Question #1 *Topic 1*

You have several Conditional Access policies that block noncompliant devices from connecting to services.
You need to identify 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 portal

D. Audit logs in the Azure Active Directory admin center

Suggested Answer: *B*
Reference:
https://docs.microsoft.com/en-us/azure/active-directory/conditional-access/troubleshoot-conditional-access

Community vote distribution

B (100%)

examdog 2 years ago

Selected Answer: B

AAD > Monitoring > Sign-in logs

upvoted 4 times

mohamed_Saed 2 years, 2 months ago

Selected Answer: B

B is correct!

upvoted 4 times

pete26 2 years, 3 months ago

Selected Answer: B

B is correct!

upvoted 4 times

NOC_NWDMICROAGE 2 years, 3 months ago

Azure AD under Sign-in logs.

B is the correct answer

upvoted 3 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

Suggested Answer: *B*

Community vote distribution

B (100%)

AmerSerhan Highly Voted 4 years, 8 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 35 times

doublekill Highly Voted 3 years, 10 months 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 8 times

Jonclark Most Recent 1 year, 10 months ago

Selected Answer: B

B is correct.

App and attribute filtering in Azure AD connect lets you control which objects will sync from your on-premises Active Directory to your new Azure Active Directory.
https://learn.microsoft.com/en-us/azure/active-directory/hybrid/how-to-connect-sync-configure-filtering

This does not meet the requirement. The correct solution is to enable password hash sync.

Leaked credential detection is done by trying a list of known-exposed credentials against your users' password hashes to discover one being used in your directory. It's done in Azure, so unless you sync password hashes into Azure AD, the service has nothing to check against.
https://learn.microsoft.com/en-us/azure/active-directory/identity-protection/concept-identity-protection-risks#password-hash-synchronization

upvoted 2 times

uchii 1 year, 11 months ago

Selected Answer: B

B is correct

upvoted 1 times

sami0712 2 years ago

B is correct

upvoted 1 times

mohamed_Saed 2 years, 2 months ago

Selected Answer: B

B is correct!

upvoted 1 times

Eltooth 2 years, 5 months ago

Selected Answer: B

B is correct answer.

upvoted 1 times

arska 2 years, 9 months ago

Selected Answer: B

No, since at least Password Hash Synchronization is required.

upvoted 1 times

Ferrix 2 years, 10 months ago

Selected Answer: B

corret

upvoted 1 times

mkoprivnj 3 years, 1 month ago

Selected Answer: B

https://docs.microsoft.com/en-us/answers/questions/391883/why-leaked-credentials-is-supported-only-in-azure.html

upvoted 1 times

MikeMatt2020 3 years, 4 months ago

Password Hash Sync is REQUIRED.

Straight from Microsoft documentation:
"Risk detections like leaked credentials require the presence of password hashes for detection to occur"
https://docs.microsoft.com/en-us/azure/active-directory/identity-protection/concept-identity-protection-risks#common-questions

upvoted 6 times

rkapoor8855 3 years, 11 months ago

The answer is NO

upvoted 2 times

svm_Terran 4 years ago

given asnwer is correct.

upvoted 2 times

kiketxu 3 years, 10 months ago

The answer is NO

upvoted 2 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

Suggested Answer: *A*

References:

https://docs.microsoft.com/en-us/azure/security/azure-ad-secure-steps

Community vote distribution

A (100%)

KeepingITreal Highly Voted 4 years, 8 months ago

Leaked credentials detection in Azure AD Identity Protection requires Password Hash Sync enabled in Azure AD Connect

upvoted 37 times

m2L Highly Voted 4 years, 11 months ago

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

upvoted 9 times

Jonclark Most Recent 1 year, 10 months ago

Selected Answer: A

Answer is correct: Enabling PHS will meet the requirement.

Leaked credential detection is done by trying a list of known-exposed credentials against your users' password hashes to discover one being used in your directory. It's done in Azure, so unless you sync password hashes into Azure AD, the service has nothing to check against.

https://learn.microsoft.com/en-us/azure/active-directory/identity-protection/concept-identity-protection-risks#password-hash-synchronization

upvoted 1 times

hb0011 1 year, 11 months ago

Why are so many people saying Yes? It clearly says hash sync is disabled! Answer is a resounding NO!

upvoted 1 times

hb0011 1 year, 11 months ago

My bad. Needed to read the solution. Carry on. It's YES.

upvoted 1 times

NarenKA 2 years, 4 months ago

A is correct answer. Password Hash Sync needs to be enabled in Azure AD Connect

upvoted 1 times

Eltooth 2 years, 5 months ago

Selected Answer: A

A is correct answer.

upvoted 1 times

arska 2 years, 9 months ago

Selected Answer: A

Yes, since the use of leaked credentials detection need Password Hash Sync.

upvoted 1 times

mkoprivnj 3 years, 1 month ago

Selected Answer: A

Leaked credentials detection in Azure AD Identity Protection requires Password Hash Sync enabled in Azure AD Connect

upvoted 2 times

kobura7 3 years, 1 month ago

Which answer is correct, A or B?

upvoted 1 times

Chris_Rock 3 years, 3 months ago

Given answer is correct. YES PHS is needed

upvoted 2 times

[Removed] 3 years, 4 months ago

the answer is A. Yes.

It is explained in this article, as previously mentioned by m2L.

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

upvoted 3 times

PrimeAltariz 3 years, 7 months 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 2 times

kiketxu 3 years, 10 months 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** 3 years, 9 months ago
>
> You need to ENABLE not modify settings....
>
> upvoted 2 times
>
> > **bingomutant** 3 years, 9 months ago
> >
> > agree - modify does not necessarily mean Enable...
> >
> > upvoted 1 times
> >
> > > **prats005** 3 years, 9 months ago
> > >
> > > what else could it mean?
> > >
> > > upvoted 2 times
> > >
> > > > **chaoscreater** 3 years, 6 months ago
> > > >
> > > > I guess people are now taking a strict englisn exam rather than an IT exam
> > > >
> > > > upvoted 5 times
> > >
> > > **llama321** 3 years, 7 months ago
> > >
> > > It has either enable or disable. Now its in disable state and modify mean enable. What else it could be? half enable?
> > >
> > > upvoted 5 times

kmsrajan 3 years, 10 months ago

Answer is no because Leaked credential detection need Password Hash sync enabled

upvoted 2 times

doublekill 3 years, 10 months ago

The answer is NO

upvoted 1 times

⊟ **AshTac** 3 years, 11 months ago

You would need to enable PHS for that..

upvoted 1 times

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

The answer is No, Correct.

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

Suggested Answer: *B*

Community vote distribution

B (100%)

O365_dude Highly Voted 4 years, 12 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 22 times

jaber1986 3 years, 4 months ago

so, the answer ist correct. B.

upvoted 1 times

CWT Highly Voted 5 years, 1 month 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

NarenKA Most Recent 2 years, 4 months ago

B is correct answer.

upvoted 1 times

Eltooth 2 years, 5 months ago

Selected Answer: B

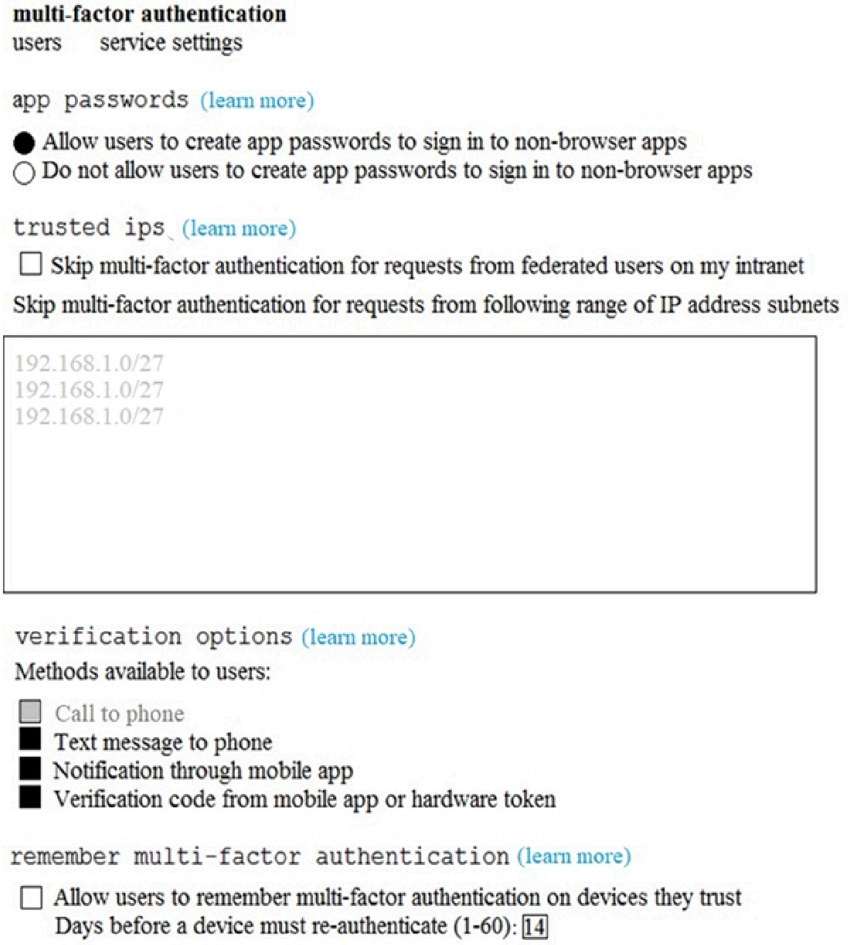
B is correct answer.

upvoted 1 times

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)

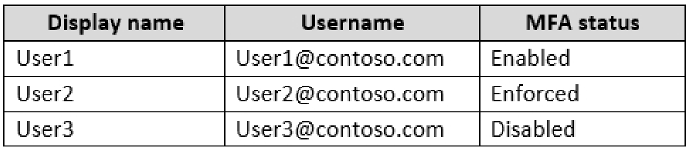
Methods available to users:

☐ 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.

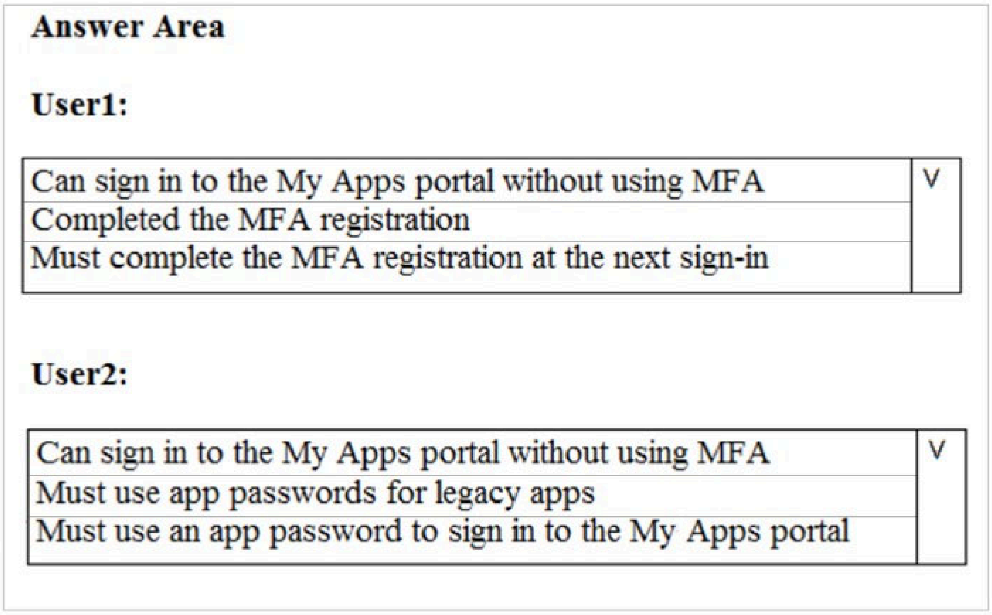


Display name	Username	MFA status
User1	User1@contoso.com	Enabled
User2	User2@contoso.com	Enforced
User3	User3@contoso.com	Disabled

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

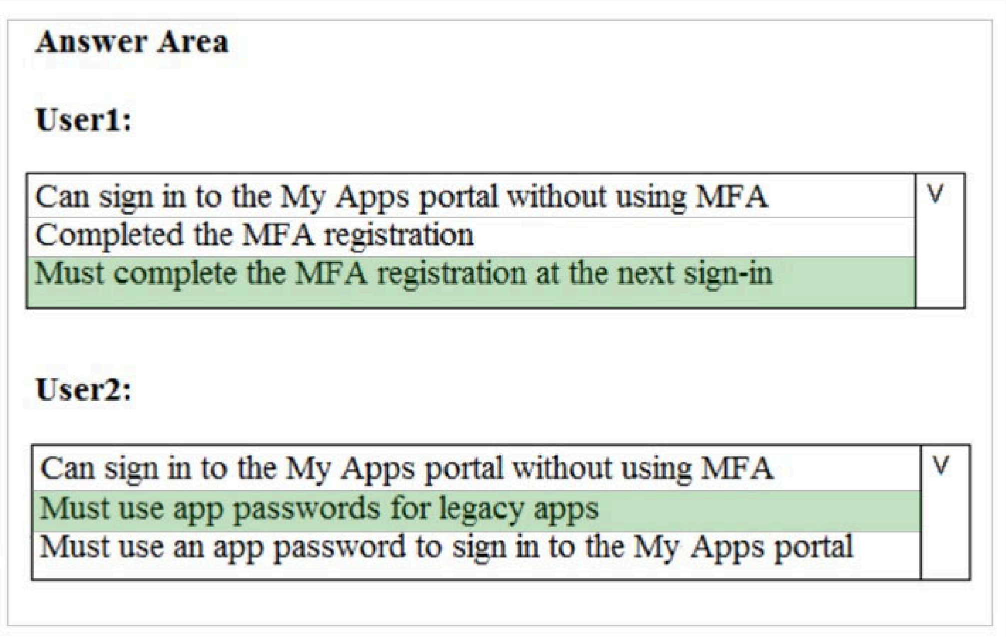
User1:

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	

Suggested Answer:



Answer Area

User1:

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

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

Jonclark 1 year, 10 months ago

Answer is correct.
User 1 was enabled for MFA but has not registered yet, so they will get prompted to set it up.
User 2 is set for enforced MFA, so apps that do not support modern auth will not work until an app password is set up and used.

Enabled: The user has been enrolled in Multi-Factor Authentication but has not completed the registration yet. The next time they log in with a modern auth enabled client or browser, they will be prompted to set it up. In the meantime, apps which do not support MFA will continue to allow sign-in.

Enforced: The user completed the registration OR an admin manually set this status and the user be prompted to register at next sign-on with an app that supports modern auth or a browser. The user will not be able to use apps that do not support modern auth until app passwords are created and used.

NOTE: you can also enforce these through conditional access policies. A user with a "disabled" MFA status can still be required to use MFA.

upvoted 2 times

examdog 2 years ago

User 2 must use the app password because non-browser/legacy app does not work with MFA. https://learn.microsoft.com/en-us/azure/active-directory/authentication/howto-mfa-app-passwords#allow-users-to-create-app-passwords

upvoted 1 times

Darsh3005 2 years, 3 months ago

User 2 state of MFA is Enforce Hence

Enforced The user is enrolled per-user in Azure AD Multi-Factor Authentication. If the user hasn't yet registered authentication methods, they receive a prompt to register the next time they sign in using modern authentication (such as via a web browser). Users who complete registration while in the Enabled state are automatically moved to the Enforced state.

Yes. Apps require app passwords.

upvoted 3 times

Darsh3005 2 years, 3 months ago

User 1 state is enabled : Hence The user is enrolled in per-user Azure AD Multi-Factor Authentication, but can still use their password for legacy authentication. If the user hasn't yet registered MFA authentication methods, they receive a prompt to register the next time they sign in using modern authentication (such as via a web browser).

upvoted 4 times

hadiwijaya 2 years ago

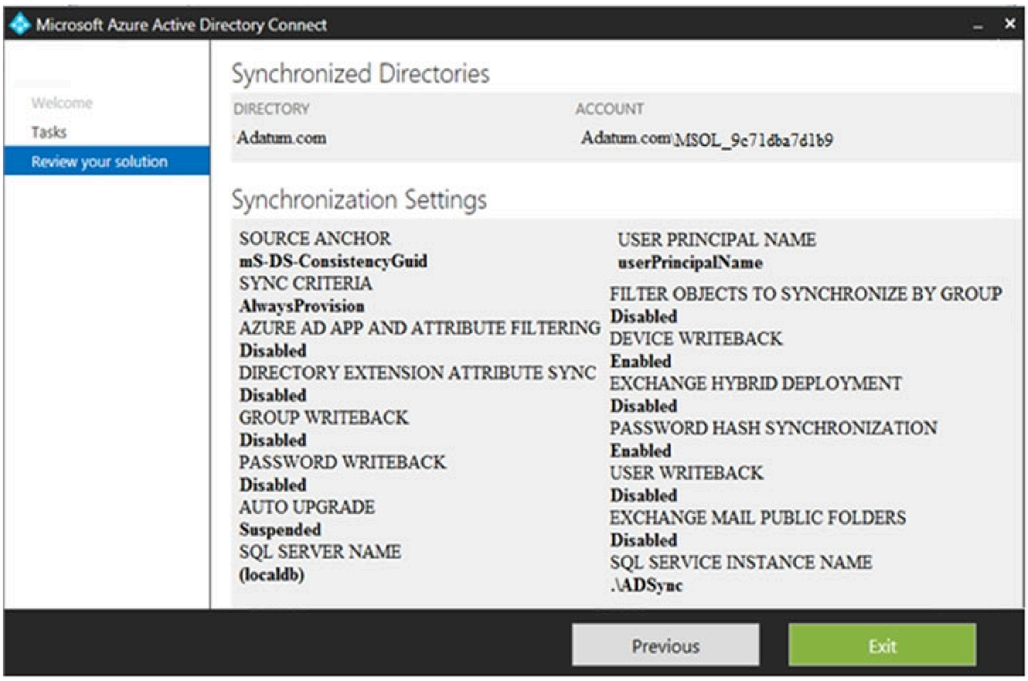
I Agree

upvoted 2 times

Question #6 — Topic 1

HOTSPOT -

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



Synchronized Directories

DIRECTORY	ACCOUNT
Adatum.com	Adatum.com\MSOL_9c71dba7d1b9

Synchronization Settings

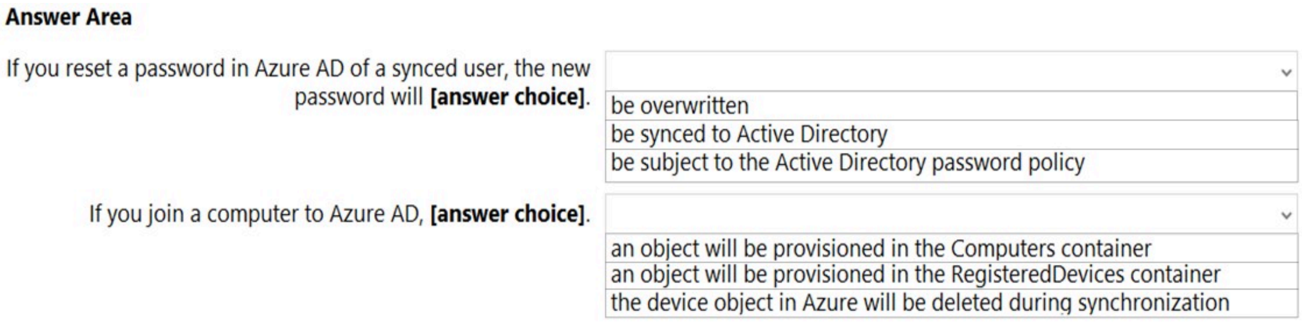
SOURCE ANCHOR
mS-DS-ConsistencyGuid
SYNC CRITERIA
AlwaysProvision
AZURE AD APP AND ATTRIBUTE FILTERING
Disabled
DIRECTORY EXTENSION ATTRIBUTE SYNC
Disabled
GROUP WRITEBACK
Disabled
PASSWORD WRITEBACK
Disabled
AUTO UPGRADE
Suspended
SQL SERVER NAME
(localdb)

USER PRINCIPAL NAME
userPrincipalName
FILTER OBJECTS TO SYNCHRONIZE BY GROUP
Disabled
DEVICE WRITEBACK
Enabled
EXCHANGE HYBRID DEPLOYMENT
Disabled
PASSWORD HASH SYNCHRONIZATION
Enabled
USER WRITEBACK
Disabled
EXCHANGE MAIL PUBLIC FOLDERS
Disabled
SQL SERVICE INSTANCE NAME
.\ADSync

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

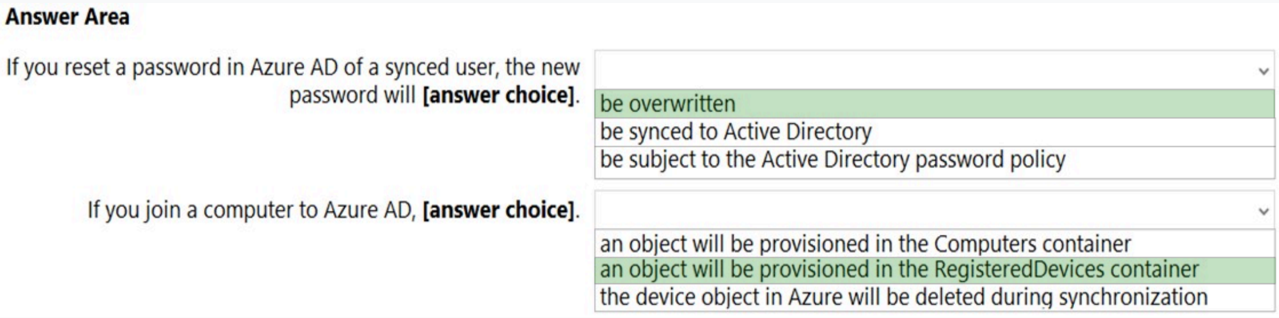
If you reset a password in Azure AD of a synced user, the new password will **[answer choice]**.

- be overwritten
- 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
- an object will be provisioned in the RegisteredDevices container
- the device object in Azure will be deleted during synchronization

Suggested Answer:



Answer Area

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

- [✓ be overwritten]
- 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
- [✓ an object will be provisioned in the RegisteredDevices container]
- the device object in Azure will be deleted during synchronization

Reference:

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

Jonclark Highly Voted 1 year, 10 months ago

The key parameters for this question are:

Password Writeback, Password Hash Sync and Device Writeback.

Password writeback is disabled. This means that the new password change in Azure AD will not synchronize back to the on-premises AD. Password hash sync is enabled. This means that the original password, still in the on-premises AD, will synchronize to Azure AD (in other words, the change is overwritten).

Because device writeback is enabled, a computer joined to Azure AD will be synchronized to the on-premises AD. Joining a computer to Azure AD does not create a full computer object in the on-premises domain, so it goes into the RegisteredDevices, not the Computers container.

upvoted 11 times

⊟ **Dan91** Highly Voted 2 years, 3 months ago

1. be overwritten until the password is changed again on-prem
2. Object will be provisioned in the RegisteredDevices container

https://docs.microsoft.com/en-us/azure/active-directory/hybrid/how-to-connect-password-hash-synchronization#:~:text=An%20administrator%20can,manually%20updated%20password.

upvoted 6 times

⊟ **NOC_NWDMICROAGE** Most Recent 2 years, 3 months ago

What does it mean by password "be overwritten"? Does it mean there will be a mismatch in the user's password between Cloud and the on-prem environment?

upvoted 4 times

⊟ **Peeeedor** 2 years ago

I assume this means the password that you reset in AAD will be overwritten by the password that has been set in your on prem ADDS. Also because password writeback is set to off in AD connect. Please correct me if I am wrong. :)

upvoted 3 times

⊟ **Perycles** 1 year, 10 months ago

When Password writeback is set to OFF, we have a message in Azure AD that says "unfortunatly, you can't reset password for this user because Pasword Writback is disabled on your tenant..." when we try to reset password. So it's no possible to set a new Azure AD Password.

upvoted 1 times

⊟ **Perycles** 1 year, 10 months ago

some modifications about the informations "sync User":

- if user is an Azure AD User Sync to AD > Reset Password is possible when Password Writeback is set to OFF

- if user is an AD User Sync to AAD > Reset Password is NOT possible when Password Writeback is set to OFF

just tested on my lab

upvoted 2 times

⊟ **pete26** 2 years, 4 months ago

1. Be overwritten
2. An object will be provisioned in the registeredDevices container

upvoted 3 times

⊟ **stewie055** 2 years, 4 months ago

is the second answer right ? The device is joined, not registered. It should be in computer container, shound't it ?

upvoted 2 times

⊟ **xyz213** 2 years, 3 months ago

It is correct.
The device is joined in Azure AD not the local AD. Gets synced down to the local AD because "Device writeback" is enabled.

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

upvoted 4 times

⊟ **amiban** 1 year, 11 months ago

Right it will be using the device writeback and it will be synced to the registered devices container only.

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 Endpoint Manager.
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

Suggested Answer: *A*
Reference:
https://docs.microsoft.com/en-us/windows-server/remote/remote-access/vpn/ad-ca-vpn-connectivity-windows10

Community vote distribution
A (86%) 14%

paulfns2020 Highly Voted 👍 4 years, 7 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 47 times

Bl0ckSh3ll 4 years, 3 months 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 7 times

kiketxu 3 years, 10 months ago
You right,thankies!
upvoted 3 times

itmp Highly Voted 👍 4 years, 8 months ago
You create the certificate here:
portal.azure.com/#blade/Microsoft_AAD_IAM/ConditionalAccessBlade/Vpn
upvoted 8 times

pompes Most Recent ◷ 1 year, 7 months ago
Was on the exam. I scored 816
upvoted 3 times

panda0107 1 year, 9 months ago
Selected Answer: A
Once a VPN certificate is created in the Azure portal, Azure AD will start using it immediately to issue short lived certificates to the VPN client.
upvoted 1 times

keithtemplin 1 year, 10 months ago
Selected Answer: C
The task is to "Create a conditional Access Policy" so the only answer that makes sense is C "Dynamic Access Control Policy"
upvoted 1 times

Jonclark 1 year, 10 months ago
Selected Answer: A
Agreed with others and adding a little more info. To create the VPN certificate, here's where you go:
In Azure AD Admin center, go to Security -> Conditional Access -> VPN Connectivity.

Here you will find a list of existing certificates and an option to create a new one. There is a link to the latest documentation on how to set up VPN for conditional access as well as this important warning:
"Once a VPN certificate is created in the Azure portal, Azure AD will start using it immediately to issue short lived certificates to the VPN client. It is critical that the VPN certificate be deployed immediately to the VPN server to avoid any issues with credential validation of the VPN client."
upvoted 3 times

Eltooth 2 years, 5 months ago

Selected Answer: A

A is correct answer.
upvoted 1 times

mkoprivnj 3 years, 1 month ago

Selected Answer: A

A is correct. See Paulfns explanation.
upvoted 1 times

Robert__Susin 3 years, 8 months 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 2 times

svm_Terran 4 years ago

this is correct.
upvoted 2 times

MSOffice 4 years, 3 months 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

Robert__Susin 3 years, 8 months 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 2 times

VTHAR 4 years, 3 months 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 8 times

junkz 4 years, 6 months 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 4 times

Prianishnikov 4 years, 4 months ago

https://docs.microsoft.com/en-us/windows-server/remote/remote-access/vpn/ad-ca-vpn-connectivity-windows10
upvoted 2 times

Robert__Susin 3 years, 8 months 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 2 times

⊟ **Guilherme** 4 years, 11 months ago

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

upvoted 7 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. Microsoft 365 Defender

B. Azure Active Directory

C. Microsoft Defender for Identity

D. Microsoft Defender for Cloud Apps

Suggested Answer: *B*

Community vote distribution

B (100%)

pete26 Highly Voted 👍 2 years, 3 months ago

Selected Answer: B

You can view the Role permissions either from Microsoft 365 Admin Center OR Azure Active Directory.

upvoted 6 times

pompes Most Recent 🕒 1 year, 7 months ago

Had a question close to that on the exam

upvoted 1 times

amiban 1 year, 11 months ago

Answer is right with option B. However the brief section of Roles can be viewed from MS admin center but detailed description of the Roles is available on the MS Azure Active Directory Admin center.

upvoted 2 times

Dhamus 1 year, 7 months ago

You are right.

upvoted 1 times

hans333 2 years, 1 month ago

old question, view from M365 admin center, or AAD

upvoted 1 times

heshmat2022 2 years, 3 months ago

https://docs.microsoft.com/en-us/azure/active-directory/roles/manage-roles-portal

upvoted 1 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. Microsoft 365 Compliance permissions

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

C. Microsoft Azure AD group management

D. Microsoft 365 user management

Suggested Answer: *B*

Community vote distribution

B (89%) 11%

Patesso 1 year, 7 months ago

Etait a l'examen

upvoted 1 times

pompes 1 year, 7 months ago

correction. Right answer B

upvoted 1 times

pompes 1 year, 7 months ago

Selected Answer: D

Was on the exam

upvoted 1 times

Jonclark 1 year, 10 months ago

Selected Answer: B

The only place you can configure permissions for a specified time period and/or tie an MFA requirement specifically to the use a role is with Privileged Identity Management.

upvoted 2 times

LarryPizzu 2 years ago

Selected Answer: B

That is the correct answer

upvoted 1 times

CertRookie 2 years, 2 months ago

Selected Answer: B

https://learn.microsoft.com/en-us/azure/active-directory/privileged-identity-management/pim-configure#:~:text=Provide%20just%2Din%2Dtime%20privileged%20access%20to%20Azure%20AD%20and%20Azure%20resources

upvoted 1 times

pete26 2 years, 3 months ago

Selected Answer: B

Correct answer is B. “Time-limited permissions” is the key here.

upvoted 4 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 app'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

Suggested Answer: *B*

Community vote distribution

B (100%)

kiketxu Highly Voted 👍 3 years, 9 months 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 25 times

joergsi 2 years, 10 months ago

Following the firrst link you will find:
There are additional benefits to using MDM with App protection policies, and companies can use App protection policies with and without MDM at the same time. For example, consider an employee that uses both a phone issued by the company, and their own personal tablet. The company phone is enrolled in MDM and protected by App protection policies while the personal device is protected by App protection policies only.

upvoted 3 times

DarkAndy Highly Voted 👍 2 years, 6 months ago

Valid on exam. Jun 10, 2022

upvoted 6 times

heshmat2022 Most Recent ⏲ 1 year, 8 months ago

You can use Intune app protection policies independent of any mobile-device management (MDM) solution. This independence helps you protect your company's data with or without enrolling devices in a device management solution. By implementing app-level policies, you can restrict access to company resources and keep data within the purview of your IT department.

upvoted 1 times

heshmat2022 1 year, 8 months ago

B is correct
You can use Intune app protection policies independent of any mobile-device management (MDM) solution. This independence helps you protect your company's data with or without enrolling devices in a device management solution. By implementing app-level policies, you can restrict access to company resources and keep data within the purview of your IT department.

upvoted 1 times

RomanV 1 year, 8 months ago

Option B is the correct answer.

An app protection policy in Microsoft Endpoint Manager can help protect company data by applying data protection policies to apps. With app protection policies, you can apply settings to the Microsoft Power BI app on personal devices to ensure that data is protected. Specifically, you can prevent users from backing up app data to iCloud, while allowing them to access the Power BI data in your tenant.

upvoted 1 times

Jonclark 1 year, 10 months ago

Selected Answer: B

The requirement is specifically about blocking users from backing up data from the app to iCloud. This is accomplished with Intune App protection.

Don't forget, though that app protection does not block these users from logging in with their web browser and copying data out. You can prevent this by adding a conditional access policy which only allows access through the app, which you have protected with your shiny new app protection policy.

upvoted 3 times

Santini 1 year, 10 months ago

lol "which you have protected with your shiny new app protection policy."

upvoted 1 times

ChachaChatra 1 year, 11 months ago

Valid on 28/01/23

upvoted 1 times

pete26 2 years, 2 months ago

Valid on exam October, 14 2022

upvoted 4 times

Daniel830 2 years, 3 months ago

B is the correct answer.

It is not talking about access, so there is no need for a conditional access.

upvoted 1 times

Eltooth 2 years, 5 months ago

Selected Answer: B

B is correct answer.

upvoted 2 times

Ferrix 2 years, 10 months ago

Selected Answer: B

Correct

upvoted 3 times

Fearless90 3 years, 1 month ago

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

App protection policies makes sure that the app-layer protections are in place.

For example, you can:

Require a PIN to open an app in a work context

Control the sharing of data between apps

Prevent the saving of company app data to a personal storage location

upvoted 1 times

mkoprivnj 3 years, 1 month ago

Selected Answer: B

I go with B.

upvoted 2 times

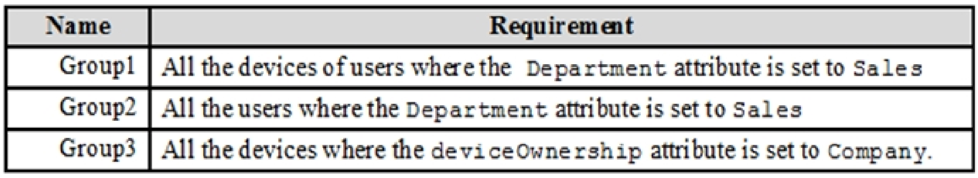
Question #11 Topic 1

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:



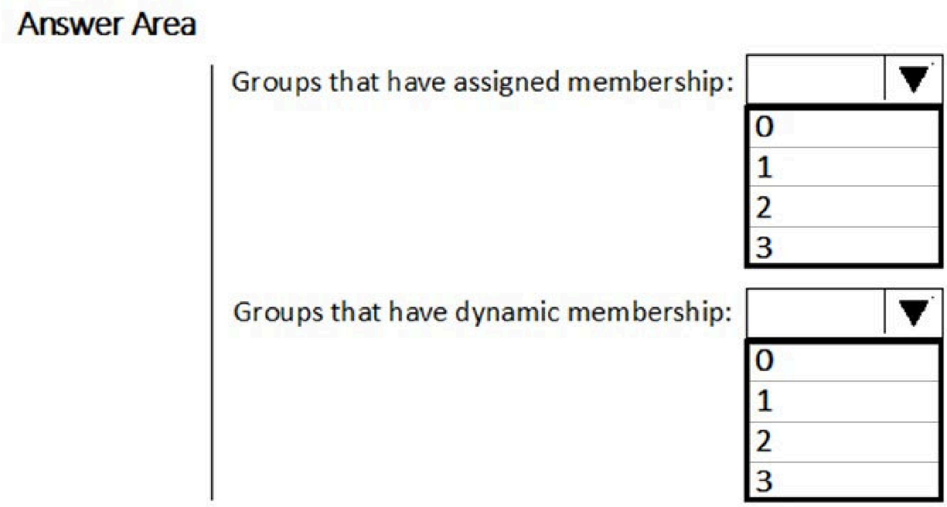
Name	Requirement
Group1	All the devices of users where the `Department` attribute is set to `Sales`
Group2	All the users where the `Department` attribute is set to `Sales`
Group3	All the devices where the `deviceOwnership` attribute is set to `Company`.

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:

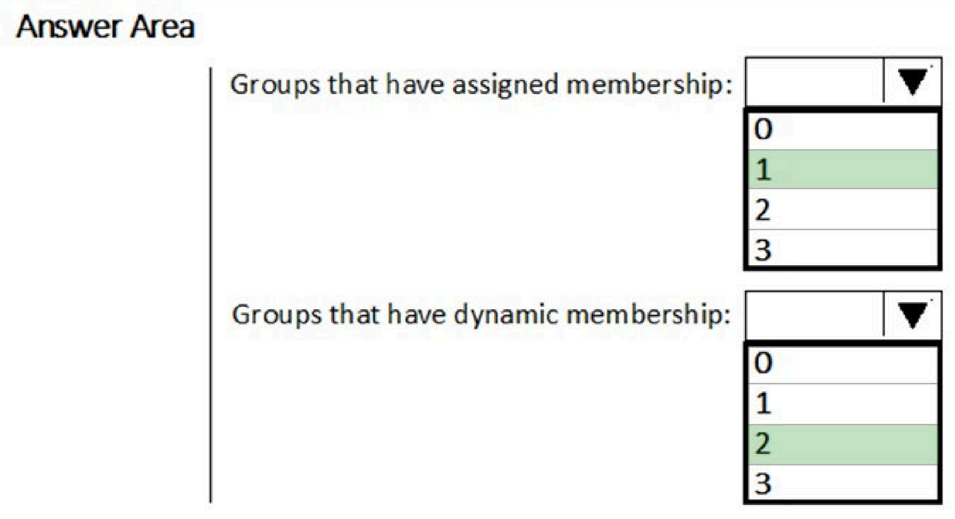


Answer Area

Groups that have assigned membership: ▼
0
1
2
3

Groups that have dynamic membership: ▼
0
1
2
3

Suggested Answer:



Answer Area

Groups that have assigned membership: ▼
0
[✓ 1]
2
3

Groups that have dynamic membership: ▼
0
1
[✓ 2]
3

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.

⊟ kiketxu Highly Voted 3 years, 9 months 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 19 times

Akc0 3 years, 9 months ago

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

upvoted 3 times

galangimani97 3 years, 9 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 6 times

WMG 3 years, 4 months ago

Group 1 is about a _Device Group_ based on _User attributes_. This does not exist as queries currently in the rule builder.

It is doable with an automation script, but that is outside the scope of the question.

upvoted 2 times

Dhamus Most Recent 1 year, 7 months ago

I'm a bit confused, I understand that there are 2 dynamic groups, but why 1 assigned?

They are referring to device only, not users and devices.

upvoted 1 times

Perycles 1 year, 11 months ago

Group 1 : "Assigned" because "department" attribut doesn't exist for device

Groups 2 and 3 : dynamic because "department" attribut exists for user and "DeviceOwnership" attribut exists for device.

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

upvoted 3 times

adarvasi 2 years, 2 months ago

Group 1 = Assigned

Group 2 and 3 = can be added in a single Dynamic rule

(user.department -eq "sales") and (device.deviceOwnership -eq "Company")

So I think the answer

1 Assigned

1 Dynamic

upvoted 1 times

SKam22 2 years, 4 months ago

Goup 1 > You can achieve this by creating assigned membership by manually choosing users and devices that you know belong to the Sale department but because you need to minimize administration efforts then this is out of scope!

