the other questions in this case study.

At the end of this case study, a review screen will appear. This screen allows you to review your answers and to make changes before you move to the next section of the exam. After you begin a new section, you cannot return to this section.

To start the case study -

To display the first question in this case study, click the Next button. Use the buttons in the left pane to explore the content of the case study before you answer the questions. Clicking these buttons displays information such as business requirements, existing environment, and problem statements. If the case study has an

All Information tab, note that the information displayed is identical to the information displayed on the subsequent tabs. When you are ready to answer a question, click the Question button to return to the question.

Overview -

Litware, Inc. is a financial company that has 1,000 users in its main office in Chicago and 100 users in a branch office in San Francisco.

Existing Environment -

Internal Network Infrastructure -

The network contains a single domain forest. The forest functional level is Windows Server 2016.

Users are subject to sign-in hour restrictions as defined in Active Directory.

The network has the IP address ranges shown in the following table.

Location	IP address range
Chicago office internal network	192.168.0.0/20
Chicago office perimeter network	172.16.0.0/24
Chicago office external network	131.107.83.0/28
San Francisco office internal network	192.168.16.0/20
San Francisco office perimeter network	172.16.16.0/24
San Francisco office external network	131.107.16.218/32

The offices connect by using Multiprotocol Label Switching (MPLS).

The following operating systems are used on the network:

Windows Server 2016

Windows 10 Enterprise

Windows 8.1 Enterprise

The internal network contains the systems shown in the following table.

Office	Name	Configuration
Chicago	DC1	Domain controller
Chicago	DC2	Domain controller
San Francisco	DC3	Domain controller
Chicago	Server1	SIEM-server

Litware uses a third-party email system.

Cloud Infrastructure -

Litware recently purchased Microsoft 365 subscription licenses for all users.

Microsoft Azure Active Directory (Azure AD) Connect is installed and uses the default authentication settings. User accounts are not yet synced to Azure AD.

You have the Microsoft 365 users and groups shown in the following table.

Name	Object type	Description
Group1	Security group	A group for testing Azure and Microsoft 365 functionality
User1	User	A test user who is a member of Group1
User2	User	A test user who is a member of Group1
User3	User	A test user who is a member of Group1
User4	User	An administrator
Guest1	Guest user	A guest user

Requirements -

Planned Changes -
Litware plans to implement the following changes:
Migrate the email system to Microsoft Exchange Online
Implement Azure AD Privileged Identity Management

Security Requirements -
Litware identifies the following security requirements:
Create a group named Group3 that will be used for publishing sensitivity labels to pilot users. Group3 must only contain user accounts
Use Azure Advanced Threat Protection (ATP) to detect any security threats that target the forest
Prevent users locked out of Active Directory from signing in to Azure AD and Active Directory
Implement a permanent eligible assignment of the Compliance administrator role for User1
Configure domain-joined servers to ensure that they report sensor data to Microsoft Defender ATP
Prevent access to Azure resources for the guest user accounts by default
Ensure that all domain-joined computers are registered to Azure AD
Multi-factor authentication (MFA) Requirements
Security features of Microsoft Office 365 and Azure will be tested by using pilot Azure user accounts.
You identify the following requirements for testing MFA:
Pilot users must use MFA unless they are signing in from the internal network of the Chicago office. MFA must NOT be used on the Chicago office internal network.
If an authentication attempt is suspicious, MFA must be used, regardless of the user location.
Any disruption of legitimate authentication attempts must be minimized.

General Requirements -
Litware wants to minimize the deployment of additional servers and services in the Active Directory forest.

Question
Which IP address space should you include in the Trusted IP MFA configuration?

A. 131.107.83.0/28

B. 192.168.16.0/20

C. 172.16.0.0/24

D. 192.168.0.0/20

b00 Highly Voted 4 months, 3 weeks ago

False:
-The subnet is the one of San Francisco Internal, but trusted IP will exclue the subnet from MFA, and we want to exclude Chicago from MFA.
-Trusted IPs can only use public IP not private IP (https://docs.microsoft.com/en-us/azure/active-directory/authentication/howto-mfa-mfasettings#trusted-ips)

Correct Answer is 131.107.83.0/28
upvoted 10 times

chaoscreater 3 weeks, 6 days ago

You said "trusted IP will exclude the subnet from MFA" and you've added the external IP range of 131.107.83.0/28 to the Trusted IP, which means it is excluded from MFA and is therefore not what the question is asking? Question asks to exclude internal IP range from MFA.
upvoted 1 times

PeterC 4 months, 3 weeks ago

b00 has the correct answer:

The trusted IPs can include private IP ranges only when you use MFA Server. For cloud-based Azure AD Multi-Factor Authentication, you can only use public IP address ranges.

upvoted 6 times

kiketxu 4 months, 3 weeks ago

Right guys, thanks!
https://docs.microsoft.com/es-es/azure/active-directory/authentication/howto-mfa-mfasettings#trusted-ips

upvoted 2 times

Fala_Fel Most Recent 2 weeks, 3 days ago

Answer has to be correct.
Firstly trusted IP's need to be external, so has to be A
This will exempt pilot group and all other users from MFA when in the Chicago office. Which is a requirement.
We can then create another policy which will enforce MFA if auth is suspicous even if from a trusted location

upvoted 1 times

chaoscreater 3 weeks, 6 days ago

I'm so confused by all the comments here.

My understanding is that sign-ins from the Trusted IP range will be excluded from MFA. Question asks you to exclude internal IP range from MFA, not external. Comments provided here says to exclude external IP range from MFA, which is not what the question is asking.

upvoted 2 times

GevedeBe 3 months, 2 weeks ago

The Trusted IP feature in Azure AD Multi-Factor Authentication ignores multi-factor authentication requests from users who sign in from a defined IP address range.

From <https://docs.microsoft.com/es-es/azure/active-directory/authentication/howto-mfa-mfasettings#trusted-ips>

Pilot users must use MFA unless they are signing in from the internal network of the Chicago office. MFA must NOT be used on the Chicago office internal network.

Chicago internal Is 192.168.0.0/20

So D is the correct answer

upvoted 3 times

Akc0 4 months, 2 weeks ago

As b00 said, correct answer is A, it is the external facing IP for Chicago which is used for MFA, not internal IPs

upvoted 3 times

chaoscreater 3 weeks, 6 days ago

And by adding the external range to Trusted IP configuration, you EXCLUDE it from MFA prompts. So this doesn't address what the question is asking.

upvoted 1 times

Question #2 *Topic 7*

Introductory Info

This is a case study. Case studies are not timed separately. You can use as much exam time as you would like to complete each case. However, there may be additional case studies and sections on this exam. You must manage your time to ensure that you are able to complete all questions included on this exam in the time provided.

To answer the questions included in a case study, you will need to reference information that is provided in the case study. Case studies might contain exhibits and other resources that provide more information about the scenario that is described in the case study. Each question is independent of the other questions in this case study.

At the end of this case study, a review screen will appear. This screen allows you to review your answers and to make changes before you move to the next section of the exam. After you begin a new section, you cannot return to this section.

To start the case study -

To display the first question in this case study, click the Next button. Use the buttons in the left pane to explore the content of the case study before you answer the questions. Clicking these buttons displays information such as business requirements, existing environment, and problem statements. If the case study has an

All Information tab, note that the information displayed is identical to the information displayed on the subsequent tabs. When you are ready to answer a question, click the Question button to return to the question.

Overview -

Litware, Inc. is a financial company that has 1,000 users in its main office in Chicago and 100 users in a branch office in San Francisco.

Existing Environment -

Internal Network Infrastructure -

The network contains a single domain forest. The forest functional level is Windows Server 2016.

Users are subject to sign-in hour restrictions as defined in Active Directory.

The network has the IP address ranges shown in the following table.

Location	IP address range
Chicago office internal network	192.168.0.0/20
Chicago office perimeter network	172.16.0.0/24
Chicago office external network	131.107.83.0/28
San Francisco office internal network	192.168.16.0/20
San Francisco office perimeter network	172.16.16.0/24
San Francisco office external network	131.107.16.218/32

The offices connect by using Multiprotocol Label Switching (MPLS).

The following operating systems are used on the network:

Windows Server 2016

Windows 10 Enterprise

Windows 8.1 Enterprise

The internal network contains the systems shown in the following table.

Office	Name	Configuration
Chicago	DC1	Domain controller
Chicago	DC2	Domain controller
San Francisco	DC3	Domain controller
Chicago	Server1	SIEM-server

Litware uses a third-party email system.

Cloud Infrastructure -

Litware recently purchased Microsoft 365 subscription licenses for all users.

Microsoft Azure Active Directory (Azure AD) Connect is installed and uses the default authentication settings. User accounts are not yet synced to Azure AD.

You have the Microsoft 365 users and groups shown in the following table.

Name	Object type	Description
Group1	Security group	A group for testing Azure and Microsoft 365 functionality
User1	User	A test user who is a member of Group1
User2	User	A test user who is a member of Group1
User3	User	A test user who is a member of Group1
User4	User	An administrator
Guest1	Guest user	A guest user

Requirements -

Planned Changes -
Litware plans to implement the following changes:
Migrate the email system to Microsoft Exchange Online
Implement Azure AD Privileged Identity Management

Security Requirements -
Litware identifies the following security requirements:
Create a group named Group3 that will be used for publishing sensitivity labels to pilot users. Group3 must only contain user accounts
Use Azure Advanced Threat Protection (ATP) to detect any security threats that target the forest
Prevent users locked out of Active Directory from signing in to Azure AD and Active Directory
Implement a permanent eligible assignment of the Compliance administrator role for User1
Configure domain-joined servers to ensure that they report sensor data to Microsoft Defender ATP
Prevent access to Azure resources for the guest user accounts by default
Ensure that all domain-joined computers are registered to Azure AD
Multi-factor authentication (MFA) Requirements
Security features of Microsoft Office 365 and Azure will be tested by using pilot Azure user accounts.
You identify the following requirements for testing MFA:
Pilot users must use MFA unless they are signing in from the internal network of the Chicago office. MFA must NOT be used on the Chicago office internal network.
If an authentication attempt is suspicious, MFA must be used, regardless of the user location.
Any disruption of legitimate authentication attempts must be minimized.

General Requirements -
Litware wants to minimize the deployment of additional servers and services in the Active Directory forest.

Question
HOTSPOT -
How should you configure Group3? To answer, select the appropriate options in the answer area.
NOTE: Each correct selection is worth one point.
Hot Area:

Answer Area

Group type:
- A Microsoft 365 group in the Microsoft 365 admin center
- A security group in Active Directory Users and Computers
- A security group in the Azure Active Directory admin center

Group membership criteria:
- A dynamic distribution list
- A dynamic membership rule set to accountEnabled Equals true
- A dynamic membership rule set to userType Equals Member

PeterC Highly Voted 4 months, 3 weeks ago
Solution:
a Security Group with dynamic user membership - Usertype -eq Member
upvoted 9 times

Beitran 4 months, 3 weeks ago

Both are possible: 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 Azure AD.
https://docs.microsoft.com/en-us/microsoft-365/compliance/sensitivity-labels?view=o365-worldwide

upvoted 1 times

kiketxu 4 months, 3 weeks ago

Thanks Peter, I'm agree. Both are right.

upvoted 2 times

Fala_Fel 2 weeks, 3 days ago

Agreed, Answers given are correct
Group Type = M365 Group as it does not specify that other groups are mail enabled which they would need to be.
Group Membership Criteria = needs to specify that the member must be a user account as per "Group3 must only contain user accounts"
"userType Equals Member" would add all users accounts, and only user accounts

upvoted 1 times

Vic08 Most Recent 2 months, 3 weeks ago

The answers are:
1) Office 365 Group in Microsoft 365 admin center.
2) Dynamic membership rule with an Advanced rule set to All users.

https://www.examtopics.com/discussions/microsoft/view/13329-exam-ms-500-topic-6-question-3-discussion/

upvoted 1 times

TimurKazan 3 months, 2 weeks ago

I dont think that this is right. For the first part of the question it can be any mail enabled group. As per the requirement of environment, users that are locked in active directory should be prevented from sign in. So I would choose accountEnabled -eq true

upvoted 1 times

TimurKazan 3 months, 2 weeks ago

Oh sorry, it has nothing to do with group for publishing labes, I believe the correct one is answer from PeterC

upvoted 1 times

Question #3 *Topic 7*

Introductory Info

This is a case study. Case studies are not timed separately. You can use as much exam time as you would like to complete each case. However, there may be additional case studies and sections on this exam. You must manage your time to ensure that you are able to complete all questions included on this exam in the time provided.

To answer the questions included in a case study, you will need to reference information that is provided in the case study. Case studies might contain exhibits and other resources that provide more information about the scenario that is described in the case study. Each question is independent of the other questions in this case study.