Group 2 > Dynamic User

Group 3 > Dynamic Device

So the answers:

Assigned > 0

Dynamic > 2

upvoted 1 times

Whatsamattr81 2 years, 6 months ago

Device Ownership: Create a filter rule based on the device's ownership property in Intune. Select Personal, Corporate, or unknown values using the -eq and -ne operators. You can't create a device group based on ‘Company’. The answer should be 2 assigned, 1 dynamic,

upvoted 2 times

YamaKen 2 years, 9 months ago

"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

mgrcic56 3 years ago

1st: 0

2nd: 3

upvoted 1 times

mkoprivnj 3 years, 1 month ago

1st: one

2nd: two

upvoted 2 times

Fcnet 3 years, 3 months ago

Answer is correct but for detail

the department attribute is a User attribute and not a device attribute

https://docs.microsoft.com/en-us/azure/active-directory-b2c/user-profile-attributes

upvoted 4 times

Xtian_ar 3 years, 6 months ago

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

upvoted 4 times

tarunkantimondal 3 years, 7 months ago

answer is confusing

upvoted 1 times

prats005 3 years, 9 months ago

Answer is correct

upvoted 4 times

prats005 3 years, 9 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 4 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

Suggested Answer: *C*
References:
https://docs.microsoft.com/en-us/azure/active-directory/conditional-access/location-condition

Community vote distribution
C (100%)

AmerSerhan Highly Voted 4 years, 8 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 29 times

theboywonder 3 years, 6 months 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 3 times

Patesso Most Recent 1 year, 7 months ago
Etait a l'examen le 18/05/2023
upvoted 2 times

Brandon1971 1 year, 10 months ago
Selected Answer: C
Yes Named Locations, https://docs.microsoft.com/en-us/azure/active-directory/conditional-access/untrusted-networks
upvoted 1 times

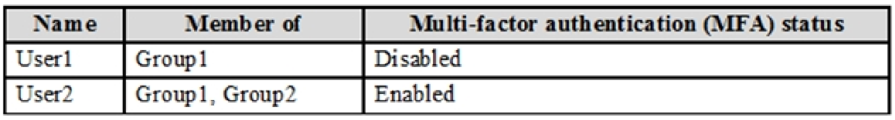
Jonclark 1 year, 10 months ago
Selected Answer: C
Named Locations are the way to be specific about locations in conditional access rules.

While sign-in risk does consider location, the condition is based on how risky a location is for the sign-in. Higher-risk locations include anonymous IPs, locations with known malware activity, sign-ins from unusual locations etc.
upvoted 2 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: User risk of Low and above

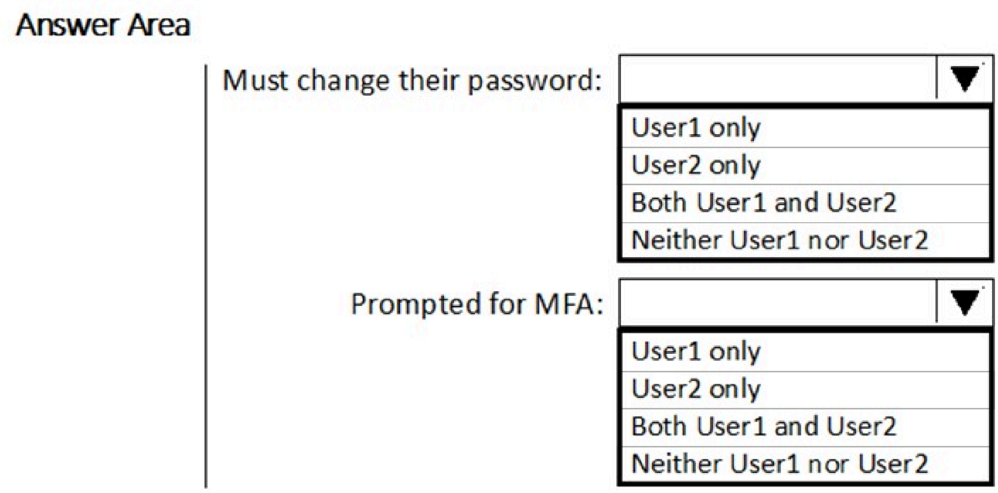
✑ Access: Allow access, Require password change

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:

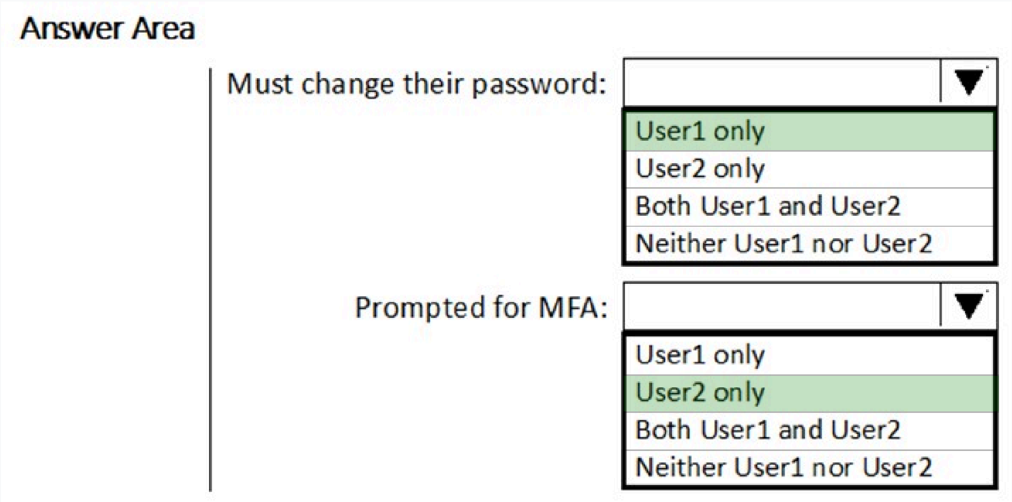


Answer Area

Must change their password: ▼
- User1 only
- User2 only
- Both User1 and User2
- Neither User1 nor User2

Prompted for MFA: ▼
- User1 only
- User2 only
- Both User1 and User2
- Neither User1 nor User2

Suggested Answer:



Answer Area

Must change their password: ▼
- [✓ User1 only]
- User2 only
- Both User1 and User2
- Neither User1 nor User2

Prompted for MFA: ▼
- User1 only
- [✓ User2 only]
- Both User1 and User2
- Neither User1 nor User2

Box 1: User1 only -

The Azure AD Identity Protection user risk policy is excluded from Group2. Exclusion overrides inclusion. Therefore, the policy will not affect User2. Thus, only

User 1 needs to change the Password.

Box 2: User2 only -

MFA will be triggered for User 2.

Reference:

https://docs.microsoft.com/en-us/azure/active-directory/identity-protection/howto-identity-protection-configure-risk-policies

⊟ kiketxu Highly Voted 3 years, 9 months ago

User1 is must change PW.

User2 prompted for MFA

upvoted 49 times

w00t 3 years, 9 months ago

This is the right answer

upvoted 7 times

Yetijo 3 years, 6 months 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 7 times

Sikula Highly Voted 👍 3 years, 9 months 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 22 times

ellik 3 years, 8 months 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 years, 8 months 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 2 times

JoelB 3 years, 6 months 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 7 times

LillyLiver 2 years, 9 months ago

Ummmm.... See, I think this is trickier than it appears.

User2's MFA status is Enabled. When they are enabled, the user can skip the MFA registration for 2 weeks before being required to register. So in this scenario User2 is Enabled so s/he will be prompted for registration, which s/he can skip. If the status was Enforced, then yes MFA will be presented to User2.

And, since the org is using per-user MFA enrollment due to User1's MFA being disabled, I think User1 will need to change their password and neither 1 or 2 will be prompted for MFA.

upvoted 2 times

LillyLiver 2 years, 9 months ago

Having gone through the Identity Protection policy again, there is no option for forcing someone to change their password. So the answer to Q1 is Neither User1 nor User2.

The answer for Q2 is still Neither User1 nor User2. For my reasons above.

upvoted 1 times

yayoayala 3 years, 8 months 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

[Removed] 3 years, 6 months ago

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

upvoted 1 times

WMG 3 years, 4 months ago

Read JoelBs answer, the correct answer is "User 1 much change password" and "User 2 will ge prompted for MFA" (User 2 will actually be enrolled into MFA as it is only Enabled)

upvoted 2 times

TomasValtor Most Recent 1 year, 6 months ago

Fisrt, sign in from an unfamiliar location is a sign-in risk, not a user risk.
So I think the right answer for both users are: "Neither User1 nor User2"

upvoted 1 times

examdog 2 years ago

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. <https://learn.microsoft.com/en-us/azure/active-directory/conditional-access/concept-conditional-access-users-groups>

upvoted 2 times

SahMat 2 years ago

If Exclusion overrides inclusion, then no User1 nor User2 will be prompted with the MFA, as MFA is disabled for group 1 and both users are members of Group 1 which is disabled for MFA .....

upvoted 2 times

pete26 2 years, 3 months ago

This is probably the most commented question for MS-500. I do agree with the answers given for both:

User1 will be asked to change password because it is a member of Group1. Group1 is included in the assignments.

User2 MFA status is set to “enabled”. This means he will be prompted for MFA. Once registered his MFA status will change to “enforced”. Yes, User2 is excluded from the user risk policy, but the user risk policy has nothing to do with MFA, a sign-in policy does. This is how Microsoft tries to get you!

upvoted 5 times

SKam22 2 years, 4 months ago

Let's break it down:
A- SSPR can only be enabled for users that have MFA
B: User risk policy can require SSPR
The users are logged in from unfamiliar location? This is related to "Sign in" risk policy not "User risk" policy therefore the correct answer for both is:

Neither User 1 nor User 2.

upvoted 3 times

Bulldozzer 2 years, 5 months ago

The correct answers are:
Q1: "Neither User1 nor User2" because there is no password change option in the Identity protection sign-in risky policy.
Q2: “User2" because even if the MFA status is set to "Enabled" the user will be prompted for MFA

upvoted 3 times

Whatsamattr81 2 years, 6 months ago

The policy doesn’t apply to user 2 but it doesn’t change their MFA status (Enabled) - so they will either be promoted for MFA or, if the first time, promoted for setup and then prompted for MFA.

upvoted 2 times

tatendazw 2 years, 7 months ago

Pwd change required for User 1 only and User risk policy does not prompt for MFA so neither User 1 nor 2 shall be prompted for MFA,
If it was a Sign in risk then User 2 will be prompted to register for MFA
https://docs.microsoft.com/en-us/azure/active-directory/authentication/howto-mfa-userstates#azure-ad-multi-factor-authentication-user-states

upvoted 1 times

rtea 2 years, 8 months ago

There is no sign-in risk condition available under a user risk policy

upvoted 2 times

VickyRajdev 2 years, 10 months ago

User1 - Must Change Password, its based on the Policy mentioned in question
User2 - Will be prompted for password, because if you see words "MULTI-FACTOR AUTH STATUS" this term is only and exactly available under PER-

USER MFA SETTINGS, hence USER2 will be prompted for the MFA based on Per-User MFA settings

upvoted 1 times

Jared144 2 years, 12 months ago

Interesting to consider that MFA is required when resetting password so perhaps It's both User1 and User 2 are prompted for the second one.

upvoted 2 times

kakakayayaya 2 years, 10 months ago

Defenetely!

upvoted 1 times

mgrcic56 3 years ago

1st: Both users

2nd: User2 only

upvoted 1 times

mkoprivnj 3 years, 1 month ago

User 1 and User 2 only.

upvoted 1 times

Rstilekar 3 years, 1 month ago

Given ans is wrong for box 2.

Box 1: User1 only -

The Azure AD Identity Protection user risk policy is excluded from Group2. Exclusion overrides inclusion. Therefore, the policy will not affect User2. Thus, only

User 1 needs to change the Password.

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).

Box 2: User2 only

MFA will be triggered for User 2.

Even though User2 is excluded by Group2 (exc overides inc), so CA is not applied for it but by nature of MFA a user will be challenged when signing on from an unfamiliar location, without a CA in place.

For User1 MFA is disabled all together so it will not be challenged for MFA.

upvoted 1 times

Rstilekar 3 years, 1 month ago

I mean given answers are correct for both

upvoted 1 times

Rstilekar 3 years, 1 month ago

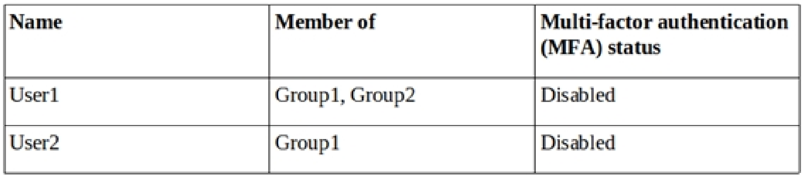
The CA in this scenario is designed for User 1. The user does not have MFA enabled and cannot be challenged, but they can be allowed and prompted action (password change).

upvoted 1 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

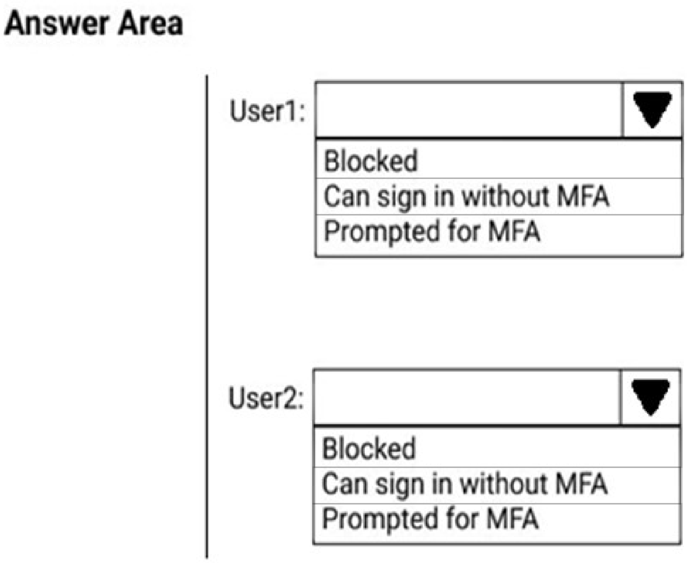
✑ Access: Allow access, Require multi-factor authentication

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:

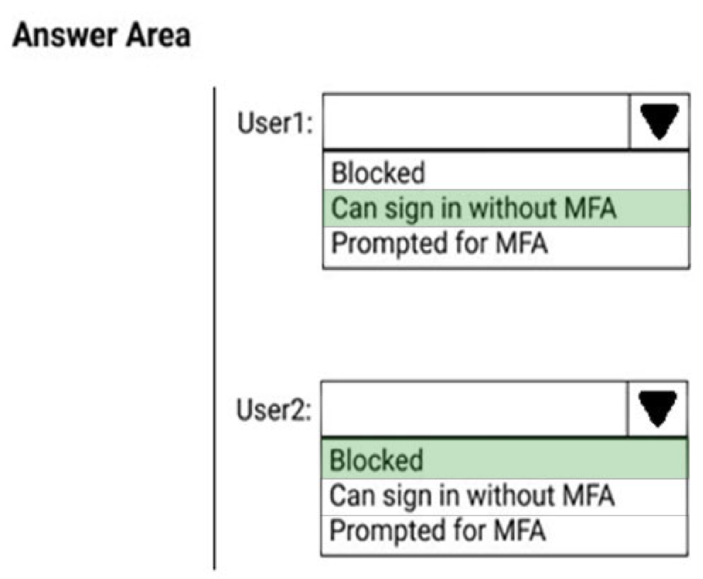


Answer Area

User1: ▼
- Blocked
- Can sign in without MFA
- Prompted for MFA

User2: ▼
- Blocked
- Can sign in without MFA
- Prompted for MFA

Suggested Answer:



Answer Area

User1: ▼
- Blocked
- [✓ Can sign in without MFA]
- Prompted for MFA

User2: ▼
- [✓ Blocked]
- Can sign in without MFA
- Prompted for MFA

⊟ **Sugar123** Highly Voted 👍 3 years, 9 months 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 39 times

Beitran 3 years, 9 months ago

Thank you!

upvoted 2 times

FrugalFungus 3 years, 9 months ago

Thanks Sugar. You are right.

upvoted 1 times

bingomutant 3 years, 9 months ago

this looks correct - thanks

upvoted 1 times

ellik 3 years, 8 months ago

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

upvoted 2 times

Lulu77 Highly Voted 3 years, 6 months ago

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

upvoted 34 times

H0TDOGG Most Recent 1 year, 8 months ago

Late to the party, but I can confirm user2 is blocked. Not prompt for MFA. Meaning, if there is no MFA linked, be it user MFA or conditional access MFA, users are blocked.

upvoted 1 times

ChachaChatra 1 year, 11 months ago

Valid on 28/01/2023

upvoted 4 times

CEEJAY83 1 year, 11 months ago

The answer is correct. The policy is applied to group 1 only, so user 1 and user 2 are blocked by default because they both are in group 1, but user 1 has an option because he's also part of another group(group 2) which overrides the policy, and MFA is also block by default which means user 1 can sign in without MFA.

upvoted 1 times

Nav90 1 year, 11 months ago

User 1 - can sign in without MFA

User 2 - Blocked (Explanation - https://learn.microsoft.com/en-us/azure/active-directory/identity-protection/howto-identity-protection-configure-risk-policies. Under Risk remediation Warning section.)

upvoted 4 times

zerrowall 2 years ago

User 2 blocked. Checked in a simple lab, this message appeared for user that has been connected from browser Brave in Tor mode:

"user2@msdxYYYYYY.onmicrosoft.com

Your sign-in was blocked

We've detected something unusual about this sign-in. For example, you might be signing in from a new location, device, or app. Before you can continue, we need to verify your identity. Please contact your admin."

upvoted 1 times

bac0n 2 years, 1 month ago

Given answer is correct. Check vunder's comment. If you follow the policy in this example and use Tor browser in Brave for an anonymous IP you will be blocked.

upvoted 1 times

Nobal 2 years, 2 months ago

User 2 will be 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."

https://learn.microsoft.com/en-us/azure/active-directory/identity-protection/howto-identity-protection-configure-risk-policies

upvoted 1 times

ewu 2 years, 4 months ago

Blocked, since the other option is prompted for mfa, which isnt the case they will be prompted for mfa registration not a mfa prompt

upvoted 1 times

Zzzkkk 2 years, 5 months ago

User 2 - Prompted for MFA.

Enabling Azure AD Multi-Factor Authentication through a Conditional Access policy doesn't change the state of the user. Don't be alarmed if users appear disabled. Conditional Access doesn't change the state.

https://docs.microsoft.com/en-us/azure/active-directory/authentication/howto-mfa-userstates
upvoted 3 times

⊟ **Whatsamattr81** 2 years, 6 months ago
MFA CA policies will not apply if legacy (per user) MFA is enabled for the user. Legacy supersedes CA. In this case the CA policy will be applied to User 2 so they will be promoted to register.
upvoted 4 times

⊟ **vunder** 2 years, 6 months ago
This is correct, User 1 will be allowed to sign in, due to the exemption made on group2 in the CA policy, (exclusions take precedence, this is standard for CA policies. User2 is blocked as the group1 is the one being applied. User2 must have MFA but since MFA is disabled therefore the sign-in is blocked.
Things to look out for when you demo this. Check for Security Defaults that is is disabled.
Use tor-browser to simulate an anonymous IP.
upvoted 2 times

⊟ **DarkAndy** 2 years, 6 months ago
Valid on exam. Jun 10, 2022
upvoted 5 times

⊟ **tatendazw** 2 years, 7 months ago
User 1 can sign in, User 2 blocked
https://docs.microsoft.com/en-us/azure/active-directory/identity-protection/howto-identity-protection-configure-risk-policies#risk-remediation
upvoted 2 times

⊟ **Ryuukossei** 2 years, 7 months ago
User 2 will NOT be blocked. Conditional Access policies that require MFA as an access control will prompt the user to register if they are not enabled or registered. The per-user MFA status does not affect this process. If they register, they will be allowed to sign in. If they do not register, THEN they will be blocked.
upvoted 5 times

⊟ **Anon617** 2 years, 9 months ago
User1 - Can sign in without MFA
User 2 - 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:
https://docs.microsoft.com/en-us/azure/active-directory/identity-protection/howto-identity-protection-configure-risk-policies
upvoted 5 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.
Solution: You use the Security event log on Server1.
Does that meet the goal?

A. Yes

B. No

Suggested Answer: *B*
References:
https://support.pingidentity.com/s/article/PingOne-How-to-troubleshoot-an-AD-Connect-Instance

pompes 1 year, 7 months ago
B.
Was on the exam. I scored 816
upvoted 1 times

Prudhvikrish1523 1 year, 10 months ago
Using the Security event log on the server running Azure AD Connect to view Azure AD Connect events is a valid solution. The Azure AD Connect installation logs events in the Windows Event log, and the Security event log is one of the logs that can be used to view these events.

Therefore, using the Security event log on Server1 to view Azure AD Connect events meets the goal.
upvoted 1 times

kmk_01 1 year, 9 months ago
No it's the application log which will contain events for AAD Connect.
upvoted 1 times

stewie055 2 years, 4 months ago
this source says some event can be found in evetn viewer
https://docs.microsoft.com/en-GB/troubleshoot/azure/active-directory/installation-configuration-wizard-errors#troubleshoot-other-error-messages

but apparently it's some specific errors and not admin changes
https://techcommunity.microsoft.com/t5/identity-authentication/azure-ad-connect-admin-audit-log/m-p/41349
upvoted 1 times

stewie055 2 years, 4 months ago
never mind, it's in the application folder of the event viewer
upvoted 1 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.

Solution: You use the System event log on Server1.

Does that meet the goal?

A. Yes

B. No

Suggested Answer: *B*

References:

https://support.pingidentity.com/s/article/PingOne-How-to-troubleshoot-an-AD-Connect-Instance

Community vote distribution

B (100%)

kmk_01 1 year, 9 months ago

Selected Answer: B

Correctamundo. It's the application event log which will contain events related to AAD connect.

upvoted 1 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.
Solution: You use the Application event log on Server1.
Does that meet the goal?

A. Yes

B. No

Suggested Answer: *A*
References:
https://support.pingidentity.com/s/article/PingOne-How-to-troubleshoot-an-AD-Connect-Instance

Community vote distribution

A (100%)

pompes 1 year, 7 months ago
A.
Was on the exam.
upvoted 3 times

Dipronil 1 year, 8 months ago
In the AAD Connect server
o Open Event Viewer.
o Expand Windows Logs, and then expand Application.
o In the Actions pane, select Filter Current Log.
o In the Event sources box, select the Directory Synchronization check box.
o Select OK. The following table lists the error name, the error details, the error source, and the steps to help resolve the error. Please follow the Microsoft documentation.
How to troubleshoot Azure Active Directory Sync tool installation and Configuration Wizard errors - Active Directory | Microsoft Learn
upvoted 2 times

Mehdi14 1 year, 11 months ago
Selected Answer: A
A is correct

https://learn.microsoft.com/en-us/troubleshoot/azure/active-directory/installation-configuration-wizard-errors#troubleshoot-other-error-messages
upvoted 1 times

CEEJAY83 1 year, 11 months ago
A is correct. Azure AD does not have Application event log.
upvoted 1 times

pete26 2 years, 3 months ago
Selected Answer: A
A is correct!
upvoted 2 times

heshmat2022 2 years, 3 months ago
AD Connect Logs

AD Connect logs to Event Viewer. Viewing these logs will help one troubleshoot outbound communication with the PingOne for Enterprise server. To examine them open up Event Viewer in Administrative Tools. Expand ‘Windows Logs’ and examine ‘Application’

upvoted 2 times

⊟ **WickedMJ** 2 years, 3 months ago

S0 is the answer correct then?

upvoted 1 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 Microsoft 365 Security admin center, download a report.

B. From Azure Log Analytics, query the logs.

C. From the Microsoft 365 Security admin center, perform an audit log search.

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

Suggested Answer: *D*
The user sign-ins report provides information on the sign-in pattern of a user, the number of users that have signed in over a week, and the status of these sign- ins.
Note:
There are several versions of this question in the exam. The question has two possible correct answers:
1. From the Enterprise applications blade of the Azure Active Directory admin center, view the sign-ins.
2. From the Azure Active Directory admin center, view the sign-ins.
Other incorrect answer options you may see on the exam include the following:
1. From the Enterprise applications blade of the Azure Active Directory admin center, view the audit logs.
2. From the Azure Active Directory admin center, view the audit logs.
Reference:
https://docs.microsoft.com/en-us/azure/active-directory/reports-monitoring/concept-sign-ins

[Removed] 1 year, 6 months ago
I don't understand. Question 19 and 22 are the same. Both different answers and they are both correct? Am I missing something?
upvoted 1 times

[Removed] 1 year, 6 months ago
Question 21. Sorry. My mistake.
upvoted 1 times

[Removed] 1 year, 6 months ago
And nevermind... Just caught it. Not enough coffee. Moderator feel free to remove my stupidity.
upvoted 2 times

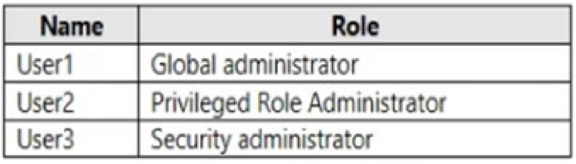
pompes 1 year, 7 months ago
D.
Was on the exam.
upvoted 2 times

JoshJosh 1 year, 11 months ago
Correct
upvoted 3 times

Question #20 *Topic 1*

HOTSPOT -

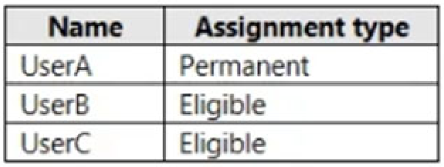
You have a Microsoft 365 subscription that contains the users shown in the following table.



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:

✑ Activation maximum duration (hours): 1 hour

✑ Require justification on activation: No

✑ Require ticket information on activation: No

✑ On activation, require Azure MFA: No

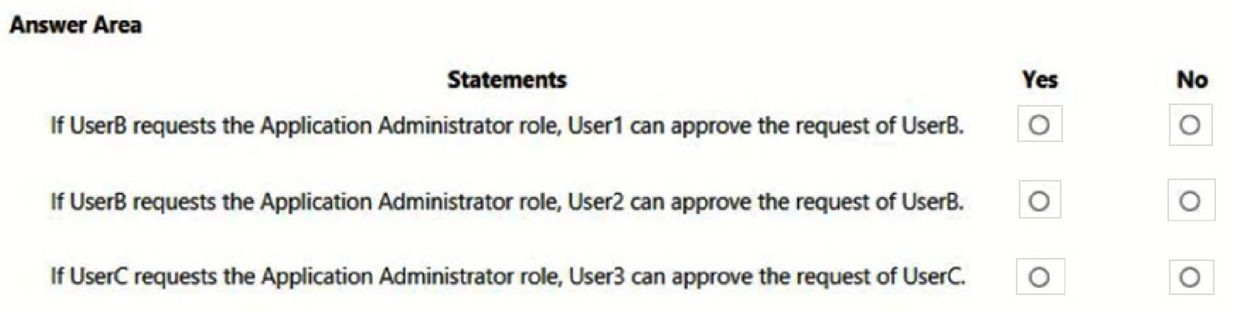
✑ Require approval to activate: Yes

✑ Approvers: 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.

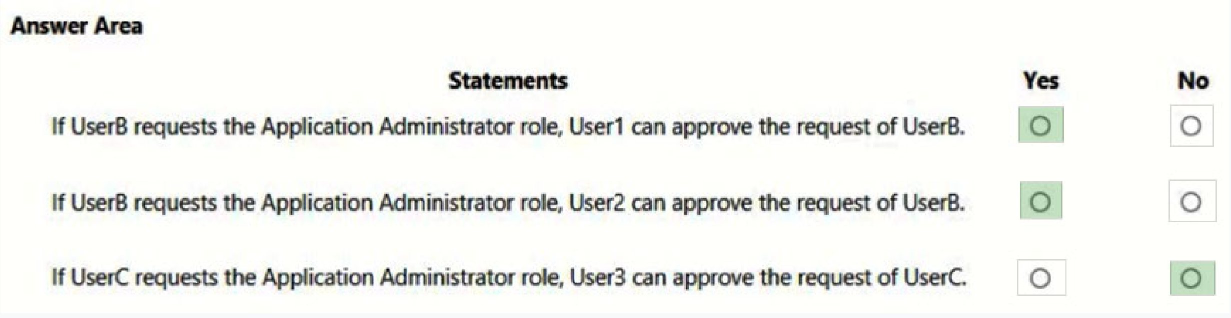
Hot Area:



Answer Area

Statements	Yes	No
If 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.	○	○

Suggested Answer:



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.	○	[✓ ○]

dakasa Highly Voted 2 years, 4 months ago

Answers are correct

proof: https://docs.microsoft.com/en-us/azure/active-directory/privileged-identity-management/pim-how-to-change-default-settings?source=recommendations

upvoted 9 times

imjoe Highly Voted 2 years, 1 month ago

After you tick the "Require approval to activate" in "Edit role setting", you will see the following: "If no specific approvers are selected, privileged role administrators/global administrators will become the default approvers."

upvoted 6 times

ccadenasa Most Recent 2 years, 2 months ago

This is correct > https://learn.microsoft.com/en-us/azure/active-directory/roles/permissions-reference#privileged-role-administrator

upvoted 1 times

⊟ **pete26** 2 years, 2 months ago

Valid on exam October 14, 2022

upvoted 3 times

⊟ **pete26** 2 years, 3 months ago

The answers given are correct!

upvoted 2 times

⊟ **Daniel830** 2 years, 3 months ago

Correct. Security Administrator role cannot asign roles.

upvoted 2 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 Microsoft 365 Security 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.

Suggested Answer: *A*
The user sign-ins report provides information on the sign-in pattern of a user, the number of users that have signed in over a week, and the status of these sign- ins.
Note:
There are several versions of this question in the exam. The question has two possible correct answers:
1. From the Enterprise applications blade of the Azure Active Directory admin center, view the sign-ins.
2. From the Azure Active Directory admin center, view the sign-ins.
Other incorrect answer options you may see on the exam include the following:
1. From Azure Log Analytics, query the logs.
2. From the Microsoft 365 Compliance center, perform an audit log search.
3. From the Microsoft 365 Defender portal, download a report.
Reference:
https://docs.microsoft.com/en-us/azure/active-directory/reports-monitoring/concept-sign-ins

Community vote distribution

A (75%) U (25%)

Dhamus 1 year, 7 months ago

A is the correct answer, you can view the type of authentication used by X user from the "Login records" section.

upvoted 1 times

amymay101 1 year, 10 months ago

I think its D, you can look in Activity / users registered by authentication method , select 'App notification' and that will give you a list of users who have used the authenticator app

upvoted 1 times

Perycles 1 year, 11 months ago

A is correct : but the information is not displayed on "Conditionnal access" column but "Authentification requirement" column.

upvoted 1 times

musiman 2 years ago

The answer is incorrect.
The correct answer is C. You can view from which app login portal (azure ad, sharepoint, etc.) someone logged in when you FIRST go to the Enterprise Applications blade and then go to Sign ins.

upvoted 1 times

> **michaukotlowski** 2 years ago
>
> @musiaman it makes sense, however, they expect us to check whether MFA was used for accessing SharePoint Online. Azure AD>Users>Sign-ins can provide that info in the Conditional Access column, which can be filtered for what users tried to access (SharePoint or else).
>
> upvoted 1 times

Wedge34 2 years, 2 months ago

Selected Answer: A

A is the answer

upvoted 3 times

rruthra 2 years, 2 months ago

Answer is A

upvoted 2 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:

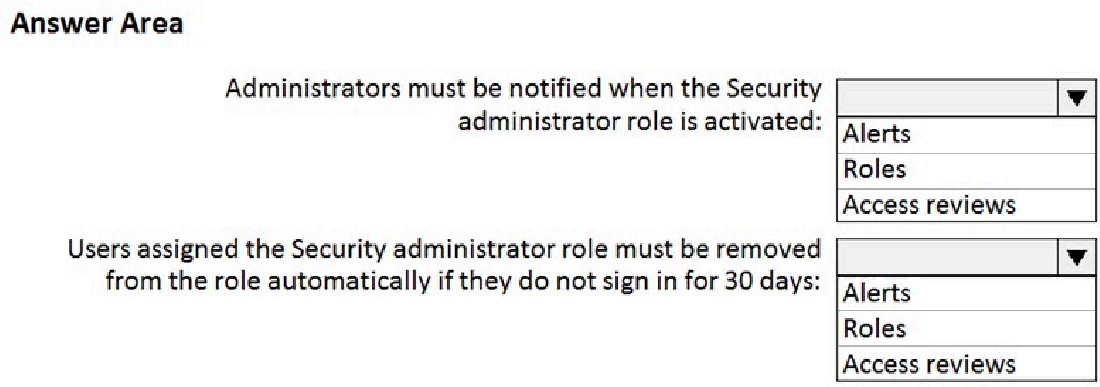
✑ Administrators must be notified when the Security administrator role is activated.

✑ 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

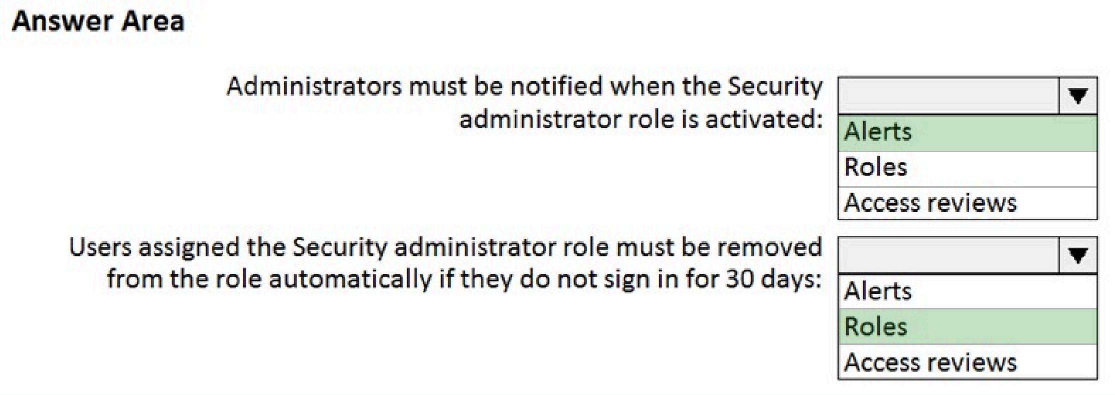
Administrators must be notified when the Security administrator role is activated:

- 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

Suggested Answer:



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

Reference:

https://docs.microsoft.com/bs-latn-ba/azure/active-directory/privileged-identity-management/pim-how-to-configure-security-alerts?tabs=new https://docs.microsoft.com/bs-latn-ba/azure/active-directory/privileged-identity-management/pim-how-to-change-default-settings?tabs=new

kiketxu Highly Voted 3 years, 9 months 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 45 times

w00t 3 years, 9 months ago

Pretty positive you're right.

#1 = ROLE

#2 = ALERT

They have the answer backwards.
upvoted 2 times

⊟ **w00t** 3 years, 9 months 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 5 times

⊟ **Anonymousse** 2 years, 2 months ago
This has been verified. They do in fact have the answer backwards. I checked in a real environment on 10/22/22. Under Roles is where you define the notifications and under alerts is where you define when to send the alert that the account has not been logged into in X days.
upvoted 2 times

⊟ **Anonymousse** 2 years, 2 months ago
The setting is under Potential stale accounts in a privileged role, but it's just the settings. I can't confirm if it "automatically" removes the role however.
upvoted 1 times

⊟ **ellik** 3 years, 8 months 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

⊟ **prabhjot** 3 years, 5 months ago
agree 1) role and 2) Access Review
upvoted 2 times

⊟ **Am3lectric** 3 years, 1 month ago
I agree. 1) Roles 2) Access Reviews
upvoted 4 times

⊟ **Rafale** Highly Voted 👍 3 years, 9 months ago
Given answers are correct
1- Alert
2- Role
upvoted 15 times

⊟ **GatesBill** Most Recent ⊙ 1 year, 9 months ago
#1: Roles
#2: Access reviews
Pretty sure about this and can be confirmed by testing in lab environments.
upvoted 4 times

⊟ **Jonclark** 1 year, 10 months ago
This question is outdated. Currently, you would configure this by logging into the Azure portal, opening Privileged Identity Management -> Roles -> (whatever role you want to set the alert for) -> Role Settings. Inside the settings, you'll see a "notifications" tab, which will allow you to set the configuration that meets the requirement.

Don't get thrown off by the word "Alert" which you will see elsewhere. Yes, this is an alert, but you configure it as a part of notifications.
upvoted 2 times

⊟ **zerrowall** 2 years ago
Regarding 2nd question. To fulfill this requirement, you can create an access review with the following options:
Inactive users (on tenant level) only - True
Days inactive - 30 days
Auto apply results to resource - Enable
If reviewer don't respond - Remove access

General doc is here: https://learn.microsoft.com/en-us/azure/active-directory/privileged-identity-management/pim-create-azure-ad-roles-and-resource-roles-review#create-access-reviews
see the item from 11: "...Or, you can create access reviews only for inactive users (preview). In the Users scope section, set the Inactive users (on tenant level) only to true. If the toggle is set to true, the scope of the review will focus on inactive users only. Then, specify Days inactive with a number of days inactive up to 730 days (two years). Users inactive for the specified number of days will be the only users in the review."
upvoted 2 times

TweetleD 2 years, 1 month ago
Answer is wrong. Notifications is under roles and to remove assignment if no sign in after 30 days has to be done in an Access Review
upvoted 3 times

ccadenasa 2 years, 2 months ago
The correct answers are Roles and Alerts. In Roles, you can see the Role settings for each role, including Role assignment Alert. Under Alerts, there is a pre-define alert for "Eligible administrators aren't activating their privileged role". By default the number of days is set to 30 but can be reduced or extend it.
upvoted 1 times

DragonsGav 2 years, 2 months ago
I believe correct answer is "Roles" for both as per, https://learn.microsoft.com/bs-latn-ba/azure/active-directory/privileged-identity-management/pim-resource-roles-configure-role-settings
upvoted 3 times

Trainee2244 2 years, 3 months ago
#1Role
# Access Review

I dont get why so many have role and alert x)
upvoted 7 times

dakasa 2 years, 4 months ago
I would say both settings are reachable from "Role".
https://docs.microsoft.com/bs-latn-ba/azure/active-directory/privileged-identity-management/pim-resource-roles-configure-role-settings
upvoted 1 times

Eltooth 2 years, 5 months ago
Roles
Access Reviews
upvoted 3 times

tatendazw 2 years, 8 months ago
Roles (Roles&Admin > Role settings > scroll to send notifications ...)
Access review (Settings > Enable reviewer decision helpers > No sign-in 30 days (If enabled, system recommends reviewers to deny users who have not signed-in within 30 days. Recommendation accounts for both interactive and non-interactive sign-ins.)
upvoted 4 times

CatoFong 2 years, 12 months ago
1. Roles
2. Access Review
upvoted 1 times

mkoprivnj 3 years, 1 month ago
#1: ROLE
#2: ACCESS REVIEWS
upvoted 1 times

xroxro 3 years, 1 month ago
#1✑ Administrators must be notified when the Security administrator role is activated.
I found the option in role->settings->notification
So for me the answer is ROLE

#2 ✑ Users assigned the Security administrator role must be removed from the role automatically if they do not sign in for 30 days.
There is such option in role
I though the answer was ACCESS REVIEW but i did not see an option to remove the role if the user does not login since ...

Any help ?

upvoted 3 times

⊟ **BuzzyC** 3 years, 1 month ago

It is absolutely

1. Roles
2. Access Reviews

Roles > Settings > Send notifications when eligible members activate this role

Access Reviews > New > Duration > 30 days, End Never

Upon completion settings > If reviewer doesn't respond > Remove access

Alerts only alert on issues (stale accounts, users not using PIM etc - it does not action anything, not does it alert on when users are enabling PIM access as they should - which is what the question is asking)

upvoted 3 times

⊟ **aryaid88** 3 years, 3 months ago

Alerts and Role - Access review is part of Identity Governance and not part of PIM. Inside PIM under Manage AD role you will find the role assignment and you can edit its attributes.

upvoted 2 times

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.

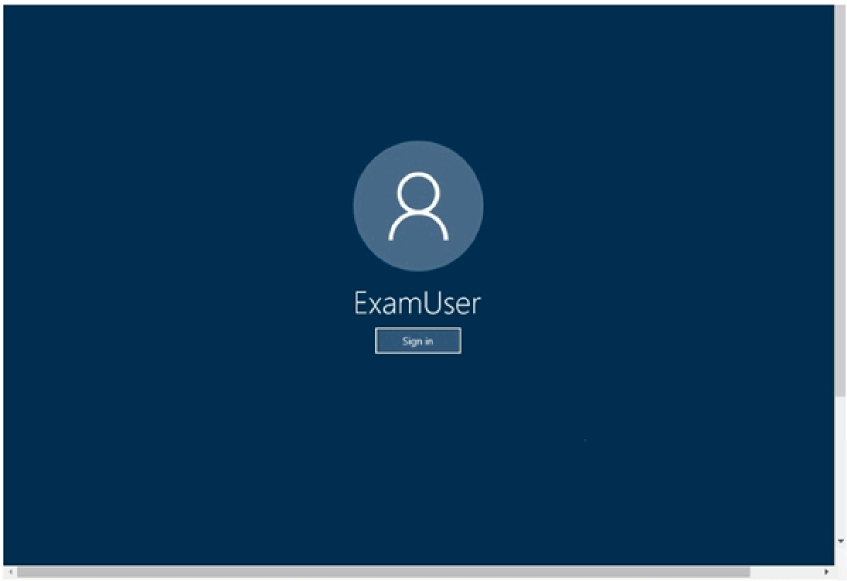
Scoring is based on the outcome of performing the tasks stated in the lab. In other words, it doesn't matter how you accomplish the task, if you successfully perform it, you will earn credit for that task.

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.

Suggested Answer: *See explanation below.*

1. In the Exchange Administration Center (EAC), navigate to Permissions > Admin Roles.
2. Select the group: Organization Management and then click on Edit.
3. In the Members section, click on Add.
4. Select the users, USGs, or other role groups you want to add to the role group, click on Add, and then click on OK.
5. Click on Save to save the changes to the role group.

Reference:

https://help.bittitan.com/hc/en-us/articles/115008104507-How-do-I-assign-the-elevated-admin-role-Organization-Management-to-the-account-that-is-performing-a-

Public-Folder-migration-
https://docs.microsoft.com/en-us/exchange/permissions-exo/permissions-exo

MikeMatt2020 Highly Voted 👍 3 years, 4 months ago

I very much disagree that the answer is to grant the user the Organization Management EXO role. This EXO role does indeed grant the user wide-spread permissions throughout Exchange. However, this role also includes "Security Admin", "Compliance Admin" and "Security Reader".

Our goal is to ensure Least Privilege. Obviously we wouldn't want to make our user a Global Admin. This breaks the goal of Least Privilege". I believe the answer is to assign the user the AAD role of "Exchange Administrator".

Regarding the Organization Management role:
"Members can also delegate role groups and management roles in the organization"
upvoted 6 times

WMG 3 years, 4 months ago

I see your point. But the "Exchange Admin" role in AAD is really the Exchange Service A
dmin in Exchange Online. The Exchange Service Admins are part of the Organization Management group and inherits all the permissions. So they are the same thing as giving the user Org Management permissions. So the answer is correct.

There are of course advantages of using AAD, e.g access review, PIM etc etc but as the question stands this is the correct answer.
upvoted 4 times

ZakS Highly Voted 👍 3 years, 7 months 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 6 times

nidentify 3 years, 5 months ago

Yes exchange admin is should be the correct answer
upvoted 1 times

Orion8575 Most Recent ⏲ 1 year, 6 months ago

Correct answer is to give Exchage Administrator permissions becouse Organization Management has permission across multiple service not just Exchange Online.
upvoted 1 times

Avaris 2 years, 1 month ago

i think it should be through 365 admin center not exchange admin
upvoted 1 times

baliuxas07 2 years, 4 months ago

Do they do labs in this certification?
upvoted 4 times

tatendazw 2 years, 8 months ago

ExchangeServiceAdmins_-xxxx is managed by Organization Management so you can only assign user via Organization Management role
upvoted 1 times

tatendazw 2 years, 8 months ago

and ExchangeServiceAdmins_-xxxx is greyed out in new and old EAC
upvoted 1 times

Ikeinater 2 years, 8 months ago

The current way to get to this as of (4/14/2022) is 365 admin center>Exchange Admin Center>Roles blade>Admin Roles>Organization Management>Assign tab upper right. Then assign the user that way. Assigning the Exchange admin role from the AAD/365 admin gives more privilege than is needed.
upvoted 4 times

oopspruu 3 years, 4 months ago

The given answer will be correct. Even if you assign the person the role of "Exchange Administrator", they will automatically be a member of the Organization Manager role group. You can see the Exchange Admin assigned users in EAC > Admin Roles > ExchangeServiceAdmins, and this ExchangeServiceAdmins role group already a member of the Organization Management role group. So I believe assigning them the Exchange Admin AD role or Organization Management role, both would be correct answers.

upvoted 1 times

Nail 3 years, 4 months ago

If you have to switch to the Exchange admin center doesn't that mean that you are LEAVING the "Microsoft 365 Office admin center"? Seems to me you would stay in the M365 admin center and just find the user and give them the Exchange Admin role.

upvoted 2 times

Nail 3 years, 4 months ago

Bah, I take this back. It seems that all of these questions have you start out in the M365 admin center, regardless of which admin center you actually need to go to. I did notice, however, that I can just to M365 admin center > Roles > and there is an Exchange tab right there where you can adjust the membership of Organization Management.

upvoted 6 times

Alex_ua1 3 years, 6 months ago

The task says -To complete this task, sign in to the Microsoft Office 365 admin center. answer is correct

upvoted 2 times

Rstilekar 3 years, 6 months ago

Yes given answer is right

upvoted 1 times

jatinKumar 3 years, 8 months ago

will this not be .. ADzure AD Role "Exchange Administrator" as it says manage all settings of exchange online.. please advise

upvoted 4 times

ellik 3 years, 8 months ago

is it AD Role "Exchange Administrator" ?

upvoted 1 times

dcasabona 3 years, 8 months ago

I think so too.

upvoted 2 times

Robert__Susin 3 years, 8 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

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.

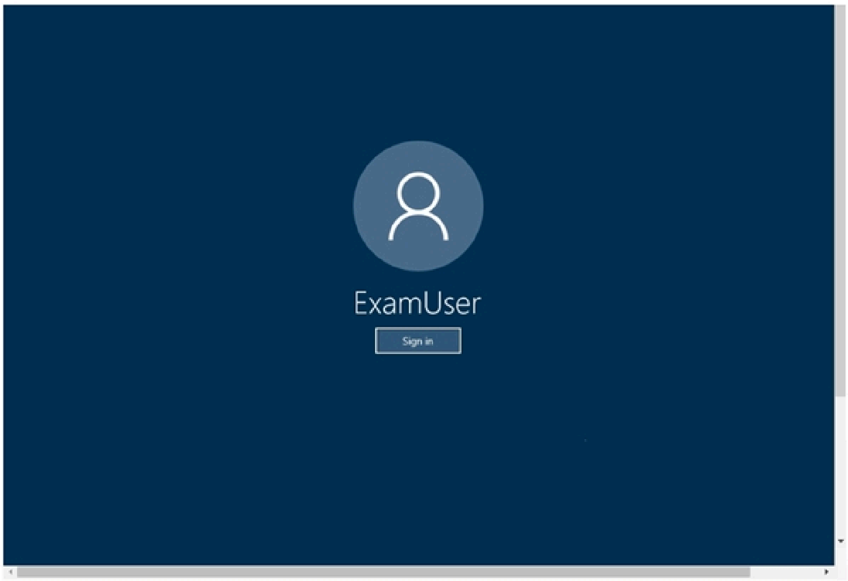
Scoring is based on the outcome of performing the tasks stated in the lab. In other words, it doesn't matter how you accomplish the task, if you successfully perform it, you will earn credit for that task.

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.

Suggested Answer: *See explanation below.*

1. After signing into the Microsoft 365 admin center, click Admin centers > Azure Active Directory > Devices.
2. Navigate to Device Settings.
3. Set the Users may join devices to Azure AD setting to All.
4. Set the Additional local administrators on Azure AD joined devices setting to None.
5. Set the Users may register their devices with Azure AD setting to All.
6. Leave the Require Multi-Factor Auth to join devices setting on it default setting.
7. Set the Maximum number of devices setting to 5.
8. Set the Users may sync settings and app data across devices setting to All.
9. Click the Save button at the top left of the screen.

Reference:

https://docs.microsoft.com/en-us/azure/active-directory/devices/device-management-azure-portal https://docs.microsoft.com/en-us/microsoft-365/compliance/use-your-free-azure-ad-subscription-in-office-365?view=o365-worldwide

Delli Highly Voted 👍 3 years, 8 months 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 14 times

fuckthisscamsite 3 years, 8 months ago

The question is about joining devices to Azure AD, not enrolling in Intune. You are wrong

upvoted 41 times

WMG 3 years, 4 months ago

Correct, joining devices to Azure AD is not the same as enrolling them in Endpoint Manager / Intune.

Upvoted also for username.

upvoted 4 times

Purist 3 years, 4 months ago

lol. same

upvoted 1 times

msysadmin 1 year, 10 months ago

Your feedback is wrong. Intune requre additional license and question is not related about intune. Even this data from your link :)

Intune device limit restrictions
Intune device limit restrictions set the maximum number of devices that a user can enroll. You can allow a user to enroll up to 15 devices. To set a device limit restriction, sign in to Microsoft Endpoint Manager admin center. Then go to Devices > Enrollment restrictions. For more information, see Create a device limit restriction.

Azure device limit restriction
Azure device limit restrictions set the maximum number of devices that either Azure AD joins or Azure AD registers. To set the Maximum number of devices per user, go to the Azure portal > Azure Active Directory > Devices. For more information, see Configure device settings

upvoted 1 times

Rstilekar Highly Voted 👍 3 years, 6 months ago

Agreed. given steps in answer are correct

upvoted 10 times

ccadenasa Most Recent 🕘 2 years, 2 months ago

The correct answer is AAD > Devices > Devices Settings > Maximum number of devices per user > 5. The recommended is 20

upvoted 3 times

adarvasi 2 years, 2 months ago

For setting the maximum number of devices (allowed) per user, the answer is correct.

upvoted 1 times

CODENAME_KND 2 years, 7 months ago

Using Azure Admin Center
Azure AD-->Devices-->Device Settings
You can find the option of setting maximum devices for each user

upvoted 7 times

LoremanReturns 2 years, 10 months ago

Right answer is from Azure AD Portal -> Devices -> Device settings -> Maximum number of devices per user. Default is 20, can be set to 5.

upvoted 6 times

Donnie21 3 years, 8 months ago

You can still use Azure.

upvoted 2 times

⊟ **Vic08** 3 years, 7 months ago

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

upvoted 2 times

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.

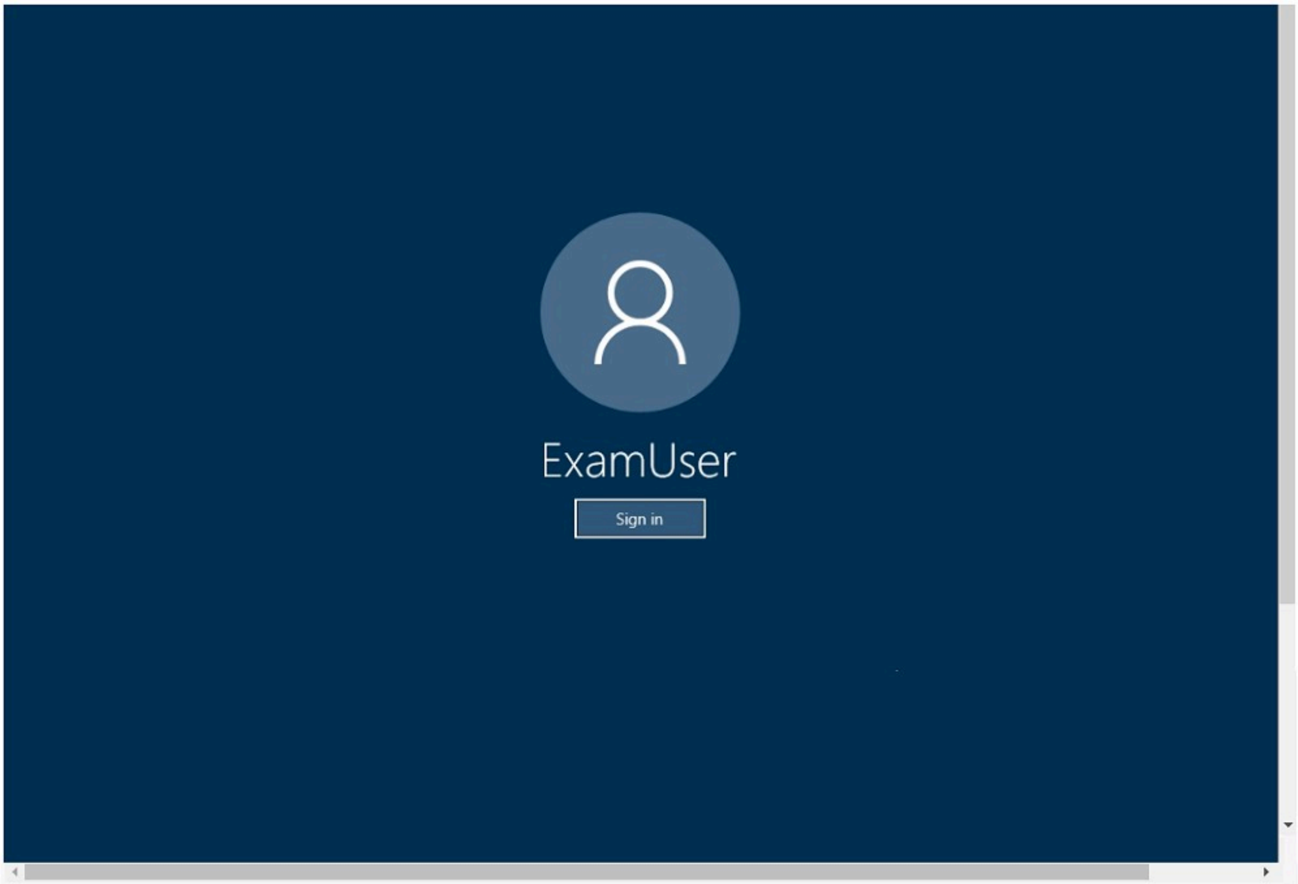
Scoring is based on the outcome of performing the tasks stated in the lab. In other words, it doesn't matter how you accomplish the task, if you successfully perform it, you will earn credit for that task.

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.

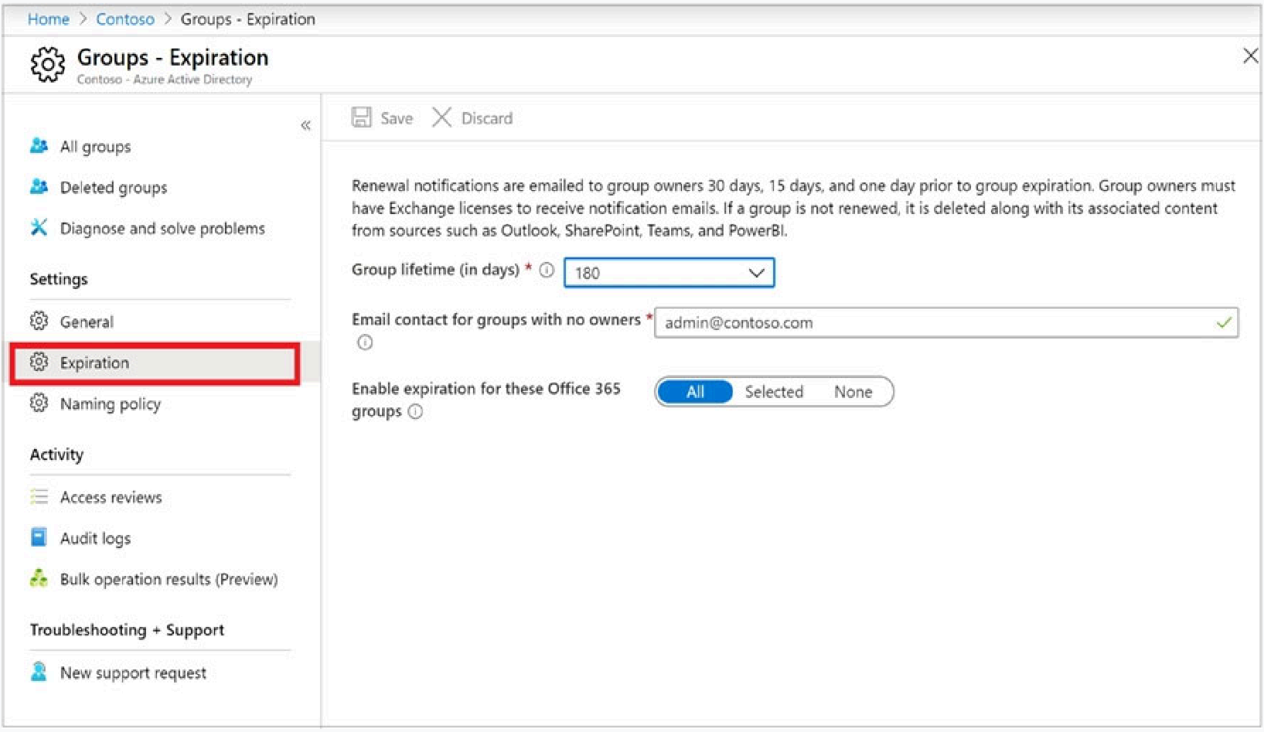
To complete this task, sign in to the Microsoft Office 365 admin center.

Suggested Answer: *See explanation below.*

Set group expiration -

1. Open the Azure AD admin center with an account that is a global administrator in your Azure AD organization.

2. Select Groups, then select Expiration to open the expiration settings.


Home > Contoso > Groups - Expiration
Groups - Expiration
Contoso - Azure Active Directory
«
All groups
Deleted groups
Diagnose and solve problems
Settings
General
Expiration
Naming policy
Activity
Access reviews
Audit logs
Bulk operation results (Preview)
Troubleshooting + Support
New support request
Save
Discard

Renewal notifications are emailed to group owners 30 days, 15 days, and one day prior to group expiration. Group owners must have Exchange licenses to receive notification emails. If a group is not renewed, it is deleted along with its associated content from sources such as Outlook, SharePoint, Teams, and PowerBI.

Group lifetime (in days) * ⓘ 180

Email contact for groups with no owners * ⓘ admin@contoso.com ✓

Enable expiration for these Office 365 groups ⓘ [✓ All] Selected None

3. On the Expiration page, you can:

➪ Set the group lifetime in days. You could select one of the preset values, or a custom value (should be 31 days or more).

➪ Specify an email address where the renewal and expiration notifications should be sent when a group has no owner.

➪ Select which Office 365 groups expire. You can set expiration for:

➪ All Office 365 groups

➪ A list of Selected Office 365 groups

➪ None to restrict expiration for all groups

Save your settings when you're done by selecting Save.

Reference:

https://docs.microsoft.com/en-us/azure/active-directory/users-groups-roles/groups-lifecycle

WMG Highly Voted 3 years, 4 months ago

Answer is correct.

upvoted 6 times

yoton 2 years, 6 months ago

Answer is correct.

upvoted 2 times

pompes Most Recent 1 year, 7 months ago

There was no simulation on my exam.

upvoted 1 times

adarvasi 2 years, 2 months ago

Correct answer. We use this setting to control "Teams" sprawl.

upvoted 1 times

Vic08 3 years, 7 months ago

https://portal.azure.com/#blade/Microsoft_AAD_IAM/GroupsManagementMenuBlade/Lifecycle

upvoted 2 times

Discuss4certi 3 years, 9 months ago

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

upvoted 1 times

mashaeg 3 years, 7 months 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 5 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.

Suggested Answer: *See explanation below.*

You need to configure the Exchange ActiveSync Access Settings.

1. Go to the Exchange admin center.
2. Click on Mobile in the left navigation pane.
3. On the Mobile Device Access page, click the Edit button in the Exchange ActiveSync Access Settings area.
4. Select the Quarantine option under When a mobile device that isn't managed by a rule or personal exemption connects to Exchange.
5. Optionally, you can configure notifications to be sent to administrators and a message to be sent to the mobile device user when a device is quarantined.
6. Click Save to save the changes.

Dooa Highly Voted 👍 3 years, 10 months ago

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

upvoted 13 times

FumerLaMoquette Highly Voted 👍 4 years, 1 month 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 7 times

Madskillz13 Most Recent ⊙ 2 years, 3 months ago

https://admin.exchange.microsoft.com/#/mobiledeviceaccess

upvoted 1 times

junior6995 2 years, 7 months ago

The "Mobile" option is not even avalible on the new Exchange Portal, very soon the access to the legacy portal will be removed and this question is very likely to be retired.

upvoted 1 times

joergsi 2 years, 10 months ago

About the provided answer:

You need to configure the Exchange ActiveSync Access Settings.

1. Go to the Exchange admin center.
2. Click on Mobile in the left navigation pane.
3. On the Mobile Device Access page, click the Edit button in the Exchange ActiveSync Access Settings area.

=> This EDIT Button is the edit button in the upper right area of your screen!

upvoted 7 times

Fernando001 2 years, 11 months ago

https://admin.microsoft.com/#/Domains/:/Settings/L1/PasswordPolicy

You can go to admin portal and search password expiration

upvoted 1 times

oopspruu 3 years, 4 months ago

I hope its a live O365 admin center environment in exam because this setting is only in classic EAC. Does anyone any way to access this in the Modern EAC or any alternate area?

upvoted 4 times

Rstilekar 3 years, 6 months ago

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

upvoted 4 times

TheGuy 3 years, 9 months ago

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

upvoted 5 times

⊟ **yassora** 3 years, 9 months 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.

Suggested Answer: *See explanation below.*

You need to configure the Password Expiration Policy.

1. Sign in to the Microsoft 365 Admin Center.
2. In the left navigation pane, expand the Settings section then select the Settings option.
3. Click on Security and Privacy.
4. Select the Password Expiration Policy.
5. Ensure that the checkbox labelled Set user passwords to expire after a number of days is ticked.
6. Enter 100 in the Days before passwords expire field.
7. Click Save changes to save the changes.

Nicholasname Highly Voted 4 years, 6 months ago

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

upvoted 21 times

Ray81 4 years, 3 months ago

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

upvoted 2 times

IvanDan 4 years, 3 months ago

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

upvoted 4 times

shanti0091 3 years, 11 months ago

true gospel

upvoted 1 times

Alpanama 3 years, 9 months ago

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

upvoted 4 times

SaadKhamis Highly Voted 1 year, 11 months ago

1. Sign in to the Microsoft 365 Admin Center.
2. In the left navigation pane, expand the Settings section then select the Org settings option.
3. Click on Security and Privacy.
4. Select the Password expiration policy.
5. Ensure that the checkbox labelled Set passwords is never expired (recommended) is not ticked.
6. Enter 100 in the Days before passwords expire field.
7. Click Save changes to save the changes.

upvoted 5 times

fr0do Most Recent 2 years, 10 months ago

Agree with Nicholas, had this also as Visual Lab is MS-100 and indeed you can do this at Settings > Org. Settings

upvoted 1 times

Shahidqk 3 years, 5 months 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 3 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.

Suggested Answer: *See explanation below.*

You need to assign the Service Administrator role to Grady Archie.

1. In the Microsoft 365 Admin Center, type Grady Archie into the Search for users, groups, settings or tasks search box.
2. Select the Grady Archie user account from the search results.
3. In the Roles section of the user account properties, click the Edit link.
4. Select the Customized Administrator option. This will display a list of admin roles.
5. Select the Service admin role.
6. Click Save to save the changes.

Reference:

https://docs.microsoft.com/en-us/office365/enterprise/view-service-health

btd2020 Highly Voted 4 years, 7 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 34 times

> **Bl0ckSh3ll** 4 years, 3 months 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 15 times
>
> > **shanti0091** 3 years, 11 months ago
> >
> > This is 100% correct.
> >
> > upvoted 4 times
>
> **alialiba** 3 years, 1 month ago
>
> Can we also do the same action via the Azure portal > Azure AD?
>
> upvoted 1 times

Cogan Highly Voted 3 years, 9 months ago

Service Support Admin Role

upvoted 6 times

Rstilekar Most Recent 3 years, 6 months ago

Checked. Its Service Support Administrator role now.

upvoted 1 times

ThBEST 3 years, 6 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

Mikula 4 years, 7 months ago

User need Service Administrator role.

https://docs.microsoft.com/en-us/office365/enterprise/view-service-health

upvoted 2 times

> **DrMe** 3 years, 12 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 10 times

Question #29 *Topic 1*

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

A. Security administrators

B. Information Protection administrator

C. Message center reader

D. Service administrator

Suggested Answer: *A*
In order to view and use the reports described in this article, you need to be a member of one of the following role groups in the Microsoft 365 Defender portal:
✑ Organization Management
✑ Security Administrator
✑ Security Reader
✑ Global Reader
Note:
There are several versions of this question in the exam. The question has two possible correct answers:
1. Security Administrator
2. Security Reader
Other incorrect answer options you may see on the exam include the following:
✑ Compliance administrator
✑ Exchange administrator
Reference:
https://docs.microsoft.com/en-us/microsoft-365/security/office-365-security/view-reports-for-mdo

Community vote distribution
A (100%)

keithtemplin 1 year, 10 months ago
Selected Answer: A
https://learn.microsoft.com/en-us/microsoft-365/security/office-365-security/reports-defender-for-office-365?view=o365-worldwide#what-permissions-are-needed-to-view-the-defender-for-office-365-reports

Membership in any of the following role groups:
Organization Management
Security Administrator
Security Reader
Global Reader
upvoted 2 times

ccadenasa 2 years, 2 months ago
Answer is correct > https://learn.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 4 times

gaida 2 years, 2 months ago
Security Reader might be correct if we go by the principle of least priv
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

Suggested Answer: *B*
The Global Admin can manage role assignments in Compliance Manager.
Incorrect Answers:
C: Portal Admin is for the now deprecated classic portal.
Reference:
https://docs.microsoft.com/en-us/microsoft-365/compliance/working-with-compliance-manager?view=o365-worldwide

Community vote distribution
B (67%) D (33%)

Mendel Highly Voted 3 years, 9 months 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 12 times

dzampar Highly Voted 4 years, 2 months 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

Maxx4 Most Recent 1 year, 6 months ago
Selected Answer: D
he answer is D, Compliance Manager Administrator.

The Compliance Manager Administrator role allows users to assign Compliance Manager roles to other users. This is the most specific role that allows User1 to perform this task, and it follows the principle of least privilege because it does not grant User1 any other unnecessary permissions.

The other roles are not as specific and would grant User1 more permissions than they need. For example, the Global Administrator role grants users full control over the Microsoft 365 subscription, and the Portal Admin role grants users the ability to manage the Compliance Manager portal.
upvoted 3 times

McMac 1 year, 6 months ago
No, the 'Compliance Admin' can but not the 'Compliance Manager Admin'
upvoted 2 times

gaida 2 years, 2 months ago
Global admin is correct when it comes to roles assignment
upvoted 2 times

Eltooth 2 years, 5 months ago

Selected Answer: B

B is correct answer.

upvoted 1 times

⊟ **LoremanReturns** 2 years, 8 months ago

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

upvoted 1 times

⊟ **arska** 2 years, 9 months ago

Selected Answer: B

See Mendel.

upvoted 2 times

⊟ **mkoprivnj** 3 years, 1 month ago

Selected Answer: B

B is correct!

upvoted 3 times

⊟ **Yetijo** 3 years, 6 months 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 4 times

⊟ **Rstilekar** 3 years, 6 months 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 4 times

⊟ **ZakS** 3 years, 7 months 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 2 times

⊟ **DudleyYVR** 3 years, 8 months ago

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

upvoted 2 times

⊟ **SerhioG** 3 years, 9 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.

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** 3 years, 9 months ago

Global Administrator is the correct answer.

No role called Portal Admin.

upvoted 1 times

⊟ **diazed** 3 years, 9 months 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** 3 years, 9 months 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** 3 years, 9 months 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** 3 years, 10 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

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

Suggested Answer: *A*
Reference:
https://docs.microsoft.com/en-us/microsoft-365/compliance/manage-gdpr-data-subject-requests-with-the-dsr-case-tool?view=o365-worldwide#step-1-assign- ediscovery-permissions-to-potential-case-members

Community vote distribution
A (100%)

⊟ **shanti0091** Highly Voted 3 years, 11 months ago
The answer is 100% correct. An E-Discovery Administrator role is superior in terms of RBAC than E-Discovery Manager.
upvoted 14 times

⊟ **Rstilekar** Highly Voted 3 years, 6 months ago
eDiscovery manager role is correct
upvoted 7 times

⊟ **heshmat2022** Most Recent 2 years, 3 months ago
The easiest way to do this is to go to the Permissions page in the compliance center and add users to the eDiscovery Manager role group.
upvoted 2 times

⊟ **yoton** 2 years, 3 months ago
The provided answer is correct.

The eDiscovery Manager role allows access specifically to cases it has created or been assigned to whereas the admin role has access to all cases.
upvoted 3 times

⊟ **preeya** 2 years, 5 months ago
Thanks to Exam topic, was able to answer this question confidently - july 27,2022
upvoted 3 times

⊟ **Eltooth** 2 years, 5 months ago
Selected Answer: A
A is correct answer.
Now in SC-400 exam.
upvoted 3 times

⊟ **mkoprivnj** 3 years, 1 month ago
Selected Answer: A
A is correct!
upvoted 3 times

⊟ **WMG** 3 years, 4 months ago
The answer is correct. the MANAGER role allows only access to cases it has created _or been assigned to_. The admin role has access to all cases.

So after assigning User 1 the MANAGER role, you would then assign the case to User 1.
upvoted 3 times

iwikneerg 3 years, 7 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 4 times

Enoll 3 years, 8 months 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 5 times

Azuanuka 3 years, 7 months 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 7 times

Enoll 3 years, 7 months ago

you are right!

upvoted 1 times

Nasser 3 years, 6 months ago

Totally agree

upvoted 1 times

NIck207 3 years, 9 months ago

E discovery manager is least privilege role, of course admin also correct but clearly stated least privilege,

upvoted 4 times

Faith 3 years, 12 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 3 years, 11 months ago

It says "Additionally, an eDiscovery Administrator can:" so Administrator is higher role than Manager.

upvoted 2 times

kiketxu 3 years, 9 months ago

Agree with eDiscovery Manager.

upvoted 2 times

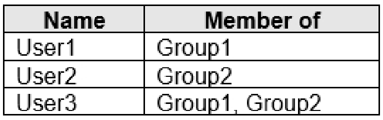
Tom993 4 years, 1 month ago

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

upvoted 2 times

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

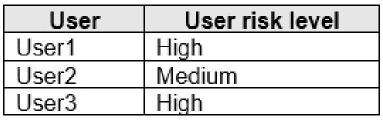
You create and enforce an Azure Active Directory (Azure AD) Identity Protection user risk policy that has the following settings:

✑ Assignments: Include Group1, Exclude Group2

✑ User-risk: 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.

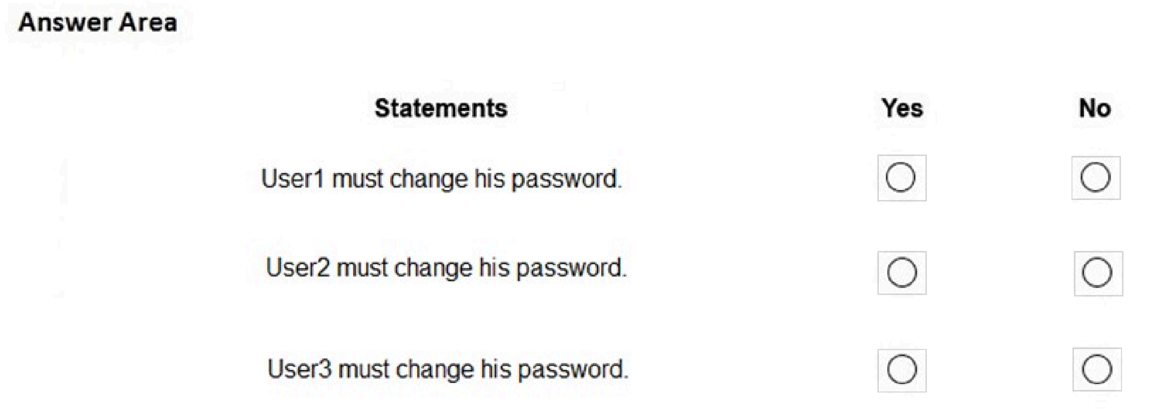


User	User risk level
User1	High
User2	Medium
User3	High

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

NOTE: Each correct selection is worth one point.

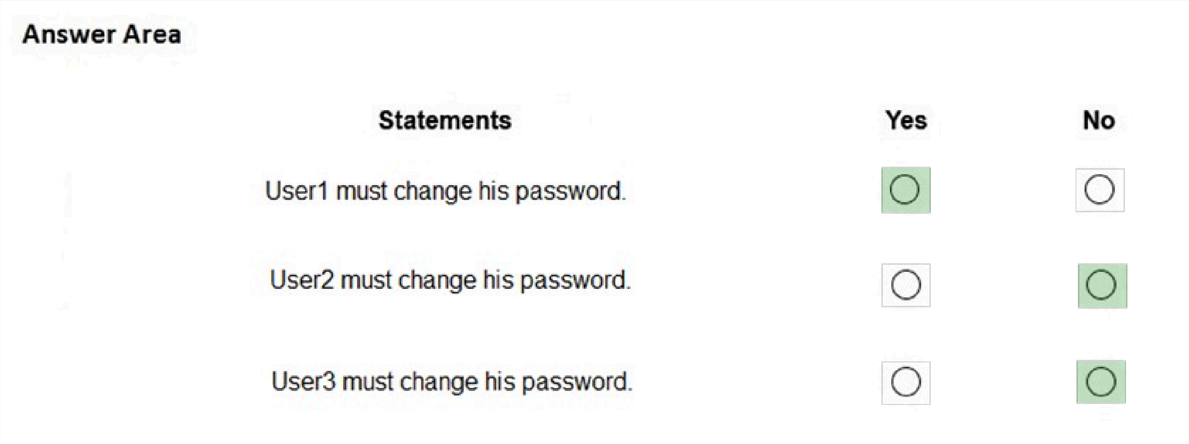
Hot Area:



Answer Area

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

Suggested Answer:



Answer Area

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

Box 1: Yes.

User1 is in Group1 which the policy applies to.

Box 2: No -

User2 is in Group2 which is excluded from the policy.

Box 3: No -

User3 is in Group1 which is included in the policy and Group2 which is excluded from the policy. In this case, the exclusion wins so the policy does not apply to
User3.

kiketxu Highly Voted 👍 3 years, 9 months ago

Yes, (High and included)

No, (Medium but excluded)

No, (High but excluded too)

upvoted 30 times

DarkAndy Highly Voted 👍 2 years, 6 months ago

Valid on exam. Jun 10, 2022

upvoted 6 times

adarvasi Most Recent ⊙ 2 years, 2 months ago

Correct answer.

Exclude overwrites include!

upvoted 3 times

pete26 2 years, 3 months ago

I think they changed the wording for this question. It says now a user risk policy. In this case the answers given are correct: Y, N, N

upvoted 5 times

SKam22 2 years, 4 months ago

N, N, N.

Sign in risk policy on supports MFA.

Password reset is for User risk policy!

upvoted 1 times

preeya 2 years, 5 months ago

valid on exam july 27,2022

upvoted 3 times

Eltooth 2 years, 5 months ago

Yes

No

No

upvoted 2 times

Bulldozzer 2 years, 5 months ago

This question is not clear or this is a trap because the Password change requirement is not an available option in the sign-in risk policy.

upvoted 1 times

> **Bulldozzer** 2 years, 5 months ago
>
> So, for me the answers should be No, No, No
>
> upvoted 2 times

[Removed] 2 years, 7 months ago

exclusion overrides inclusion, yes, no, no

upvoted 3 times

mkoprivnj 3 years, 1 month ago

Yes, (High and included)

No, (Medium but excluded)

No, (High but excluded too)

upvoted 2 times

MikeMatt2020 3 years, 4 months ago

I could be wrong, but the action for a sign-in risk policy to to "Require MFA". The USER RISK POLICY action is to require a password change. Are they trying to trick us with this question? The sign-in risk policy that is mentioned would not force the user to change his/her password, it would require MFA

Shouldn't it be NO, NO, NO

upvoted 4 times

Rstilekar 3 years, 6 months ago

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

upvoted 1 times

Dawid321 3 years, 8 months ago

Tricky, sign-in risk policy required MFA confirmation

upvoted 2 times

⊟ **ellik** 3 years, 8 months ago

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

upvoted 2 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

Suggested Answer: *B*
Reference:
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- atp-reports

Community vote distribution

B (100%)

Rstilekar Highly Voted 3 years, 6 months 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 15 times

Robert__Susin 3 years, 5 months ago
Correction: in the Microsoft 365 Defender portal
upvoted 2 times

Maxx4 Most Recent 1 year, 6 months ago
Selected Answer: B
The answer is B, Security reader.

The Security reader role allows users to view security reports, including ATP reports. This is the most specific role that allows User1 to perform this task, and it follows the principle of least privilege because it does not grant User1 any other unnecessary permissions.