At the end of this case study, a review screen will appear. This screen allows you to review your answers and to make changes before you move to the next section of the exam. After you begin a new section, you cannot return to this section.

To start the case study -

To display the first question in this case study, click the Next button. Use the buttons in the left pane to explore the content of the case study before you answer the questions. Clicking these buttons displays information such as business requirements, existing environment, and problem statements. If the case study has an

All Information tab, note that the information displayed is identical to the information displayed on the subsequent tabs. When you are ready to answer a question, click the Question button to return to the question.

Overview -

Litware, Inc. is a financial company that has 1,000 users in its main office in Chicago and 100 users in a branch office in San Francisco.

Existing Environment -

Internal Network Infrastructure -

The network contains a single domain forest. The forest functional level is Windows Server 2016.

Users are subject to sign-in hour restrictions as defined in Active Directory.

The network has the IP address ranges shown in the following table.

Location	IP address range
Chicago office internal network	192.168.0.0/20
Chicago office perimeter network	172.16.0.0/24
Chicago office external network	131.107.83.0/28
San Francisco office internal network	192.168.16.0/20
San Francisco office perimeter network	172.16.16.0/24
San Francisco office external network	131.107.16.218/32

The offices connect by using Multiprotocol Label Switching (MPLS).

The following operating systems are used on the network:

Windows Server 2016

Windows 10 Enterprise

Windows 8.1 Enterprise

The internal network contains the systems shown in the following table.

Office	Name	Configuration
Chicago	DC1	Domain controller
Chicago	DC2	Domain controller
San Francisco	DC3	Domain controller
Chicago	Server1	SIEM-server

Litware uses a third-party email system.

Cloud Infrastructure -

Litware recently purchased Microsoft 365 subscription licenses for all users.

Microsoft Azure Active Directory (Azure AD) Connect is installed and uses the default authentication settings. User accounts are not yet synced to Azure AD.

You have the Microsoft 365 users and groups shown in the following table.

Name	Object type	Description
Group1	Security group	A group for testing Azure and Microsoft 365 functionality
User1	User	A test user who is a member of Group1
User2	User	A test user who is a member of Group1
User3	User	A test user who is a member of Group1
User4	User	An administrator
Guest1	Guest user	A guest user

Requirements -

Planned Changes -
Litware plans to implement the following changes:
Migrate the email system to Microsoft Exchange Online
Implement Azure AD Privileged Identity Management

Security Requirements -
Litware identifies the following security requirements:
Create a group named Group3 that will be used for publishing sensitivity labels to pilot users. Group3 must only contain user accounts
Use Azure Advanced Threat Protection (ATP) to detect any security threats that target the forest
Prevent users locked out of Active Directory from signing in to Azure AD and Active Directory
Implement a permanent eligible assignment of the Compliance administrator role for User1
Configure domain-joined servers to ensure that they report sensor data to Microsoft Defender ATP
Prevent access to Azure resources for the guest user accounts by default
Ensure that all domain-joined computers are registered to Azure AD
Multi-factor authentication (MFA) Requirements
Security features of Microsoft Office 365 and Azure will be tested by using pilot Azure user accounts.
You identify the following requirements for testing MFA:
Pilot users must use MFA unless they are signing in from the internal network of the Chicago office. MFA must NOT be used on the Chicago office internal network.
If an authentication attempt is suspicious, MFA must be used, regardless of the user location.
Any disruption of legitimate authentication attempts must be minimized.

General Requirements -
Litware wants to minimize the deployment of additional servers and services in the Active Directory forest.

Question
HOTSPOT -
How should you configure Azure AD Connect? To answer, select the appropriate options in the answer area.
NOTE: Each correct selection is worth one point.
Hot Area:

Answer Area

User sign-in settings:
- Password Synchronization with single-sign on
- Pass-through authentication with single sign-on
- Federation with Active Directory Federation Services (AD FS)

Device options:
- Hybrid Azure AD Join
- Enable Device writeback
- Disable Device writeback

Robert__Susin 2 months, 2 weeks ago
I dont get it why is not PHS, the question states it must minimize the need of extra servers, and also it dosent state any need for pass through method.
The PHS asure that the login will be blocked in anytime if it is or was blocked on prem.

upvoted 2 times

Sido1 4 months, 3 weeks ago

The default setting is " Password Harsh synchronization with SSO"

upvoted 2 times

paperinop541 2 months, 3 weeks ago

this setting does not block the login if the user is locked out on ADDS

upvoted 1 times

Robert__Susin 2 months, 2 weeks ago

Yes it does, PHS only authenticate via Azure AD but it does by syncing the hash from on prem, if its blocked on prem it will be blocked on Azure AD auth as well, i dont get it why the answer is Pass through

upvoted 1 times

kiketxu 4 months, 3 weeks ago

Agreed with both.
https://www.examtopics.com/discussions/microsoft/view/9011-exam-ms-500-topic-6-question-4-discussion/

upvoted 4 times

arunjana 2 months, 2 weeks ago

Pass through authentication & Hybrid AD joined are the correct answers here

upvoted 1 times

Fala_Fel 2 weeks, 3 days ago

Yep given answers are correct. "Users are subject to sign-in hour restrictions as defined in Active Directory." this will require pass through auth PTA.

upvoted 1 times

Question #4 *Topic 7*

Introductory Info

This is a case study. Case studies are not timed separately. You can use as much exam time as you would like to complete each case. However, there may be additional case studies and sections on this exam. You must manage your time to ensure that you are able to complete all questions included on this exam in the time provided.

To answer the questions included in a case study, you will need to reference information that is provided in the case study. Case studies might contain exhibits and other resources that provide more information about the scenario that is described in the case study. Each question is independent of the other questions in this case study.

At the end of this case study, a review screen will appear. This screen allows you to review your answers and to make changes before you move to the next section of the exam. After you begin a new section, you cannot return to this section.

To start the case study -

To display the first question in this case study, click the Next button. Use the buttons in the left pane to explore the content of the case study before you answer the questions. Clicking these buttons displays information such as business requirements, existing environment, and problem statements. If the case study has an

All Information tab, note that the information displayed is identical to the information displayed on the subsequent tabs. When you are ready to answer a question, click the Question button to return to the question.

Overview -

Litware, Inc. is a financial company that has 1,000 users in its main office in Chicago and 100 users in a branch office in San Francisco.

Existing Environment -

Internal Network Infrastructure -

The network contains a single domain forest. The forest functional level is Windows Server 2016.

Users are subject to sign-in hour restrictions as defined in Active Directory.

The network has the IP address ranges shown in the following table.

Location	IP address range
Chicago office internal network	192.168.0.0/20
Chicago office perimeter network	172.16.0.0/24
Chicago office external network	131.107.83.0/28
San Francisco office internal network	192.168.16.0/20
San Francisco office perimeter network	172.16.16.0/24
San Francisco office external network	131.107.16.218/32

The offices connect by using Multiprotocol Label Switching (MPLS).

The following operating systems are used on the network:

Windows Server 2016

Windows 10 Enterprise

Windows 8.1 Enterprise

The internal network contains the systems shown in the following table.

Office	Name	Configuration
Chicago	DC1	Domain controller
Chicago	DC2	Domain controller
San Francisco	DC3	Domain controller
Chicago	Server1	SIEM-server

Litware uses a third-party email system.

Cloud Infrastructure -

Litware recently purchased Microsoft 365 subscription licenses for all users.

Microsoft Azure Active Directory (Azure AD) Connect is installed and uses the default authentication settings. User accounts are not yet synced to Azure AD.

You have the Microsoft 365 users and groups shown in the following table.

Name	Object type	Description
Group1	Security group	A group for testing Azure and Microsoft 365 functionality
User1	User	A test user who is a member of Group1
User2	User	A test user who is a member of Group1
User3	User	A test user who is a member of Group1
User4	User	An administrator
Guest1	Guest user	A guest user

Requirements -

Planned Changes -
Litware plans to implement the following changes:
Migrate the email system to Microsoft Exchange Online
Implement Azure AD Privileged Identity Management

Security Requirements -
Litware identifies the following security requirements:
Create a group named Group3 that will be used for publishing sensitivity labels to pilot users. Group3 must only contain user accounts
Use Azure Advanced Threat Protection (ATP) to detect any security threats that target the forest
Prevent users locked out of Active Directory from signing in to Azure AD and Active Directory
Implement a permanent eligible assignment of the Compliance administrator role for User1
Configure domain-joined servers to ensure that they report sensor data to Microsoft Defender ATP
Prevent access to Azure resources for the guest user accounts by default
Ensure that all domain-joined computers are registered to Azure AD
Multi-factor authentication (MFA) Requirements
Security features of Microsoft Office 365 and Azure will be tested by using pilot Azure user accounts.
You identify the following requirements for testing MFA:
Pilot users must use MFA unless they are signing in from the internal network of the Chicago office. MFA must NOT be used on the Chicago office internal network.
If an authentication attempt is suspicious, MFA must be used, regardless of the user location.
Any disruption of legitimate authentication attempts must be minimized.

General Requirements -
Litware wants to minimize the deployment of additional servers and services in the Active Directory forest.

Question
You need to create Group3.
What are two possible ways to create the group?

A. a Microsoft 365 group in the Microsoft 365 admin center

B. a mail-enabled security group in the Microsoft 365 admin center

C. a security group in the Microsoft 365 admin center

D. a distribution list in the Microsoft 365 admin center

E. a security group in the Azure AD admin center

Fala_Fel 2 weeks, 3 days ago

Answer can be A, B & D, so question must be wrong.
"Labels can be published to any specific user or email-enabled security group, distribution group, or Microsoft 365 group "
https://docs.microsoft.com/en-us/microsoft-365/compliance/sensitivity-labels?view=o365-worldwide
upvoted 1 times

Vic08 2 months, 3 weeks ago

Any specific user or email-enabled security group, distribution group, or Microsoft 365 group.

https://docs.microsoft.com/en-us/microsoft-365/compliance/encryption-sensitivity-labels?view=o365-worldwide#add-users-or-groups
upvoted 2 times

Yetijo 1 month, 3 weeks ago

I mean, email-enabled security group is the very fist group mention.
Any specific user or email-enabled security group, distribution group, or Microsoft 365 group (formerly Office 365 group) in Azure AD

upvoted 1 times

Rockalm 3 months, 1 week ago

I think it should be A and B. A distribution list can only be used to forward emails. For publishing labels you need a security group. Am I wrong?

upvoted 4 times

arunjana 2 months, 2 weeks ago

Another confusing MS question. I'd also go for M365 group/Mail enabled security group

upvoted 2 times

kiketxu 4 months, 3 weeks ago

given answer are right.

upvoted 4 times

Topic 8 - Testlet 3

Question #1 *Topic 8*

Introductory Info

This is a case study. Case studies are not timed separately. You can use as much exam time as you would like to complete each case. However, there may be additional case studies and sections on this exam. You must manage your time to ensure that you are able to complete all questions included on this exam in the time provided.

To answer the questions included in a case study, you will need to reference information that is provided in the case study. Case studies might contain exhibits and other resources that provide more information about the scenario that is described in the case study. Each question is independent of the other questions in this case study.

At the end of this case study, a review screen will appear. This screen allows you to review your answers and to make changes before you move to the next section of the exam. After you begin a new section, you cannot return to this section.

To start the case study -

To display the first question in this case study, click the Next button. Use the buttons in the left pane to explore the content of the case study before you answer the questions. Clicking these buttons displays information such as business requirements, existing environment, and problem statements. If the case study has an

All Information tab, note that the information displayed is identical to the information displayed on the subsequent tabs. When you are ready to answer a question, click the Question button to return to the question.

Overview -

Contoso, Ltd. is a consulting company that has a main office in Montreal and two branch offices in Seattle and New York.

The company has the offices shown in the following table.

Location	Employees	Laptops	Desktop computers	Mobile devices
Montreal	2,500	2,800	300	3,100
Seattle	1,000	1,100	200	1,500
New York	300	320	30	400

Contoso has IT, human resources (HR), legal, marketing, and finance departments. Contoso uses Microsoft 365.

Existing Environment -

Infrastructure -

The network contains an Active Directory domain named contoso.com that is synced to a Microsoft Azure Active Directory (Azure AD) tenant.

Password writeback is enabled.

The domain contains servers that run Windows Server 2016. The domain contains laptops and desktop computers that run Windows 10 Enterprise.

Each client computer has a single volume.

Each office connects to the Internet by using a NAT device. The offices have the IP addresses shown in the following table.

Location	IP address space	Public NAT segment
Montreal	10.10.0.0/16	190.15.1.0/24
Seattle	172.16.0.0/16	194.25.2.0/24
New York	192.168.0.0/16	198.35.3.0/24

Named locations are defined in Azure AD as shown in the following table.