The other roles are not as specific and would grant User1 more permissions than they need. For example, the Compliance administrator role grants users the ability to manage compliance policies, and the Message center reader role grants users the ability to view messages in the Message center.
upvoted 1 times

mbecile 2 years, 11 months ago
In order to view and use the ATP reports, you need to be a member of one of the following role groups in the Microsoft 365 Defender portal:

Organization Management
Security Administrator
Security Reader*
Global Reader

*Least Privilege

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 3 times

⊟ **mkoprivnj** 3 years, 1 month ago

Selected Answer: B

B is correct. Security reader.

upvoted 4 times

⊟ **kiketxu** 3 years, 9 months 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 3 times

⊟ **Alpanama** 3 years, 9 months ago

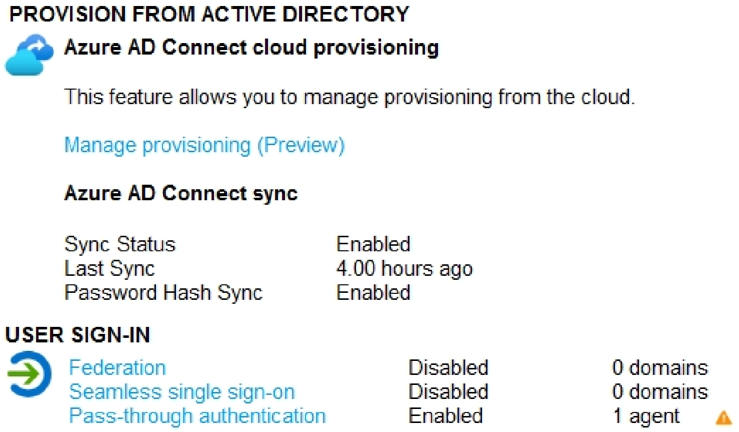
Changed to https://docs.microsoft.com/en-us/microsoft-365/security/office-365-security/view-reports-for-mdo?view=o365-worldwide#what-permissions-are-needed-to-view-the-defender-for-office-365-reports

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.



PROVISION FROM ACTIVE DIRECTORY

Azure AD Connect cloud provisioning

This feature allows you to manage provisioning from the cloud.

Manage provisioning (Preview)

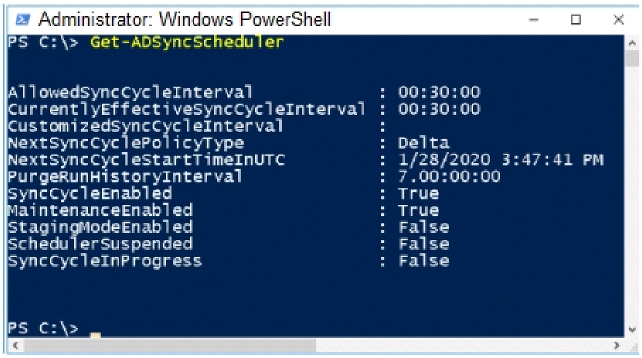
Azure AD Connect sync

Sync Status	Enabled
Last Sync	4.00 hours ago
Password Hash Sync	Enabled

USER SIGN-IN

Federation	Disabled	0 domains
Seamless single sign-on	Disabled	0 domains
Pass-through authentication	Enabled	1 agent ⚠

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



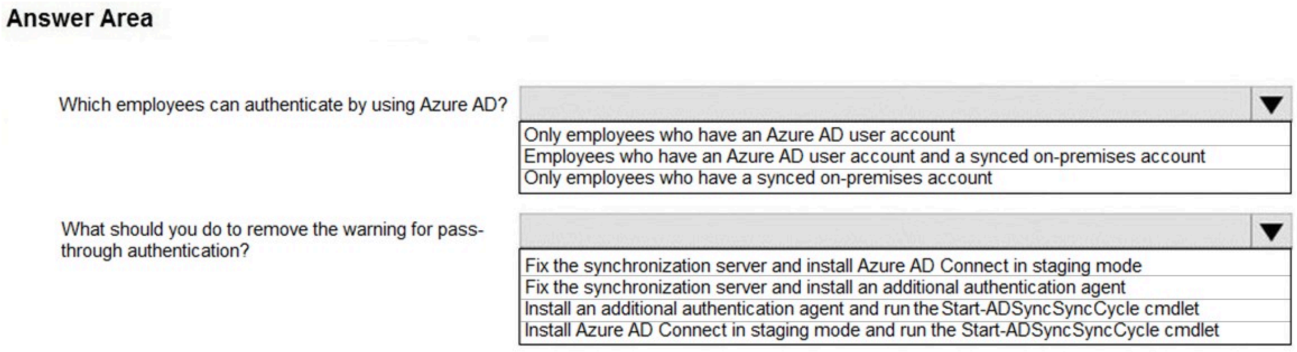
Administrator: Windows PowerShell

```
PS C:\> Get-ADSyncScheduler


AllowedSyncCycleInterval               : 00:30:00
CurrentlyEffectiveSyncCycleInterval : 00:30:00
CustomizedSyncCycleInterval            :
NextSyncCyclePolicyType                : Delta
NextSyncCycleStartTimeInUTC            : 1/28/2020 3:47:41 PM
PurgeRunHistoryInterval                : 7.00:00:00
SyncCycleEnabled                       : True
MaintenanceEnabled                     : True
StagingModeEnabled                     : False
SchedulerSuspended                     : False
SyncCycleInProgress                    : False



PS C:\> _
```

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

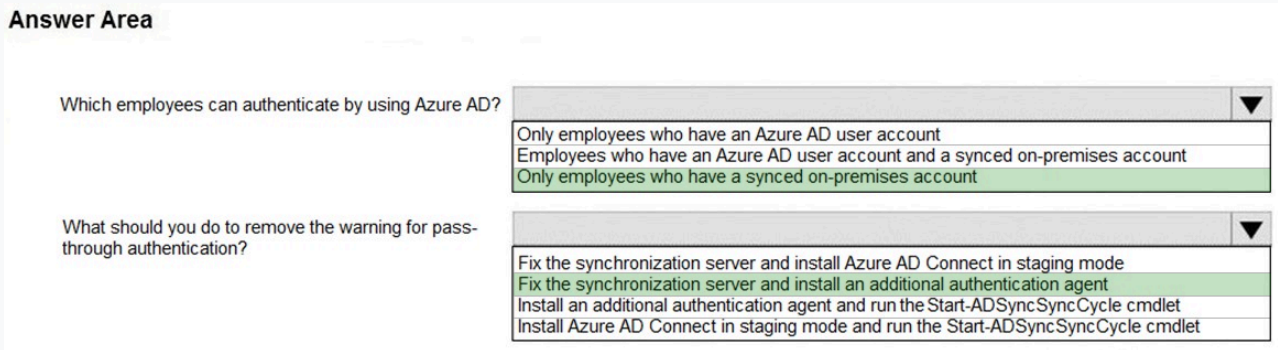
Which employees can authenticate by using Azure AD? ▼

- 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

Suggested Answer:



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

paperinop541 Highly Voted 3 years, 8 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 32 times

Vexix 1 year, 11 months ago
But the option 2 means that employee must have both accounts. Employees who have cloud account AND synced account, not OR. Bit of a trick answer and how you interpret the question.
upvoted 1 times

msysadmin 1 year, 10 months ago
I agree with paperinop541. It not saying both account, if it say like via Azure AD Connect then it will be right. Azure AD mean, it does not matter user synced from on-prem or registered on Cloud. Need to focus to question.
upvoted 2 times

gisbern Highly Voted 3 years, 8 months 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 13 times

Trevor 2 years, 11 months ago
You are required to have PTA agent HA to remove warnings if it goes down. Install 2 agents.. its a warning question.
upvoted 4 times

gisbern 3 years, 8 months 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 3 times

EzeQ 3 years, 1 month ago
But the ash sync is enabled, doesn't that count for something?
upvoted 2 times

EzeQ 3 years, 1 month ago
I reminded that might be just got password reset
upvoted 1 times

Bouncy 2 years, 9 months ago
No, it doesn't:
https://docs.microsoft.com/en-us/azure/active-directory/hybrid/how-to-connect-pta-faq
Does password hash synchronization act as a fallback to Pass-through Authentication?

No. Pass-through Authentication does not automatically failover to password hash synchronization.
upvoted 4 times

Anonymousse 2 years, 2 months ago
https://cloudacademy.com/blog/azure-hybrid-identity-authentication-methods/
upvoted 1 times

Orion8575 Most Recent 1 year, 6 months ago
Correct answer is 1-1 and 2-2 because it says that it did not sync for 4h, which means that if Azure AD Connect stops syncing, PTA functionality may be impacted. Users may experience issues logging in to Microsoft 365 as the authentication requests won't be processed against the on-premises directory.
upvoted 2 times

ChachaChatra 1 year, 11 months ago
Valid on 28/01/2023
upvoted 3 times

zerrowall 2 years ago
PTA is not now working due to 4 hours last time sync when the interval is only 30 minutes.
At the same time, Pass-through Authentication does not automatically failover to password hash synchronization, look here
https://learn.microsoft.com/en-us/azure/active-directory/hybrid/how-to-connect-pta-faq#does-password-hash-synchronization-act-as-a-fallback-to-pass-through-authentication-

In this case, only AAD users can authenticate.

This is 1st answer to the 1st question.

Regarding the 2nd question, we need to fix a problem and add an additional agent for HA to avoid warning. So the answer here is 2.

Eventually:

1 - 1

2 - 2

upvoted 4 times

bac0n 2 years, 1 month ago

I see no reason whatsoever why an Azure AD account would not be able to sign in if there were any issues on-prem. I'm going with 2 and 2.

upvoted 4 times

gaida 2 years, 2 months ago

Only on prem synced ac can authenticate as it uses passthrough auth instead of PHS.

Agent status has warning which is a key service for PTA. Ans is correct.

upvoted 2 times

pete26 2 years, 2 months ago

Valid on exam October 14, 2022

upvoted 4 times

SKam22 2 years, 4 months ago

According to the screenshot the AAD Connect sync stopped working but it synced before so the on-prem user and password databse were synced to AAD. Users who were already synced to AAD and all AAD users can still login to Azure AD. PTA agent is still running and can validate the password policies.

I would pick option 2 for Q1.

upvoted 1 times

ndilru 2 years, 9 months ago

3 ways of connecting your workstations to Microsoft Azure

* Azure AD Registered - BYOD concept, user can use a local account to log in and still use corporate 365 services with SSO
* Azure AD Joined - when configured users have to use user@xxx.com to login to their PC
* Hybrid Azure AD Joined - user has to provide a local domain username to access the PC.

So the question is, which employees can authenticate by using Azure AD?

according to the screenshot, we can see this is a hybrid setup, so the on-prem DC will be the primary authentication point.

So the answer is Only employees who have an on-premises account.

Note: they can also use Aure AD creds to access portal.office.com when they log in to the workstation inside.

upvoted 3 times

kanew 2 years, 10 months ago

I make it option 2 for both answers and even though I have worked with this for years I had to Lab it up to be sure (and still the MS wording is tricky!)

Firstly, even tho the sync server hasn't synced for hours the PTA agent still works (i tested this) so users with an AD synced a/c can still authenticate by logging in via AAD. The agent will still pick up their creds from the service bus. AAD users authenticate directly against AAD anyway so they can as well.

Second Question - Adding a second PTA authentication agent does fix the warning as everyone has said (tested). However, running start-AdSyncSyncCycle give an error if the AAD config wizard has been left open(the most likely problem and also tested) so only option 2 is correct.

upvoted 9 times

martinods 2 years, 10 months ago

Azure AD account (cloud only) and synced account can authenticate

upvoted 1 times

mbecile 2 years, 11 months ago

Question 1 = Answer 3, Only Synced On-Prem accounts can authenticate with Azure AD to sign into their On-Prem domain.

Answer 2 is incorrect because it states that they also need an Azure account on top of their synced On-Prem account, when they only require the latter, not both.

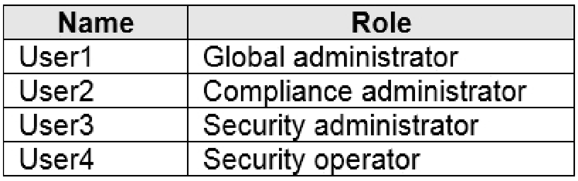
Question 2 (and it's answers) didn't make the most sense for me, so I'm going with the flow for that one and going with their answer.

upvoted 3 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:

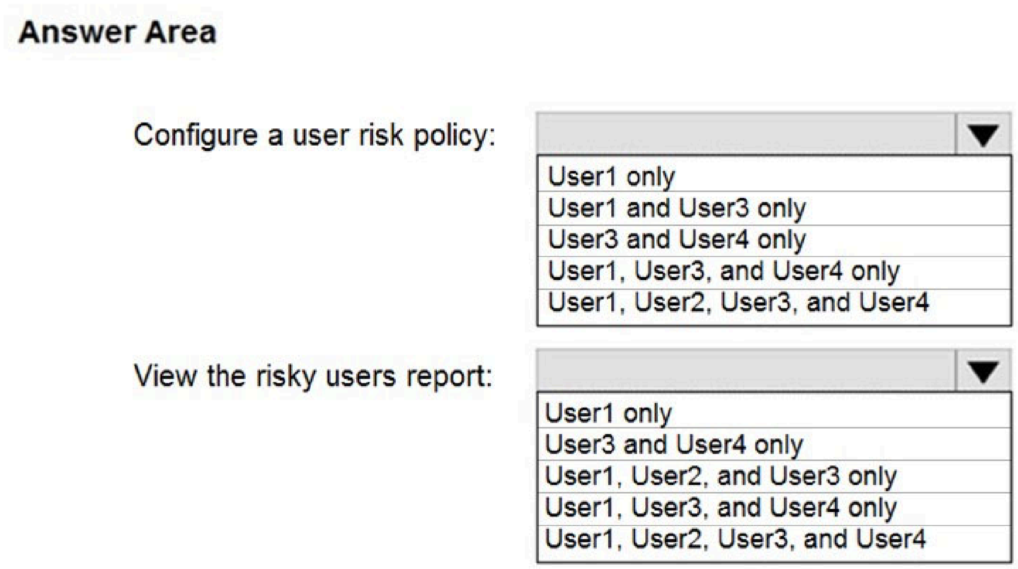
✑ Configure a user risk policy.

✑ 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

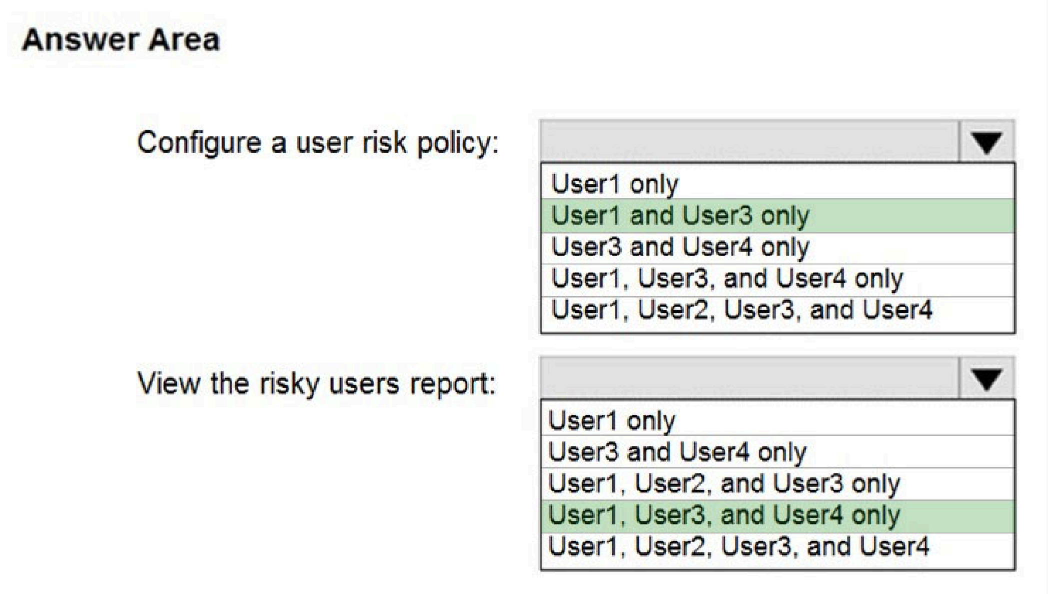
Configure a user risk policy: ▼

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

Suggested Answer:



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

Reference:

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

kiketxu Highly Voted 3 years, 9 months 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 37 times

ellik 3 years, 8 months 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 5 times

Grudo 2 years, 11 months ago

Because risky sign-ins and risky users are two different reports

upvoted 5 times

ccadenasa Most Recent 2 years, 1 month ago

Answers are correct > https://learn.microsoft.com/en-us/azure/active-directory/identity-protection/overview-identity-protection#required-roles

upvoted 1 times

mkoprivnj 3 years, 1 month ago

1.- User1 and User3

2.- User1, User3, User4

upvoted 2 times

iwikneerg 3 years, 7 months ago

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

upvoted 1 times

Sethoo 3 years, 9 months ago

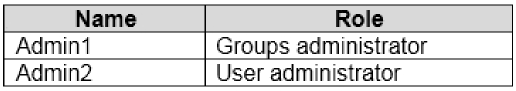
So the answer for 2 should be 1 &3 as well, but that is not in the options. So we go with 1 3 and 4 for now as in old times

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

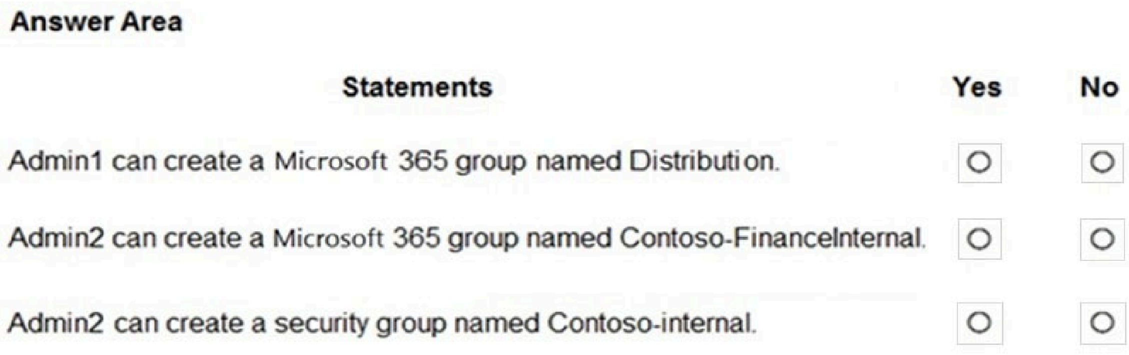
You add internal as a blocked word in the group naming policy for contoso.com.

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.

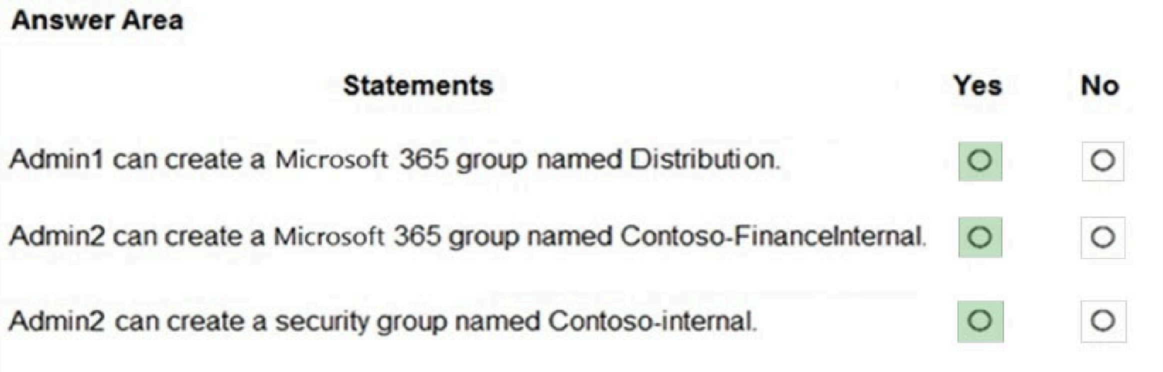
Hot Area:



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.	○	○

Suggested Answer:



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.	●	○

User Admin and Global Admin are exempt from group password policies.

Reference:

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

skalolaz Highly Voted 3 years, 8 months ago

N, Y, Y?

Groups admin is not an exempt.

upvoted 28 times

arunjana 3 years, 7 months 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 3 years, 7 months ago

N,Y,Y should be the correct answers

upvoted 10 times

Tam0924 3 years, 7 months ago

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

upvoted 6 times

⊟ **Ocico** 3 years, 7 months ago

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

upvoted 7 times

⊟ **Ocico** 3 years, 7 months ago

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

upvoted 5 times

⊟ **Chrissie73** 2 years, 7 months ago

YYY: You both are missing one thing. "To create a naming policy for distribution groups, see Create a distribution group naming policy." It is another kind of policy than described in the text. For that reason the policy for the prefix won't apply

upvoted 2 times

⊟ **chickenroaster** 1 year, 10 months ago

Some administrator roles are exempted from these policies, across all group workloads and endpoints, so that they can create groups using blocked words and with their own naming conventions. The following administrator roles are exempted from the group naming policy:

Global Administrator
User Administrator
https://learn.microsoft.com/en-us/azure/active-directory/enterprise-users/groups-naming-policy

upvoted 1 times

⊟ **prats005** Highly Voted 3 years, 4 months ago

N Y Y Roles and permissions
To configure naming policy, one of the following roles is required:

Global Administrator
Group Administrator
Directory Writer
Some administrator roles are exempted from these policies, across all group workloads and endpoints, so that they can create groups using blocked words and with their own naming conventions. The following administrator roles are exempted from the group naming policy:

Global Administrator
User Administrator

upvoted 17 times

⊟ **AVN1711** Most Recent 1 year, 3 months ago

may be I loose something ? are the answers should be Y,Y,N ?
or may be the order of questions was changed/updated recently? N for the question:
Admin2 (user administrator) can create a security group named Contoso-internal (internal – blocked word)

upvoted 1 times

⊟ **czaaa** 1 year, 6 months ago

Custom blocked words
You can enter a comma separated list of blocked words that will be blocked in group names and aliases.

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.

Things to look out for:

The blocked words are case-insensitive.

When a user enters a blocked word, the group client will show an error message with the blocked word.

There are no character restrictions in the blocked words used.

There is a limit of 5000 words that can be set as blocked words.

upvoted 1 times

⊟ **pompes** 1 year, 7 months ago

Agree with the answer it was on the exam

upvoted 2 times

⊟ **Dhamus** 1 year, 8 months ago

NO: The Group Administrator role is not exempt from the policy.

YES and YES: The User Administrator is exempt from the directive so he can do whatever he wants.

upvoted 1 times

⊟ **GatesBill** 1 year, 9 months ago

Just tested the exact given scenario in a lab and these are the results:

N (suffix/prefix warning) - Groups admins are not an exempt!

Y

Y

upvoted 2 times

⊟ **naylinu** 1 year, 10 months ago

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

upvoted 1 times

⊟ **hans333** 2 years ago

Created users with mentioned permissons in lab, also created Block Words and Group naming policy. Then tested, could create all 3 groups. so its YYY

upvoted 1 times

⊟ **rick001** 1 year, 11 months ago

TL;DR N,Y,Y

On topic : How is that possible since Group Admin is not exempted. So you get <PREFIX>-Distribution.. not what the questions states.

So i recreated this in a live environment on 31/01/2023 :

1. N - not exempted so you get prefix <group> as Group Admin.
2. Y - As User Admin you can bypass / overrule the policy.
3. Y - As User Admin you can bypass / overrule the policy.

If you had 3. with GROUPS ADMIN then it would also be YES since it only applies to Microsoft 365 groups and not security (FYI)

upvoted 2 times

⊟ **bac0n** 2 years, 1 month ago

Given answer is wrong. It's NYY. Just tested in my lab.

upvoted 1 times

⊟ **ccadenasa** 2 years, 1 month ago

Disregard my first answer. The correct answer is No, Yes, Yes

upvoted 1 times

⊟ **ccadenasa** 2 years, 1 month ago

The answer is correct: Yes, Yes, Yes. Tested in my Lab > https://techcommunity.microsoft.com/t5/microsoft-365-groups/introducing-the-groups-admin-role/m-p/978995

upvoted 1 times

⊟ **TweetleD** 2 years, 1 month ago

Answer is wrong. Should be Yes Yes Yes because Distribution is not a blocked word and User Administrator is exempt from blocked words and can override

upvoted 2 times

⊟ **pete26** 2 years, 2 months ago

Valid on exam October 14, 2022

upvoted 3 times

⊟ **CertRookie** 2 years, 2 months ago

Which one is valid? The site answer Y/Y/Y or forum N/Y/Y?

upvoted 3 times

⊟ **heshmat2022** 2 years, 3 months ago

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

upvoted 1 times

⊟ **Trainee2244** 2 years, 3 months ago

N,Y,Y Because the Groups Admin has to follow the Naming Policy, User Admin is excepted from any Naming Policy and Naming Policys are valid for M365 Groups only.

upvoted 2 times

⊟ **NarenKA** 2 years, 4 months ago

The Answer is: Y Y Y

The following admin roles are exempt from the group naming policy:

Global admin
User account admin
Partner Tier 1 Support
Partner Tier 2 Support
Therefore User1 and User2 don't need to follow the group naming policies

upvoted 3 times

Question #37 *Topic 1*

DRAG DROP -

You have a Microsoft 365 tenant.

User attributes are synced from your company'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:

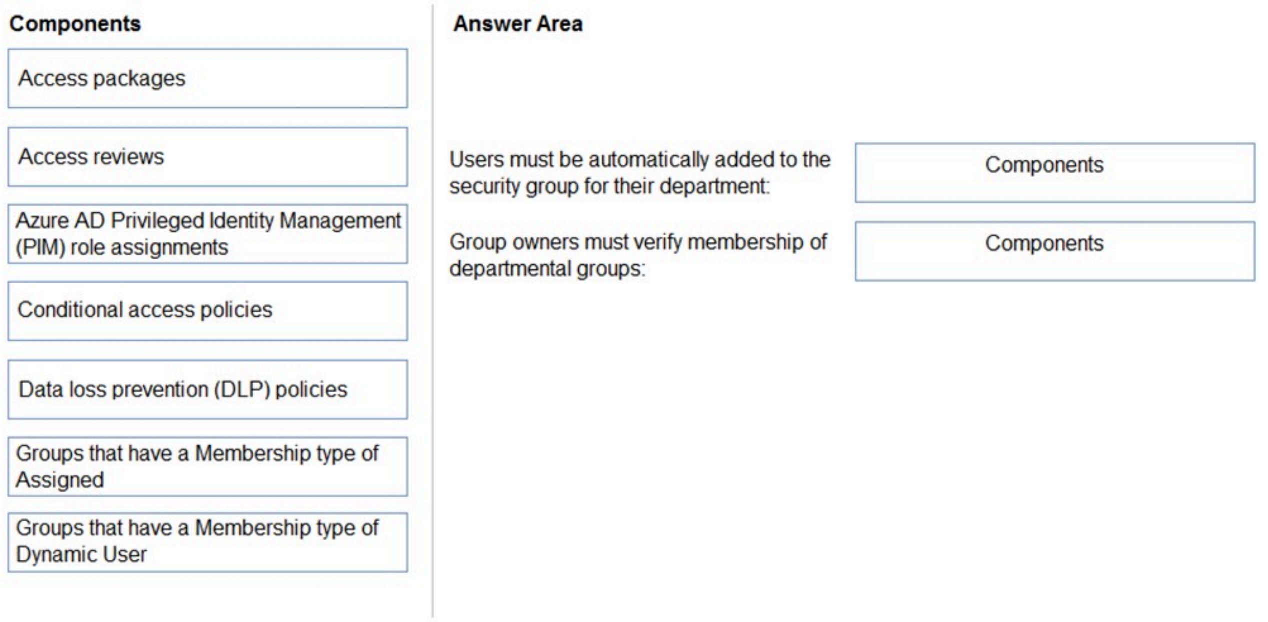
✑ Users must be added automatically to the security group of their department.

✑ 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:



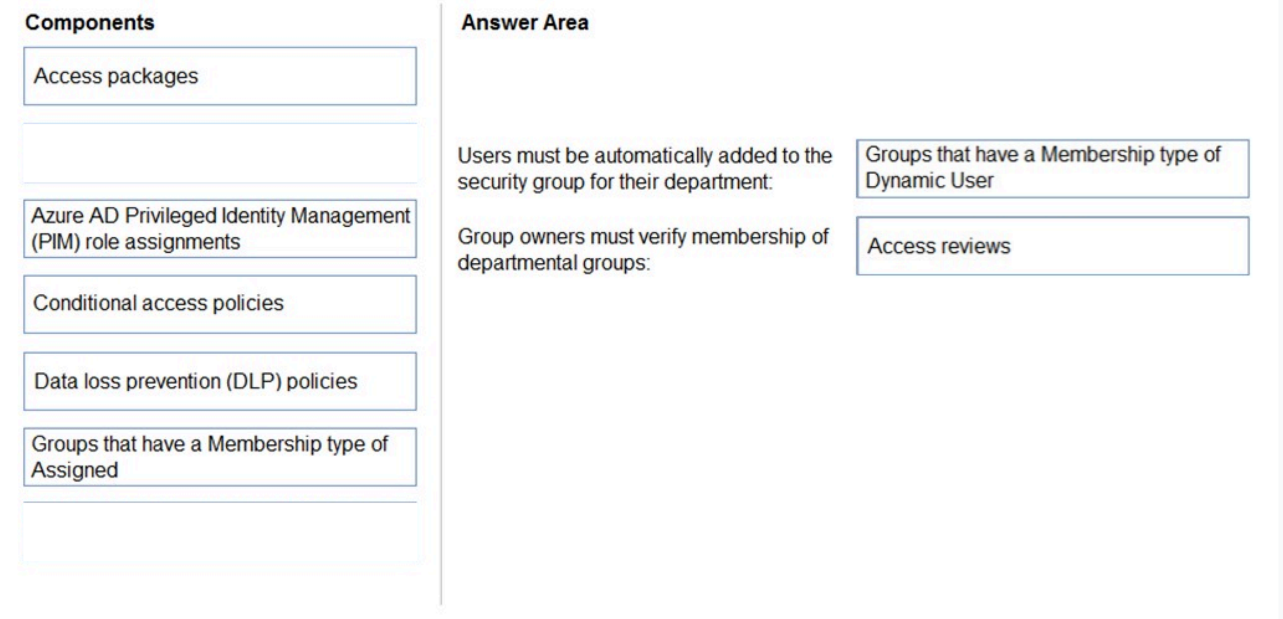
Components

- 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

Suggested Answer:



Components

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

Answer Area

Users must be automatically added to the security group for their department:	Groups that have a Membership type of Dynamic User
Group owners must verify membership of departmental groups:	Access reviews

Reference:

https://cloudbuild.co.uk/tag/create-a-dynamic-security-group-in-azure-ad/ https://docs.microsoft.com/en-us/azure/active-directory/governance/access-reviews-overview

kiketxu Highly Voted 3 years, 9 months ago given answers are correct

upvoted 28 times

⊟ **Patesso** Most Recent 1 year, 7 months ago

etait a l'examen 18/05/2023

upvoted 2 times

⊟ **lcaothu92** 1 year, 10 months ago

given answers are correct

upvoted 1 times

⊟ **ccadenasa** 2 years, 1 month ago

answers are correct

upvoted 2 times

⊟ **adarvasi** 2 years, 2 months ago

The given solution is correct.

We use these settings in the same way.

upvoted 1 times

⊟ **KarambaFr** 2 years, 3 months ago

If site is only accessible to users that are from the department (using dynamic groups), it's not really usefull to run access review :)

However answers are correct

upvoted 1 times

⊟ **ciaphas** 2 years, 3 months ago

can't do access review on dynamic groups

https://learn.microsoft.com/en-us/azure/active-directory/governance/create-access-review

upvoted 1 times

⊟ **gaida** 2 years, 2 months ago

sounds like Dynamic group for guest user rules only. Not for internal user dynamic group membership based on department.

upvoted 1 times

⊟ **preeya** 2 years, 5 months ago

valid on exam july 27,2022

upvoted 4 times

⊟ **mkoprivnj** 3 years, 1 month ago

1st: Dynamic User

2nd: Access review

upvoted 2 times

⊟ **armandolubaba** 3 years, 5 months ago

The answers are correct

upvoted 3 times

⊟ **iwikneerg** 3 years, 7 months ago

given answers are correct

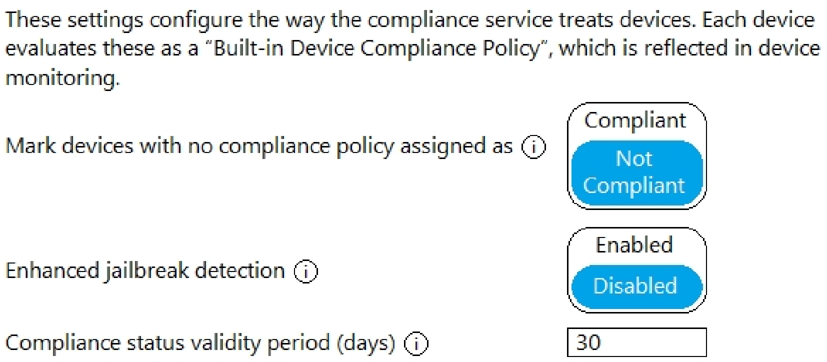
upvoted 3 times

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.



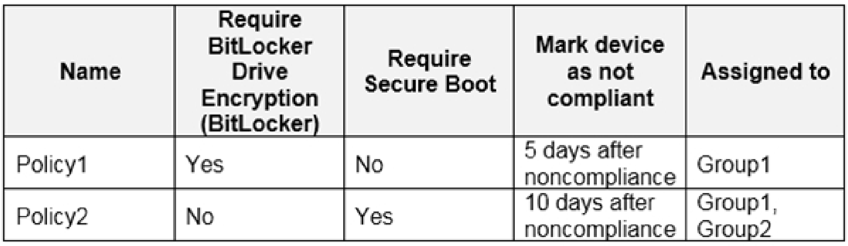
These settings configure the way the compliance service treats devices. Each device evaluates these as a "Built-in Device Compliance Policy", which is reflected in device monitoring.

Mark devices with no compliance policy assigned as ⓘ Compliant [✓ Not Compliant]

Enhanced jailbreak detection ⓘ Enabled [✓ Disabled]

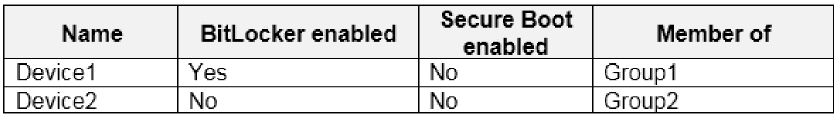
Compliance status validity period (days) ⓘ 30

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

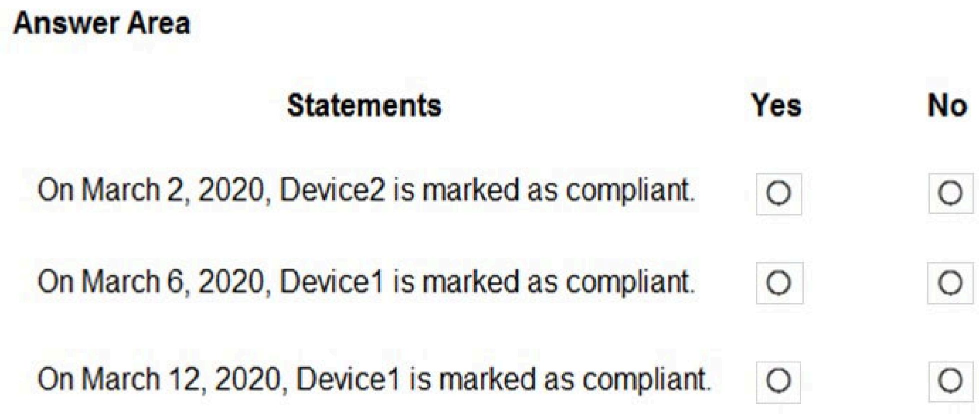


Name	BitLocker enabled	Secure Boot enabled	Member of
Device1	Yes	No	Group1
Device2	No	No	Group2

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

NOTE: Each correct selection is worth one point.

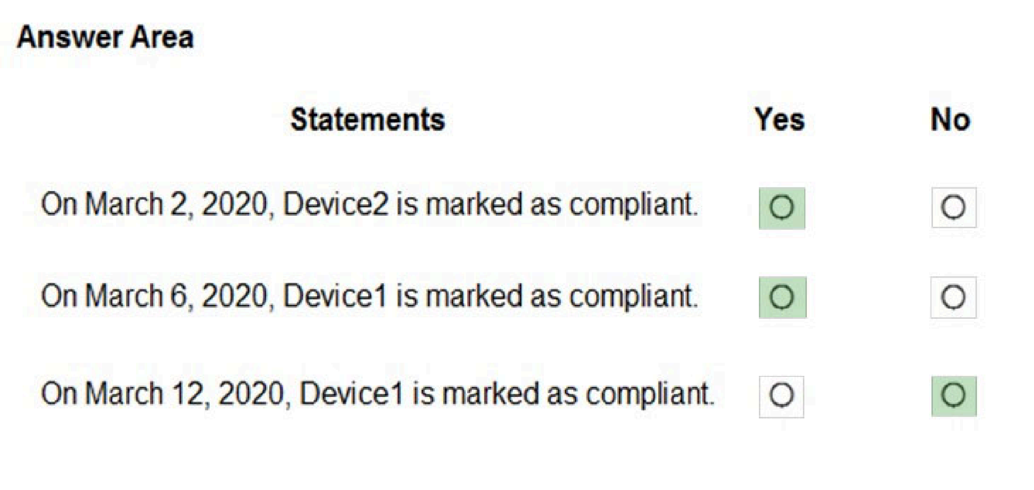
Hot Area:



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.	○	○

Suggested Answer:



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.	○	[✓ ○]

Box 1: Yes -

Device2 is in Group2 so Policy2 applies.

Device2 is not compliant with Policy2. However, the device won't be marked as non-compliant until 10 days after the device was enrolled.

Box 2: Yes -

Device1 is in Group1 and Group2 so both Policy1 and Policy2 apply.

Device1 is compliant with Policy1 but non-compliant with Policy2. However, the device won't be marked as non-compliant until 10 days after the device was enrolled.

Box 3: No -

Device1 is in Group1 and Group2 so both Policy1 and Policy2 apply.

Device1 is compliant with Policy1 but non-compliant with Policy2. th

March 12 -

is more than 10 days after the device was enrolled so it will now be marked as non-compliant by Policy2.

WMG Highly Voted 3 years, 4 months ago

There are only two states in Endpoint Manager for devices; compliant or non-compliant. The screenshot shows that devices without a compliance policy assigned are marked non-compliant. All the devices have a compliance policy in this example so they will be marked as compliant as default.

The devices are enrolled on March 1. They become compliant as a policy is assigned to them. Then the evaluation of the policy kicks in, which may or may not change the compliance state.

On March 2, Device 2 is marked as compliant. Policy 2 states non-compliant after 10 days only.

On March 6, Device 1 is marked as compliant. Policy 2 states non-compliant after 10 days only.

On march 12, Device 1 is marked as _noncompliant_ as it has been 11 days and Policy2 states 10 days max.

Answers are correct (Y/Y/N). Note that the default grace period is 0 days, but the example has 5 and 10 days instead. If there is no mention of this in the question, then always assume 0.

upvoted 22 times

Magheno 2 years, 9 months ago

Policy 2 does not apply to Device 1 is it is linked to Group 2 and device 2 is not linked to group 2. So that make Y/Y/Y for me.

upvoted 1 times

LillyLiver 2 years, 9 months ago

Sorry, wrong.

Policy2 does apply as the policies are applied in order. Meaning Policy1 applies to Group1, which Device1 is a member, but policy2 is also applied to Group1. Since Policy2 is applied to Group1 last, it has precedence. So the re-evaluation time for Device1 is 10 days.

These policies are applied just like Group Policies in Active Directory. The last one applied has the precedence.

Given answers are correct.
upvoted 2 times

CharlieBash 1 year, 10 months ago
Guees that's wrong too. Multiple compliance policy don't work with precedence but which one is most strict. So that would be non-comliant after 5 days and makes device 1 at 6 march non-comliant. So Y N N
https://learn.microsoft.com/en-us/mem/intune/configuration/device-profile-troubleshoot#if-multiple-policies-are-assigned-to-the-same-user-or-device-how-do-i-know-which-settings-gets-applied
upvoted 2 times

ZakS Highly Voted 3 years, 7 months 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 12 times

WMG 3 years, 4 months ago
Not correct, the In grace period is defined as 5 and 10 days. Devices are marked as compliant per having a policy. When they do not fulfill the requirements of a specific policy setting, the grace period kicks in. This does not change it to non-compliant; it is still listed as compliant until grace period ends. The grace period is to make sure users get can compliant without being non-compliant - for all intents and purposes the device is compliant and CA policies apply etc.
upvoted 3 times

danb67 3 years, 2 months ago
When you change the default schedule, you provide a grace period in which a user can remediate issues or become compliant without being marked as non-compliant.

This action is supported on all platforms supported by Intune.
upvoted 1 times

martinods 3 years ago
what is grace period ? you means Compliance status validity period (days) ?
from MS Compliance status validity period (days)
Specify a period in which devices must successfully report on all their received compliance policies. If a device fails to report its compliance status for a policy before the validity period expires, the device is treated as noncompliant.
In this case the correct answers are YYN
upvoted 4 times

examdog Most Recent 2 years ago
The given answer YYN is correct. The third question is about the conflict among policies. "If you have deployed multiple compliance policies, Intune uses the most secure of these policies." https://learn.microsoft.com/en-us/mem/intune/protect/compliance-policy-monitor
upvoted 1 times

gaida 2 years, 2 months ago
answers are correct but the explanation are not correct. As Device1 is not the member of group1 and grop2. It is actually the policy applied to both group which hits Device1
upvoted 1 times

Ufuk_Ari 2 years, 4 months ago
Valid on Exam, 29.08.22
upvoted 4 times

heyhey12345 2 years, 5 months ago
can these get any more confusing... my god
upvoted 6 times

Whatsamattr81 2 years, 6 months ago
The devices won't be marked as compliant (green), they will be marked as "in grace period" for 5 days, upon which they will marked non compliant. This is nothing to do with access, just tagging on the portal. These machines never get marked as compliant, ever.
upvoted 1 times

Whatsamattr81 2 years, 6 months ago

Surely NNN. Mark devices non compliant after 30 days just means the device (whether compliant or not) will be marked on compliant if it doesn’t report status (whatever status) after 30 days. These devices, once added will all report as non compliant immediately. The 5 day grace period is for machines that were previously compliant but have (for whatever reason) become non compliant. When two conflicting policies apply to a group, the most restrictive settings are adopted. These devices, once added will be non compliant, and remain non compliant.
upvoted 1 times

Whatsamattr81 2 years, 6 months ago
https://docs.microsoft.com/en-us/mem/intune/protect/create-compliance-policy
None of these devices get marked compliant as there device settings wouldnt allow it. . They will all be in grace period until the clock runs out then get marked non compliant.
upvoted 1 times

ARYMBS 2 years, 7 months ago
N/Y/N
Why everyone misses "Mark devices with no compliance policy assigned as Non Compliant"?

N - Device2 has no Secure Boot Enabled which is a requirement of Policy2. So Device has no Compliance policy. Now Merge this with "Mark devices with no compliance policy assigned as Non Compliant" and we get the answer.
Y - Device1 Has Bitlocker and does not have Secure Boot Enabled. So it passes Policy1 but does not passes Policy2. So, basically, it passes Policy1 requirements but does not Policy2 requirements. This upon device Enrollment will mark Device1 as Compliant during the period 2020-03-01 - 2020-03-11. At 2020-03-12 will kick in Policy2 "Mark device as not compliant" and device from this day on will be marked as not compliant.
N - Device1 Has Bitlocker and does not have Secure Boot Enabled. So it passes Policy1 but does not passes Policy2. So, basically, it passes Policy1 requirements but does not Policy2 requirements. This upon device Enrollment will mark Device1 as Compliant during the period 2020-03-01 - 2020-03-11. At 2020-03-12 will kick in Policy2 "Mark device as not compliant" and device from this day on will be marked as not compliant.
upvoted 2 times

sliix 2 years, 7 months ago
Device2 has a compliance policy assigned, which is Policy2 (you even said this yourself). Of course in this case it does not meet the requirement, but does not mean it doesn't have the policy applied. "Mark devices with no compliance policy assigned as Non Compliant" you said here is for device without any policy assigned at all.
upvoted 2 times

ARYMBS 2 years, 6 months ago
Good answer. Thanks.
upvoted 1 times

kjarant 2 years, 8 months ago
Anyone consider leap year?
upvoted 2 times

mbecile 2 years, 11 months ago
Don't trip yourself up over semantics.
It's a boolean measurement, so it can only be one or the other.
Very black and white determinations.
- Is it non-compliant?
- "Well, not right now. Technically."
- Cool! I'll go ahead an mark it as the only other option then.
upvoted 2 times

phatboi 2 years, 12 months ago
let us learn to understand scenarios here; yes the default ms compliance policy is 0 however in this scenario a grace period was mentioned. Having said that.
The devices are enrolled on March 1. They become compliant as a policy is assigned to them. Then the evaluation of the policy kicks in, which may or may not change the compliance state.

On March 2, Device 2 is marked as compliant. Policy 2 states non-compliant after 10 days only. the device is still within the grace period of 2days.

On March 6, Device 1 is marked as compliant. Policy 2 states non-compliant after 10 days only. the device is still within the grace period of 6 days

On march 12, Device 1 is marked as _noncompliant_ as it has been 11 days and Policy2 states 10 days max. Device 1 which is a member of group 1 and group 1 is a member of plicy 2 will become non-compliant as grace period of 10days has elasped.

upvoted 3 times

Ginaglia 2 years, 1 month ago

Why Device1 shall become non-compliant if its settings are compliant with Policy1?

upvoted 1 times

lojlkdnfvlirez 3 years, 3 months ago

YYN: "When you change the default schedule, you provide a grace period in which a user can remediate issues or become compliant without being marked as non-compliant." Source : https://docs.microsoft.com/en-us/mem/intune/protect/actions-for-noncompliance

upvoted 2 times

Carlonerosse 3 years, 4 months ago

I Prepared my Microsoft MS-500 Exam within 3 days with the help of Validexamdumps Updated Microsoft 365 Security Administration MS-500 Practice Test Material. On the Final Exam Day, I Easily Attempted All questions and I Got Success in Microsoft MS-500 exam the First Attempt.

upvoted 1 times

CAINBJJ 3 years, 6 months ago

I a gree with ZakS

upvoted 1 times

Not_A_Bot_ 3 years, 7 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 4 times

Not_A_Bot_ 3 years, 6 months 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 3 times

Thespy45 3 years, 6 months 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

danb67 3 years, 2 months ago

When you change the default schedule, you provide a grace period in which a user can remediate issues or become compliant without being marked as non-compliant.

So the device is noncompliant but is still tagged as compliant so therefore wont get blocked because only when a device is tagged as non compliant will it then trigger the ca policy which blocked access.

upvoted 1 times

MikeMatt2020 3 years, 4 months ago

I see what you're saying in terms of access. But I think the answer is ultimately N/N/N

"In-grace period: The device is targeted with one or more device compliance policy settings. But, the user hasn't applied the policies yet. This status means the device is not-compliant, but it's in the grace-period defined by the admin."

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

upvoted 2 times

Topgeer123 3 years, 8 months ago

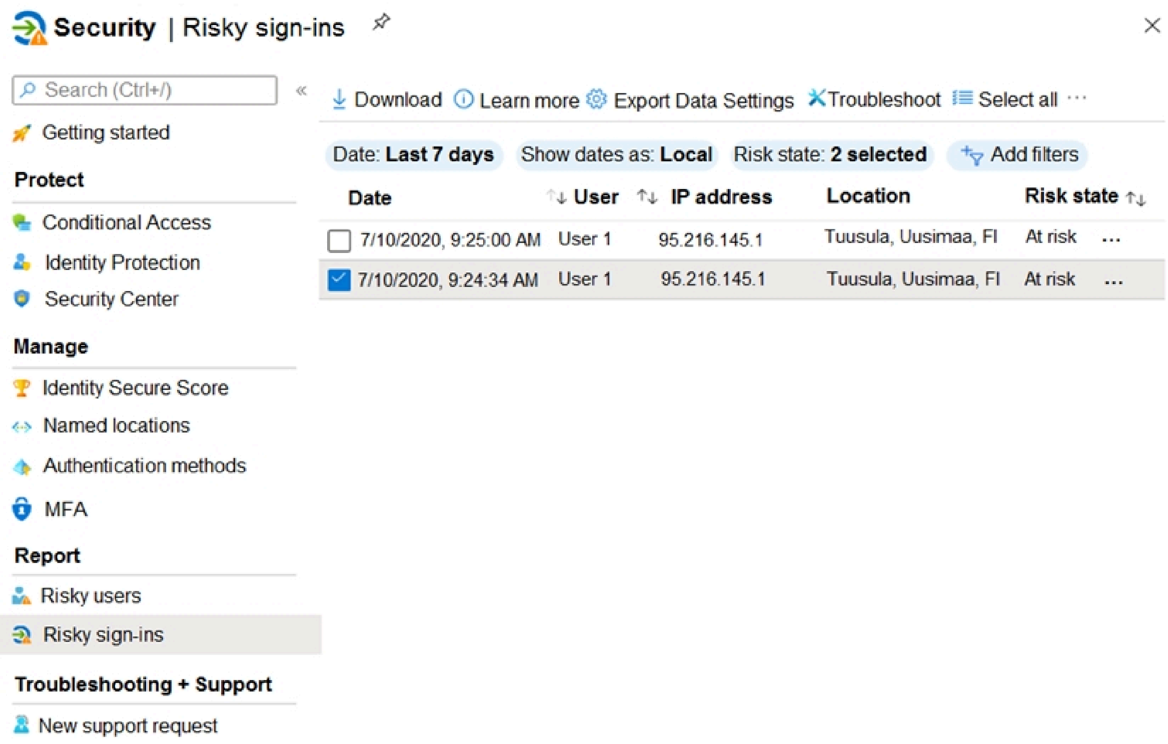
given answers are correct, device1 is assigned to group1 and policy1 and policy2 are both assigned to group1 and policy2 is also assigned to group1. so device1 got both policies and 5 days later the device is still compliant due to the settings of policy2 :)

upvoted 1 times

Question #39 Topic 1

You have a Microsoft 365 tenant.

From the Azure Active Directory admin center, you review the Risky sign-ins report as shown in the following exhibit.



Security | Risky sign-ins

Date: **Last 7 days** Show dates as: **Local** Risk state: **2 selected** Add filters

	Date	User	IP address	Location	Risk state	
☐	7/10/2020, 9:25:00 AM	User 1	95.216.145.1	Tuusula, Uusimaa, FI	At risk	...
☑	7/10/2020, 9:24:34 AM	User 1	95.216.145.1	Tuusula, Uusimaa, FI	At risk	...

You need to ensure that you can see additional details including the risk level and the risk detection type.

What should you do?

A. Purchase Microsoft 365 Enterprise E5 licenses.

B. Activate an instance of Microsoft Defender for Identity.

C. Configure Diagnostic settings in Azure Active Directory (Azure AD).

D. Deploy Azure Sentinel and add a Microsoft Office 365 connector.

Suggested Answer: *A*

Community vote distribution

A (67%) U (33%)

king001 1 year, 7 months ago

Selected Answer: A

E5 license which has P2 is correct

upvoted 1 times

Dhamus 1 year, 7 months ago

That's right, you need to get a P2 to view and configure additional details.

upvoted 1 times

rick001 1 year, 12 months ago

he can open the risky sign in so that means he has a P2... so this answer is not correct..?

upvoted 1 times

Tommy0000 1 year, 10 months ago

Actually, you can access a limited version of risky sign-in with free and P1 licenses

https://learn.microsoft.com/en-us/azure/active-directory/identity-protection/overview-identity-protection#license-requirements

upvoted 2 times

fuduran 1 year, 12 months ago

I just hate it when answer is incomplete as purchasing licenses but not assigning them will do nothing

upvoted 2 times

⊟ **gaida** 2 years, 2 months ago

AAD P2 is not an option, therefore, E5 license which has P2 as al la carte is correct

upvoted 1 times

⊟ **EzeQ** 2 years, 3 months ago

Selected Answer: A

As per the link you need a AAD premium P2license to do some good stuff, and in other articles to get more risk info

As per the link you need a AAD premium P2 license to get more risk info - AAD P2 is part of the Microsoft E5 license.

https://learn.microsoft.com/en-us/azure/active-directory/identity-protection/overview-identity-protection#license-requirements

upvoted 1 times

Question #40 *Topic 1*

You have a Microsoft 365 E5 subscription.

You plan to create a conditional access policy named Policy1.

You need to be able to use the sign-in risk level condition in Policy1.

What should you do first?

A. Connect Microsoft Endpoint Manager and Microsoft Defender for Endpoint.

B. From the Azure Active Directory admin center, configure the Diagnostics settings.

C. From the Endpoint Management admin center, create a device compliance policy.

D. Onboard Azure Active Directory (Azure AD) Identity Protection.

Suggested Answer: *D*

Reference:

https://docs.microsoft.com/en-us/azure/active-directory/conditional-access/howto-conditional-access-policy-risk

MayTheForceBeWithYou Highly Voted 👍 2 years, 3 months ago

Risk Levels indicates Protection as a reference...

upvoted 6 times

H0TDOGG Most Recent 🕒 1 year, 8 months ago

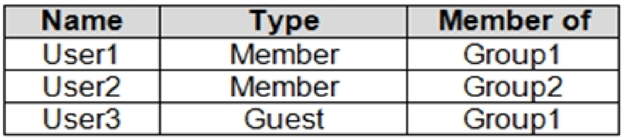
The wording, Onboarding, irritates me. Enable the Identity protection yes, not onboard.

upvoted 3 times

Question #41 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	Type	Member of
User1	Member	Group1
User2	Member	Group2
User3	Guest	Group1

You assign an enterprise application named App1 to Group1 and User2.

You configure an Azure AD access review of App1. The review has the following settings:

✑ Review name: Review1

✑ Start date: 01`"15`"2020

✑ Frequency: One time

✑ End date: 02`"14`"2020

✑ Users to review: Assigned to an application

✑ Scope: Everyone

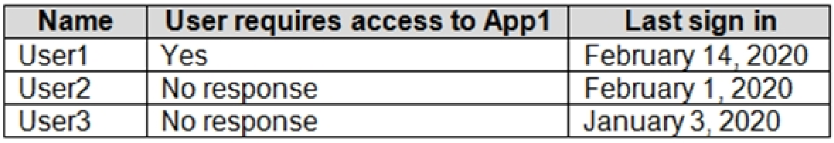
✑ Applications: App1

✑ Reviewers: Members (self)

✑ Auto apply results to resource: Enable

✑ Should reviewer not respond: Take recommendations

On February 15, 2020, you review the access review report and see the entries shown in the following table:

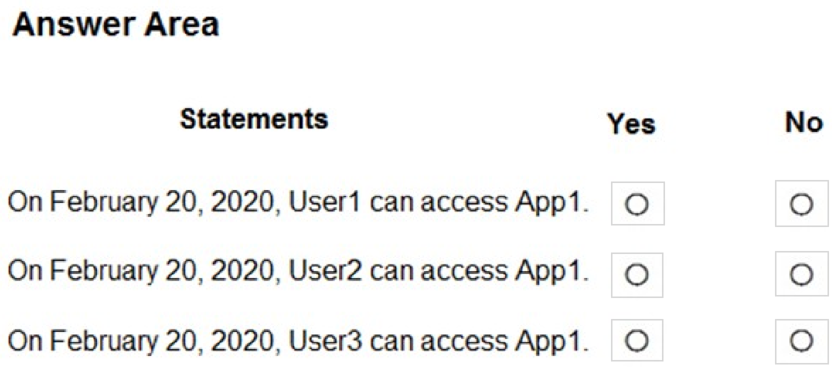


Name	User requires access to App1	Last sign in
User1	Yes	February 14, 2020
User2	No response	February 1, 2020
User3	No response	January 3, 2020

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

NOTE: Each correct selection is worth one point.

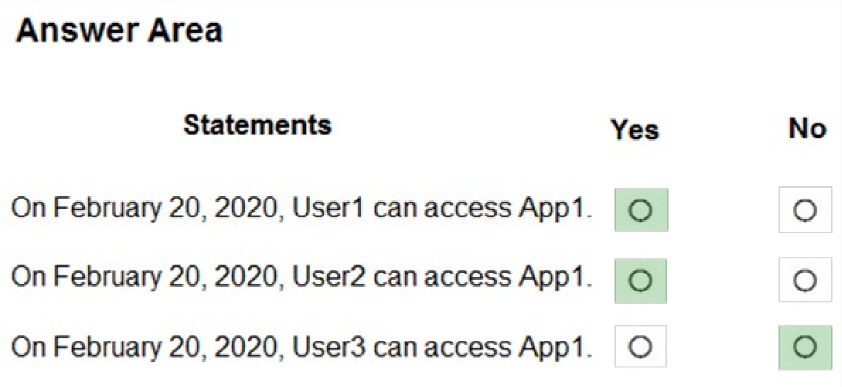
Hot Area:



Answer Area

Statements	Yes	No
On February 20, 2020, User1 can access App1.	○	○
On February 20, 2020, User2 can access App1.	○	○
On February 20, 2020, User3 can access App1.	○	○

Suggested Answer:



Answer Area

Statements	Yes	No
On February 20, 2020, User1 can access App1.	[✓ ○]	○
On February 20, 2020, User2 can access App1.	[✓ ○]	○
On February 20, 2020, User3 can access App1.	○	[✓ ○]

Reference:

https://docs.microsoft.com/en-us/azure/active-directory/governance/perform-access-review

kanag1 Highly Voted 2 years, 3 months ago

The given answers are correct.

As per the link in the answer area:

To make access reviews easier and faster for you, we also provide recommendations that you can accept with a single selection. There are two ways that the system generates recommendations for the reviewer. One method is by the user's sign-in activity. If a user has been inactive for 30 days or more, the system will recommend that the reviewer deny access.

upvoted 8 times

GatesBill Most Recent 1 year, 9 months ago

The given answers are correct. Simply put as follows:

- User1 gained (further) access through the access review.
- No response was given for User2, so the recommended actions took place; which are checking last sign-in date (should be < 30 days) & checking peer's access (which is User1 in this case). As User2 HAS signed in within the past 30 days and its peer (User1) HAS access to the app, User2 will gain access also.
- No response was given for User3, so the recommended actions took place. As User3 DID NOT sign in within the past 30 days and has no known peer which has access, User3's access will be revoked.

upvoted 3 times

josh_josh 1 year, 9 months ago

On Feb 20, 2020:

User1 can access App1 - NO
User2 can access App1 - NO
User3 can access App1 - NO

This is because User1 was reviewed as requiring access to App1 and last signed in on Feb 14, 2020, before the end of the review period. However, User2 did not respond to the review, so the "Take recommendations" option was applied, which means that their access to App1 will be revoked. User3 is a guest and was not assigned to App1, so they cannot access it.

upvoted 2 times

blazefather 2 years, 1 month ago

The answer should be N,N,N. They are to sign in just once and the End date: 02`"14`"2020.

upvoted 2 times

gaida 2 years, 2 months ago

members only and guest cannot approve access from them

upvoted 1 times

gaida 2 years, 2 months ago

reviewed the portal and guest user does have self approve. My response is incorrect and Knag1 is correct

upvoted 1 times

billo79152718 2 years, 3 months ago

Not sure about the last one

upvoted 2 times

EzeQ 2 years, 3 months ago

The user last sign-in is over 30 days and he did not reply, the recommendation will be to deny access. (as Kanag1 explains)

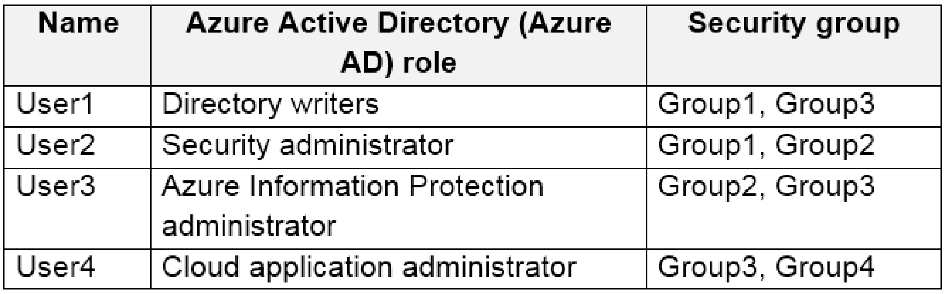
upvoted 2 times

Question #42 *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 that contains the users shown in the following table.



Name	Azure Active Directory (Azure AD) role	Security group
User1	Directory writers	Group1, Group3
User2	Security administrator	Group1, Group2
User3	Azure Information Protection administrator	Group2, Group3
User4	Cloud application administrator	Group3, Group4

You need to ensure that User1, User2, and User3 can use self-service password reset (SSPR). The solution must not affect User4.

Solution: You enable SSPR for Group3.

Does that meet the goal?

A. Yes

B. No

Suggested Answer: *B*

By default, self-service password reset is enabled for Directory writers and Security administrator but not for Azure Information Protection administrators and

Cloud application administrators. Therefore, we must enable SSPR for User3 by applying it to Group2 and not Group3 as User4 is in Group3.

User4 would thus be affected if we enable it on Group3.

Reference:

https://docs.microsoft.com/en-us/azure/active-directory/authentication/concept-sspr-policy#administrator-reset-policy-differences

garryevanson99 2 years, 3 months ago

this is wrong as ditrectory writers and security admin are enabled for sspr by default?

upvoted 1 times

garryevanson99 2 years, 3 months ago

ignore - most not effect user 4

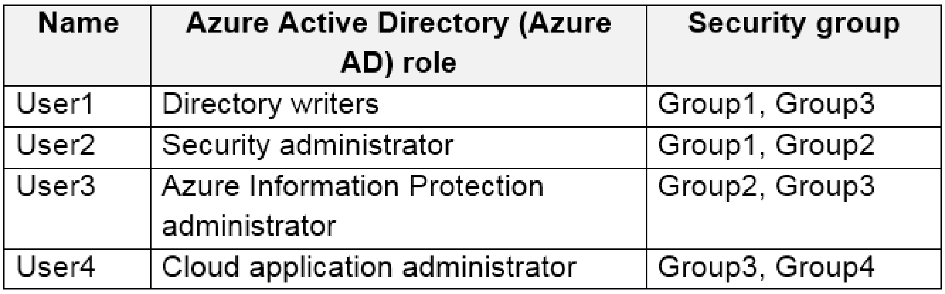
upvoted 2 times

Question #43 *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 that contains the users shown in the following table.



Name	Azure Active Directory (Azure AD) role	Security group
User1	Directory writers	Group1, Group3
User2	Security administrator	Group1, Group2
User3	Azure Information Protection administrator	Group2, Group3
User4	Cloud application administrator	Group3, Group4

You need to ensure that User1, User2, and User3 can use self-service password reset (SSPR). The solution must not affect User4.

Solution: You enable SSPR for Group2.

Does that meet the goal?

A. Yes

B. No

Suggested Answer: *A*

By default, self-service password reset is enabled for Directory writers and Security administrator but not for Azure Information Protection administrators and

Cloud application administrators.

Reference:

https://docs.microsoft.com/en-us/azure/active-directory/authentication/concept-sspr-policy#administrator-reset-policy-differences

Community vote distribution

A (100%)

Lomak Highly Voted 2 years, 3 months ago

Selected Answer: A

Answer is correct

User1 and User2 have SSPR by default

https://docs.microsoft.com/en-gb/azure/active-directory/authentication/concept-sspr-policy#administrator-reset-policy-differences

upvoted 7 times

skycrap Most Recent 2 years ago

Selected Answer: A

A is correct, Directory Writers are already enabled for sspr

upvoted 1 times

xyz213 2 years, 3 months ago

Yeah but user 1 is enabled by default. So it is correct in my opinion!

upvoted 2 times

Trainee2244 2 years, 3 months ago

Answer is wrong. Should be no because User 1 wouldnt be affected

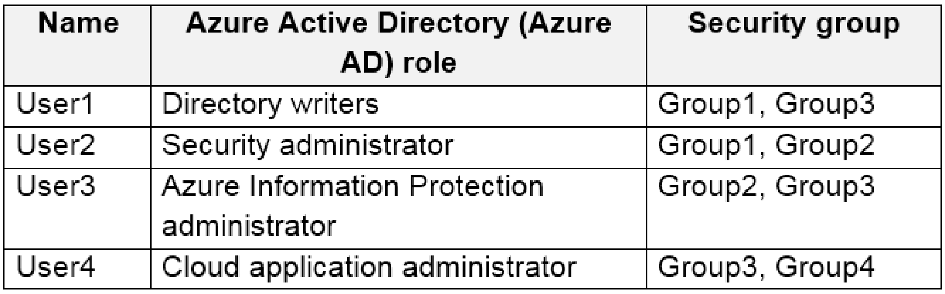
upvoted 2 times

Question #44 *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 that contains the users shown in the following table.



Name	Azure Active Directory (Azure AD) role	Security group
User1	Directory writers	Group1, Group3
User2	Security administrator	Group1, Group2
User3	Azure Information Protection administrator	Group2, Group3
User4	Cloud application administrator	Group3, Group4

You need to ensure that User1, User2, and User3 can use self-service password reset (SSPR). The solution must not affect User4.

Solution: You enable SSPR for Group1.

Does that meet the goal?

A. Yes

B. No

Suggested Answer: *B*

By default, self-service password reset is enabled for Directory writers and Security administrator but not for Azure Information Protection administrators and

Cloud application administrators. Thus, we must enable SSPR for User3 by applying it to Group2.

Reference:

https://docs.microsoft.com/en-us/azure/active-directory/authentication/concept-sspr-policy#administrator-reset-policy-differences

RomanV 1 year, 8 months ago

Given answer is correct.

"By default, administrator accounts are enabled for self-service password reset.."

Source where you also can find the list of admin roles that have SSPR enabled by default -> https://learn.microsoft.com/en-us/azure/active-directory/authentication/concept-sspr-policy#administrator-reset-policy-differences

upvoted 1 times

ChocolateNagaViper 2 years, 1 month ago

https://docs.microsoft.com/en-gb/azure/active-directory/authentication/concept-sspr-policy#administrator-reset-policy-differences

User 3 needs to be enabled for sspr. Users 1 and 2 have it by default and user 4 needs to be excluded.

upvoted 2 times

Dinraj 2 years, 4 months ago

I think Answer should be Yes

upvoted 3 times

garryevanson99 2 years, 3 months ago

user 3 wont be enabled for sspr

upvoted 3 times

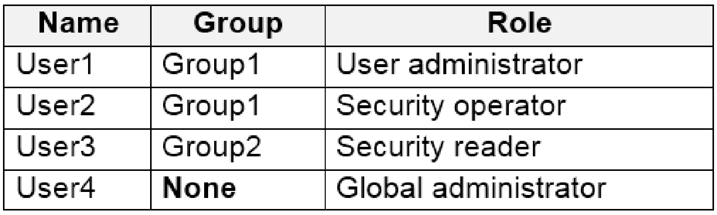
skycrap 2 years, 3 months ago

Correct as user3 don't have sspr enabled by default

upvoted 1 times

Question #45 Topic 1

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



Name	Group	Role
User1	Group1	User administrator
User2	Group1	Security operator
User3	Group2	Security reader
User4	None	Global administrator

You enable self-service password reset for Group1 and configure security questions as the only authentication method for self-service password reset.

You need to identity which user must answer security questions to reset their password.

Which user should you identify?

A. User1

B. User2

C. User3

D. User4

Suggested Answer: *B*

Self-service password reset (SSPR) is only enabled for Group1 (User1 and User2). User1 cannot use security questions for SSPR because User1 has an administrative security role. Therefore, only User2 can use SSPR with security questions as the authentication method.

Reference:

https://docs.microsoft.com/en-us/azure/active-directory/authentication/concept-sspr-policy#administrator-reset-policy-differences

ccadenasa Highly Voted 2 years, 1 month ago

This is correct > https://learn.microsoft.com/en-us/azure/active-directory/authentication/concept-sspr-policy#administrator-reset-policy-differences > "With a two-gate policy, administrators don't have the ability to use security questions."

upvoted 6 times

heshmat2022 Most Recent 1 year, 8 months ago

By default, administrator accounts are enabled for self-service password reset, and a strong default two-gate password reset policy is enforced. This policy may be different from the one you have defined for your users, and this policy can't be changed. You should always test password reset functionality as a user without any Azure administrator roles assigned.-

With a two-gate policy, administrators don't have the ability to use security questions.

upvoted 2 times

RomanV 1 year, 8 months ago

Answer is correct.

"administrators don't have the ability to use security questions."

https://learn.microsoft.com/en-us/azure/active-directory/authentication/concept-sspr-policy#administrator-reset-policy-differences

upvoted 1 times

billo79152718 2 years, 3 months ago

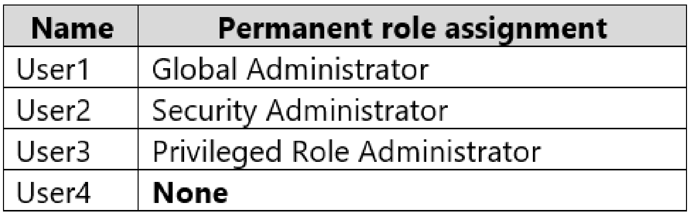
correct

upvoted 3 times

Question #46 *Topic 1*

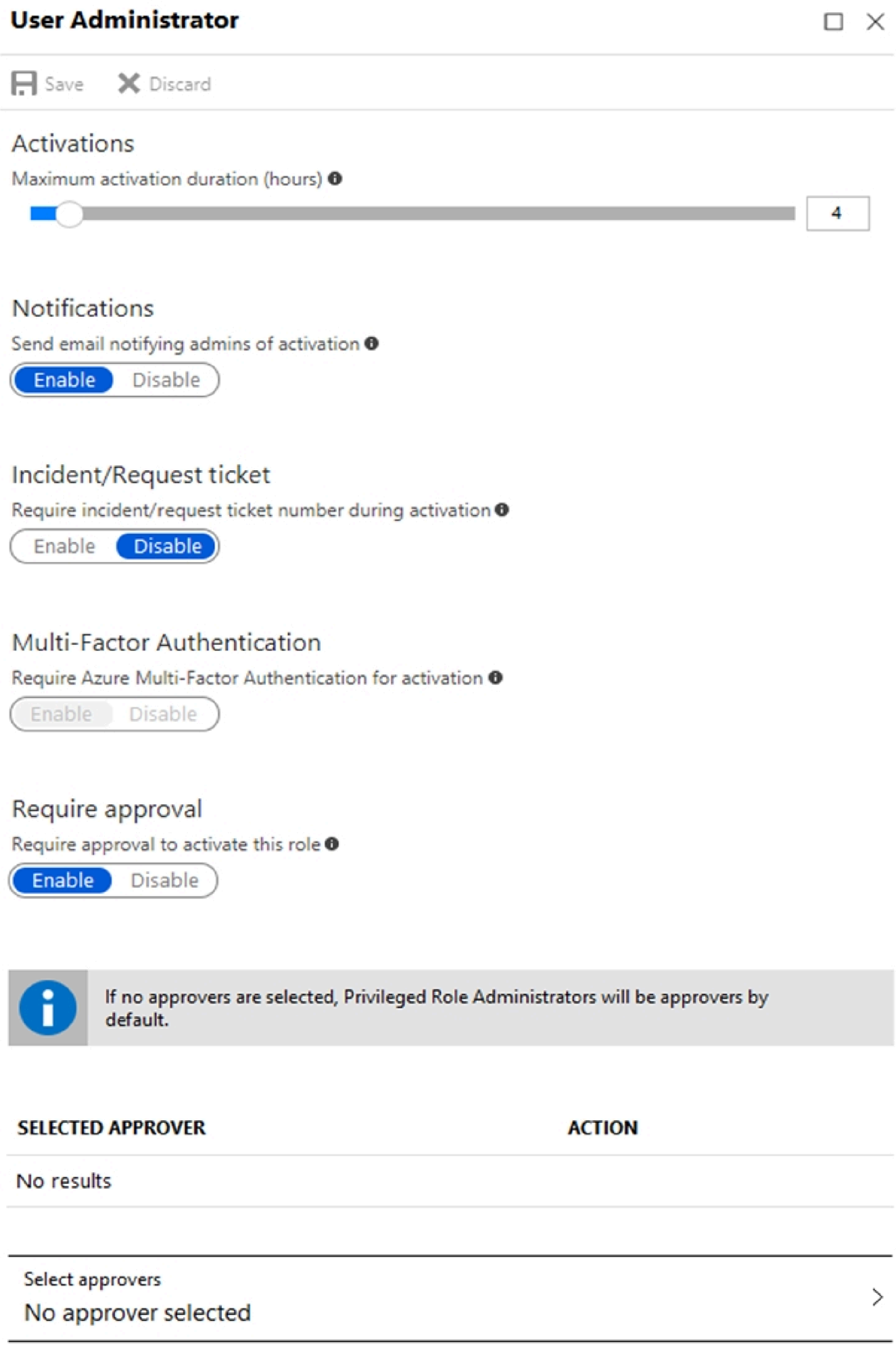
HOTSPOT -

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



Name	Permanent role assignment
User1	Global Administrator
User2	Security Administrator
User3	Privileged Role Administrator
User4	**None**

The User Administrator role is configured in Azure AD Privileged Identity Management (PIM) as shown in the following exhibit.



User Administrator

Save Discard

Activations

Maximum activation duration (hours): 4

Notifications

Send email notifying admins of activation

[✓ Enable] Disable

Incident/Request ticket

Require incident/request ticket number during activation

Enable [✓ Disable]

Multi-Factor Authentication

Require Azure Multi-Factor Authentication for activation

Enable Disable

Require approval

Require approval to activate this role

[✓ Enable] Disable

If no approvers are selected, Privileged Role Administrators will be approvers by default.

SELECTED APPROVER	ACTION
No results	

Select approvers

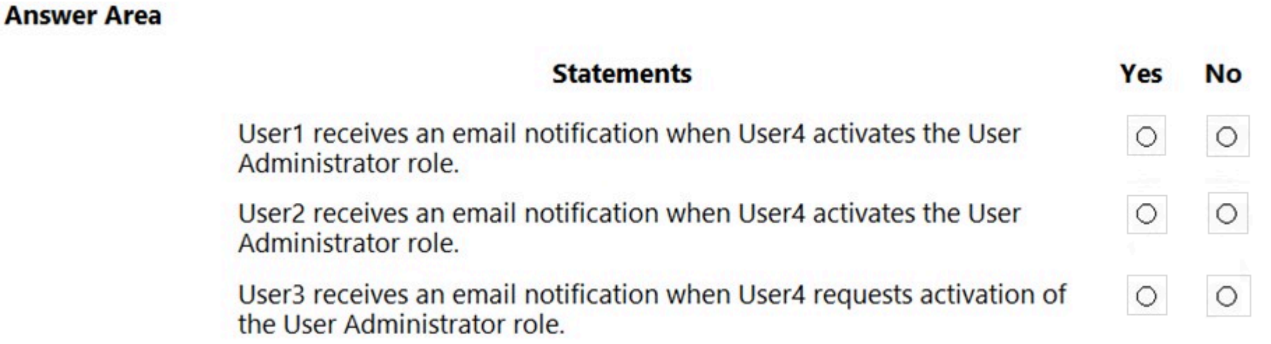
No approver selected

You make User4 eligible for the User Administrator role.

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

NOTE: Each correct selection is worth one point.

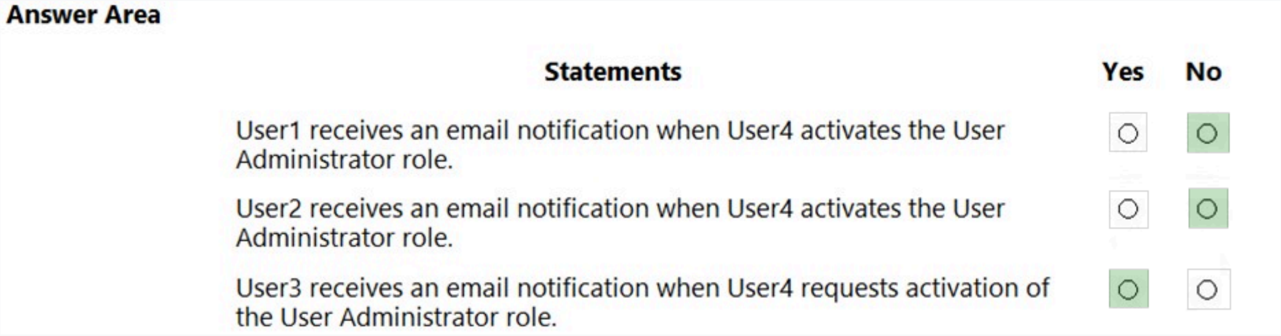
Hot Area:



Answer Area

Statements	Yes	No
User1 receives an email notification when User4 activates the User Administrator role.	○	○
User2 receives an email notification when User4 activates the User Administrator role.	○	○
User3 receives an email notification when User4 requests activation of the User Administrator role.	○	○

Suggested Answer:



Answer Area

Statements	Yes	No
User1 receives an email notification when User4 activates the User Administrator role.	○	[✓ ○]
User2 receives an email notification when User4 activates the User Administrator role.	○	[✓ ○]
User3 receives an email notification when User4 requests activation of the User Administrator role.	[✓ ○]	○

⊟ **BabiBu5** Highly Voted 2 years, 4 months ago

Y,Y,Y

https://docs.microsoft.com/en-us/azure/active-directory/privileged-identity-management/pim-email-notifications

upvoted 44 times

⊟ **examdj101j** 1 year, 8 months ago

The way the question is written is Y, Y, Y as BabiBu5 has noted. The question is worded poorly and you have to assume that they meant to word it the same as the 3rd question which would mean N, N, Y

upvoted 1 times

⊟ **Dhamus** 1 year, 8 months ago

I don't understand, is this question wrong?

upvoted 1 times

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

Wouldn't it be Yes, No Yes?