Name	IP address range	Trusted
Montreal	10.10.0.0/16	Yes
New York	192.168.0.0/16	No

From the Multi-Factor Authentication page, an address space of 198.35.3.0/24 is defined in the trusted IPs list.

Azure Multi-Factor Authentication (MFA) is enabled for the users in the finance department.

The tenant contains the users shown in the following table.

Name	User type	City	Role
User1	Member	Seattle	*None*
User2	Member	Sea	Password administrator
User3	Member	SEATTLE	*None*
User4	Guest	SEA	*None*
User5	Member	London	*None*
User6	Member	London	Customer LockBox Access Approver
User7	Member	Sydney	Reports reader
User8	Member	Sydney	User administrator
User9	Member	Montreal	*None*

The tenant contains the groups shown in the following table.

Name	Group type	Dynamic membership rule
ADGroup1	Security	user.city -contains "SEA"
ADGroup2	Office 365	user.city -match "Sea*"

Customer Lockbox is enabled in Microsoft 365.

Microsoft Endpoint Manager Configuration

The devices enrolled in Microsoft Endpoint Manager are configured as shown in the following table.

Name	Platform	Encryption	Member of
Device1	Android	Disabled	GroupA, GroupC
Device2	Windows 10	Enabled	GroupB, GroupC
Device3	Android	Disabled	GroupB, GroupC
Device4	Windows 10	Disabled	GroupB
Device5	iOS	*Not applicable*	GroupA
Device6	Windows 10	Enabled	*None*

The device compliance policies in Microsoft Endpoint Manager are configured as shown in the following table.

Name	Platform	Encryption	Assigned
DevicePolicy1	Android	Not configured	Yes
DevicePolicy2	Windows 10	Required	Yes
DevicePolicy3	Android	Required	Yes

The device compliance policies have the assignments shown in the following table.

Name	Include	Exclude
DevicePolicy1	GroupC	*None*
DevicePolicy2	GroupB	GroupC
DevicePolicy3	GroupA	*None*

The Mark devices with no compliance policy assigned as setting is set to Compliant.

Requirements -

Technical Requirements -

Contoso identifies the following technical requirements:

Use the principle of least privilege

Enable User1 to assign the Reports reader role to users

Ensure that User6 approves Customer Lockbox requests as quickly as possible

Ensure that User9 can enable and configure Azure AD Privileged Identity Management

Question

HOTSPOT -

Which users are members of ADGroup1 and ADGroup2? To answer, select the appropriate options in the answer area.

NOTE: Each correct selection is worth one point.

Hot Area:

Answer Area

ADGroup1:

None ∨
User1 and User2 only
User2 and User4 only
User3 and User4 only
User1, User2, User3, and User4

ADGroup2:

None ∨
User1 and User2 only
User2 and User4 only
User3 and User4 only
User1, User2, User3, and User4

kiketxu Highly Voted 4 months, 3 weeks ago

wrong!
ADGroup1 = Users 1,2,3,4
ADGroup2 = Users 1,2,3,4

Microsoft Doc:
The -match operator is used for matching any regular expression. Examples:
user.displayName -match "Da.*"
Da, Dav, David evaluate to true, aDa evaluates to false.

String and regex operations are not case sensitive.

Source: https://docs.microsoft.com/en-us/azure/active-directory/users-groups-roles/groups-dynamic-membership

upvoted 13 times

SimoneV 1 month, 1 week ago

I agree with ADGroup2 = 1,2,3,4. But
ADGroup1 = 2 and 4
Microsoft provides the following examples:
10,20,30,20,10 -contains 20 # True
10,20,30 -contains "10" # True
"010",20,30 -contains 10 # False
So in this case "Seattle" is 1 value. And -contains only checks if a value occurs and doesn't check if a part of that value matches. So if you use -contains "Sea" it will only evaluate to true for "Sea" and not "Seattle".
https://docs.microsoft.com/en-us/powershell/scripting/lang-spec/chapter-07?view=powershell-7.1#782-containment-operators

upvoted 1 times

Lugo 4 months, 1 week ago

Agree with the first one but the second one they have used "SEA*" and not "SEA.*" like your article

upvoted 3 times

Beitran 4 months, 3 weeks ago

Neh, if it's regex then "SEA*" would match SEASEA but not SEAttle

upvoted 2 times

martindude Highly Voted 3 months, 3 weeks ago

Gents.
you can easily check in the PowerShell.
ADGroup1 = Users 2 and 4 only
ADGroup2 = Users 1,2,3,4

upvoted 13 times

Fala_Fel Most Recent 2 weeks, 3 days ago

ADGroup1 = Users 1,2,3,4
ADGroup2 = Users 1,2,3,4
I tested in Azure dynamic groups validate, which is where it counts, not powershell and both
-contains "eng"
-match "eng*"
added engineers to the group.

upvoted 2 times

Fala_Fel 2 weeks, 3 days ago

Answer is
ADGroup1 = Users 1,2,3,4
ADGroup2 = Users 1,2,3,4

I tested the -contains parameter (not in Powershell) but in Azure Dynamic Groups validate which is where it counts. -contains "eng" included all engineers.

upvoted 2 times

Ocico 2 months, 3 weeks ago

as always. the question is, will the given answer the right from the exam perspective, or should I follow the suggestions made in the comments section

upvoted 4 times

ismossss 2 months, 4 weeks ago

Azure Ad has a new validate rule "preview" function.
On that function i get:
ADGroup1 = Users 1,2,3,4
ADGroup2 = Users 1,2,3,4

upvoted 4 times

Resquia 3 months, 1 week ago

"Seattle" -contains "SEA"
"Seattle" -match "Sea*"

"Sea" -contains "SEA"
"Sea" -match "Sea*"

"SEATTLE" -contains "SEA"
"SEATTLE" -match "Sea*"

"SEA" -contains "SEA"
"SEA" -match "Sea*"

ADGROUP1 = User2,User4
ADGROUP2 = User1,User2,User3,User4

upvoted 3 times

Shahidqk 2 weeks, 6 days ago

Totally agreed

upvoted 1 times

chaoscreater 3 weeks, 6 days ago

Tested and confirmed myself in Powershell as well.

upvoted 1 times

ellik 3 months, 1 week ago

I tested by creating exactly the same info, also tested SEA*" and not "SEA.*" but no difference in the answer.
the members were added :

ADGroup1 = Users 1,2,3,4
ADGroup2 = Users 1,2,3,4

upvoted 3 times

Rockalm 3 months, 1 week ago

It's like martindude says:
ADGroup1 = Users 2 and 4 only
ADGroup2 = Users 1,2,3,4
check wit Powershell:
"SEA" -contains "Sea"
"SEATTLE" -match "SEA*"

upvoted 1 times

Question #2 *Topic 8*

Introductory Info

This is a case study. Case studies are not timed separately. You can use as much exam time as you would like to complete each case. However, there may be additional case studies and sections on this exam. You must manage your time to ensure that you are able to complete all questions included on this exam in the time provided.

To answer the questions included in a case study, you will need to reference information that is provided in the case study. Case studies might contain exhibits and other resources that provide more information about the scenario that is described in the case study. Each question is independent of the other questions in this case study.

At the end of this case study, a review screen will appear. This screen allows you to review your answers and to make changes before you move to the next section of the exam. After you begin a new section, you cannot return to this section.

To start the case study -

To display the first question in this case study, click the Next button. Use the buttons in the left pane to explore the content of the case study before you answer the questions. Clicking these buttons displays information such as business requirements, existing environment, and problem statements. If the case study has an

All Information tab, note that the information displayed is identical to the information displayed on the subsequent tabs. When you are ready to answer a question, click the Question button to return to the question.

Overview -

Contoso, Ltd. is a consulting company that has a main office in Montreal and two branch offices in Seattle and New York.

The company has the offices shown in the following table.

Location	Employees	Laptops	Desktop computers	Mobile devices
Montreal	2,500	2,800	300	3,100
Seattle	1,000	1,100	200	1,500
New York	300	320	30	400

Contoso has IT, human resources (HR), legal, marketing, and finance departments. Contoso uses Microsoft 365.

Existing Environment -

Infrastructure -

The network contains an Active Directory domain named contoso.com that is synced to a Microsoft Azure Active Directory (Azure AD) tenant.

Password writeback is enabled.

The domain contains servers that run Windows Server 2016. The domain contains laptops and desktop computers that run Windows 10 Enterprise.

Each client computer has a single volume.

Each office connects to the Internet by using a NAT device. The offices have the IP addresses shown in the following table.

Location	IP address space	Public NAT segment
Montreal	10.10.0.0/16	190.15.1.0/24
Seattle	172.16.0.0/16	194.25.2.0/24
New York	192.168.0.0/16	198.35.3.0/24

Named locations are defined in Azure AD as shown in the following table.

Name	IP address range	Trusted
Montreal	10.10.0.0/16	Yes
New York	192.168.0.0/16	No

From the Multi-Factor Authentication page, an address space of 198.35.3.0/24 is defined in the trusted IPs list.

Azure Multi-Factor Authentication (MFA) is enabled for the users in the finance department.

The tenant contains the users shown in the following table.

Name	User type	City	Role
User1	Member	Seattle	*None*
User2	Member	Sea	Password administrator
User3	Member	SEATTLE	*None*
User4	Guest	SEA	*None*
User5	Member	London	*None*
User6	Member	London	Customer LockBox Access Approver
User7	Member	Sydney	Reports reader
User8	Member	Sydney	User administrator
User9	Member	Montreal	*None*

The tenant contains the groups shown in the following table.

Name	Group type	Dynamic membership rule
ADGroup1	Security	user.city -contains "SEA"
ADGroup2	Office 365	user.city -match "Sea*"

Customer Lockbox is enabled in Microsoft 365.

Microsoft Endpoint Manager Configuration

The devices enrolled in Microsoft Endpoint Manager are configured as shown in the following table.

Name	Platform	Encryption	Member of
Device1	Android	Disabled	GroupA, GroupC
Device2	Windows 10	Enabled	GroupB, GroupC
Device3	Android	Disabled	GroupB, GroupC
Device4	Windows 10	Disabled	GroupB
Device5	iOS	*Not applicable*	GroupA
Device6	Windows 10	Enabled	*None*

The device compliance policies in Microsoft Endpoint Manager are configured as shown in the following table.

Name	Platform	Encryption	Assigned
DevicePolicy1	Android	Not configured	Yes
DevicePolicy2	Windows 10	Required	Yes
DevicePolicy3	Android	Required	Yes

The device compliance policies have the assignments shown in the following table.

Name	Include	Exclude
DevicePolicy1	GroupC	*None*
DevicePolicy2	GroupB	GroupC
DevicePolicy3	GroupA	*None*

The Mark devices with no compliance policy assigned as setting is set to Compliant.

Requirements -

Technical Requirements -

Contoso identifies the following technical requirements:

Use the principle of least privilege

Enable User1 to assign the Reports reader role to users

Ensure that User6 approves Customer Lockbox requests as quickly as possible

Ensure that User9 can enable and configure Azure AD Privileged Identity Management

Question

HOTSPOT -

You are evaluating which finance department users will be prompted for Azure MFA credentials.

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
A finance department user who has an IP address from the Montreal office will be prompted for Azure MFA credentials.	○	○
A finance department user who works from home and who has an IP address of 193.77.140.140 will be prompted for Azure MFA credentials.	○	○
A finance department user who has an IP address from the New York office will be prompted for Azure MFA credentials.	○	○

b00 Highly Voted 4 months, 3 weeks ago

not correct to me MFA exception could be only set for public IP so onlyNew York Office is excluded. So YES YES NO

upvoted 14 times

kiketxu Highly Voted 4 months, 3 weeks ago

I also believe the answers are YES, YES, NO.
1. Montreal private IP range is trusted in Azure AD Named Location which is not valid for MFAif you don't have MFA server. So, YES
2. Clear YES
3. New York office NAT IP is in MFA trusted IP list. So, NO.

upvoted 9 times

Sikula 4 months, 1 week ago

from my point of view w00t described it correctly

upvoted 1 times

Sikula 4 months, 1 week ago

Sorry my mistake, bellow table is "From the Multi-Factor Authentication page, an address space of 198.35.3.0/24 is defined in the trusted IPs list." so kitetxu answers are correct (you cannot add these internal ranges as trusted)

upvoted 2 times

Sido1 Most Recent 4 months, 3 weeks ago

No Yes No

upvoted 4 times

w00t 4 months, 1 week ago

I'm quite positive this is correct.