When users activate their role and the role setting requires approval, approvers will receive two emails for each approval:

Request to approve or deny the user's activation request (sent by the request approval engine)

The user's request is approved (sent by the request approval engine)

Also, Global Administrators and Privileged Role Administrators receive an email for each approval:

The user's role is activated (sent by Privileged Identity Management)

https://docs.microsoft.com/en-us/azure/active-directory/privileged-identity-management/pim-email-notifications

Security Administrator, doesn't have the same access as a PRM

https://learn.microsoft.com/en-us/azure/active-directory/roles/permissions-reference#security-administrator

https://learn.microsoft.com/en-us/azure/active-directory/roles/permissions-reference#privileged-role-administrator

upvoted 10 times

⊟ **ariania** 2 years, 2 months ago

https://learn.microsoft.com/en-us/azure/active-directory/privileged-identity-management/pim-email-notifications check the table "Role activation request is completed" - it goes to Global Admin, Privileged role Admin and Security Admin.

upvoted 4 times

yoton 1 year, 11 months ago

THIS! Documentation states, "If the Notifications setting is set to Enable," (which it is for this questions) emails are sent when role activation request is completed for the following users Privileged Role Administrator, Security Administrator, and Global Administrator.

Wouldn't this make the answer YYY?

Ref: https://learn.microsoft.com/en-us/azure/active-directory/privileged-identity-management/pim-email-notifications

upvoted 3 times

BigDazza_111 2 years, 1 month ago

agreed YNY, global admins do recieve a notification email when users role is activated by Priv Role admin, your link proves this https://docs.microsoft.com/en-us/azure/active-directory/privileged-identity-management/pim-email-notifications

upvoted 3 times

czaaa Most Recent 1 year, 6 months ago

When users activate their role and the role setting requires approval, approvers will receive two emails for each approval:

Request to approve or deny the user's activation request (sent by the request approval engine)
The user's request is approved (sent by the request approval engine)
Also, Global Administrators and Privileged Role Administrators receive an email for each approval:

The user's role is activated (sent by Privileged Identity Management)

upvoted 1 times

McMac 1 year, 6 months ago

User Role activation is pending approval Role activation request is completed PIM is enabled
Privileged Role Administrator
(Activated) Yes
(only if no explicit approvers are specified) Yes* Yes
Security Administrator
(Activated) No Yes* Yes
Global Administrator
(Activated) No Yes* Yes

upvoted 1 times

GPerez73 1 year, 7 months ago

Y,Y,Y tested in lab

upvoted 4 times

Dhamus 1 year, 7 months ago

Y: The global admin can receive notifications by default according to the documentation.
Y: The security administrator can receive notifications by default according to the documentation.
Y: The Privileged Role Manager will receive notifications only when the appropriate approvers have not been specified.

https://learn.microsoft.com/en-us/azure/active-directory/privileged-identity-management/pim-email-notifications

upvoted 1 times

heshmat2022 1 year, 8 months ago

When users activate their role and the role setting requires approval, approvers will receive two emails for each approval:

Request to approve or deny the user's activation request (sent by the request approval engine)
The user's request is approved (sent by the request approval engine)
Also, Global Administrators and Privileged Role Administrators receive an email for each approval:

upvoted 1 times

RomanV 1 year, 8 months ago

Correct answer should be Y, Y, Y.

Reasons:

Privileged Role Administrators receive an email notification when a role activation is pending approval (if no explicit approvers are specified), when a role activation request is completed, and when PIM is enabled.

Security Administrators receive an email notification only when a role activation request is completed or when PIM is enabled. They do not receive a notification when a role activation is pending approval.
Global Administrators do not receive email notifications when a role activation is pending approval, but they do receive a notification when a role activation request is completed or when PIM is enabled.

Read also the last question "User4 REQUESTS activation" & the first 2 questions are "User4 ACTIVATES"
upvoted 1 times

GatesBill 1 year, 9 months ago
When we look in the given URL below, we'll see that Global Admin and Security Admin will not receive a mail when the request for activation is still pending.

The tricky past in this question is however that User4 "activates" a role thus this still needs to be approved first before activation is completed (THEN the other admins will get a mail).

It is indeed a weirdly constructed question as "activates" would still mean "yet activated", but seemingly not in Microsoft terms...

https://learn.microsoft.com/en-us/azure/active-directory/privileged-identity-management/pim-email-notifications#notifications-for-azure-ad-roles
upvoted 1 times

Dislexsick 1 year, 11 months ago
Another horribly worded question.

Here the trick is "when X activates the role" vs. "when X requests activation of the role"

While everyone in comments here seems to be looking deeper and noting that post-approval more emails get sent out I think it's much simpler -- Option A, and B are impossible actions, it's a trick question since they don't activate it directly (Though we as logical people are treating their request, with approval as the indirect activation which it is)

tl;dr: User is not activating the role, they are requesting activation of the role, thus A and B aren't things that can even occur in this bad example, and B is correct.
upvoted 6 times

Brigg5 1 year, 11 months ago
Y Y N When an activation is completed, Global Admins, Security Admins, and Privileged Role Admins receive a notification. When an activation is pending, only the Privileged Role Admin receives a notification.The last question is a request, not an activation.
upvoted 3 times

rick001 1 year, 11 months ago
Correct. Key is in the REQUEST and not ACTIVATE.

Y Y N
upvoted 1 times

ysm 1 year, 9 months ago
But User 3 is Privileged Role Admin
upvoted 1 times

Ksumeet91 2 years ago
User Role activation is pending approval Role activation request is completed PIM is enabled
Privileged Role Administrator
(Activated/Eligible) Yes
(only if no explicit approvers are specified) Yes* Yes
Security Administrator
(Activated/Eligible) No Yes* Yes
Global Administrator
(Activated/Eligible) No Yes* Yes

So, answer is Y,Y,Y
upvoted 1 times

JonK 2 years ago

N,N,Y is correct!

Question 1 is "activates"
Question 2 is "activates"
Question 3 is "requests"

https://docs.microsoft.com/en-us/azure/active-directory/privileged-identity-management/pim-email-notifications

Answer chart pulled from the link above:

Privileged Role Administrator (Activated/Eligible):
--Role activation is pending approval (only if no explicit approvers are specified): Yes
--Role activation request is completed: Yes*
--PIM is enabled: Yes

Security Administrator (Activated/Eligible):
--Role activation is pending approval (only if no explicit approvers are specified): No
--Role activation request is completed: Yes*
--PIM is enabled: Yes

Global Administrator (Activated/Eligible)(Activated/Eligible):
--Role activation is pending approval (only if no explicit approvers are specified): No
--Role activation request is completed: Yes*
--PIM is enabled: Yes

upvoted 4 times

⊟ **Paul_white** 1 year, 11 months ago

The confusion here is, User Activates the role and notification is sent to approver before the role gets activated

upvoted 2 times

⊟ **ccadenasa** 2 years, 1 month ago

The answer is Y,Y,Y. I did a test in my Lab to double-check the output based on this information > https://learn.microsoft.com/en-us/azure/active-directory/privileged-identity-management/pim-email-notifications#notifications-for-azure-ad-roles

upvoted 4 times

⊟ **HartMS** 2 years, 1 month ago

Y,Y,Y is a correct answer. These admins get a notification when a role is activated, if enable notification tab is set to enabled:
Global Administrators
Security Administrators
Privileged Role Administrator

Here is the proof: https://docs.microsoft.com/en-us/azure/active-directory/privileged-identity-management/pim-email-notifications

upvoted 3 times

⊟ **gaida** 2 years, 2 months ago

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

upvoted 1 times

⊟ **maniaX** 2 years, 3 months ago

Correct answer is Y/Y/Y:
First two questions asks if the users receive notification when role was successfully activated. NOT TALKING ABOUT ACTIVATION REQUEST
Third question is about notification which will be send to user who must approve role activation and since there are no approvers specified then only Privileged Role Administrator will receive notification.

upvoted 2 times

Question #47 *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 contains a user named User1.
The Azure Active Directory (Azure AD) Identity Protection risky users report identifies User1.
For User1, you select Confirm user compromised.
User1 can still sign in.
You need to prevent User1 from signing in. The solution must minimize the impact on users at a lower risk level.
Solution: You configure the user risk policy to block access when the user risk level is high.
Does this meet the goal?

A. Yes

B. No

Suggested Answer: *B*
Reference:
https://docs.microsoft.com/en-us/azure/active-directory/identity-protection/howto-identity-protection-investigate-risk

Community vote distribution
A (71%) B (29%)

AVN1711 1 year, 3 months ago
Selected Answer: A
Hi everyone,

I am a bit confused. Regarding to this:
"How do the feedback mechanisms in Identity Protection work?
Confirm compromised (on a sign-in) – Informs Azure AD Identity Protection that the sign-in wasn't performed by the identity owner and indicates a compromise.
Upon receiving this feedback, we move the sign-in and user risk state to Confirmed compromised and risk level to High.
(https://learn.microsoft.com/en-us/azure/active-directory/identity-protection/troubleshooting-identity-protection-faq)"

So, after you selected Confirm user compromised and set the policy to block user with risk level High, he should be blocked for sign-ins, right?

I think right answer is A (Yes)
upvoted 1 times

RomanV 1 year, 8 months ago
Read the question again and again until you understand it. It's not talking about a high risky user but about a user that is reported as risky which YOU confirm as 'comprimised'.

Read what Microsoft has to say about that:

If after investigation, an account is confirmed compromised:
Select the event or user in the Risky sign-ins or Risky users reports and choose "Confirm compromised".
If a risk-based policy wasn't triggered, and the risk wasn't self-remediated, then do one or more of the followings:
Request a password reset.
Block the user if you suspect the attacker can reset the password or do multifactor authentication for the user.
Revoke refresh tokens.
Disable any devices that are considered compromised.
If using continuous access evaluation, revoke all access tokens.

You can answer the question yourself now. ;)

Source: https://learn.microsoft.com/en-us/azure/active-directory/identity-protection/howto-identity-protection-remediate-unblock#confirm-a-user-to-be-compromised

upvoted 2 times

Franc_Coetzee 1 year, 10 months ago

Selected Answer: B

You only need User1 to not be able to sign in

upvoted 1 times

tecnicosoffshoretech 1 year, 10 months ago

Selected Answer: A

In my opinion it should be A, since it is only blocking high risk users and lower risk users are not affected

upvoted 4 times

hpl1908 1 year, 10 months ago

Selected Answer: B

The solution must minimize the impact on users at a *lower risk level*.

Solution: You configure the user risk policy to block access when the user risk level is *high*.

So the answer is No.

upvoted 1 times

costaluisc 1 year, 11 months ago

The requirement is "You need to prevent User1 from signing in". So we need an action that only affects that user.

upvoted 2 times

Stig_88 1 year, 8 months ago

It says prevent User1 from signing in and NOT prevent "only" User1 from signing in.

You need to prevent User1 from signing in. YES this is satisfied with the solution.

The solution must minimize the impact on users at a lower risk level. YES this is satisfied and in fact solution not only minimize the impact to users at lower risk level but it gives NO impact as it ONLY impacts High Risks level.

upvoted 1 times

Stig_88 1 year, 8 months ago

In addition for the other 2 instance of this question,

An administrator may choose to block a sign-in based on their risk policy or investigations. A block may occur based on either "sign-in" or "user risk"

upvoted 1 times

abill 1 year, 11 months ago

Should it not be Yes?

upvoted 1 times

gaida 2 years, 2 months ago

it is correct, as it should enforce password change instead

upvoted 2 times

doody 2 years ago

no, when the user is confirmed as compromised then he will be moved to 'high risk', hence any remediation action (block, password change) while setting the user risk policy level as high will impact only the 'high risk' users and not the lower risk level users

https://learn.microsoft.com/en-us/azure/active-directory/identity-protection/howto-identity-protection-remediate-unblock#confirm-a-user-to-be-compromised

upvoted 2 times

dwilding 2 years, 3 months ago

"The solution must minimize the impact on users at a lower risk level"

upvoted 1 times

Question #48 *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 contains a user named User1.
The Azure Active Directory (Azure AD) Identity Protection risky users report identifies User1.
For User1, you select Confirm user compromised.
User1 can still sign in.
You need to prevent User1 from signing in. The solution must minimize the impact on users at a lower risk level.
Solution: You configure the sign-in risk policy to block access when the sign-in risk level is high.
Does this meet the goal?

A. Yes

B. No

Suggested Answer: *B*
Reference:
https://docs.microsoft.com/en-us/azure/active-directory/identity-protection/howto-identity-protection-investigate-risk

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

AVN1711 1 year, 3 months ago
to Moderator, please disregard it
upvoted 1 times

AVN1711 1 year, 3 months ago
Selected Answer: A
Hi everyone,

I am a bit confused. Regarding to this:
"How do the feedback mechanisms in Identity Protection work?
Confirm compromised (on a sign-in) – Informs Azure AD Identity Protection that the sign-in wasn't performed by the identity owner and indicates a compromise.
Upon receiving this feedback, we move the sign-in and user risk state to Confirmed compromised and risk level to High.
(https://learn.microsoft.com/en-us/azure/active-directory/identity-protection/troubleshooting-identity-protection-faq)"

So, after you selected Confirm user compromised and set the policy to block user with risk level High, he should be blocked for sign-ins, right?

I think right answer is A (Yes)
upvoted 1 times

McMac 1 year, 6 months ago
Should be 'Yes' as compromised user is "High' risk and doesn't affect lower risk users
upvoted 1 times

Brigg5 1 year, 7 months ago
Tricky Question. The user has been identified as a "Risky User" this is completely separate from "Risky Sign-ins." So the policy has zero affect on the user. The answer is NO.
upvoted 1 times

H0TDOGG 1 year, 8 months ago
My understanding here after reading the comments.

If we set Sign-in risk Policy to block high risk users, this will in fact block User1, as User1 was flagged as compromised, moving his account into a High risk stake.

The catch is, there should be zero impact on ALL other users. Enabling the policy could/will block other users in the high-risk category also.

The policy will do the job and block User1, but it could block User16 as a random choice, who is working over seas, as an example.

So technically, no this will not remedy the issue. To remediate, block the user directly in User1's config in AAD.

upvoted 1 times

⊟ **Dhamus** 1 year, 8 months ago

Being a compromised user, we are talking about a High Risk user, why is the answer No?

upvoted 1 times

⊟ **keithtemplin** 1 year, 10 months ago

Selected Answer: B

https://learn.microsoft.com/en-us/azure/active-directory/identity-protection/howto-identity-protection-remediate-unblock#confirm-a-user-to-be-compromised

This link show specific steps to take after the user is confirmed compromised

upvoted 1 times

⊟ **hpl1908** 1 year, 10 months ago

Selected Answer: B

The solution must minimize the impact on users at a *lower risk level*.

Solution: You configure the sign-in risk policy to block access when the sign-in risk level is *high*.

So the answer is No

upvoted 1 times

⊟ **costaluisc** 1 year, 11 months ago

The requirement is "You need to prevent User1 from signing in". So we need an action that only affects that user.

upvoted 1 times

⊟ **Paul_white** 1 year, 11 months ago

It may not make sense, but i will say the solution must minimize impact to other low risk users, this solution may impact another high risk user, so it would make sense to directly block access to specific user by going to Access and selecting the specific user and blocking their access as opposed to configuring a policy.

upvoted 1 times

⊟ **JonK** 2 years ago

I am missing something here and the cited article does not make the answer apparent. Anyone have info what the missing item here is that will make this answer make sense?

upvoted 1 times

⊟ **dwilding** 2 years, 3 months ago

"The solution must minimize the impact on users at a lower risk level"

upvoted 1 times

> ⊟ **abill** 1 year, 11 months ago
>
> I Still dont understand how this is correct as this user is at high risk it doesnt impact users at lower risk level? So shouldnt it be yes
>
> upvoted 2 times

Question #49 *Topic 1*

Note: This question is part of a series of questions that present the same scenario. Each question in the series contains a unique solution that might meet the stated goals. Some question sets might have more than one correct solution, while others might not have a correct solution.

After you answer a question in this section, you will NOT be able to return to it. As a result, these questions will not appear in the review screen.

You have a Microsoft 365 E5 subscription that contains a user named User1.

The Azure Active Directory (Azure AD) Identity Protection risky users report identifies User1.

For User1, you select Confirm user compromised.

User1 can still sign in.

You need to prevent User1 from signing in. The solution must minimize the impact on users at a lower risk level.

Solution: From the Access settings, you select Block access for User1.

Does this meet the goal?

A. Yes

B. No

Suggested Answer: *A*

Reference:

https://docs.microsoft.com/en-us/azure/active-directory/identity-protection/howto-identity-protection-investigate-risk

RomanV 1 year, 8 months ago

Answer Yes:

If after investigation, an account is confirmed compromised:

Select the event or user in the Risky sign-ins or Risky users reports and choose "Confirm compromised".

If a risk-based policy wasn't triggered, and the risk wasn't self-remediated, then do one or more of the followings:

Request a password reset.

Block the user if you suspect the attacker can reset the password or do multifactor authentication for the user.

Revoke refresh tokens.

Disable any devices that are considered compromised.

If using continuous access evaluation, revoke all access tokens.

Source: https://learn.microsoft.com/en-us/azure/active-directory/identity-protection/howto-identity-protection-remediate-unblock#confirm-a-user-to-be-compromised

upvoted 1 times

H0TDOGG 1 year, 8 months ago

Where are the access settings that the remediation mentions?

upvoted 1 times

Dzuljzebari 1 year, 11 months ago

Answer in this is not the complete solution. User Risk Policy > Assignments: User 1 > User Risk: High > Controls: block. I would select 2 previous solutions as YES (Low and Medium risk user will not be affected) and this one as no NO - solution not properly described.

upvoted 2 times

costaluisc 1 year, 11 months ago

The requirement is "You need to prevent User1 from signing in". So we need an action that only affects that user.

upvoted 1 times

zerrowall 2 years ago

How can we assign an individual user to block when others at the same time allow access?

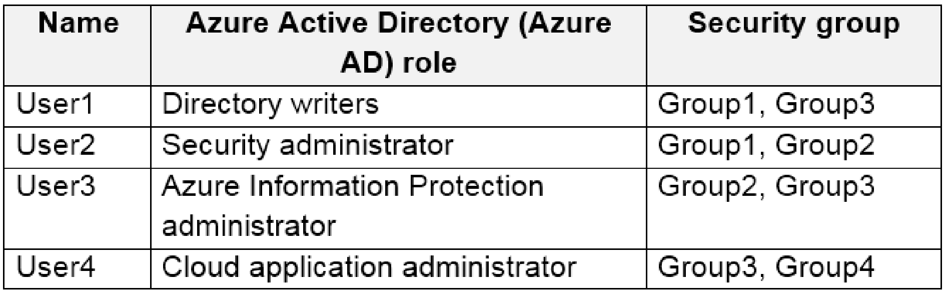
upvoted 1 times

Question #50 *Topic 1*

Note: This question is part of a series of questions that present the same scenario. Each question in the series contains a unique solution that might meet the stated goals. Some question sets might have more than one correct solution, while others might not have a correct solution.

After you answer a question in this section, you will NOT be able to return to it. As a result, these questions will not appear in the review screen.

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



Name	Azure Active Directory (Azure AD) role	Security group
User1	Directory writers	Group1, Group3
User2	Security administrator	Group1, Group2
User3	Azure Information Protection administrator	Group2, Group3
User4	Cloud application administrator	Group3, Group4

You need to ensure that User1, User2, and User3 can use self-service password reset (SSPR). The solution must not affect User4.

Solution: You create a conditional access policy for User1, User2, and User3.

Does that meet the goal?

A. Yes

B. No

Suggested Answer: *B*

Reference:

https://docs.microsoft.com/en-us/azure/active-directory/authentication/tutorial-enable-sspr

Community vote distribution

B (100%)

H0TDOGG 1 year, 8 months ago

Selected Answer: B

I first selected A, Yes as the rules stress only against users, not the groups. So the groups are irrelevant, and this still stands true.

On further review, I feel the answer is B, No.

Why? - Yes you can use a conditional access policy in relation to SSPR, but the policy is purely to force specific users to enrol their verification types. To use SSPR, you must enable it in the Password reset element of AAD, selecting to who the SSPR policy is applied.

upvoted 1 times

Unicorn02 2 years ago

Selected Answer: B

SSPR is not enforced/configured via Conditional Access Policy.

It is part of the "Password Reset" menu in AAD.

https://learn.microsoft.com/en-us/azure/active-directory/authentication/tutorial-enable-sspr#enable-self-service-password-reset

upvoted 4 times

NOC_NWDMICROAGE 2 years, 3 months ago

No, because directory writer + security admin have SSPR enabled by default. So you would only need to enable SSPR for Group 2.

upvoted 3 times

Question #51 *Topic 1*

You have a Microsoft 365 tenant that is linked to a hybrid Azure Active Directory (Azure AD) tenant named contoso.com.
You need to enable Azure AD Seamless Single Sign-On (Azure AD SSO) for contoso.com.
What should you use?

A. Azure AD Connect

B. the Microsoft 365 Defender portal

C. the Microsoft 365 Security admin center

D. the Microsoft 365 admin center

Suggested Answer: *A*
Reference:
https://docs.microsoft.com/en-us/azure/active-directory/hybrid/how-to-connect-sso-quick-start

Braaah 1 year, 6 months ago

Isn't aad connect already installed and functioning if it is already an hybdrid environement? The only thing that would be left to configure is SSO in my opinion. That would be in admin center, if i remember well. Thoughts?

upvoted 1 times

RomanV 1 year, 6 months ago

This is talking about SSSO, not SSO.

Single sign on (SSO) is an authentication method that lets you use a single username and password to access multiple applications. Seamless SSO occurs when a user is automatically signed into their connected applications when they're on corporate desktops connected to the corporate network.

upvoted 1 times

formazionehs 2 years ago

Given answer is correct https://learn.microsoft.com/en-us/azure/active-directory/hybrid/how-to-connect-sso-quick-start?source=recommendations

upvoted 2 times

rivetting 2 years ago

I think the question is wrong, shouldn't it be AD not AAD?

upvoted 2 times

RomanV 1 year, 8 months ago

No, there is no difference between Azure AD Connect and AD Connect. Azure AD Connect is the updated name for the tool formerly known as AD Connect.

upvoted 1 times

Question #52 *Topic 1*

You have a Microsoft 365 subscription.
You need to recommend a passwordless authentication solution that uses biometric authentication.
What should you include in the recommendation?

A. Windows Hello for Business

B. a smart card

C. the Microsoft Authenticator app

D. a PIN

Suggested Answer: *A*
Reference:
https://docs.microsoft.com/en-us/windows/security/identity-protection/hello-for-business/hello-overview

Bob27745 Highly Voted 👍 2 years, 3 months ago
Valid on Exam 9/21/2022
upvoted 6 times

WickedMJ 2 years, 3 months ago
So what's the correct answer?
upvoted 1 times

MayTheForceBeWithYou 2 years, 3 months ago
A.
Is the Answer
upvoted 3 times

RomanV 1 year, 8 months ago
Pff... If you don't know these very basic non-MS500 questions, what are you doing here? Go learn and study first to strengthen your knowledge. :)

Windows Hello for Business provides biometric authentication as one of the available authentication methods. It allows users to sign in to their Windows 10 devices using their face, fingerprint, or iris.
upvoted 1 times

Naveedkarjikar 2 years, 2 months ago
How are you dear. Did you wrote the exam recently.
I am preparing for the exam. Can you please share your experience of the exam.
Did you get any LABS? if yes. How many LABS
upvoted 2 times

pompes Most Recent 🕒 1 year, 7 months ago
A.
Was on the exam
upvoted 2 times

Question #53 *Topic 1*

Your network contains an on-premises Active Directory domain and a Microsoft 365 subscription.
You plan to deploy a hybrid Azure Active Directory (Azure AD) tenant that has Azure AD Identity Protection risk policies enabled.
You need to configure Azure AD Connect to support the planned deployment.
Which Azure AD Connect authentication method should you select?

A. Federation with AD FS

B. Federation with PingFederate

C. Password Hash Synchronization

D. Pass-through authentication

Suggested Answer: *A*

Community vote distribution

C (100%)

xyz213 Highly Voted 👍 2 years, 3 months ago

Selected Answer: C

One of the protection risk policies is a “Use risk policy”. It will require a password change. For this to work in a hybrid environment:
Make sure you have PHS, Password Writeback and SSPR enabled

upvoted 12 times

Ivkopivko12tka Highly Voted 👍 2 years ago

Selected Answer: C

Honestly, I don't understand the fact that answers to such trivial questions are wrong. This exam is full of wrong answers, any idea how to change it?

upvoted 8 times

RomanV 1 year, 8 months ago

To learn and tackle them yourself. This is challenging us and keeping us awake :)

upvoted 1 times

GPerez73 Most Recent 🕓 1 year, 8 months ago

Selected Answer: C

I have a lab with an hybrid enviroment and I don't need ADFS to use risk sign in policies. So it is C

upvoted 1 times

GatesBill 1 year, 9 months ago

Correct answer should be C indeed.
Password writeback should be enabled as stated also in the following article:
https://learn.microsoft.com/en-us/azure/active-directory/identity-protection/howto-identity-protection-configure-risk-policies#choosing-acceptable-risk-levels

upvoted 2 times

examdj101j 1 year, 8 months ago

Should be C, there's documented proof that A is the correct answer. So community answer it is, this is probably taken out of the Exam as I took it 2 weeks ago and failed, don't remember this one

upvoted 1 times

examdj101j 1 year, 8 months ago

I meant to say there is no documented proof that A is correct

upvoted 1 times

ajjihad1 1 year, 10 months ago

To support the deployment of a hybrid Azure Active Directory (Azure AD) tenant with Azure AD Identity Protection risk policies enabled, you should use the "Pass-through Authentication" (PTA) method in Azure AD Connect.

PTA is a simple and secure authentication method that allows users to use their on-premises passwords to authenticate with Azure AD. When users sign in to Azure AD-connected applications, their passwords are validated against your on-premises Active Directory, so there's no need to store passwords in the cloud. Additionally, PTA supports the use of Azure AD Identity Protection risk policies, which help to detect and prevent risky sign-ins.

The other two authentication methods in Azure AD Connect are "Password Hash Synchronization" and "Active Directory Federation Services" (AD FS). While both of these methods are also compatible with Azure AD Identity Protection, PTA is the recommended method for its simplicity and security benefits.

So, you should select the "Pass-through Authentication" option when configuring Azure AD Connect for your hybrid deployment.

upvoted 3 times

Eve123 1 year, 11 months ago

Optionally, you can set up password hash synchronization as a backup if you decide to use Federation with Active Directory Federation Services (AD FS) as your sign-in method.

https://learn.microsoft.com/en-us/azure/active-directory/hybrid/whatis-phs

upvoted 1 times

examdog 2 years ago

Selected Answer: C

When using Federation, the authentication is done on-prem. So C is the answer.

upvoted 3 times

foster1 2 years ago

Pretty sure thats C

upvoted 2 times

VJO 2 years, 1 month ago

Federation for AD FS allows for more rigorous levels of access controls. This is a requirement in the question regarding risk policies. Password Hash is a part of Federation for AD FS if needed.

upvoted 1 times

ccadenasa 2 years, 1 month ago

C is the correct answer for sure

upvoted 1 times

HartMS 2 years, 2 months ago

Selected Answer: C

C for Sure

upvoted 2 times

SDK91 2 years, 2 months ago

Selected Answer: C

Makes more sense

upvoted 2 times

mohamed_Saed 2 years, 2 months ago

Selected Answer: C

c is more likely

upvoted 4 times

01001010101 2 years, 2 months ago

So what is valid on the exam??

upvoted 1 times

JimboJones99 2 years, 3 months ago

Selected Answer: C

PHS makes the most sense for this scenario

upvoted 1 times

LittleScratch 2 years, 3 months ago

Selected Answer: C

Agree with Dan91 & Pete26

upvoted 3 times

pete26 2 years, 3 months ago

Selected Answer: C

One of the protection risk policies is a “Use risk policy”. It will require a password change. For this to work in a hybrid environment:

Make sure you have PHS, Password Writeback and SSPR enabled.

I will go with PHS for an answer.

upvoted 3 times

Question #54 *Topic 1*

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

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

B. the Device compliance trends report in the Microsoft Endpoint Manager admin center

C. Activity log in the Cloud App Security portal

D. the Conditional Access Insights and Reporting workbook in the Azure Active Directory admin center

Suggested Answer: *D*
Reference:
https://docs.microsoft.com/en-us/azure/active-directory/conditional-access/howto-conditional-access-insights-reporting

Community vote distribution

D (100%)

zik4 1 year, 12 months ago

This question was present on Dec 05 exam.

upvoted 3 times

examdog 2 years ago

Selected Answer: D

The endpoint admin center does have a Device Compliance report. However, the key point from the question is that "You have SEVERAL Conditional Access policies that block noncompliant devices".

upvoted 1 times

TheManaMan 2 years, 1 month ago

The correct answer is D as Endpoint Manager would not show which devices are blocked as 'Non-Complaint' based on the specific CA Policy.

upvoted 1 times

ccadenasa 2 years, 1 month ago

I think the correct answer is A. To see Conditional Access insights and reporting, you need to enable Azure Monitor logs and this is not an statement in the question. The CA blocked access based on non-compliance devices so checking the compliance report in Intune will show the lists of non-compliance devices.

upvoted 1 times

pete26 2 years, 3 months ago

Selected Answer: D

It should be D.
https://docs.microsoft.com/en-us/azure/active-directory/conditional-access/howto-conditional-access-insights-reporting

upvoted 2 times

Question #55 *Topic 1*

You have a Microsoft 365 subscription named contoso.com.

You need to configure Microsoft OneDrive for Business external sharing to meet the following requirements:

✑ Enable file sharing for users that have a Microsoft account.

✑ Block file sharing for anonymous users.

What should you do?

A. From Advanced settings for external sharing, select Allow or block sharing with people on specific domains and add contoso.com.

B. From the External sharing settings for OneDrive, select Only people in your organization.

C. From the External sharing settings for OneDrive, select Existing external users.

D. From the External sharing settings for OneDrive, select New and existing external users.

Suggested Answer: *D*

Reference:

https://www.sharepointdiary.com/2020/09/enable-external-sharing-in-onedrive-for-business.html

ccadenasa 2 years, 1 month ago

That's is correct. Checked in my Lab

upvoted 4 times

ChocolateNagaViper 2 years, 1 month ago

correct: https://learn.microsoft.com/en-us/sharepoint/change-external-sharing-site?source=recommendations

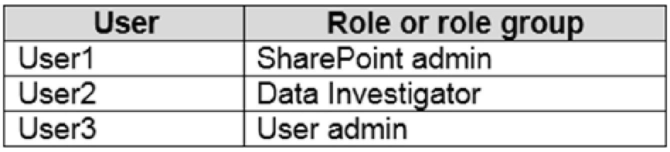
upvoted 2 times

Question #56 Topic 1

DRAG DROP -

You have a Microsoft 365 E5 tenant that contains three users named User1, User2, and User3.

You need to assign roles or role groups to the users as shown in the following table.

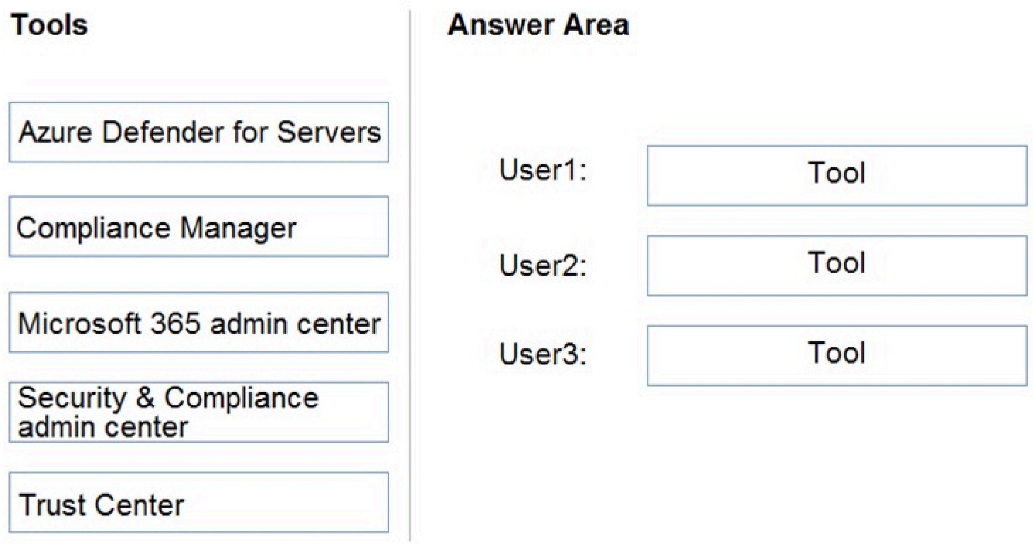


User	Role or role group
User1	SharePoint admin
User2	Data Investigator
User3	User admin

What should you use to assign a role or role group to each user? To answer, drag the appropriate tools to the correct roles or role groups. Each tool may be used once, more than once, or not at all. You may need to drag the split bar between panes or scroll to view content.

NOTE: Each correct selection is worth one point.

Select and Place:



Tools

Azure Defender for Servers

Compliance Manager

Microsoft 365 admin center

Security & Compliance admin center

Trust Center

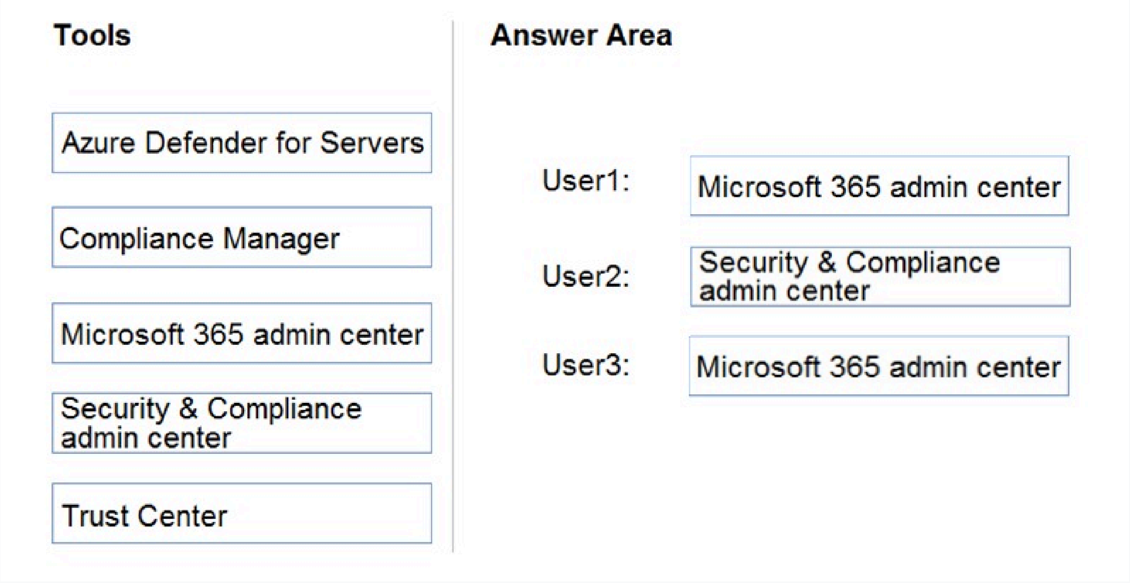
Answer Area

User1: Tool

User2: Tool

User3: Tool

Suggested Answer:



Tools

Azure Defender for Servers

Compliance Manager

Microsoft 365 admin center

Security & Compliance admin center

Trust Center

Answer Area

User1: Microsoft 365 admin center

User2: Security & Compliance admin center

User3: Microsoft 365 admin center

Reference:

https://docs.microsoft.com/en-us/microsoft-365/security/office-365-security/permissions-in-the-security-and-compliance-center?view=o365-worldwide

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

Valid on exam 10/22/22

upvoted 8 times

⊟ **QuanN7** Highly Voted 2 years, 1 month ago

User2 role has to be assigned in Microsoft Purview

upvoted 8 times

⊟ **Tanasi** 1 year, 10 months ago

This question is before they named it Purview; but yes, you are correct.

upvoted 1 times

Question #57 *Topic 1*

Your network contains an on-premises Active Directory domain named contoso.local that has a forest functional level of Windows Server 2008 R2.
You have a Microsoft 365 E5 subscription linked to an Azure Active Directory (Azure AD) tenant named contoso.com.
You plan to install Azure AD Connect and enable single sign-on (SSO).
You need to prepare the domain to support SSO. The solution must minimize administrative effort.
What should you do?

A. Raise the forest functional level to Windows Server 2016.

B. Modify the UPN suffix of all domain users.

C. Populate the mail attribute of all domain users.

D. Rename the domain.

Suggested Answer: *B*
Reference:
https://docs.microsoft.com/en-us/microsoft-365/enterprise/prepare-a-non-routable-domain-for-directory-synchronization?view=o365-worldwide

Community vote distribution

B (100%)

yoton Highly Voted 👍 2 years, 3 months ago

I believe the answer can be found here:
https://docs.microsoft.com/en-us/microsoft-365/enterprise/prepare-a-non-routable-domain-for-directory-synchronization?view=o365-worldwide#add-upn-suffixes-and-update-your-users-to-them

"You can solve the ".local" problem by registering new UPN suffix or suffixes in AD DS to match the domain (or domains) you verified in Microsoft 365. "

upvoted 9 times

pete26 Highly Voted 👍 2 years, 3 months ago

Selected Answer: B

B is correct!

upvoted 8 times

ChachaChatra Most Recent 🕓 1 year, 11 months ago

Valid on28/01/23

upvoted 3 times

TweetleD 2 years, 1 month ago

Domain functional level is supported back to 2003 or later. Not about what version OS AD Connect runs on. B is correct answer

upvoted 1 times

pipojede 2 years, 3 months ago

AD Connect is no longer supported in 2008 and from August 2022 not even in 2012 R2.

SQL Server 2019 requires Windows Server 2016 or newer as a server operating system. Since Azure AD Connect v2 contains SQL Server 2019 components, we no longer can support older Windows Server versions.
https://learn.microsoft.com/en-us/azure/active-directory/hybrid/whatis-azure-ad-connect-v2

upvoted 2 times

> **pipojede** 2 years, 3 months ago
>
> Please delete, comment was about OS.
> Functional level must be Windows Server 2003 or later.
>
> upvoted 1 times

Bob27745 2 years, 3 months ago

Valid on Exam 9/21/2022

upvoted 5 times

⊟ **Anonymousse** 2 years, 2 months ago

and 10/22/22

upvoted 2 times

⊟ **Tanasi** 1 year, 10 months ago

and on 13/feb/2023

upvoted 1 times

⊟ **Nelson13** 2 years, 2 months ago

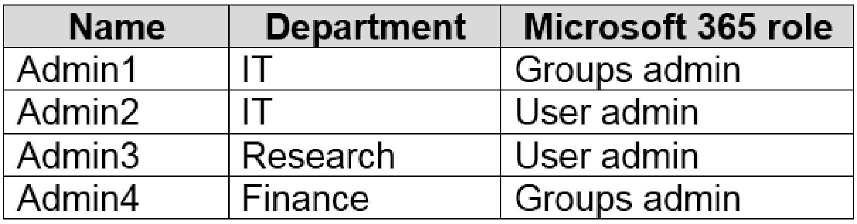
Being B the correct?

upvoted 1 times

Question #58 *Topic 1*

HOTSPOT -

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

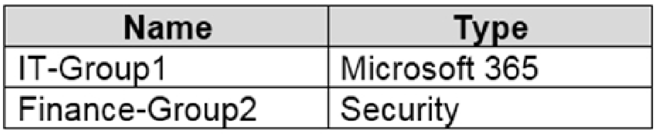


Name	Department	Microsoft 365 role
Admin1	IT	Groups admin
Admin2	IT	User admin
Admin3	Research	User admin
Admin4	Finance	Groups admin

For contoso.com, you create a group naming policy that has the following configuration.

<Department> - <Group name>

You plan to create the groups shown in the following table.

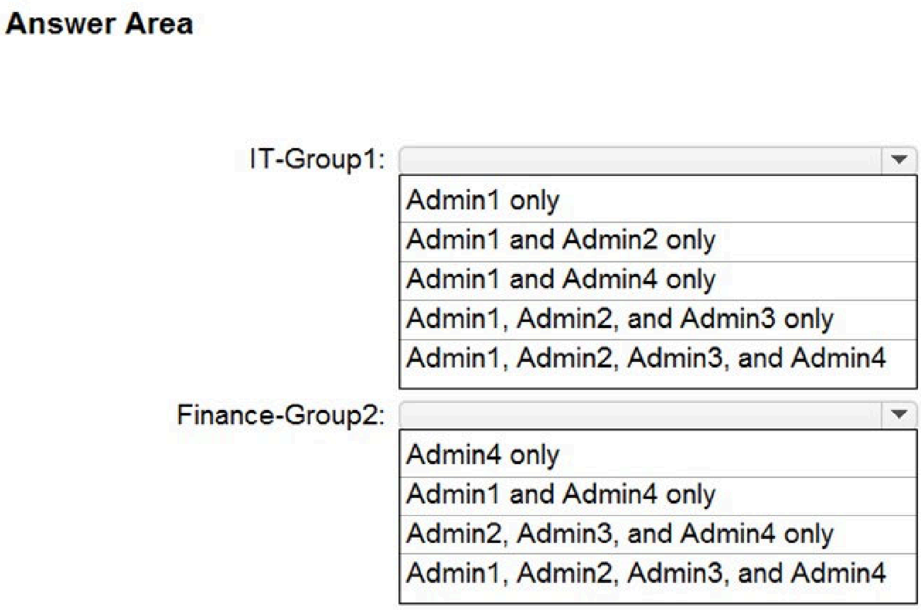


Name	Type
IT-Group1	Microsoft 365
Finance-Group2	Security

Which users can be used to create each group? To answer, select the appropriate options in the answer area.

NOTE: Each correct selection is worth one point.

Hot Area:



Answer Area

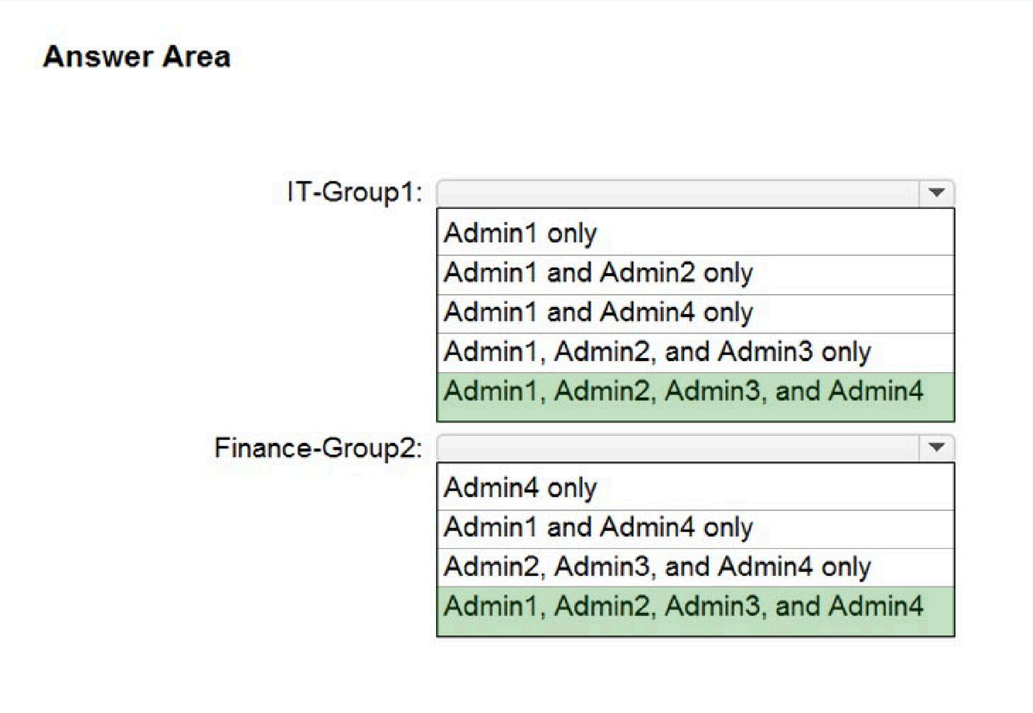
IT-Group1:

- Admin1 only
- Admin1 and Admin2 only
- Admin1 and Admin4 only
- Admin1, Admin2, and Admin3 only
- Admin1, Admin2, Admin3, and Admin4

Finance-Group2:

- Admin4 only
- Admin1 and Admin4 only
- Admin2, Admin3, and Admin4 only
- Admin1, Admin2, Admin3, and Admin4

Suggested Answer:



Answer Area

IT-Group1:

Admin1 only

Admin1 and Admin2 only

Admin1 and Admin4 only

Admin1, Admin2, and Admin3 only

[✓ Admin1, Admin2, Admin3, and Admin4]

Finance-Group2:

Admin4 only

Admin1 and Admin4 only

Admin2, Admin3, and Admin4 only

[✓ Admin1, Admin2, Admin3, and Admin4]

Reference:

https://office365itpros.com/2020/01/22/using-groups-admin-role/ https://docs.microsoft.com/en-us/azure/active-directory/roles/permissions-reference

pete26 Highly Voted 2 years, 3 months ago

Answers appear to be correct. 4 and 4

upvoted 11 times

RJ06 Highly Voted 2 years, 2 months ago

I think it will be:

IT-Group1 - admin1, admin2 admin3 (admin-4 belongs to Finance dept and wont be able to create it).

Finance-Group2 - admin1, admin2, admin3 and admin4 (security group - group naming policy won't apply)

upvoted 5 times

RJ06 2 years, 2 months ago

think I made it a bit too complex. All 4 for both are correct.

upvoted 4 times

costaluisc 2 years ago

Admin4 is not excluded from the naming policy, only Global Administrator and User Administrator are excluded. I will not be able to create the group since it´s department is "Finance"

upvoted 3 times

GatesBill Most Recent 1 year, 9 months ago

The given answers are correct.

In this case it doesn't matter if which roles are exempted (User Admin & Global Admin) as the given group names DO meet the given Group Naming Policy requirements.

upvoted 2 times

rick001 1 year, 11 months ago

IT - 1,2,3, - group admins not exempted.

Finance : is a security - group policy doesn't apply at all.

upvoted 3 times

kimble3k 2 years ago

The new groups would be according to the naming policy? Nothing would block the admins from creating the groups. So 4 and 4, answer appear to be correct?

upvoted 2 times

kimble3k 2 years ago

if there were Custom blocked words, then the Groups admin are not exempted, only User admin (and Global admin) are exempted

upvoted 2 times

⊟ **Ksumeet91** 2 years ago

Agreed with mcclane654

IT: 1,2,3 as group admins aren't exempted
Finance: All -Security groups are not affected by naming policy

upvoted 1 times

⊟ **mcclane654** 2 years ago

IT: 1,2,3 as group admins aren't exempted
Finance: All -Security groups are not affected by naming policy

"Some administrator roles are exempted from these policies, across all group workloads and endpoints, so that they can create groups using blocked words and with their own naming conventions. The following administrator roles are exempted from the group naming policy:

Global Administrator
User Administrator"
ref: https://learn.microsoft.com/en-us/azure/active-directory/enterprise-users/groups-naming-policy?WT.mc_id=Portal-Microsoft_AAD_IAM

upvoted 5 times

⊟ **yaza85** 1 year, 11 months ago

True, security groups are not affected by naming policy so they can be created like shown in the exhibit

upvoted 1 times

⊟ **Brigg5** 1 year, 11 months ago

This is correct. More info here https://learn.microsoft.com/en-us/azure/active-directory/enterprise-users/groups-naming-policy

upvoted 1 times

⊟ **usr001** 2 years, 2 months ago

Some administrator roles are exempted from these policies, across all group workloads and endpoints, so that they can create groups using blocked words and with their own naming conventions. The following administrator roles are exempted from the group naming policy:

Global Administrator
User Administrator

upvoted 3 times

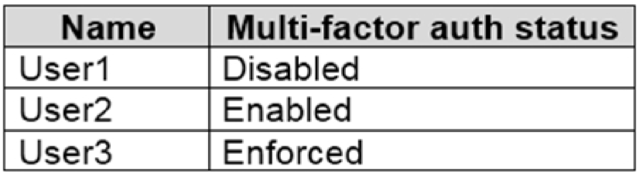
⊟ **Bob27745** 2 years, 3 months ago

Valid on Exam 9/21/2022

upvoted 4 times

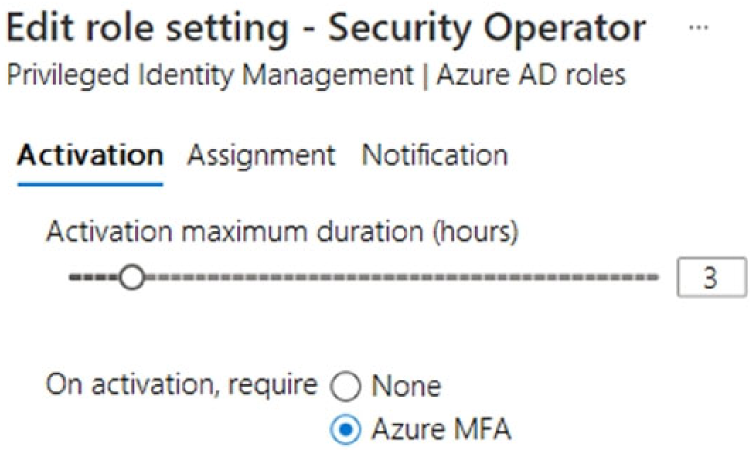
Question #59 Topic 1

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



Name	Multi-factor auth status
User1	Disabled
User2	Enabled
User3	Enforced

You configure the Security Operator role in Azure AD Privileged Identity Management (PIM) as shown in the following exhibit.



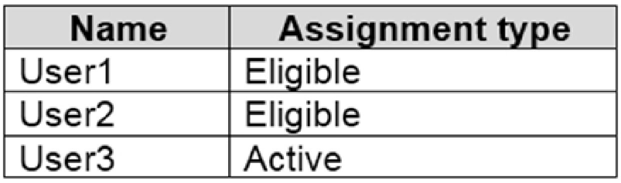
Edit role setting - Security Operator ...

Privileged Identity Management | Azure AD roles

Activation maximum duration (hours) 3

On activation, require ○ None
● Azure MFA

You add assignments to the Security Operator role as shown in the following table.



Name	Assignment type
User1	Eligible
User2	Eligible
User3	Active

Which users can activate the Security Operator role?

A. User2 only

B. User3 only

C. User1 and User2 only

D. User2 and User3 only

E. User1, User2, and User3

Suggested Answer: *D*

Community vote distribution

C (69%) D (31%)

xyz213 Highly Voted 2 years, 3 months ago

For me it is C "User1 and User2 only":

https://docs.microsoft.com/en-us/answers/questions/529070/user-mfa-is-disabled-however-pim-activation-is-ask.html

"PIM takes precedence and will override any other MFA settings"

User3 cannot explicitly activate the role.

upvoted 15 times

BoxGhost 2 years ago

I agree but for a different reason. It states it will require the user to use 'Azure MFA'. The fact that MFA is disabled for the user is irrelevent since you don't enable Azure MFA using the legacy portal anyway, it's enforced by conditional access or other conditions such as this.

upvoted 1 times

doody 2 years ago

I tested it and the answer is User 1 and User 2

upvoted 1 times

tibodenbeer 2 years ago

PIM takes precedent over MFA. I tested this in my trial tenant as well. I was able to activate the role for a user where MFA was disabled but I had to go through the MFA process to get the role enabled.

Conclusion: Answer = C

upvoted 1 times

Citmerian 1 year, 6 months ago

PIM takes precedent over MFA. OK
Elegible vs active: https://learn.microsoft.com/en-us/azure/active-directory/privileged-identity-management/pim-configure

upvoted 1 times

Citmerian 1 year, 6 months ago

C I'ts OK

upvoted 1 times

KrisyMay Most Recent 1 year, 9 months ago

Selected Answer: D

The question says users and also makes mention of MFA, User 2 and 3 have MFA enabled and can therefore assign the role. User 1 can not assign role

upvoted 3 times

examdj101j 1 year, 8 months ago

This is correct by the way Microsoft Books, and reference guides state it. However it may not work in the environment based on many variables. D is the correct answer by measureUp prep as I use their services also.

upvoted 1 times

kimble3k 2 years ago

Selected Answer: C

Because:
1. Active assignments don't require the member to activate the role before usage. Members assigned as active have the privileges assigned ready to use. This type of assignment is also available to customers that don't use Azure AD PIM
2. https://learn.microsoft.com/en-us/answers/questions/529070/user-mfa-is-disabled-however-pim-activation-is-ask.html

upvoted 4 times

examdog 2 years ago

Selected Answer: C

Active assignments don't require the member to activate the role before usage. https://learn.microsoft.com/en-us/azure/active-directory/privileged-identity-management/pim-resource-roles-assign-roles

upvoted 2 times

tibodenbeer 2 years ago

Selected Answer: C

PIM takes precedent over MFA (https://learn.microsoft.com/en-us/answers/questions/529070/user-mfa-is-disabled-however-pim-activation-is-ask.html). I tested this in my trial tenant as well. I was able to activate the role for a user where MFA was disabled but I had to go through the MFA process to get the role activated.

Conclusion: Answer = C

upvoted 2 times

skycrap 2 years ago

Selected Answer: C

I go also for C: see comment of xyz213

upvoted 1 times

zied01 2 years, 1 month ago

The anwser is correct

User 1 doesn't have MFA , and it is required to acivated the role like mentionned in the capture.

Also the role will be activated only for 3 hours , after this period the user will be challenged to demand the role

upvoted 1 times

Wedge34 2 years, 2 months ago

Selected Answer: C

Answer is C "User1 and User2 only"

upvoted 1 times

Wedge34 2 years, 2 months ago

Selected Answer: C

For me it is C "User1 and User2 only"

upvoted 1 times

Trainee2244 2 years, 3 months ago

Question is little bit confusing to me. I did the scenario myself and only User1 needs to MFA. User2 can activate the Role without MFA and User3 can´t activate the because he´s Active.

upvoted 1 times

> **xyz213** 2 years, 3 months ago
>
> See my comment. I hope I am right with this and can clear this up.
>
> User1 can activate with MFA.
> User2 can activate (most likely without MFA because of "MFA caching")
> https://www.microsoftpartnercommunity.com/t5/Multi-Factor-Authentication-MFA/PIM-Role-Activation-amp-MFA-Enforcement/m-p/38009)
>
> User3 can´t activate the because he´s Active.
>
> upvoted 1 times

Trainee2244 2 years, 3 months ago

i think User1 and User2 only, because User3 is already activated obviously and User1 will be MFA registered after he requests the role to autenticated this is a separate process from settings in the MFA per User Option

upvoted 4 times

pete26 2 years, 3 months ago

Selected Answer: D

User2 and User3. User3 may be already active, but the question asks which users can activate a role.

upvoted 2 times

> **MaartenC** 2 years, 3 months ago
>
> Well. since the User3 has the role permanently active,, this user is not able to activate it himself. So isnt User2 only the better answer?
>
> upvoted 8 times

Mikeee10 2 years, 4 months ago

User 3 is already Active so doesn't need to activate the role. They would simply have the permissions without the need for activation. This would suggest User2 only but looking to see what anyone else thinks.

upvoted 3 times

> **MaartenC** 2 years, 3 months ago
>
> User3 cannot explicitly activate the role so i'm leaning towards User2 only as the answer. The question is simply not precise enough which is a pity as usual.
>
> upvoted 3 times

Question #60 *Topic 1*

You have a Microsoft 365 tenant.
You need to implement a policy to enforce the following requirements:
✑ If a user uses a Windows 10 device that is NOT hybrid Azure Active Directory (Azure AD) joined, the user must be allowed to connect to Microsoft SharePoint
Online only from a web browser. The user must be prevented from downloading files or syncing files from SharePoint Online.
✑ If a user uses a Windows 10 device that is hybrid Azure AD joined, the user must be able connect to SharePoint Online from any client application, download files, and sync files.
What should you create?

A. a conditional access policy in Azure AD that has Client apps conditions configured

B. a conditional access policy in Azure AD that has Session controls configured

C. a compliance policy in Microsoft Endpoint Manager that has the Device Properties settings configured

D. a compliance policy in Microsoft Endpoint Manager that has the Device Health settings configured

Suggested Answer: *B*
Reference:
https://docs.microsoft.com/en-us/azure/active-directory/conditional-access/concept-conditional-access-session

Community vote distribution
B (100%)

CaracasCCS1 Highly Voted 2 years, 3 months ago
Selected Answer: B
B!
Because the Application enforced restrictions..

https://docs.microsoft.com/en-us/azure/active-directory/conditional-access/concept-conditional-access-session
upvoted 6 times

RomanV Highly Voted 1 year, 8 months ago
Correct answer is B.
Within a Conditional Access policy, an administrator can make use of session controls to enable limited experiences within specific cloud applications.

Source: https://learn.microsoft.com/en-us/azure/active-directory/conditional-access/concept-conditional-access-session#persistent-browser-session

If you already reached to question 60, success with your exam. You can pass it. ;)
upvoted 6 times

Stig_88 Most Recent 1 year, 8 months ago
Selected Answer: B
under session, use app enforced restriction.
refer here: https://learn.microsoft.com/en-us/sharepoint/control-access-from-unmanaged-devices

Limiting access allows users to remain productive while addressing the risk of accidental data loss on unmanaged devices. When you limit access, users on managed devices will have full access (unless they use one of the browser and operating system combinations listed in Supported browsers). Users on unmanaged devices will have browser-only access with no ability to download, print, or sync files. They also won't be able to access content through apps, including the Microsoft Office desktop apps. When you limit access, you can choose to allow or block editing files in the browser. When web access is limited, users will see the following message at the top of sites.
upvoted 1 times

King_Khong 1 year, 9 months ago
in my exam 17/03/23
upvoted 3 times

Question #61 *Topic 1*

You have a hybrid deployment of Azure Active Directory (Azure AD) that contains two users named User1 and User2.
You need to assign Role Based Access Control (RBAC) roles to User1 and User2 to meet the following requirements:
✑ Use the principle of least privilege.
✑ Enable User1 to view sync errors by using Azure AD Connect Health.
✑ Enable User2 to configure Azure Active Directory Connect Health Settings.
Which two roles should you assign? Each correct answer presents part of the solution.
NOTE: Each correct selection is worth one point.

A. The Monitoring Reader role in Azure AD Connect Health to User1

B. The Security reader role in Azure AD to User1

C. The Reports reader role in Azure AD to User1

D. The Contributor role in Azure AD Connect Health to User2

E. The Monitoring Contributor role in Azure AD Connect Health to User2

F. The Security operator role in Azure AD to User2

Suggested Answer: *AE*
A: The Monitoring Reader can read all monitoring data (metrics, logs, etc.).
Note: Assign the Monitoring reader role to the Azure Active Directory application on the subscription, resource group or resource you want to monitor.
E: Monitoring Contributor can read all monitoring data and edit monitoring settings.
Incorrect:
Not B: Security Reader can view permissions for Security Center. Can view recommendations, alerts, a security policy, and security states, but cannot make changes
Not D: Contributor grants full access to manage all resources, but does not allow you to assign roles in Azure RBAC, manage assignments in Azure Blueprints, or share image galleries.
Reference:
https://docs.microsoft.com/en-us/azure/role-based-access-control/built-in-roles

Community vote distribution
AD (100%)

KarimaMaf 1 year, 6 months ago
A and D
Monitoring reader to read monitoring data about the ressource ad connect health
D because we need to change the settings of the ressource so we need the role contributor of ad connect health cause monitoring contributor can be used only to change monitoring setting pf ad connect healt and not the ressource settings
upvoted 1 times

Tanasi 1 year, 7 months ago
These questions are so so bullshit. Why do I have to remember each miniscule role.
upvoted 3 times

AJCG 1 year, 8 months ago
@jay_op do not provide incorrect information unless you have checked . Monitoring reader role does exist.
upvoted 1 times

kmk_01 1 year, 9 months ago
Selected Answer: AD
There is no monitoring reader role in Azure AD Connect Health, but there is a reader role.
upvoted 1 times

examdj101j 1 year, 8 months ago
I have the same exact question in another exam prep and the answer is AD.
upvoted 1 times

msysadmin 1 year, 10 months ago

Correct Answers AD,
Azure AD Connect Health supports the following built-in roles:
Role Permissions

Owner Owners can manage access (for example, assign a role to a user or group), view all information (for example, view alerts) from the portal, and change settings (for example, email notifications) within Azure AD Connect Health.

By default, Azure AD Hybrid Identity Administrators are assigned this role, and this cannot be changed.

Contributor Contributors can view all information (for example, view alerts) from the portal, and change settings (for example, email notifications) within Azure AD Connect Health.

Reader Readers can view all information (for example, view alerts) from the portal within Azure AD Connect Health.
https://learn.microsoft.com/en-us/azure/active-directory/hybrid/how-to-connect-health-operations
upvoted 1 times

⊟ **fjfg** 1 year, 11 months ago
Selected Answer: AD
For the second role I would select the Contributor role in AAC Connect Health (Option D) rather than the Monitoring Contributor role (option E), which doesn´t exist in the latest documentation, AFAIK
https://learn.microsoft.com/en-us/azure/active-directory/hybrid/how-to-connect-health-operations#manage-access-with-azure-rbac
https://learn.microsoft.com/en-us/azure/active-directory/roles/delegate-by-task#connect-health
upvoted 1 times

⊟ **Tanasi** 1 year, 7 months ago
You cannot find it in the documentation, but it is in the portal.
https://portal.azure.com/#view/Microsoft_Azure_ADHybridHealth/AadHealthMenuBlade/~/RBAC_IAM
upvoted 1 times

⊟ **ccadenasa** 2 years, 1 month ago
answer is correct and can be validated here > https://learn.microsoft.com/en-us/azure/active-directory/hybrid/how-to-connect-health-operations#manage-access-with-azure-rbac
upvoted 3 times

⊟ **billo79152718** 2 years, 3 months ago
correct
upvoted 3 times

Question #62 *Topic 1*

You have a Microsoft 365 subscription that contains a user named User1.
You need to assign User1 permissions to search Microsoft Office 365 audit logs.
What should you use?

A. the Azure Active Directory admin center

B. the Exchange admin center

C. the Microsoft 365 Defender portal

D. the Microsoft 365 Compliance center

Suggested Answer: *B*
To give a user the ability to search the audit log with the minimum level of privileges, you can create a custom role group in Exchange Online, add the View-Only
Audit Logs or Audit Logs role, and then add the user as a member of the new role group.
Incorrect:
Not D: If you assign a user the View-Only Audit Logs or Audit Logs role on the Permissions page in the compliance portal, they won't be able to search the audit log. You have to assign the permissions in Exchange Online. This is because the underlying cmdlet used to search the audit log is an Exchange Online cmdlet.
You can also use the Exchange admin center (EAC).
Reference:
https://docs.microsoft.com/en-us/microsoft-365/compliance/search-the-audit-log-in-security-and-compliance

Community vote distribution

B (70%) A (20%) 10%

Anonymousse Highly Voted 2 years, 2 months ago

You have to be assigned the View-Only Audit Logs or Audit Logs role in Exchange Online to search the audit log.
From: https://learn.microsoft.com/en-us/microsoft-365/compliance/search-the-audit-log-in-security-and-compliance?view=o365-worldwide

upvoted 5 times

Felxxry Most Recent 1 year ago

Selected Answer: C

Managing Audit permissions from the Exchange admin center will be discontinued starting February 2, 2024. You should start using the compliance portal now to manage Audit permissions and familiarize yourselves with the new permissions controls. To minimize impact to your organization, all existing Audit permissions currently assigned in the Exchange admin center will be automatically configured in the compliance portal on February 2, 2024.

upvoted 1 times

pompes 1 year, 7 months ago

Correct. Was on the exam

upvoted 2 times

RomanV 1 year, 8 months ago

The Exchange admin center can also be used to assign permissions for searching Office 365 audit logs, but it is not the recommended method. In the Exchange admin center, you can assign the 'Mailbox Search' role to a user, which will give them access to search mailboxes for specific content. However, this role does not provide the necessary permissions to search the Office 365 audit logs.

The recommended method for assigning permissions to search Office 365 audit logs is through the Microsoft 365 Compliance center, which provides more granular controls and better visibility into compliance-related activities. The Compliance center also allows you to assign other compliance-related roles and permissions, such as eDiscovery permissions and data loss prevention policies.

So the answer should be D. the Microsoft 365 Compliance center

upvoted 1 times

RomanV 1 year, 8 months ago

Ignore the above, just follow Microsoft and choose answer B:

"You have to be assigned the View-Only Audit Logs or Audit Logs role in Exchange Online to search the audit log. By default, these roles are assigned to the Compliance Management and Organization Management role groups on the Permissions page in the Exchange admin center. Global administrators in Office 365 and Microsoft 365 are automatically added as members of the Organization Management role group in Exchange Online. To give a user the ability to search the audit log with the minimum level of privileges, you can create a custom role group in Exchange Online, add the View-Only Audit Logs or Audit Logs role, and then add the user as a member of the new role group."

upvoted 1 times

nsss 1 year, 9 months ago

This makes zero sense, why would you have to do this in the Exchange admin center?

upvoted 2 times

Pointless 1 year, 9 months ago

“This is because the underlying cmdlet used to search the audit log is an Exchange Online cmdlet.”

Hmm ok.

upvoted 1 times

mcclane654 2 years ago

Selected Answer: A

I think its unclear what Audit logs they are asking about. but Azure AD Audit logs requires: Reports reader.

you all are talking about compliance audit logs.

ref: https://learn.microsoft.com/en-us/azure/active-directory/roles/delegate-by-task#monitoring---audit-logs

upvoted 1 times

tibodenbeer 2 years ago

Selected Answer: B

You have to be assigned the View-Only Audit Logs or Audit Logs role in Exchange Online to search the audit log. By default, these roles are assigned to the Compliance Management and Organization Management role groups on the Permissions page in the Exchange admin center. Global administrators in Office 365 and Microsoft 365 are automatically added as members of the Organization Management role group in Exchange Online. To give a user the ability to search the audit log with the minimum level of privileges, you can create a custom role group in Exchange Online, add the View-Only Audit Logs or Audit Logs role, and then add the user as a member of the new role group. For more information, see Manage role groups in Exchange Online.

Source:

https://learn.microsoft.com/en-us/microsoft-365/compliance/audit-log-search?view=o365-worldwide

upvoted 3 times

skycrap 2 years ago

Selected Answer: B

I agree with B. https://learn.microsoft.com/en-us/microsoft-365/compliance/audit-standard-setup?source=recommendations&view=o365-worldwide see Step 2

upvoted 1 times

mohamed_Saed 2 years, 2 months ago

Selected Answer: A

i think it is A

upvoted 1 times

PhyMac 2 years, 3 months ago

I believe B is correct.

https://learn.microsoft.com/en-us/microsoft-365/compliance/search-the-audit-log-in-security-and-compliance?view=o365-worldwide

"You have to be assigned the View-Only Audit Logs or Audit Logs role in Exchange Online to search the audit log. By default, these roles are assigned to the Compliance Management and Organization Management role groups on the Permissions page in the Exchange admin center."

upvoted 4 times

KarambaFr 2 years, 3 months ago

indeed, the comment helps to validate this answer.

upvoted 2 times

EzeQ 2 years, 3 months ago

Selected Answer: B

the reference is correct and it points to the given reply

upvoted 3 times

⊟ **fx500** 2 years, 3 months ago

I think “C” is correct

upvoted 1 times

⊟ **Brigg5** 1 year, 11 months ago

The ability to run an audit search is available in the Defender portal but you can not enable the permissions there. B is correct, even though it doesn't make sense, you have to use the Exchange Admin Center.

upvoted 1 times

⊟ **Aki_007** 2 years, 2 months ago

better go in a circus

upvoted 1 times

Question #63 *Topic 1*

You have a Microsoft 365 tenant that has modern authentication enabled.
You have Windows 10, MacOS, Android, and iOS devices that are managed by using Microsoft Endpoint Manager.
Some users have older email client applications that use Basic authentication to connect to Microsoft Exchange Online.
You need to implement a solution to meet the following security requirements:
✑ Allow users to connect to Exchange Online only by using email client applications that support modern authentication protocols based on OAuth 2.0.
✑ Block connections to Exchange Online by any email client applications that do NOT support modern authentication.
What should you implement?

A. a conditional access policy in Azure Active Directory (Azure AD)

B. an application control profile in Microsoft Endpoint Manager

C. a compliance policy in Microsoft Endpoint Manager

D. an OAuth app policy in Microsoft Defender for Cloud Apps

Suggested Answer: *A*
Block clients that don't support multi-factor with a Conditional Access policy.
Note: Clients that do not use modern authentication can bypass Conditional Access policies, so it's important to block these.
Incorrect:
Not D: OAuth app policies enable you to investigate which permissions each app requested and which users authorized them for Office 365, Google Workspace, and Salesforce. You're also able to mark these permissions as approved or banned.
Reference:
https://docs.microsoft.com/en-us/microsoft-365/security/office-365-security/identity-access-policies

⊟ **pete26** Highly Voted 2 years, 2 months ago
Valid on exam October 14, 2022
upvoted 6 times

⊟ **RomanV** Most Recent 1 year, 8 months ago
Correct answer is A. A conditional access policy in Azure Active Directory (Azure AD) is the best option to implement to meet the security requirements. Once the policy is created, it will block any email client application that does not support modern authentication from accessing Exchange Online, and users will be allowed to connect to Exchange Online only by using email client applications that support modern authentication protocols based on OAuth 2.0.
upvoted 1 times

Question #64 *Topic 1*

HOTSPOT -

You have a Microsoft 365 E5 subscription linked to an Azure Active Directory (Azure AD) tenant. The tenant contains a user named User1 and multiple Windows

10 devices. The devices are Azure AD joined and protected by using BitLocker Drive Encryption (BitLocker).

You need to ensure that User1 can perform the following actions:

✑ View BitLocker recovery keys.

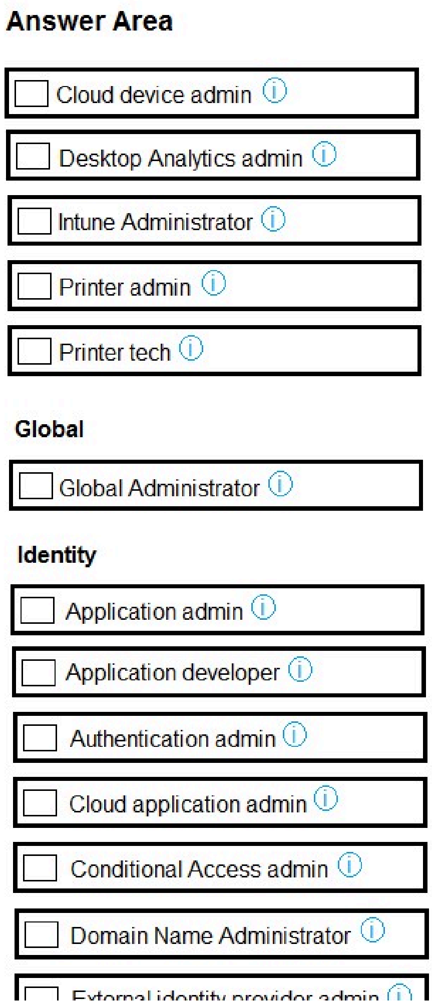
✑ Configure the usage location for the users in the tenant.

The solution must use the principle of least privilege.

Which two roles should you assign to User1 in the Microsoft 365 admin center? To answer, select the appropriate roles in the answer area.

NOTE: Each correct selection is worth one point.

Hot Area:



Answer Area

- □ Cloud device admin ⓘ
- □ Desktop Analytics admin ⓘ
- □ Intune Administrator ⓘ
- □ Printer admin ⓘ
- □ Printer tech ⓘ

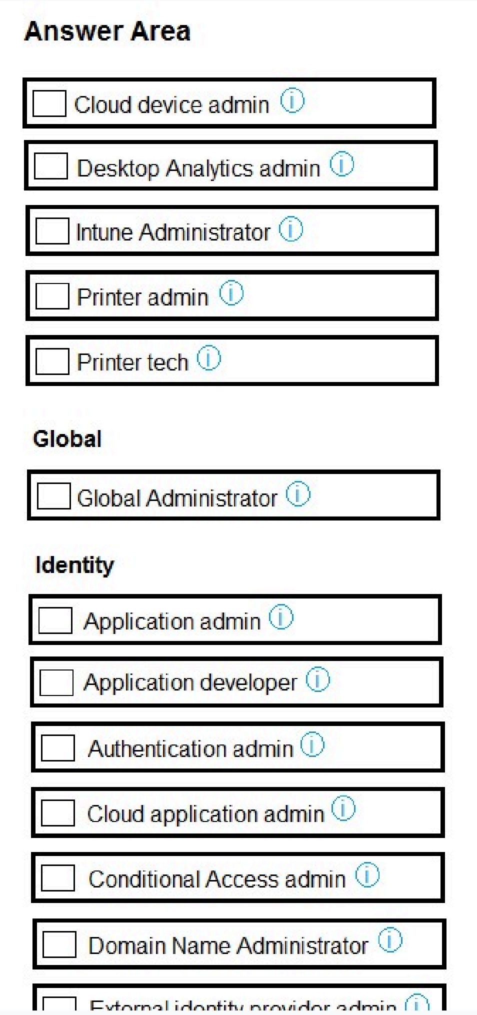
Global

- □ Global Administrator ⓘ

Identity

- □ Application admin ⓘ
- □ Application developer ⓘ
- □ Authentication admin ⓘ
- □ Cloud application admin ⓘ
- □ Conditional Access admin ⓘ
- □ Domain Name Administrator ⓘ
- □ External identity provider admin ⓘ

Suggested Answer:



Answer Area

□ Cloud device admin ⓘ

□ Desktop Analytics admin ⓘ

□ Intune Administrator ⓘ

□ Printer admin ⓘ

□ Printer tech ⓘ

Global

□ Global Administrator ⓘ

Identity

□ Application admin ⓘ

□ Application developer ⓘ

□ Authentication admin ⓘ

□ Cloud application admin ⓘ

□ Conditional Access admin ⓘ

□ Domain Name Administrator ⓘ

□ External identity provider admin ⓘ

Box 1: Helpdesk admin -
View BitLocker recovery keys.
Helpdesk Admins can read bitlocker metadata and key on devices
Note: One of the following should be enough:

Global admins -

Intune Service Administrators -

Security Administrators -

Security Readers -

Helpdesk Admins -

Box 2: User Administrator -
Configure the usage location for the users in the tenant.
The User Administrator can manage all aspects of users and groups, including resetting passwords for limited admins.
The User Administrator cam manage all user properties including User Principal Name

Update (FIDO) device keys -
Reference:
https://docs.microsoft.com/en-us/azure/active-directory/roles/permissions-reference

⊟ fjfg Highly Voted 1 year, 11 months ago
According to the following link the least privileged role that can read BitLocker keys is the Cloud Device Administrator.
https://learn.microsoft.com/en-us/azure/active-directory/roles/delegate-by-task
upvoted 9 times

⊟ pete26 Highly Voted 2 years, 2 months ago

Valid on exam October 14, 2022

upvoted 6 times

RomanV Most Recent 1 year, 8 months ago

Least privileged role to read BitLocker keys:
- Cloud Device Administrator

Additional roles:
- Helpdesk Administrator
- Intune Administrator
- Security Administrator
- Security Reader

And for the 2nd request: User Administrator

Source: https://learn.microsoft.com/en-us/azure/active-directory/roles/delegate-by-task

upvoted 2 times

examdj101j 1 year, 8 months ago

On my screen I wasn't able to even see all the options available.

upvoted 4 times

JoeP1 1 year, 10 months ago

All of the correct answers are cut off in the picture!

upvoted 5 times

msysadmin 1 year, 10 months ago

This question is bit complicated. Agree with fjfg & Dzuljzebari.
Cloud Device Admin also have a same permisson.

Cloud Device Administrator
microsoft.directory/bitlockerKeys/key/read Read bitlocker metadata and key on devices.

upvoted 1 times

Dzuljzebari 1 year, 11 months ago

Tested in lab, Helpdesk admin role allows to view the BitLocker key. Tricky as it is not described in the role description while it clearly mentions this capability for Cloud Device Administrator role.

upvoted 2 times

brotown22 1 year, 12 months ago

Tricky as full list of roles not provided, however if following 'least privilege role':
role #1 - helpdesk admin
role #2 - licence admin (only role with specific microsoft.directory/users/usageLocation/update permission)
ref: https://learn.microsoft.com/en-us/azure/active-directory/roles/permissions-reference#license-administrator

upvoted 1 times

hans333 2 years ago

I think, its:
Bitlocker: Intune administrator
Usage location: User administrator

upvoted 3 times

Naveedkarjikar 2 years, 2 months ago

How ato answer this

upvoted 2 times

ariania 2 years, 2 months ago

This question is a little strange. If you are actually watching the answer area it should be "Intunes Admin" and "Global Admin". But study on the roles in solution area incase it has different forms in the exam.

upvoted 2 times

> **ariania** 2 years, 2 months ago
>
> Note that we dont see the full list, so my answer is from what we see.
>
> upvoted 1 times

Question #65 *Topic 1*

HOTSPOT -

Your on-premises network contains an Active Directory domain that syncs to Azure Active Directory (Azure AD) by using Azure AD Connect. The functional level of the domain is Windows Server 2019.

You need to deploy Windows Hello for Business. The solution must meet the following requirements:

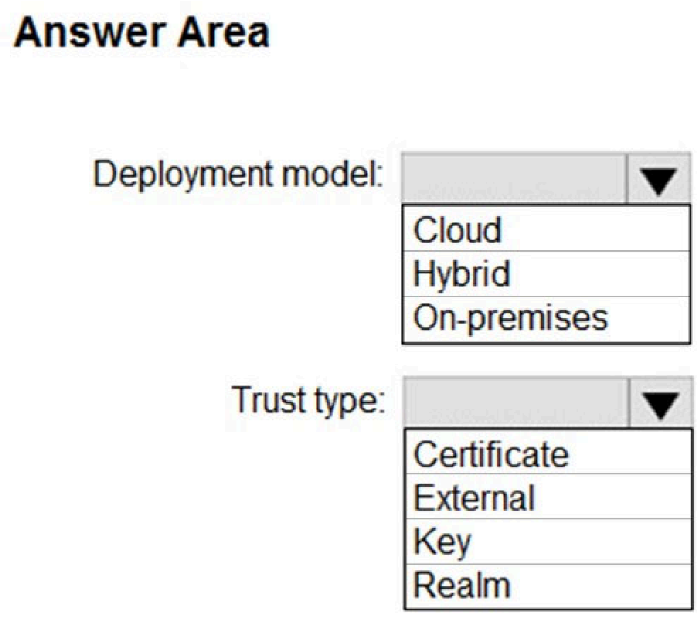
✑ Ensure that users can access Microsoft 365 services and on-premises resources.