NO= Montreal office IP is added as a Trusted Location within its network location (Named Location)
YES = Obvious
NO = New York office has its PUBLIC nat address added as a Trusted IP ("The trusted IPs can include private IP ranges only when you use MFA Server. For cloud-based Azure AD Multi-Factor Authentication, you can ONLY USE PUBLIC IP address ranges.")
Given that the PUBLIC IP is being used, The Trusted IP of the New York office is valid.

upvoted 5 times

Cbruce 1 month, 4 weeks ago

Please explain why Montreal is trusted when the internal IP range was used as the trust and not the external range? I'm now thinking it should be YES, YES, NO because of your explanation.

upvoted 2 times

Question #3 *Topic 8*

Introductory Info

This is a case study. Case studies are not timed separately. You can use as much exam time as you would like to complete each case. However, there may be additional case studies and sections on this exam. You must manage your time to ensure that you are able to complete all questions included on this exam in the time provided.

To answer the questions included in a case study, you will need to reference information that is provided in the case study. Case studies might contain exhibits and other resources that provide more information about the scenario that is described in the case study. Each question is independent of the other questions in this case study.

At the end of this case study, a review screen will appear. This screen allows you to review your answers and to make changes before you move to the next section of the exam. After you begin a new section, you cannot return to this section.

To start the case study -

To display the first question in this case study, click the Next button. Use the buttons in the left pane to explore the content of the case study before you answer the questions. Clicking these buttons displays information such as business requirements, existing environment, and problem statements. If the case study has an

All Information tab, note that the information displayed is identical to the information displayed on the subsequent tabs. When you are ready to answer a question, click the Question button to return to the question.

Overview -

Contoso, Ltd. is a consulting company that has a main office in Montreal and two branch offices in Seattle and New York.

The company has the offices shown in the following table.

Location	Employees	Laptops	Desktop computers	Mobile devices
Montreal	2,500	2,800	300	3,100
Seattle	1,000	1,100	200	1,500
New York	300	320	30	400

Contoso has IT, human resources (HR), legal, marketing, and finance departments. Contoso uses Microsoft 365.

Existing Environment -

Infrastructure -

The network contains an Active Directory domain named contoso.com that is synced to a Microsoft Azure Active Directory (Azure AD) tenant.

Password writeback is enabled.

The domain contains servers that run Windows Server 2016. The domain contains laptops and desktop computers that run Windows 10 Enterprise.

Each client computer has a single volume.

Each office connects to the Internet by using a NAT device. The offices have the IP addresses shown in the following table.

Location	IP address space	Public NAT segment
Montreal	10.10.0.0/16	190.15.1.0/24
Seattle	172.16.0.0/16	194.25.2.0/24
New York	192.168.0.0/16	198.35.3.0/24

Named locations are defined in Azure AD as shown in the following table.

Name	IP address range	Trusted
Montreal	10.10.0.0/16	Yes
New York	192.168.0.0/16	No

From the Multi-Factor Authentication page, an address space of 198.35.3.0/24 is defined in the trusted IPs list.

Azure Multi-Factor Authentication (MFA) is enabled for the users in the finance department.

The tenant contains the users shown in the following table.

Name	User type	City	Role
User1	Member	Seattle	*None*
User2	Member	Sea	Password administrator
User3	Member	SEATTLE	*None*
User4	Guest	SEA	*None*
User5	Member	London	*None*
User6	Member	London	Customer LockBox Access Approver
User7	Member	Sydney	Reports reader
User8	Member	Sydney	User administrator
User9	Member	Montreal	*None*

The tenant contains the groups shown in the following table.

Name	Group type	Dynamic membership rule
ADGroup1	Security	user.city -contains "SEA"
ADGroup2	Office 365	user.city -match "Sea*"

Customer Lockbox is enabled in Microsoft 365.

Microsoft Endpoint Manager Configuration

The devices enrolled in Microsoft Endpoint Manager are configured as shown in the following table.

Name	Platform	Encryption	Member of
Device1	Android	Disabled	GroupA, GroupC
Device2	Windows 10	Enabled	GroupB, GroupC
Device3	Android	Disabled	GroupB, GroupC
Device4	Windows 10	Disabled	GroupB
Device5	iOS	*Not applicable*	GroupA
Device6	Windows 10	Enabled	*None*

The device compliance policies in Microsoft Endpoint Manager are configured as shown in the following table.

Name	Platform	Encryption	Assigned
DevicePolicy1	Android	Not configured	Yes
DevicePolicy2	Windows 10	Required	Yes
DevicePolicy3	Android	Required	Yes

The device compliance policies have the assignments shown in the following table.

Name	Include	Exclude
DevicePolicy1	GroupC	*None*
DevicePolicy2	GroupB	GroupC
DevicePolicy3	GroupA	*None*

The Mark devices with no compliance policy assigned as setting is set to Compliant.

Requirements -

Technical Requirements -

Contoso identifies the following technical requirements:

Use the principle of least privilege

Enable User1 to assign the Reports reader role to users

Ensure that User6 approves Customer Lockbox requests as quickly as possible

Ensure that User9 can enable and configure Azure AD Privileged Identity Management

Question

Which user passwords will User2 be prevented from resetting?

A. User6 and User7

B. User4 and User6

C. User4 only

D. User7 and User8

E. User8 only

TimurKazan Highly Voted 3 months ago

if you look there you will acknowledge that 7 (reports readre) and 8 (user admin)can not have their password reset by Password Admin:
https://docs.microsoft.com/en-us/azure/active-directory/roles/permissions-reference#password-reset-permissions

upvoted 10 times

Kalzonee3611 Highly Voted 2 months, 2 weeks ago

Wish these questions were updated. Reading everyone's points/discussions makes this more confusing.

upvoted 6 times

chaoscreater Most Recent 3 weeks, 2 days ago

Shouldn't User 4 be one of the answers as well? You cannot reset password of guest accounts, because they belong in another tenant....

Helpdesk admin and user admin can reset passwords of non-admin users. No-one can reset passwords of guest accounts since these accounts are held and managed by another Azure AD tenant/instance.
Reference:
https://docs.microsoft.com/en-us/azure/active-directory/users-groups-roles/directory-assign-admin-roles

From <https://www.examtopics.com/exams/microsoft/ms-500/view/33/>

upvoted 1 times

GeO15 1 month, 1 week ago

Must be answer A:
Password admin cannot reset pasword for Reports reader (https://docs.microsoft.com/en-us/azure/active-directory/roles/permissions-reference#password-reset-permissions)

Customer Lockbox access approver role: Only global admins can reset the passwords of people assigned to this role as it's considered a privileged role (https://techcommunity.microsoft.com/t5/security-compliance-and-identity/customer-lockbox-approver-role-now-available/ba-p/223393).

upvoted 1 times

arunjana 2 months, 2 weeks ago

If it's password admin, he/she can't reset it for User 7 & User 8
If it's helpdesk admin, he/she can't reset it for User 8 only

upvoted 1 times

arunjana 2 months, 2 weeks ago

Reference: https://docs.microsoft.com/en-US/azure/active-directory/roles/permissions-reference#password-reset-permissions (5/5/2021)

upvoted 2 times

jatinKumar 3 months, 4 weeks ago

i just tried .. creating the same scenario... password admin is not able to change password for any of the users in the list... so i guess its a wrong question . as it says "Which user passwords will User2 be prevented from resetting?"
but as i did this just now .. user2 is who is a password admin is prevented from changing any other user;s password in this list.. the only password a password admin can chage is "User accounts + Other password Admins"

upvoted 1 times

prats005 4 months ago

If your Azure AD tenant is the home directory for a user, you can reset the user's password from the Azure portal. But you can't directly reset a password for a guest user who signs in with an account that's managed by another Azure AD directory or external identity provider. Only the guest user or an administrator in the user's home directory can reset the password. Here are some examples of how password reset works for guest users | https://docs.microsoft.com/en-us/azure/active-directory/external-identities/faq#:~:text=If%20the%20guest%20user%27s%20home%20directory%20is%20your,can%20reset%20their%20password%20from%20the%20Azure%20portal.

upvoted 1 times

Dodier 4 months ago

Correct answer : D (User7 and User8)
Source : https://docs.microsoft.com/en-US/azure/active-directory/roles/permissions-reference#password-reset-permissions

upvoted 4 times

prats005 4 months ago

but user 4 is a guest account and not a guest Guest Inviter

upvoted 1 times

kiketxu 4 months, 3 weeks ago

taking into account that Passowrd admin has been renamed to Helpdesk Admin and this question could be change for examen. I will take User2 as Helpdesk admin to reply.

I would say this role can change to User7 and 8.

https://docs.microsoft.com/es-es/azure/active-directory/roles/permissions-reference#helpdesk-administrator

https://docs.microsoft.com/es-es/azure/active-directory/roles/permissions-reference#password-reset-permissions

upvoted 3 times

MarcJornet 4 months, 2 weeks ago

They're asking which passwords can NOT be changed. A password for a Guest user cannot be changed so the answer is User 4

upvoted 2 times

Discuss4certi 4 months, 2 weeks ago

Looking a the articles you linked: the password admins still exists. The scope of a Helpdesk admin is a lot broader than the password admin too.

upvoted 2 times

Discuss4certi 4 months, 2 weeks ago

But i would say the answer provided is wrong, it should be (D User 7 and 8.
https://docs.microsoft.com/en-US/azure/active-directory/roles/permissions-reference#helpdesk-administrator

upvoted 5 times

maxstv 3 months, 4 weeks ago

User 7 and User 8

https://docs.microsoft.com/en-US/azure/active-directory/roles/permissions-reference#password-reset-permissions

upvoted 4 times

james1 1 month, 2 weeks ago

This is correct, clearly states Password admin can't reset the passwords for User Admin or Reports Reader - article was lat updates 2 weeks ago

upvoted 1 times

Question #4 *Topic 8*

Introductory Info

This is a case study. Case studies are not timed separately. You can use as much exam time as you would like to complete each case. However, there may be additional case studies and sections on this exam. You must manage your time to ensure that you are able to complete all questions included on this exam in the time provided.

To answer the questions included in a case study, you will need to reference information that is provided in the case study. Case studies might contain exhibits and other resources that provide more information about the scenario that is described in the case study. Each question is independent of the other questions in this case study.

At the end of this case study, a review screen will appear. This screen allows you to review your answers and to make changes before you move to the next section of the exam. After you begin a new section, you cannot return to this section.

To start the case study -

To display the first question in this case study, click the Next button. Use the buttons in the left pane to explore the content of the case study before you answer the questions. Clicking these buttons displays information such as business requirements, existing environment, and problem statements. If the case study has an

All Information tab, note that the information displayed is identical to the information displayed on the subsequent tabs. When you are ready to answer a question, click the Question button to return to the question.

Overview -

Contoso, Ltd. is a consulting company that has a main office in Montreal and two branch offices in Seattle and New York.

The company has the offices shown in the following table.

Location	Employees	Laptops	Desktop computers	Mobile devices
Montreal	2,500	2,800	300	3,100
Seattle	1,000	1,100	200	1,500
New York	300	320	30	400

Contoso has IT, human resources (HR), legal, marketing, and finance departments. Contoso uses Microsoft 365.

Existing Environment -

Infrastructure -

The network contains an Active Directory domain named contoso.com that is synced to a Microsoft Azure Active Directory (Azure AD) tenant.

Password writeback is enabled.

The domain contains servers that run Windows Server 2016. The domain contains laptops and desktop computers that run Windows 10 Enterprise.

Each client computer has a single volume.

Each office connects to the Internet by using a NAT device. The offices have the IP addresses shown in the following table.

Location	IP address space	Public NAT segment
Montreal	10.10.0.0/16	190.15.1.0/24
Seattle	172.16.0.0/16	194.25.2.0/24
New York	192.168.0.0/16	198.35.3.0/24

Named locations are defined in Azure AD as shown in the following table.

Name	IP address range	Trusted
Montreal	10.10.0.0/16	Yes
New York	192.168.0.0/16	No

From the Multi-Factor Authentication page, an address space of 198.35.3.0/24 is defined in the trusted IPs list.

Azure Multi-Factor Authentication (MFA) is enabled for the users in the finance department.

The tenant contains the users shown in the following table.

Name	User type	City	Role
User1	Member	Seattle	*None*
User2	Member	Sea	Password administrator
User3	Member	SEATTLE	*None*
User4	Guest	SEA	*None*
User5	Member	London	*None*
User6	Member	London	Customer LockBox Access Approver
User7	Member	Sydney	Reports reader
User8	Member	Sydney	User administrator
User9	Member	Montreal	*None*

The tenant contains the groups shown in the following table.

Name	Group type	Dynamic membership rule
ADGroup1	Security	user.city -contains "SEA"
ADGroup2	Office 365	user.city -match "Sea*"

Customer Lockbox is enabled in Microsoft 365.

Microsoft Endpoint Manager Configuration

The devices enrolled in Microsoft Endpoint Manager are configured as shown in the following table.

Name	Platform	Encryption	Member of
Device1	Android	Disabled	GroupA, GroupC
Device2	Windows 10	Enabled	GroupB, GroupC
Device3	Android	Disabled	GroupB, GroupC
Device4	Windows 10	Disabled	GroupB
Device5	iOS	*Not applicable*	GroupA
Device6	Windows 10	Enabled	*None*

The device compliance policies in Microsoft Endpoint Manager are configured as shown in the following table.

Name	Platform	Encryption	Assigned
DevicePolicy1	Android	Not configured	Yes
DevicePolicy2	Windows 10	Required	Yes
DevicePolicy3	Android	Required	Yes

The device compliance policies have the assignments shown in the following table.

Name	Include	Exclude
DevicePolicy1	GroupC	*None*
DevicePolicy2	GroupB	GroupC
DevicePolicy3	GroupA	*None*

The Mark devices with no compliance policy assigned as setting is set to Compliant.

Requirements -

Technical Requirements -

Contoso identifies the following technical requirements:

Use the principle of least privilege

Enable User1 to assign the Reports reader role to users

Ensure that User6 approves Customer Lockbox requests as quickly as possible

Ensure that User9 can enable and configure Azure AD Privileged Identity Management

Question

You need to meet the technical requirements for User9. What should you do?

A. Assign the Privileged administrator role to User9 and configure a mobile phone number for User9

B. Assign the Compliance administrator role to User9 and configure a mobile phone number for User9

C. Assign the Security administrator role to User9

D. Assign the Global administrator role to User9

Cbruce 1 month, 4 weeks ago

You need one Global Administrator to assign the PIM admin role to someone else. I don't know if the question is not worded correctly here or what, but there is no Global Admin defined in the table. So I'm going with D to enable a Global Admin for User 9.

upvoted 1 times

prats005 4 months ago

D is the correct answer

upvoted 3 times

Dodier 4 months ago

According to the Requirements: Use the principle of least privilege
The correct answer should be A.
Source: https://docs.microsoft.com/fr-fr/azure/active-directory/privileged-identity-management/pim-configure

upvoted 2 times

kiketxu 4 months, 3 weeks ago

In the past, only Global Admin could enable first PIM. Now it has changed to "Privileged Roles" but it hasn't sense to add the phone for anything. So, I would still mantain D as correct answer.

" When a user who is active in a privileged role in an Azure AD organization with a Premium P2 license goes to Roles and administrators in Azure AD and selects a role (or even just visits Privileged Identity Management):
We automatically enable PIM for the organization
Their experience is now that they can either assign a "regular" role assignment or an eligible role assignment"

https://docs.microsoft.com/es-es/azure/active-directory/privileged-identity-management/pim-getting-started#prerequisites.

Btw, you need one of the following to PIM:
Azure AD Premium P2
Enterprise Mobility + Security (EMS) E5

upvoted 3 times

arunjana 2 months, 2 weeks ago

Thanks for the clarification. The answer should be global admin. Only a global admin can initialize the PIM and later on a privileged admin can manage it

upvoted 1 times

moose 4 months, 3 weeks ago

I think also it is D, because to enable PIM you need to be Global Admin. Afterwards you could only be Privileged Administrator.

upvoted 1 times

b00 4 months, 3 weeks ago

Only Global Admin can enable and do the first config of PIM. Reason whay I think the answer is correct: https://docs.microsoft.com/en-us/azure/active-directory/roles/security-planning?toc=/azure/active-directory/privileged-identity-management/toc.json#stage-1-critical-items-to-do-right-now

upvoted 1 times

NIck207 4 months, 3 weeks ago

I think A is correct answer -- >> refer the below link https://docs.microsoft.com/en-us/azure/active-directory/privileged-identity-management/pim-how-to-give-access-to-pimA. Assign the Privileged administrator role to User9 and configure a mobile phone number for User9

upvoted 2 times

Vic08 2 months, 4 weeks ago

Ensure that User9 can enable and configure Azure AD Privileged Identity Management.

Only Global Admin can enable and configure PIM.

upvoted 1 times

Question #5 *Topic 8*

Introductory Info

This is a case study. Case studies are not timed separately. You can use as much exam time as you would like to complete each case. However, there may be additional case studies and sections on this exam. You must manage your time to ensure that you are able to complete all questions included on this exam in the time provided.

To answer the questions included in a case study, you will need to reference information that is provided in the case study. Case studies might contain exhibits and other resources that provide more information about the scenario that is described in the case study. Each question is independent of the other questions in this case study.

At the end of this case study, a review screen will appear. This screen allows you to review your answers and to make changes before you move to the next section of the exam. After you begin a new section, you cannot return to this section.

To start the case study -

To display the first question in this case study, click the Next button. Use the buttons in the left pane to explore the content of the case study before you answer the questions. Clicking these buttons displays information such as business requirements, existing environment, and problem statements. If the case study has an

All Information tab, note that the information displayed is identical to the information displayed on the subsequent tabs. When you are ready to answer a question, click the Question button to return to the question.

Overview -

Contoso, Ltd. is a consulting company that has a main office in Montreal and two branch offices in Seattle and New York.

The company has the offices shown in the following table.

Location	Employees	Laptops	Desktop computers	Mobile devices
Montreal	2,500	2,800	300	3,100
Seattle	1,000	1,100	200	1,500
New York	300	320	30	400

Contoso has IT, human resources (HR), legal, marketing, and finance departments. Contoso uses Microsoft 365.

Existing Environment -

Infrastructure -

The network contains an Active Directory domain named contoso.com that is synced to a Microsoft Azure Active Directory (Azure AD) tenant.

Password writeback is enabled.

The domain contains servers that run Windows Server 2016. The domain contains laptops and desktop computers that run Windows 10 Enterprise.

Each client computer has a single volume.

Each office connects to the Internet by using a NAT device. The offices have the IP addresses shown in the following table.

Location	IP address space	Public NAT segment
Montreal	10.10.0.0/16	190.15.1.0/24
Seattle	172.16.0.0/16	194.25.2.0/24
New York	192.168.0.0/16	198.35.3.0/24

Named locations are defined in Azure AD as shown in the following table.

Name	IP address range	Trusted
Montreal	10.10.0.0/16	Yes
New York	192.168.0.0/16	No

From the Multi-Factor Authentication page, an address space of 198.35.3.0/24 is defined in the trusted IPs list.

Azure Multi-Factor Authentication (MFA) is enabled for the users in the finance department.

The tenant contains the users shown in the following table.

Name	User type	City	Role
User1	Member	Seattle	*None*
User2	Member	Sea	Password administrator
User3	Member	SEATTLE	*None*
User4	Guest	SEA	*None*
User5	Member	London	*None*
User6	Member	London	Customer LockBox Access Approver
User7	Member	Sydney	Reports reader
User8	Member	Sydney	User administrator
User9	Member	Montreal	*None*

The tenant contains the groups shown in the following table.

Name	Group type	Dynamic membership rule
ADGroup1	Security	user.city -contains "SEA"
ADGroup2	Office 365	user.city -match "Sea*"

Customer Lockbox is enabled in Microsoft 365.

Microsoft Endpoint Manager Configuration

The devices enrolled in Microsoft Endpoint Manager are configured as shown in the following table.

Name	Platform	Encryption	Member of
Device1	Android	Disabled	GroupA, GroupC
Device2	Windows 10	Enabled	GroupB, GroupC
Device3	Android	Disabled	GroupB, GroupC
Device4	Windows 10	Disabled	GroupB
Device5	iOS	*Not applicable*	GroupA
Device6	Windows 10	Enabled	*None*

The device compliance policies in Microsoft Endpoint Manager are configured as shown in the following table.

Name	Platform	Encryption	Assigned
DevicePolicy1	Android	Not configured	Yes
DevicePolicy2	Windows 10	Required	Yes
DevicePolicy3	Android	Required	Yes

The device compliance policies have the assignments shown in the following table.

Name	Include	Exclude
DevicePolicy1	GroupC	*None*
DevicePolicy2	GroupB	GroupC
DevicePolicy3	GroupA	*None*

The Mark devices with no compliance policy assigned as setting is set to Compliant.

Requirements -

Technical Requirements -

Contoso identifies the following technical requirements:

Use the principle of least privilege

Enable User1 to assign the Reports reader role to users

Ensure that User6 approves Customer Lockbox requests as quickly as possible

Ensure that User9 can enable and configure Azure AD Privileged Identity Management

Question

Which role should you assign to User1?

A. Global administrator

B. User administrator

C. Privileged role administrator

D. Security administrator

belyo 3 months, 3 weeks ago

C - Privileged Role Administrator
Users with this role can manage role assignments in Azure Active Directory, as well as within Azure AD Privileged Identity Management.
Security admin cannot assign roles

upvoted 3 times

Topic 9 - Testlet 4

upvoted 3 times

Question #1 *Topic 9*

Introductory Info

Overview -

Fabrikam, Inc. is manufacturing company that sells products through partner retail stores. Fabrikam has 5,000 employees located in offices throughout Europe.

Existing Environment -

Network Infrastructure -

The network contains an Active Directory forest named fabrikam.com. Fabrikam has a hybrid Microsoft Azure Active Directory (Azure AD) environment.

The company maintains some on-premises servers for specific applications, but most end-user applications are provided by a Microsoft 365 E5 subscription.

Problem Statements -

Fabrikam identifies the following issues:

Since last Friday, the IT team has been receiving automated email messages that contain "Unhealthy Identity Synchronization Notification" in the subject line.

Several users recently opened email attachments that contained malware. The process to remove the malware was time consuming.

Requirements -

Planned Changes -

Fabrikam plans to implement the following changes:

Fabrikam plans to monitor and investigate suspicious sign-ins to Active Directory

Fabrikam plans to provide partners with access to some of the data stored in Microsoft 365

Application Administration -

Fabrikam identifies the following application requirements for managing workload applications:

User administrators will work from different countries

User administrators will use the Azure Active Directory admin center

Two new administrators named Admin1 and Admin2 will be responsible for managing Microsoft Exchange Online only

Security Requirements -

Fabrikam identifies the following security requirements:

Access to the Azure Active Directory admin center by the user administrators must be reviewed every seven days. If an administrator fails to respond to an access request within three days, access must be removed

Users who manage Microsoft 365 workloads must only be allowed to perform administrative tasks for up to three hours at a time. Global administrators must be exempt from this requirement

Users must be prevented from inviting external users to view company data. Only global administrators and a user named User1 must be able to send

- invitations

Azure Advanced Threat Protection (ATP) must capture security group modifications for sensitive groups, such as Domain Admins in Active Directory

Workload administrators must use multi-factor authentication (MFA) when signing in from an anonymous or an unfamiliar location

The location of the user administrators must be audited when the administrators authenticate to Azure AD

Email messages that include attachments containing malware must be delivered without the attachment

The principle of least privilege must be used whenever possible

Question

HOTSPOT -

You need to recommend an email malware solution that meets the security requirements.

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

NOTE: Each correct selection is worth one point.

Hot Area:

Answer Area

Policy to create:

ATP safe attachments
ATP Safe Links
Exchange Online Anti-spam
Exchange Online Anti-malware

Option to configure:

Block
Replace
Dynamic Delivery
Monitor
Quarantine message

jack987 Highly Voted 1 year, 1 month ago

The answer is correct.

Block Prevents messages with detected malware attachments from proceeding
Sends messages with detected malware to quarantine in Office 365 where a security administrator or analyst can review and release (or delete) those messages
Blocks future messages and attachments automatically Safeguard your organization from repeated attacks using the same malware attachments
Replace Removes detected malware attachments
Notifies recipients that attachments have been removed
Sends messages with detected malware to quarantine in Office 365 where a security administrator or analyst can review and release (or delete) those messages Raise visibility to recipients that attachments were removed because of detected malware

Source:

upvoted 11 times

jack987 1 year, 1 month ago

Source: https://docs.microsoft.com/en-us/microsoft-365/security/office-365-security/set-up-atp-safe-attachments-policies?view=o365-worldwide

upvoted 2 times

dzampar Highly Voted 9 months, 1 week ago

Below the options from Safe Attachments policy on Officce 365 Security and Compliance portal.

Off - Attachment will not be scanned for malware.

Monitor - Continue delivering the message after malware is detected; track scan results.

Block - Block the current and future email and attachments with detected malware.

Replace - Block the attachments with detected malware, continue to deliver the message.

Dynamic Delivery (Preview Feature)- Deliver the message without attachments immediately and reattach once scan is complete.

upvoted 7 times

Robert__Susin 2 months, 2 weeks ago

Yup, but the question is old as refer ATP and not Office Defender so we can expect in this case was meant for Block, and we can hope in exam as of now its prob updated and Dynamic Delivery will be for sure the right one.

upvoted 1 times

Robert__Susin 2 months, 2 weeks ago

Sorry, i meant replace as its stated

upvoted 1 times

kiketxu Most Recent 4 months, 3 weeks ago

given answer are right.

upvoted 1 times

Sido1 4 months, 3 weeks ago

correct
upvoted 1 times

VTHAR 10 months, 1 week ago
Answer is correct.
upvoted 1 times

Sisko 1 year, 1 month ago
Dynamic delivery would also accomplish the desired behaviour, wouldn't it?
upvoted 1 times

Sisko 1 year, 1 month ago
Ah, never mind. I see "If an attachment is determined to be malicious, it is sent to quarantine", in the Dynamic Delivery documentation.
https://docs.microsoft.com/en-us/microsoft-365/security/office-365-security/dynamic-delivery-and-previewing?view=o365-worldwide
upvoted 1 times

profitchannel 1 year, 6 months ago
Isn't this
- Exchange Online - Anti Malware
- Quarantine
?
upvoted 1 times

WoneSix 1 year, 6 months ago
"Email messages that include attachments containing malware must be delivered without the attachment" To do this, you need ATP Safe Attachments, and replace malware content.
upvoted 16 times

Question #2 *Topic 9*

Introductory Info

Overview -

Fabrikam, Inc. is manufacturing company that sells products through partner retail stores. Fabrikam has 5,000 employees located in offices throughout Europe.

Existing Environment -

Network Infrastructure -

The network contains an Active Directory forest named fabrikam.com. Fabrikam has a hybrid Microsoft Azure Active Directory (Azure AD) environment.

The company maintains some on-premises servers for specific applications, but most end-user applications are provided by a Microsoft 365 E5 subscription.

Problem Statements -

Fabrikam identifies the following issues:

Since last Friday, the IT team has been receiving automated email messages that contain "Unhealthy Identity Synchronization Notification" in the subject line.

Several users recently opened email attachments that contained malware. The process to remove the malware was time consuming.

Requirements -

Planned Changes -

Fabrikam plans to implement the following changes:

Fabrikam plans to monitor and investigate suspicious sign-ins to Active Directory

Fabrikam plans to provide partners with access to some of the data stored in Microsoft 365

Application Administration -

Fabrikam identifies the following application requirements for managing workload applications:

User administrators will work from different countries

User administrators will use the Azure Active Directory admin center

Two new administrators named Admin1 and Admin2 will be responsible for managing Microsoft Exchange Online only

Security Requirements -

Fabrikam identifies the following security requirements:

Access to the Azure Active Directory admin center by the user administrators must be reviewed every seven days. If an administrator fails to respond to an access request within three days, access must be removed

Users who manage Microsoft 365 workloads must only be allowed to perform administrative tasks for up to three hours at a time. Global administrators must be exempt from this requirement

Users must be prevented from inviting external users to view company data. Only global administrators and a user named User1 must be able to send

- invitations

Azure Advanced Threat Protection (ATP) must capture security group modifications for sensitive groups, such as Domain Admins in Active Directory

Workload administrators must use multi-factor authentication (MFA) when signing in from an anonymous or an unfamiliar location

The location of the user administrators must be audited when the administrators authenticate to Azure AD

Email messages that include attachments containing malware must be delivered without the attachment

The principle of least privilege must be used whenever possible

Question

HOTSPOT -

You install Azure ATP sensors on domain controllers.

You add a member to the Domain Admins group. You view the timeline in Azure ATP and discover that information regarding the membership change is missing.

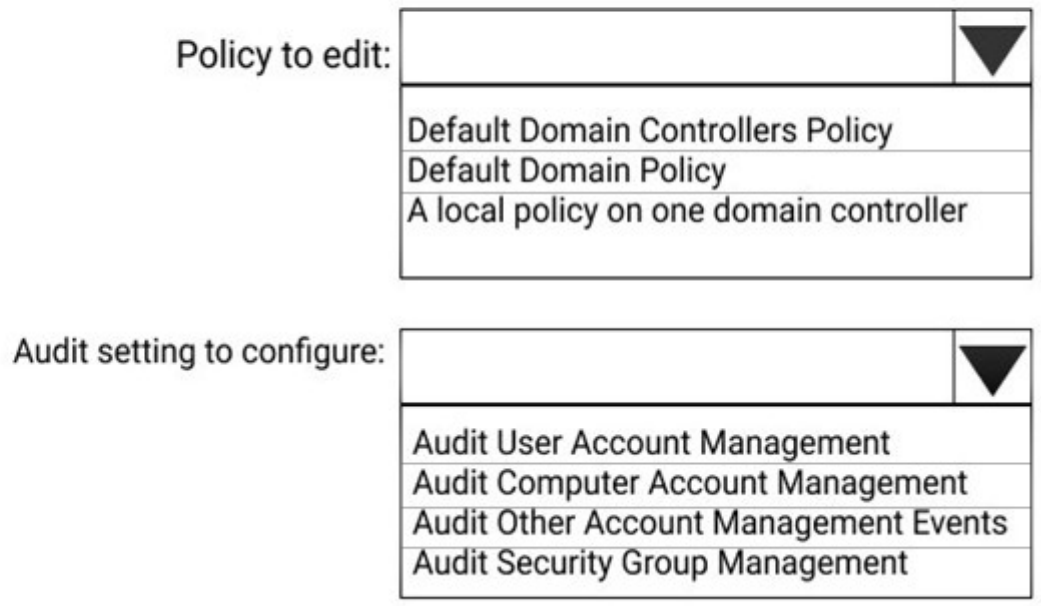
You need to meet the security requirements for Azure ATP reporting.

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

NOTE: Each correct selection is worth one point.

Hot Area:

Answer Area



kiketxu 4 months, 3 weeks ago

Agree. Thank you for sharing dude! ;)

upvoted 2 times

TDAC 10 months, 1 week ago

Answer is correct. The step by step guide on how to setup Audit policy to collect these events is here: https://docs.microsoft.com/en-us/azure-advanced-threat-protection/configure-windows-event-collection - once these events are logged, they can be collected by the Azure ATP sensor.

upvoted 4 times

Topic 10 - Testlet 5

Question #1 *Topic 10*

Introductory Info

This is a case study. Case studies are not timed separately. You can use as much exam time as you would like to complete each case. However, there may be additional case studies and sections on this exam. You must manage your time to ensure that you are able to complete all questions included on this exam in the time provided.

To answer the questions included in a case study, you will need to reference information that is provided in the case study. Case studies might contain exhibits and other resources that provide more information about the scenario that is described in the case study. Each question is independent of the other questions in this case study.

At the end of this case study, a review screen will appear. This screen allows you to review your answers and to make changes before you move to the next section of the exam. After you begin a new section, you cannot return to this section.

To start the case study -

To display the first question in this case study, click the Next button. Use the buttons in the left pane to explore the content of the case study before you answer the questions. Clicking these buttons displays information such as business requirements, existing environment, and problem statements. If the case study has an

All Information tab, note that the information displayed is identical to the information displayed on the subsequent tabs. When you are ready to answer a question, click the Question button to return to the question.

Overview -

Litware, Inc. is a financial company that has 1,000 users in its main office in Chicago and 100 users in a branch office in San Francisco.

Existing Environment -

Internal Network Infrastructure -

The network contains a single domain forest. The forest functional level is Windows Server 2016.

Users are subject to sign-in hour restrictions as defined in Active Directory.

The network has the IP address ranges shown in the following table.

Location	IP address range
Chicago office internal network	192.168.0.0/20
Chicago office perimeter network	172.16.0.0/24
Chicago office external network	131.107.83.0/28
San Francisco office internal network	192.168.16.0/20
San Francisco office perimeter network	172.16.16.0/24
San Francisco office external network	131.107.16.218/32

The offices connect by using Multiprotocol Label Switching (MPLS).

The following operating systems are used on the network:

Windows Server 2016

Windows 10 Enterprise

Windows 8.1 Enterprise

The internal network contains the systems shown in the following table.

Office	Name	Configuration
Chicago	DC1	Domain controller
Chicago	DC2	Domain controller
San Francisco	DC3	Domain controller
Chicago	Server1	SIEM-server

Litware uses a third-party email system.

Cloud Infrastructure -

Litware recently purchased Microsoft 365 subscription licenses for all users.

Microsoft Azure Active Directory (Azure AD) Connect is installed and uses the default authentication settings. User accounts are not yet synced to Azure AD.

You have the Microsoft 365 users and groups shown in the following table.

Name	Object type	Description
Group1	Security group	A group for testing Azure and Microsoft 365 functionality
User1	User	A test user who is a member of Group1
User2	User	A test user who is a member of Group1
User3	User	A test user who is a member of Group1
User4	User	An administrator
Guest1	Guest user	A guest user

Requirements -

Planned Changes -
Litware plans to implement the following changes:
Migrate the email system to Microsoft Exchange Online
Implement Azure AD Privileged Identity Management

Security Requirements -
Litware identifies the following security requirements:
Create a group named Group3 that will be used for publishing sensitivity labels to pilot users. Group3 must only contain user accounts
Use Azure Advanced Threat Protection (ATP) to detect any security threats that target the forest
Prevent users locked out of Active Directory from signing in to Azure AD and Active Directory
Implement a permanent eligible assignment of the Compliance administrator role for User1
Configure domain-joined servers to ensure that they report sensor data to Microsoft Defender ATP
Prevent access to Azure resources for the guest user accounts by default
Ensure that all domain-joined computers are registered to Azure AD
Multi-factor authentication (MFA) Requirements
Security features of Microsoft Office 365 and Azure will be tested by using pilot Azure user accounts.
You identify the following requirements for testing MFA:
Pilot users must use MFA unless they are signing in from the internal network of the Chicago office. MFA must NOT be used on the Chicago office internal network.
If an authentication attempt is suspicious, MFA must be used, regardless of the user location.
Any disruption of legitimate authentication attempts must be minimized.

General Requirements -
Litware wants to minimize the deployment of additional servers and services in the Active Directory forest.

Question
DRAG DROP -
You need to configure threat detection for Active Directory. The solution must meet the security requirements.
Which three actions should you perform in sequence? To answer, move the appropriate actions from the list of actions to the answer area and arrange them in the correct order.
Select and Place:

Actions

- Configure the Directory services setting in Azure ATP
- Download and install the ATA Gateway on DC1, DC2, and DC3
- Download and install the Azure ATP sensor package on DC1, DC2, and DC3
- Configure a site-to-site VPN
- Create a workspace in Azure ATP
- Download and install the ATA Center on Server1

Answer Area

Rafale Highly Voted 4 months, 1 week ago

1-Create ATP
2-Configure ATP
3-Downloald ATP

upvoted 5 times

Rafale 3 months ago

1-Create ATP
2-Download ATP
3-Configure ATP

upvoted 2 times

arunjana Most Recent 2 months, 2 weeks ago

1. Create MS Defender for Identity instance
2. Configure directory services
3. Download the ATP sensors and install on the DCs

upvoted 3 times

kiketxu 4 months, 3 weeks ago

This was wrong, in the past you should connect to Directory services before install sensors. But, this has change algo a bit more, no only the name....personally I would expect similar question without workspace preparing neither.
https://docs.microsoft.com/en-us/defender-for-identity/install-step1

upvoted 2 times

Question #2 *Topic 10*

Introductory Info

This is a case study. Case studies are not timed separately. You can use as much exam time as you would like to complete each case. However, there may be additional case studies and sections on this exam. You must manage your time to ensure that you are able to complete all questions included on this exam in the time provided.

To answer the questions included in a case study, you will need to reference information that is provided in the case study. Case studies might contain exhibits and other resources that provide more information about the scenario that is described in the case study. Each question is independent of the other questions in this case study.

At the end of this case study, a review screen will appear. This screen allows you to review your answers and to make changes before you move to the next section of the exam. After you begin a new section, you cannot return to this section.

To start the case study -

To display the first question in this case study, click the Next button. Use the buttons in the left pane to explore the content of the case study before you answer the questions. Clicking these buttons displays information such as business requirements, existing environment, and problem statements. If the case study has an

All Information tab, note that the information displayed is identical to the information displayed on the subsequent tabs. When you are ready to answer a question, click the Question button to return to the question.

Overview -

Litware, Inc. is a financial company that has 1,000 users in its main office in Chicago and 100 users in a branch office in San Francisco.

Existing Environment -

Internal Network Infrastructure -

The network contains a single domain forest. The forest functional level is Windows Server 2016.

Users are subject to sign-in hour restrictions as defined in Active Directory.

The network has the IP address ranges shown in the following table.

Location	IP address range
Chicago office internal network	192.168.0.0/20
Chicago office perimeter network	172.16.0.0/24
Chicago office external network	131.107.83.0/28
San Francisco office internal network	192.168.16.0/20
San Francisco office perimeter network	172.16.16.0/24
San Francisco office external network	131.107.16.218/32

The offices connect by using Multiprotocol Label Switching (MPLS).

The following operating systems are used on the network:

Windows Server 2016

Windows 10 Enterprise

Windows 8.1 Enterprise

The internal network contains the systems shown in the following table.

Office	Name	Configuration
Chicago	DC1	Domain controller
Chicago	DC2	Domain controller
San Francisco	DC3	Domain controller
Chicago	Server1	SIEM-server

Litware uses a third-party email system.

Cloud Infrastructure -

Litware recently purchased Microsoft 365 subscription licenses for all users.

Microsoft Azure Active Directory (Azure AD) Connect is installed and uses the default authentication settings. User accounts are not yet synced to Azure AD.

You have the Microsoft 365 users and groups shown in the following table.

Name	Object type	Description
Group1	Security group	A group for testing Azure and Microsoft 365 functionality
User1	User	A test user who is a member of Group1
User2	User	A test user who is a member of Group1
User3	User	A test user who is a member of Group1
User4	User	An administrator
Guest1	Guest user	A guest user

Requirements -

Planned Changes -
Litware plans to implement the following changes:
Migrate the email system to Microsoft Exchange Online
Implement Azure AD Privileged Identity Management

Security Requirements -
Litware identifies the following security requirements:
Create a group named Group3 that will be used for publishing sensitivity labels to pilot users. Group3 must only contain user accounts
Use Azure Advanced Threat Protection (ATP) to detect any security threats that target the forest
Prevent users locked out of Active Directory from signing in to Azure AD and Active Directory
Implement a permanent eligible assignment of the Compliance administrator role for User1
Configure domain-joined servers to ensure that they report sensor data to Microsoft Defender ATP
Prevent access to Azure resources for the guest user accounts by default
Ensure that all domain-joined computers are registered to Azure AD
Multi-factor authentication (MFA) Requirements
Security features of Microsoft Office 365 and Azure will be tested by using pilot Azure user accounts.
You identify the following requirements for testing MFA:
Pilot users must use MFA unless they are signing in from the internal network of the Chicago office. MFA must NOT be used on the Chicago office internal network.
If an authentication attempt is suspicious, MFA must be used, regardless of the user location.
Any disruption of legitimate authentication attempts must be minimized.

General Requirements -
Litware wants to minimize the deployment of additional servers and services in the Active Directory forest.

Question
You need to enable and configure Microsoft Defender for Endpoint to meet the security requirements. What should you do?

A. Configure port mirroring

B. Create the ForceDefenderPassiveMode registry setting

C. Download and install the Microsoft Monitoring Agent

D. Run WindowsDefenderATPOnboardingScript.cmd

Vic08 2 months, 4 weeks ago

https://docs.microsoft.com/en-us/mem/configmgr/protect/deploy-use/defender-advanced-threat-protection#about-onboarding-to-atp-with-configuration-manager

Topic 11 - Testlet 6

Question #1 *Topic 11*

Introductory Info

This is a case study. Case studies are not timed separately. You can use as much exam time as you would like to complete each case. However, there may be additional case studies and sections on this exam. You must manage your time to ensure that you are able to complete all questions included on this exam in the time provided.

To answer the questions included in a case study, you will need to reference information that is provided in the case study. Case studies might contain exhibits and other resources that provide more information about the scenario that is described in the case study. Each question is independent of the other questions in this case study.

At the end of this case study, a review screen will appear. This screen allows you to review your answers and to make changes before you move to the next section of the exam. After you begin a new section, you cannot return to this section.

To start the case study -

To display the first question in this case study, click the Next button. Use the buttons in the left pane to explore the content of the case study before you answer the questions. Clicking these buttons displays information such as business requirements, existing environment, and problem statements. If the case study has an

All Information tab, note that the information displayed is identical to the information displayed on the subsequent tabs. When you are ready to answer a question, click the Question button to return to the question.

Overview -

Contoso, Ltd. is a consulting company that has a main office in Montreal and two branch offices in Seattle and New York.

The company has the offices shown in the following table.

Location	Employees	Laptops	Desktop computers	Mobile devices
Montreal	2,500	2,800	300	3,100
Seattle	1,000	1,100	200	1,500
New York	300	320	30	400

Contoso has IT, human resources (HR), legal, marketing, and finance departments. Contoso uses Microsoft 365.

Existing Environment -

Infrastructure -

The network contains an Active Directory domain named contoso.com that is synced to a Microsoft Azure Active Directory (Azure AD) tenant.

Password writeback is enabled.

The domain contains servers that run Windows Server 2016. The domain contains laptops and desktop computers that run Windows 10 Enterprise.

Each client computer has a single volume.

Each office connects to the Internet by using a NAT device. The offices have the IP addresses shown in the following table.

Location	IP address space	Public NAT segment
Montreal	10.10.0.0/16	190.15.1.0/24
Seattle	172.16.0.0/16	194.25.2.0/24
New York	192.168.0.0/16	198.35.3.0/24

Named locations are defined in Azure AD as shown in the following table.

Name	IP address range	Trusted
Montreal	10.10.0.0/16	Yes
New York	192.168.0.0/16	No

From the Multi-Factor Authentication page, an address space of 198.35.3.0/24 is defined in the trusted IPs list.

Azure Multi-Factor Authentication (MFA) is enabled for the users in the finance department.

The tenant contains the users shown in the following table.

Name	User type	City	Role
User1	Member	Seattle	*None*
User2	Member	Sea	Password administrator
User3	Member	SEATTLE	*None*
User4	Guest	SEA	*None*
User5	Member	London	*None*
User6	Member	London	Customer LockBox Access Approver
User7	Member	Sydney	Reports reader
User8	Member	Sydney	User administrator
User9	Member	Montreal	*None*

The tenant contains the groups shown in the following table.

Name	Group type	Dynamic membership rule
ADGroup1	Security	user.city -contains "SEA"
ADGroup2	Office 365	user.city -match "Sea*"

Customer Lockbox is enabled in Microsoft 365.

Microsoft Endpoint Manager Configuration

The devices enrolled in Microsoft Endpoint Manager are configured as shown in the following table.

Name	Platform	Encryption	Member of
Device1	Android	Disabled	GroupA, GroupC
Device2	Windows 10	Enabled	GroupB, GroupC
Device3	Android	Disabled	GroupB, GroupC
Device4	Windows 10	Disabled	GroupB
Device5	iOS	*Not applicable*	GroupA
Device6	Windows 10	Enabled	*None*

The device compliance policies in Microsoft Endpoint Manager are configured as shown in the following table.

Name	Platform	Encryption	Assigned
DevicePolicy1	Android	Not configured	Yes
DevicePolicy2	Windows 10	Required	Yes
DevicePolicy3	Android	Required	Yes

The device compliance policies have the assignments shown in the following table.

Name	Include	Exclude
DevicePolicy1	GroupC	*None*
DevicePolicy2	GroupB	GroupC
DevicePolicy3	GroupA	*None*

The Mark devices with no compliance policy assigned as setting is set to Compliant.

Requirements -

Technical Requirements -

Contoso identifies the following technical requirements:

Use the principle of least privilege

Enable User1 to assign the Reports reader role to users

Ensure that User6 approves Customer Lockbox requests as quickly as possible

Ensure that User9 can enable and configure Azure AD Privileged Identity Management

Question

HOTSPOT -

You are evaluating which devices are compliant in Endpoint Manager.

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
Device2 is compliant.	○	○
Device5 is compliant.	○	○
Device6 is compliant.	○	○

NickTheo Highly Voted 4 months, 3 weeks ago

I think that the Device 5 is compliant because the device policy3 is assigned to Android only devices. So Y-Y-Y

upvoted 12 times

w00t 4 months, 1 week ago

Device5 is on iOS, not Android. Therefore the original answer is correct.

Y - N - Y

upvoted 6 times

chaoscreater Most Recent 3 weeks, 6 days ago

Answer is YYY.

The key sentence is this - "The Mark devices with no compliance policy assigned as setting is set to Compliant."

Device2 is Win10 and the only policy that applies to Win10 is DevicePolicy2. DevicePolicy2 includes GroupB but excludes GroupC. Device2 is part of both GroupB and GroupC and because of the GroupC exclusion, the policy doesn't apply to it.

Device5 is iOS. None of the policies apply to iOS, so nothing applies to Device5.

Device6 is Win10. It is not part of any group. All the policies are targeted to a specific group. Policy doesn't apply to Device6 here.

upvoted 3 times

Fala_Fel 2 weeks, 2 days ago

agreed. Y Y Y Good explanation.

upvoted 1 times

ThBEST 1 month, 3 weeks ago

The given answer is correct Y-N-Y, Device5 is non-compliant because it is not encrypted which is required by DevicePolicy2 and DevicePolicy3. And although DevicePolicy1 include Group C and does not exclude any other group Device5 is non-compliant with this policy because it is an iOS device. So because of this I believe Device5 is a no.

upvoted 1 times

mroczyslaw 1 month, 3 weeks ago

First of all, Device5 has nothing to DevicePolicy2, only DevicePolicy3 is applicable (for GroupA, which is member of). Secundo - Device5 is iOS, but DevicePolicy3 is for Android, so doesn't do anything. Device is compliant.
YYY

upvoted 1 times

tarunkantimondal 1 month, 4 weeks ago

All will Yes .

upvoted 1 times

Cbruce 1 month, 4 weeks ago

I agree YYY, Device 5 is IOS and added to a group that is for android devices. It will do nothing to the device when trying to apply the policy because it's not the right OS to apply. It doesn't make it non-compliant because someone added an IOS device to an Android group.

upvoted 3 times

MikeSA 4 months ago

I would say yes for all too. iOS has no policy so Device5 is marked as compliant due to 'The Mark devices with no compliance policy assigned as setting is set to Compliant.'

upvoted 4 times

prats005 4 months ago

Can someone explain which policy is applied on device 6?

upvoted 1 times

Rockalm 3 months, 1 week ago

device 6 is in no group, so no policy is applied.

Question #2 *Topic 11*

Introductory Info

This is a case study. Case studies are not timed separately. You can use as much exam time as you would like to complete each case. However, there may be additional case studies and sections on this exam. You must manage your time to ensure that you are able to complete all questions included on this exam in the time provided.

To answer the questions included in a case study, you will need to reference information that is provided in the case study. Case studies might contain exhibits and other resources that provide more information about the scenario that is described in the case study. Each question is independent of the other questions in this case study.

At the end of this case study, a review screen will appear. This screen allows you to review your answers and to make changes before you move to the next section of the exam. After you begin a new section, you cannot return to this section.

To start the case study -

To display the first question in this case study, click the Next button. Use the buttons in the left pane to explore the content of the case study before you answer the questions. Clicking these buttons displays information such as business requirements, existing environment, and problem statements. If the case study has an

All Information tab, note that the information displayed is identical to the information displayed on the subsequent tabs. When you are ready to answer a question, click the Question button to return to the question.

Overview -

Contoso, Ltd. is a consulting company that has a main office in Montreal and two branch offices in Seattle and New York.

The company has the offices shown in the following table.

Location	Employees	Laptops	Desktop computers	Mobile devices
Montreal	2,500	2,800	300	3,100
Seattle	1,000	1,100	200	1,500
New York	300	320	30	400

Contoso has IT, human resources (HR), legal, marketing, and finance departments. Contoso uses Microsoft 365.

Existing Environment -

Infrastructure -

The network contains an Active Directory domain named contoso.com that is synced to a Microsoft Azure Active Directory (Azure AD) tenant.

Password writeback is enabled.

The domain contains servers that run Windows Server 2016. The domain contains laptops and desktop computers that run Windows 10 Enterprise.

Each client computer has a single volume.

Each office connects to the Internet by using a NAT device. The offices have the IP addresses shown in the following table.

Location	IP address space	Public NAT segment
Montreal	10.10.0.0/16	190.15.1.0/24
Seattle	172.16.0.0/16	194.25.2.0/24
New York	192.168.0.0/16	198.35.3.0/24

Named locations are defined in Azure AD as shown in the following table.

Name	IP address range	Trusted
Montreal	10.10.0.0/16	Yes
New York	192.168.0.0/16	No

From the Multi-Factor Authentication page, an address space of 198.35.3.0/24 is defined in the trusted IPs list.

Azure Multi-Factor Authentication (MFA) is enabled for the users in the finance department.

The tenant contains the users shown in the following table.

Name	User type	City	Role
User1	Member	Seattle	*None*
User2	Member	Sea	Password administrator
User3	Member	SEATTLE	*None*
User4	Guest	SEA	*None*
User5	Member	London	*None*
User6	Member	London	Customer LockBox Access Approver
User7	Member	Sydney	Reports reader
User8	Member	Sydney	User administrator
User9	Member	Montreal	*None*

The tenant contains the groups shown in the following table.

Name	Group type	Dynamic membership rule
ADGroup1	Security	user.city -contains "SEA"
ADGroup2	Office 365	user.city -match "Sea*"

Customer Lockbox is enabled in Microsoft 365.

Microsoft Endpoint Manager Configuration

The devices enrolled in Microsoft Endpoint Manager are configured as shown in the following table.

Name	Platform	Encryption	Member of
Device1	Android	Disabled	GroupA, GroupC
Device2	Windows 10	Enabled	GroupB, GroupC
Device3	Android	Disabled	GroupB, GroupC
Device4	Windows 10	Disabled	GroupB
Device5	iOS	*Not applicable*	GroupA
Device6	Windows 10	Enabled	*None*

The device compliance policies in Microsoft Endpoint Manager are configured as shown in the following table.

Name	Platform	Encryption	Assigned
DevicePolicy1	Android	Not configured	Yes
DevicePolicy2	Windows 10	Required	Yes
DevicePolicy3	Android	Required	Yes

The device compliance policies have the assignments shown in the following table.

Name	Include	Exclude
DevicePolicy1	GroupC	*None*
DevicePolicy2	GroupB	GroupC
DevicePolicy3	GroupA	*None*

The Mark devices with no compliance policy assigned as setting is set to Compliant.

Requirements -

Technical Requirements -

Contoso identifies the following technical requirements:

Use the principle of least privilege

Enable User1 to assign the Reports reader role to users

Ensure that User6 approves Customer Lockbox requests as quickly as possible

Ensure that User9 can enable and configure Azure AD Privileged Identity Management

Question

HOTSPOT -

Which policies apply to which devices? To answer, select the appropriate options in the answer area.

NOTE: Each correct selection is worth one point.

Hot Area:

Answer Area

DevicePolicy1:	None Device1 only Device3 only Device2 and Device3 only Device1 and Device3 only Device1, Device2, and Device3
DevicePolicy2:	None Device4 only Device2 and Device4 only Device2, Device3, and Device 4 only

Rockalm Highly Voted 3 months, 1 week ago
The question is : "Which policies APPLY to which devices?" So the answers are correct.
upvoted 7 times

mroczyslaw Most Recent 1 month, 3 weeks ago
DevicePolicy1: GroupC but only Android devices = Device1 and Device3 (Device2 not because of Windows10)
DevicePolicy2: GroupB but not GroupC (excluding) +and only Windows10 devices = Device4 only
upvoted 2 times

M3ridi3n 1 month, 2 weeks ago
but Device 4 has it's encryption DISABLED !
upvoted 1 times

Fala_Fel 2 weeks, 2 days ago
As far as I understand. Device 4 has the policy applied, which means encryption is checked, it is disabled therefore Device4 is non compliant, but the policy is still applied. That's how it was found to be none compliant.
upvoted 2 times

Kalzonee3611 2 months, 3 weeks ago
It says requires encryption right? How is it device 4?
upvoted 4 times

Sethoo 4 months, 1 week ago
I would think the answer to the second part will be none
upvoted 2 times

w00t 4 months, 1 week ago
Policy2 = Device 2 I believe...

encryption is DISABLED on device4 - Policy2 requires encryption to be enabled.
Device 2 = Windows 10, ENABLED encryption, GROUP B (and C, but Group C is excluded).
upvoted 4 times

chaoscreater 3 weeks, 6 days ago
Nope. "The question is : Which policies APPLY to which devices?", not "Which device is COMPLIANT". Policy can apply to devices and whether they are compliant or not is another matter.
upvoted 2 times

Topic 12 - Testlet 7

upvoted 4 times

Kalzonee3611 2 months, 2 weeks ago
How? How is device4 compliant?
upvoted 1 times

chaoscreater 3 weeks, 6 days ago
Doesn't matter if it's comliant. "The question is : "Which policies APPLY to which devices?" So the answers are correct."
upvoted 1 times

Question #1 *Topic 12*

Introductory Info

This is a case study. Case studies are not timed separately. You can use as much exam time as you would like to complete each case. However, there may be additional case studies and sections on this exam. You must manage your time to ensure that you are able to complete all questions included on this exam in the time provided.

To answer the questions included in a case study, you will need to reference information that is provided in the case study. Case studies might contain exhibits and other resources that provide more information about the scenario that is described in the case study. Each question is independent of the other questions in this case study.

At the end of this case study, a review screen will appear. This screen allows you to review your answers and to make changes before you move to the next section of the exam. After you begin a new section, you cannot return to this section.

To start the case study -

To display the first question in this case study, click the Next button. Use the buttons in the left pane to explore the content of the case study before you answer the questions. Clicking these buttons displays information such as business requirements, existing environment, and problem statements. If the case study has an All Information tab, note that the information displayed is identical to the information displayed on the subsequent tabs. When you are ready to answer a question, click the Question button to return to the question.

Overview -

Fabrikam, Inc. is manufacturing company that sells products through partner retail stores. Fabrikam has 5,000 employees located in offices throughout Europe.

Existing Environment -

Network Infrastructure -

The network contains an Active Directory forest named fabrikam.com. Fabrikam has a hybrid Microsoft Azure Active Directory (Azure AD) environment.

The company maintains some on-premises servers for specific applications, but most end-user applications are provided by a Microsoft 365 E5 subscription.

Problem Statements -

Fabrikam identifies the following issues:

Since last Friday, the IT team has been receiving automated email messages that contain "Unhealthy Identity Synchronization Notification" in the subject line.

Several users recently opened email attachments that contained malware. The process to remove the malware was time consuming.

Requirements -

Planned Changes -

Fabrikam plans to implement the following changes:

Fabrikam plans to monitor and investigate suspicious sign-ins to Active Directory

Fabrikam plans to provide partners with access to some of the data stored in Microsoft 365

Application Administration -

Fabrikam identifies the following application requirements for managing workload applications:

User administrators will work from different countries

User administrators will use the Azure Active Directory admin center

Two new administrators named Admin1 and Admin2 will be responsible for managing Microsoft Exchange Online only

Security Requirements -

Fabrikam identifies the following security requirements:

Access to the Azure Active Directory admin center by the user administrators must be reviewed every seven days. If an administrator fails to respond to an access request within three days, access must be removed

Users who manage Microsoft 365 workloads must only be allowed to perform administrative tasks for up to three hours at a time. Global administrators must be exempt from this requirement

Users must be prevented from inviting external users to view company data. Only global administrators and a user named User1 must be able to send invitations

Azure Advanced Threat Protection (ATP) must capture security group modifications for sensitive groups, such as Domain Admins in Active Directory

Workload administrators must use multi-factor authentication (MFA) when signing in from an anonymous or an unfamiliar location

The location of the user administrators must be audited when the administrators authenticate to Azure AD

Email messages that include attachments containing malware must be delivered without the attachment

The principle of least privilege must be used whenever possible

Question

You need to recommend a solution that meets the technical and security requirements for sharing data with the partners.

What should you include in the recommendation? Each correct answer presents part of the solution.

NOTE: Each correct selection is worth one point.

A. Create an access review

B. Assign the Global administrator role to User1

C. Assign the Guest inviter role to User1

D. Modify the External collaboration settings in the Azure Active Directory admin center

kiketxu Highly Voted 4 months, 3 weeks ago

This is correct.

upvoted 6 times

Topic 13 - Testlet 8

Question #1 *Topic 13*

Introductory Info

This is a case study. Case studies are not timed separately. You can use as much exam time as you would like to complete each case. However, there may be additional case studies and sections on this exam. You must manage your time to ensure that you are able to complete all questions included on this exam in the time provided.

To answer the questions included in a case study, you will need to reference information that is provided in the case study. Case studies might contain exhibits and other resources that provide more information about the scenario that is described in the case study. Each question is independent of the other questions in this case study.

At the end of this case study, a review screen will appear. This screen allows you to review your answers and to make changes before you move to the next section of the exam. After you begin a new section, you cannot return to this section.

To start the case study -

To display the first question in this case study, click the Next button. Use the buttons in the left pane to explore the content of the case study before you answer the questions. Clicking these buttons displays information such as business requirements, existing environment, and problem statements. If the case study has an

All Information tab, note that the information displayed is identical to the information displayed on the subsequent tabs. When you are ready to answer a question, click the Question button to return to the question.

Overview -

Contoso, Ltd. is a consulting company that has a main office in Montreal and two branch offices in Seattle and New York.

The company has the offices shown in the following table.

Location	Employees	Laptops	Desktop computers	Mobile devices
Montreal	2,500	2,800	300	3,100
Seattle	1,000	1,100	200	1,500
New York	300	320	30	400

Contoso has IT, human resources (HR), legal, marketing, and finance departments. Contoso uses Microsoft 365.

Existing Environment -

Infrastructure -

The network contains an Active Directory domain named contoso.com that is synced to a Microsoft Azure Active Directory (Azure AD) tenant.

Password writeback is enabled.

The domain contains servers that run Windows Server 2016. The domain contains laptops and desktop computers that run Windows 10 Enterprise.

Each client computer has a single volume.

Each office connects to the Internet by using a NAT device. The offices have the IP addresses shown in the following table.

Location	IP address space	Public NAT segment
Montreal	10.10.0.0/16	190.15.1.0/24
Seattle	172.16.0.0/16	194.25.2.0/24
New York	192.168.0.0/16	198.35.3.0/24

Named locations are defined in Azure AD as shown in the following table.

Name	IP address range	Trusted
Montreal	10.10.0.0/16	Yes
New York	192.168.0.0/16	No

From the Multi-Factor Authentication page, an address space of 198.35.3.0/24 is defined in the trusted IPs list.

Azure Multi-Factor Authentication (MFA) is enabled for the users in the finance department.

The tenant contains the users shown in the following table.

Name	User type	City	Role
User1	Member	Seattle	*None*
User2	Member	Sea	Password administrator
User3	Member	SEATTLE	*None*
User4	Guest	SEA	*None*
User5	Member	London	*None*
User6	Member	London	Customer LockBox Access Approver
User7	Member	Sydney	Reports reader
User8	Member	Sydney	User administrator
User9	Member	Montreal	*None*

The tenant contains the groups shown in the following table.

Name	Group type	Dynamic membership rule
ADGroup1	Security	user.city -contains "SEA"
ADGroup2	Office 365	user.city -match "Sea*"

Customer Lockbox is enabled in Microsoft 365.

Microsoft Endpoint Manager Configuration

The devices enrolled in Microsoft Endpoint Manager are configured as shown in the following table.

Name	Platform	Encryption	Member of
Device1	Android	Disabled	GroupA, GroupC
Device2	Windows 10	Enabled	GroupB, GroupC
Device3	Android	Disabled	GroupB, GroupC
Device4	Windows 10	Disabled	GroupB
Device5	iOS	*Not applicable*	GroupA
Device6	Windows 10	Enabled	*None*

The device compliance policies in Microsoft Endpoint Manager are configured as shown in the following table.

Name	Platform	Encryption	Assigned
DevicePolicy1	Android	Not configured	Yes
DevicePolicy2	Windows 10	Required	Yes
DevicePolicy3	Android	Required	Yes

The device compliance policies have the assignments shown in the following table.

Name	Include	Exclude
DevicePolicy1	GroupC	*None*
DevicePolicy2	GroupB	GroupC
DevicePolicy3	GroupA	*None*

The Mark devices with no compliance policy assigned as setting is set to Compliant.

Requirements -

Technical Requirements -

Contoso identifies the following technical requirements:

Use the principle of least privilege

Enable User1 to assign the Reports reader role to users

Ensure that User6 approves Customer Lockbox requests as quickly as possible

Ensure that User9 can enable and configure Azure AD Privileged Identity Management

Question

What should User6 use to meet the technical requirements?

A. Supervision in the Security & Compliance admin center

B. Service requests in the Microsoft 365 admin center

C. Security & privacy in the Microsoft 365 admin center

D. Data subject requests in the Security & Compliance admin center

tarunkantimondal 1 month, 4 weeks ago

Answer is right

upvoted 1 times

arunjana 2 months, 2 weeks ago

Microsoft 365 Admin Center > Support > Customer Lockbox Requests

Customer lockbox approver role has to be assigned for User6 as mentioned by kiketxu

upvoted 2 times

kiketxu 4 months, 3 weeks ago

this answer is right, but don't expect to see this in the exam as this role has change to:
https://techcommunity.microsoft.com/t5/microsoft-security-and/customer-lockbox-approver-role-now-available/ba-p/223393

https://docs.microsoft.com/en-us/microsoft-365/admin/add-users/azure-ad-roles-in-the-mac?view=o365-worldwide

upvoted 4 times