✑ Minimize administrative effort.

How should you deploy Windows Hello for Business and which type of trust should you use? To answer, select the appropriate options in the answer area.

NOTE: Each correct selection is worth one point.

Hot Area:

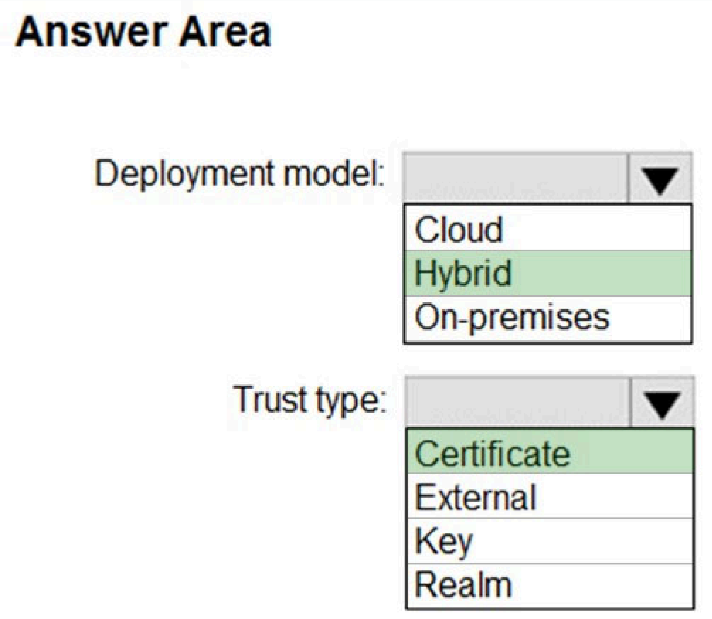


Answer Area

Deployment model:
- Cloud
- Hybrid
- On-premises

Trust type:
- Certificate
- External
- Key
- Realm

Suggested Answer:



Answer Area

Deployment model:
- Cloud
- [✓ Hybrid]
- On-premises

Trust type:
- [✓ Certificate]
- External
- Key
- Realm

Box 1: Hybrid -

Hybrid environments are distributed systems that enable organizations to use on-premises and Azure-based identities and resources.

Box 2: Certificate -

The Windows Hello for Business deployment depends on an enterprise public key infrastructure as trust anchor for authentication. Domain controllers for hybrid deployments need a certificate in order for Windows devices to trust the domain controller.

Reference:

https://docs.microsoft.com/en-us/windows/security/identity-protection/hello-for-business/hello-hybrid-cert-trust-prereqs

lear87 1 year, 6 months ago

1. Hybrid
2. Key

upvoted 1 times

RomanV 1 year, 8 months ago

Her is your answer:

The key trust type does not require issuing authentication certificates to end users. Users authenticate using a hardware-bound key created during the built-in provisioning experience. This requires an adequate distribution of Windows Server 2016 or later domain controllers relative to your existing authentication and the number of users included in your Windows Hello for Business deployment. Read the Planning an adequate number of Windows Server 2016 or later Domain Controllers for Windows Hello for Business deployments to learn more.

The certificate trust type issues authentication certificates to end users. Users authenticate using a certificate requested using a hardware-bound key created during the built-in provisioning experience. Unlike key trust, certificate trust does not require Windows Server 2016 domain controllers (but still requires Windows Server 2016 or later Active Directory schema). Users can use their certificate to authenticate to any Windows Server 2008 R2, or later, domain controller.

1. Hybrid
2. Certificate

Source: https://learn.microsoft.com/en-us/windows/security/identity-protection/hello-for-business/hello-planning-guide

upvoted 1 times

msysadmin 1 year, 10 months ago

Certificate model is wrong because it saying minimum admin effort:

Certificate model: Prerequisites

Directories and directory synchronization
Federated authentication to Azure AD ---- This one require is huge amount admin effort
Device registration
Public Key Infrastructure
Multi-factor authentication
Device management

Hybrid key trust: Prerequisites

Directories and directory synchronization
Authentication to Azure AD ---- This is easy can be pass hash sync or pass-through
Device registration
Public Key Infrastructure
Multi-factor authentication
Device management

upvoted 1 times

RomanV 1 year, 8 months ago

The certificate trust type issues authentication certificates to end users. Users authenticate using a certificate requested using a hardware-bound key created during the built-in provisioning experience. Unlike key trust, certificate trust does not require Windows Server 2016 domain controllers.

upvoted 1 times

msysadmin 1 year, 10 months ago

The question itself is incorrect. Probably it mention about domain functional level 2016. Because the Windows Server 2016 is the most recent forest and domain functional level. Windows server 2019 and 2022 are using the Windows Server 2016 forest and domain functional level.

upvoted 1 times

kimble3k 2 years ago

I think the answer is correct, hybrid - certificate, because here:
https://learn.microsoft.com/en-us/windows/security/identity-protection/hello-for-business/hello-hybrid-cert-trust-prereqs
so it has to be hybrid, but not sure which deployment type is easier, I guess Certificate, because it has less steps in the guide? :D

upvoted 1 times

⊟ **EzeQ** 2 years, 3 months ago

https://docs.microsoft.com/en-us/windows/security/identity-protection/hello-for-business/hello-overview#comparing-key-based-and-certificate-based-authentication

"Enterprises that don't use PKI or want to reduce the effort associated with managing user certificates can rely on key-based credentials for Windows Hello."

https://learn.microsoft.com/en-us/windows/security/identity-protection/hello-for-business/hello-deployment-guide

"The key-trust model is for enterprises who do not want to issue end-entity certificates to their users and have an adequate number of 2016 domain controllers in each site to support authentication. This still requires Active Directory Certificate Services for domain controller certificates."

For last the name in the URL is my reply

https://learn.microsoft.com/en-us/windows/security/identity-protection/hello-for-business/hello-hybrid-key-trust

upvoted 4 times

⊟ **BoxGhost** 2 years ago

Agree I think key based is the better answer because it specifically mentions they have a domain level of 2019

upvoted 1 times

⊟ **yoton** 1 year, 10 months ago

It would be cert from my understanding. You need to meet the requirements to even be able to setup/use the key

"Once the prerequisites are met, deploying Windows Hello for Business with a hybrid key trust model consists of the following steps:

Configure and validate the PKI"

The follow up to that..

"An enterprise PKI is required as trust anchor for authentication. Domain controllers require a certificate for Windows clients to trust them."

upvoted 1 times

⊟ **yoton** 1 year, 10 months ago

To further my point:

"The certificate trust type issues authentication certificates to end users. Users authenticate using a certificate requested using a hardware-bound key created during the built-in provisioning experience. Unlike key trust, certificate trust does not require Windows Server 2016 domain controllers (but still requires Windows Server 2016 or later Active Directory schema). Users can use their certificate to authenticate to any Windows Server 2008 R2, or later, domain controller."

https://learn.microsoft.com/en-us/windows/security/identity-protection/hello-for-business/hello-planning-guide

upvoted 2 times

Question #66 *Topic 1*

HOTSPOT -

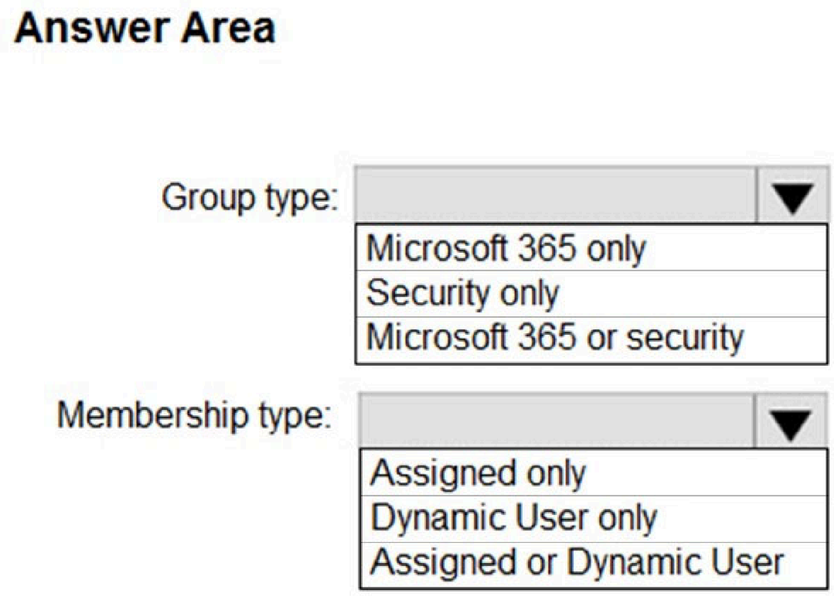
You have a Microsoft 365 E5 subscription.

You need to create a role-assignable group. The solution must ensure that you can nest the group.

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

NOTE: Each correct selection is worth one point.

Hot Area:

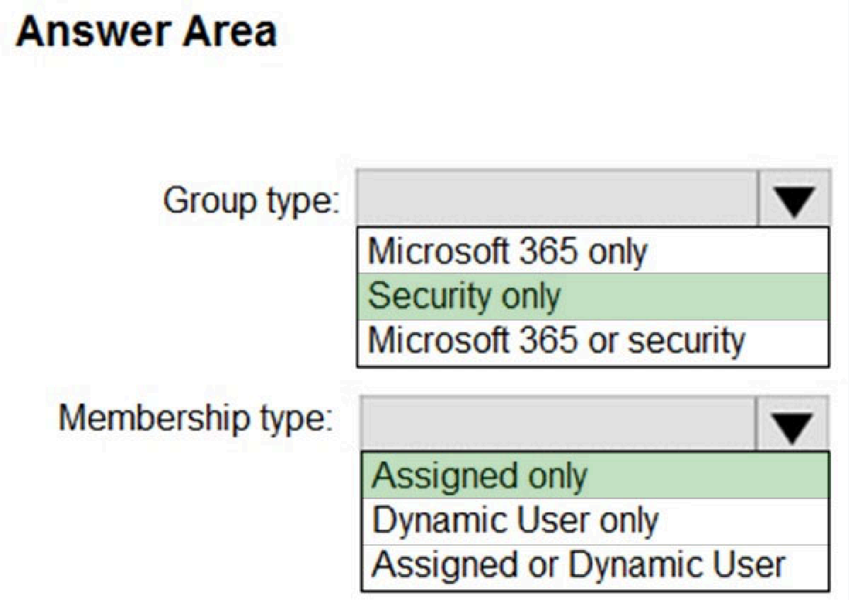


Answer Area

Group type: ▼
- Microsoft 365 only
- Security only
- Microsoft 365 or security

Membership type: ▼
- Assigned only
- Dynamic User only
- Assigned or Dynamic User

Suggested Answer:



Answer Area

Group type: ▼
- Microsoft 365 only
- [✓ Security only]
- Microsoft 365 or security

Membership type: ▼
- [✓ Assigned only]
- Dynamic User only
- Assigned or Dynamic User

Box 1: Security only -

You can add an existing Security group to another existing Security group (also known as nested groups), creating a member group (subgroup) and a parent group. The member group inherits the attributes and properties of the parent group, saving you configuration time.

Incorrect:

Not supported:

Adding Security groups to Microsoft 365 groups.

Adding Microsoft 365 groups to Security groups or other Microsoft 365 groups.

Box 2: Assigned only -

The membership type for role-assignable groups must be Assigned and can't be an Azure AD dynamic group.

Reference:

https://docs.microsoft.com/en-us/azure/active-directory/fundamentals/active-directory-groups-membership-azure-portal

⊟ **RVR** Highly Voted 2 years, 3 months ago

Group Type: Microsoft 365 or security

Reference: "To assign a role to a group, you must create a new security or Microsoft 365 group with the isAssignableToRole property set to true"

Membership type: Assigned only

Reference: "The membership type for role-assignable groups must be Assigned and can't be an Azure AD dynamic group."

Link: https://learn.microsoft.com/en-us/azure/active-directory/roles/groups-concept

upvoted 10 times

Pretsan 2 years, 2 months ago

It informs that you can ensure you can nest the group and MS 365 don't support nesting so I would go for:

Group type: Security group

Membership type: Assigned only

upvoted 15 times

msysadmin 1 year, 10 months ago

Agree: Answer is correct.

"Microsoft 365 Groups don't support nesting with other Microsoft 365 Groups or with distribution or security groups"

upvoted 2 times

Dhamus Most Recent 1 year, 7 months ago

Microsoft 365 group does not support nesting, that is, you cannot add groups within this group.

upvoted 1 times

SaadKhamis 1 year, 11 months ago

Based on https://learn.microsoft.com/en-us/azure/active-directory/roles/groups-concept#how-are-role-assignable-groups-protected

- Group nesting is not supported. A group can't be added as a member of a role-assignable group.

So, what is the right answer?

upvoted 1 times

amymay101 1 year, 11 months ago

M365 or Security group and 'assigned' only

upvoted 1 times

kmk_01 1 year, 9 months ago

You can't nest M365 groups.

upvoted 2 times

tibodenbeer 2 years ago

As of now, the answer is correct. Tried to nest an Microsoft365 group but the option is grayed out:

- Create M365 group

- Go to Groups memberships

--> Add memberships is grayed out.

If you do the same with a security group, the "add memberships" is available.

So the answer is correct (for now, since they specifically ask for a non nesting.)

Security group --> Assigned

upvoted 4 times

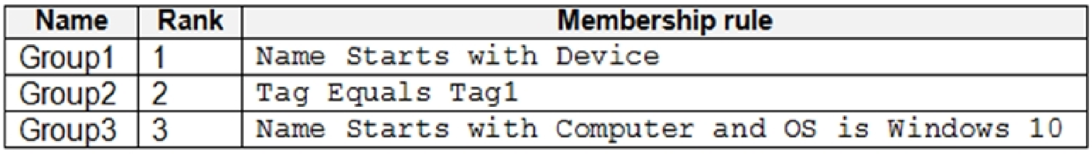
ccadenasa 2 years, 1 month ago

I think the answer is correct however, Microsoft 365 groups support nesting through dynamic groups in Azure Active Directory according to this information > https://learn.microsoft.com/en-us/microsoft-365/admin/create-groups/compare-groups?view=o365-worldwide#microsoft-365-groups but it is in preview > https://learn.microsoft.com/en-us/azure/active-directory/enterprise-users/groups-dynamic-rule-member-of which is not relevant for an exam

upvoted 1 times

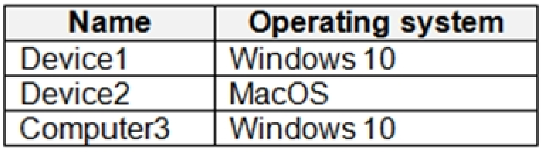
HOTSPOT -

You create device groups in Microsoft Defender for Endpoint as shown in the following table.



Name	Rank	Membership rule
Group1	1	`Name Starts with Device`
Group2	2	`Tag Equals Tag1`
Group3	3	`Name Starts with Computer and OS is Windows 10`

You onboard three devices to Microsoft Defender for Endpoint as shown in the following table.



Name	Operating system
Device1	Windows 10
Device2	MacOS
Computer3	Windows 10

After the devices are onboarded, you perform the following actions:

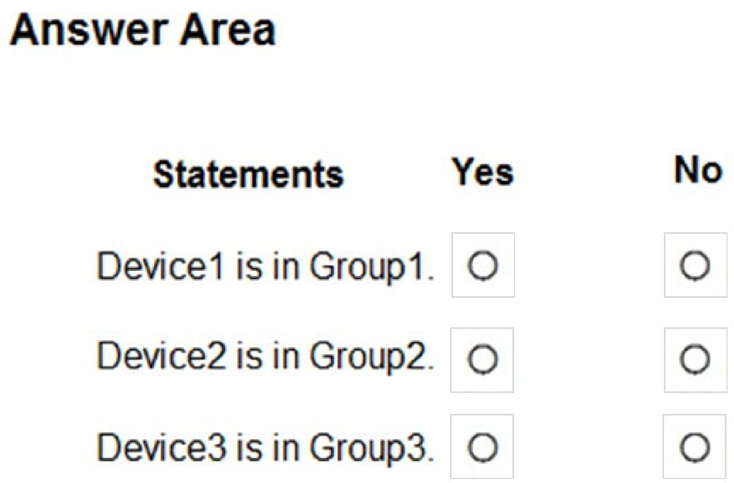
✑ Add a tag named Tag1 to Device1.

✑ Rename Computer3 as Device3.

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

NOTE: Each correct selection is worth one point.

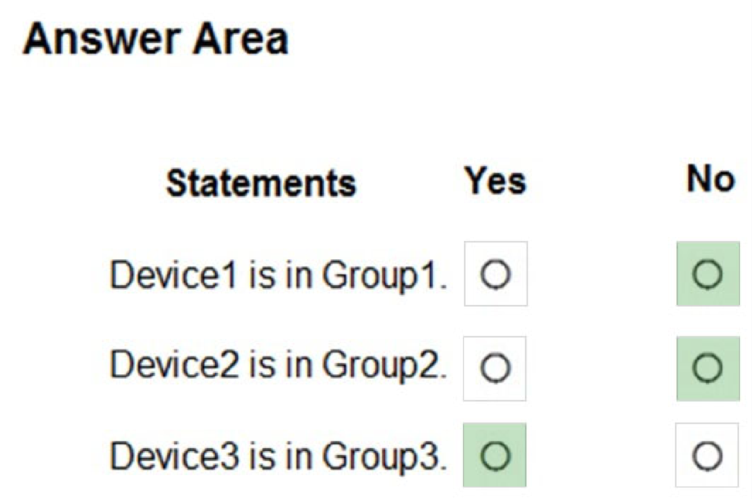
Hot Area:



Answer Area

Statements	Yes	No
Device1 is in Group1.	○	○
Device2 is in Group2.	○	○
Device3 is in Group3.	○	○

Suggested Answer:



Answer Area

Statements	Yes	No
Device1 is in Group1.	○	[✓ ○]
Device2 is in Group2.	○	[✓ ○]
Device3 is in Group3.	[✓ ○]	○

Box 1: No -

The Group1 membership rule 'Name Start with Device' applies to Device1.

However, the higher ranked Group2 membership rule 'Tag Equals Tag1' also applies to Device1, and overrules the lower ranked rule.

Note: 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.

Box 2: No -

The Group1 membership rule 'Name Start with Device' applies Device2.

No other rule applies.

Box 3: Yes -
The Group3 rule applies for Computer3.
Reference:
https://docs.microsoft.com/en-us/microsoft-365/security/defender-endpoint/machine-groups

⊟ **Dinraj** Highly Voted 👍 2 years, 3 months ago

Ans Must be Y N N
1st one is higher rank, which is Group 1
3rd is Compter3 rename to Device3 which will Apply to Group1

upvoted 57 times

⊟ **tibodenbeer** 2 years ago

Correct as written here:
As you create policies in Defender for Business, an order of priority is assigned. If you apply multiple policies to a given set of devices, those devices will receive the first applied policy only. For more information, see Understand policy order in Defender for Business.

https://learn.microsoft.com/en-us/microsoft-365/security/defender-business/mdb-create-edit-device-groups?view=o365-worldwide#what-is-a-device-group

upvoted 4 times

⊟ **tibodenbeer** 2 years ago

Also:
https://learn.microsoft.com/en-us/microsoft-365/security/defender-business/mdb-create-edit-device-groups?view=o365-worldwide#what-is-a-device-group

upvoted 1 times

⊟ **Trainee2244** Highly Voted 👍 2 years, 3 months ago

NNN, Add Tag1 to Device1 so Device 1 is in Group2 and Device2 is in Group1. Rename Computer3 to Device3 so Device3 is in Group1

upvoted 10 times

⊟ **Lomak** 2 years, 2 months ago

Being called "Device*" would match the highest rank (1) so 'Device1' would go into Group 1

upvoted 8 times

⊟ **darkschneider** Most Recent 🕒 1 year, 8 months ago

Correct answer is Y,N,N
https://learn.microsoft.com/en-us/microsoft-365/security/defender-endpoint/machine-groups?view=o365-worldwide
Paragraph "Manage device groups": (...) A device group with a rank of 1 is the highest ranked group. When a device is matched to more than one group, it's added only to the highest ranked group. (...)
Thus: all 3 devices (being named Device1 or 2 or 3) end up in Group1,

upvoted 2 times

⊟ **GatesBill** 1 year, 9 months ago

Assuming these are Dynamic Device Groups (as formulated in the question itself), devices will be reassigned whenever there is a change is the specified attribute.

Also: "A device group with a rank of 1 is the highest ranked group" - https://learn.microsoft.com/en-us/microsoft-365/security/defender-endpoint/machine-groups?view=o365-worldwide#manage-device-groups

upvoted 1 times

⊟ **ajjihad1** 1 year, 10 months ago

https://learn.microsoft.com/en-us/microsoft-365/security/defender-endpoint/machine-groups?view=o365-worldwide

upvoted 1 times

⊟ **ajjihad1** 1 year, 10 months ago

Key points to remember about policy order
Policies are assigned an order of priority.
Devices receive the first applied policy only.
You can change the order of priority for policies.
Default policies are given the lowest order of priority.

upvoted 1 times

⊟ **ajjihad1** 1 year, 10 months ago

The important thing to remember about multiple policies is that devices will receive the first applied policy only. Referring to our earlier example of three next-generation policies, suppose that you have devices that are targeted by all three policies. In this case, those devices will receive policy number 1, but won't receive policies numbered 2 and 3.

upvoted 1 times

⊟ **Ksumeet91** 2 years ago

Y N N is correct

upvoted 1 times

⊟ **Lomak** 2 years, 2 months ago

Y, N, N
Rank 1 is highest
(there is a Rank called 'Last' which confirms this)
https://learn.microsoft.com/en-us/microsoft-365/security/defender-endpoint/machine-groups?view=o365-worldwide#manage-device-groups

upvoted 5 times

⊟ **mohamed_Saed** 2 years, 2 months ago

Y N N

1st one is higher rank

upvoted 3 times

⊟ **yoton** 2 years, 3 months ago

Listing the incorrect answer to this question had me messed up. Thank you to everyone who responded. I too agree that, based off the Microsoft docs, Rank 1 will out rank the others.

upvoted 2 times

⊟ **yoton** 2 years, 3 months ago

More explanation as detailed in the Microsoft docs:
"A device group with a rank of 1 is the highest ranked group. When a device is matched to more than one group, it's added only to the highest ranked group. You can also edit and delete groups."

https://learn.microsoft.com/en-us/microsoft-365/security/defender-endpoint/machine-groups?view=o365-worldwide#manage-device-groups

upvoted 3 times

⊟ **dwilding** 2 years, 3 months ago

The "solution" answer is incorrect with regard to the higher ranked group..

From Microsoft: A device group with a rank of 1 is the highest ranked group. When a device is matched to more than one group, it's added only to the highest ranked group

https://learn.microsoft.com/en-us/microsoft-365/security/defender-endpoint/machine-groups?view=o365-worldwide

upvoted 1 times

⊟ **ashkins** 2 years, 3 months ago

Y/N/N
Device 1- https://learn.microsoft.com/en-us/microsoft-365/security/defender-endpoint/machine-groups?view=o365-worldwide
"You can promote or demote the rank of a device group so that it's given higher or lower priority during matching. A device group with a rank of 1 is the highest ranked group. When a device is matched to more than one group, it's added only to the highest ranked group. You can also edit and delete groups."

Device 3- does not use the "or" operator. "Use the 'OR' operator between rows of the same condition type, which allows multiple values per property. You can add up to 10 rows (values) for each property type - tag, device name, domain."

upvoted 5 times

⊟ **JimboJones99** 2 years, 3 months ago

Surely Device1 would hit the first rule and place the device in group1 as it has a higher ranking than group2?

upvoted 2 times

⊟ **ashkins** 2 years, 3 months ago

Correct- https://learn.microsoft.com/en-us/microsoft-365/security/defender-endpoint/machine-groups?view=o365-worldwide
"You can promote or demote the rank of a device group so that it's given higher or lower priority during matching. A device group with a rank

of 1 is the highest ranked group. When a device is matched to more than one group, it's added only to the highest ranked group. You can also edit and delete groups."

upvoted 2 times

⊟ **MaartenC** 2 years, 3 months ago

Isnt "Rank 1" higher than "Rank 2" (and higher than the default "Rank Last")? if so, the answer to the first question is incorrect.

upvoted 6 times

⊟ **EzeQ** 2 years, 3 months ago

"A device group with a rank of 1 is the highest ranked group. When a device is matched to more than one group, it's added only to the highest ranked group. "

https://learn.microsoft.com/en-us/microsoft-365/security/defender-endpoint/machine-groups?view=o365-worldwide#manage-device-groups

upvoted 5 times

Question #68 *Topic 1*

You have a Microsoft 365 E5 subscription that contains 100 users. Each user has a computer that runs Windows 10 and either an Android mobile device or an iOS mobile device. All the devices are registered with Azure Active Directory (Azure AD).

You enable passwordless authentication for all the users.

You need to ensure that the users can sign in to the subscription by using passwordless authentication.

What should you instruct the users to do on their mobile device first?

A. Install a device certificate.

B. Install a user certificate.

C. Install the Microsoft Authenticator app.

D. Register for self-service password reset (SSPR).

Suggested Answer: *C*

The Authenticator App turns any iOS or Android phone into a strong, passwordless credential.

Note: Microsoft Authenticator App

You can allow your employee's phone to become a passwordless authentication method. You may already be using the Microsoft Authenticator App as a convenient multi-factor authentication option in addition to a password. You can also use the Authenticator App as a passwordless option.

Reference:

https://docs.microsoft.com/en-us/azure/active-directory/authentication/concept-authentication-passwordless

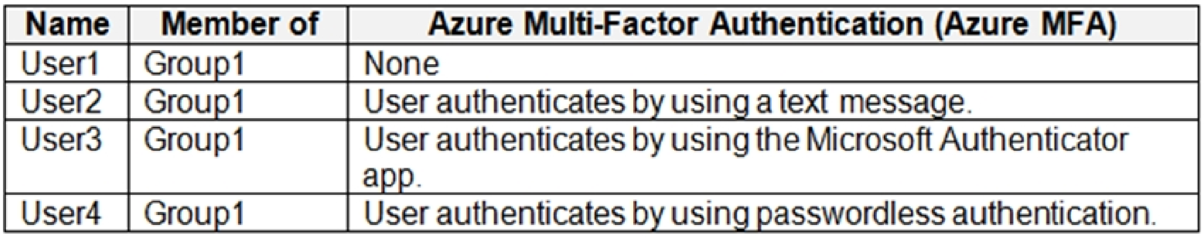
Just2a 2 years, 1 month ago

C is the answer!

upvoted 4 times

Question #69 *Topic 1*

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



Name	Member of	Azure Multi-Factor Authentication (Azure MFA)
User1	Group1	None
User2	Group1	User authenticates by using a text message.
User3	Group1	User authenticates by using the Microsoft Authenticator app.
User4	Group1	User authenticates by using passwordless authentication.

You enable the authentication methods registration campaign and configure the Microsoft Authenticator method for Group1.

Which users will be prompted to configure authentication during sign in?

A. User1 only

B. User2 only

C. User2 and User3 only

D. User1 and User2 only

E. User2 and User3 only

F. User1, User2, and User3 only

Suggested Answer: *D*

You can nudge users to set up Microsoft Authenticator during sign-in. Users will go through their regular sign-in, perform multifactor authentication as usual, and then be prompted to set up Microsoft Authenticator. You can include or exclude users or groups to control who gets nudged to set up the app. This allows targeted campaigns to move users from less secure authentication methods to Microsoft Authenticator.

Incorrect:

Not C, Not E, Not F: Not User3 since the user must not have already set up Microsoft Authenticator for push notifications on their account.

Reference:

https://docs.microsoft.com/en-us/azure/active-directory/authentication/how-to-mfa-registration-campaign

Community vote distribution

D (100%)

dwilding Highly Voted 2 years, 3 months ago

correct, key word = configure. User 3 and 4 already have this configured

upvoted 5 times

Dhamus Most Recent 1 year, 8 months ago

According to ChatGPT,

Text notifications are push.

I'm confused

upvoted 1 times

Dhamus 1 year, 8 months ago

Forget it, the answer is correct.

Technically, text messages (SMS) are not considered push notifications, as they do not require an internet connection to be delivered. Push notifications, on the other hand, are sent over an internet connection and require a specific app to receive and acknowledge the notification.

upvoted 1 times

Lomak 2 years, 2 months ago

Selected Answer: D

"Authentication methods registration campaign" currently only nudges users for Microsoft Authenticator setup. Given answers are correct

https://learn.microsoft.com/en-us/azure/active-directory/authentication/how-to-mfa-registration-campaign

upvoted 1 times

wuzime 2 years, 3 months ago

correct.

upvoted 1 times

⊟ **billo79152718** 2 years, 3 months ago

I am pretty sure that given answers are correct

upvoted 3 times

⊟ **Dinraj** 2 years, 3 months ago

I think Ans should be A(user1 only)

upvoted 1 times

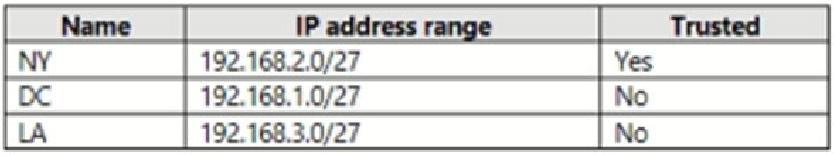
Question #70

Topic 1

HOTSPOT -

You have a Microsoft 365 subscription that contains three users named User1, User2, and User3.

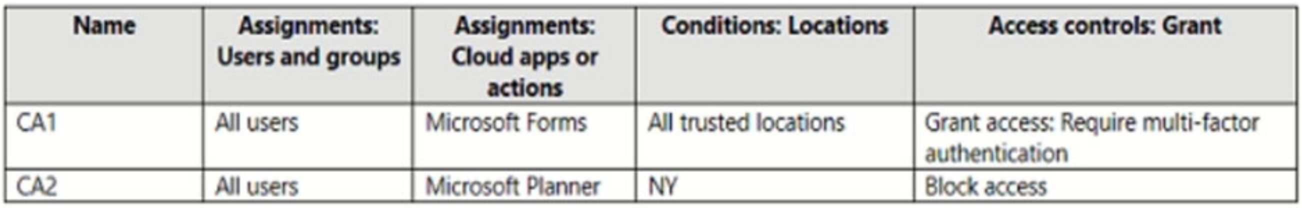
You have the named locations shown in the following table.



Name	IP address range	Trusted
NY	192.168.2.0/27	Yes
DC	192.168.1.0/27	No
LA	192.168.3.0/27	No

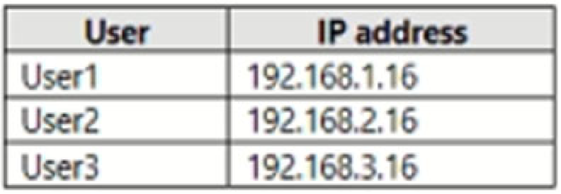
You configure an Azure Multi-Factor Authentication (MFA) trusted IP address range of 192.168.1.0/27.

You have the Conditional Access policies shown in the following table.



Name	Assignments: Users and groups	Assignments: Cloud apps or actions	Conditions: Locations	Access controls: Grant
CA1	All users	Microsoft Forms	All trusted locations	Grant access: Require multi-factor authentication
CA2	All users	Microsoft Planner	NY	Block access

The users have the IP addresses shown in the following table.

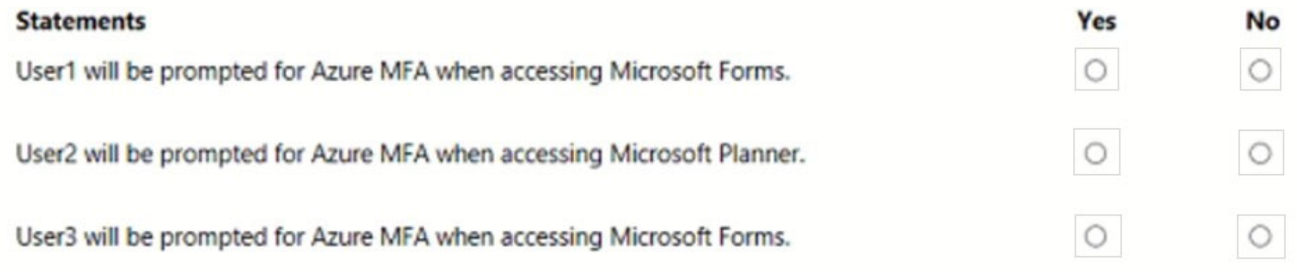


User	IP address
User1	192.168.1.16
User2	192.168.2.16
User3	192.168.3.16

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

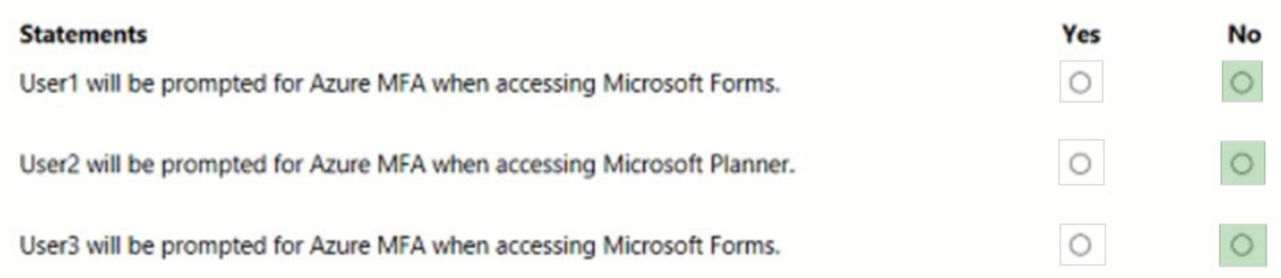
NOTE: Each correct selection is worth one point.

Hot Area:



Statements	Yes	No
User1 will be prompted for Azure MFA when accessing Microsoft Forms.	○	○
User2 will be prompted for Azure MFA when accessing Microsoft Planner.	○	○
User3 will be prompted for Azure MFA when accessing Microsoft Forms.	○	○

Suggested Answer:



Statements	Yes	No
User1 will be prompted for Azure MFA when accessing Microsoft Forms.	○	[✓ ○]
User2 will be prompted for Azure MFA when accessing Microsoft Planner.	○	[✓ ○]
User3 will be prompted for Azure MFA when accessing Microsoft Forms.	○	[✓ ○]

Box 1: No -

User1 has IP address 192.168.1.16, which is in DC named location. DC is not trusted.

CA1 applies. Access will not be granted.

Box 2: No -

User2 has IP address 192.168.2.16, which is in NY named location. NY is trusted. However, CA2 blocks Microsoft Planner NY access.

Box 3: No -

User3 is in LA. LA is not trusted.

Reference:

https://docs.microsoft.com/en-us/azure/active-directory/conditional-access/concept-conditional-access-policies

Dan91 Highly Voted 👍 2 years, 3 months ago

Y, N, N

"All trusted locations" condition applies to All locations that have been marked as trusted location and MFA Trusted IPs (if configured)

https://docs.microsoft.com/en-us/azure/active-directory/conditional-access/location-condition#all-trusted-locations:~:text=the%20corporate%20network.-,All%20trusted%20locations,MFA%20Trusted%20IPs%20(if%20configured),-Selected%20locations

upvoted 16 times

CertRookie 2 years, 2 months ago

Provided answers are correct: N N N

"User1 has IP address 192.168.1.16, which is in DC named location. DC is not trusted.

CA1 applies. Access will not be granted."

upvoted 1 times

BoxGhost 2 years ago

Also as someone else already said, private IP's are not supported. So the trusted locations will have no effect:

https://learn.microsoft.com/en-us/azure/active-directory/conditional-access/location-condition

upvoted 3 times

Tweety1972 1 year, 6 months ago

WRONG. Tested with IP address 192.168.1.0/27 and no problems

upvoted 1 times

Lomak 2 years, 2 months ago

User 1 :

(DC) Trusted = NO

MFA Trusted IP range Trusted = YES

Named + MFA location = 'All Trusted Locations'

so User 1 will 'Grant Access: Require MFA

unless Trusted Location overrides MFA Location?

upvoted 3 times

billo79152718 Highly Voted 👍 2 years, 3 months ago

I would say Yes, No, NO

upvoted 7 times

ms260591 Most Recent ⊙ 1 year, 6 months ago

user 1 will have access with MFA. MFA trusted IPs are included in 'All trusted locations' See - https://learn.microsoft.com/en-us/azure/active-directory/conditional-access/location-condition#all-trusted-locations

upvoted 1 times

RomanV 1 year, 8 months ago

Y, N, N (prove me wrong ;))

Based on the information provided, it appears that DC 1 has an IP address within the range of 192.168.1.0/27, which is also the IP address range that has been configured as a trusted IP address range for Azure Multi-Factor Authentication (MFA).

Therefore, if the conditional access policy is configured to allow access from all trusted locations but requires MFA, DC 1 should be able to access Microsoft Forms requiring MFA, since it is located within the trusted IP address range.

The trusted IP address range you configured in Azure MFA overlaps with the IP address range of DC 1, so the conditional access policy should allow DC 1 to access Microsoft Forms from its current location.

upvoted 1 times

Dislexsick 1 year, 11 months ago

Not even considering the discussion on MFA trusted locations actually do count for Trusted Locations in CAPs (and the internal IP discussion)

Answer write-up states that "DC is not trusted. CA1 applies. Access will not be granted."

DC1 is not trusted -> therefore CA1 does NOT apply since it failed to meet a condition -> CA1 is NOT applied, which does not mean access is blocked, but rather in the absence of another CAP that blocks access then access is in fact GRANTED.

upvoted 1 times

⊟ **rick001** 1 year, 11 months ago

it says : You have the Conditional Access policies shown in the following table.

Which means NAMED LOCATION. Which also means all the IP Ranges have to be external. Azure AD CA policies do not accept internal IP's.

Due to this the answer should be Y,Y,Y - no policies are applied. But you cannot create this whole setup in the first place....

With MFA Trusted locations you can use internal IP addresses but only with an MFA server / NPS.

The trusted IPs can include private IP ranges only when you use MFA Server. For cloud-based Azure AD Multi-Factor Authentication, you can use only public IP address ranges.

https://learn.microsoft.com/en-us/azure/active-directory/authentication/howto-mfa-mfasettings

TL:DR this question is stupid and makes no sense. I would go for Y,Y,Y

upvoted 3 times

⊟ **Ksumeet91** 2 years ago

Y N N

Azure MFA Trusted IP ranges option is still valid beside the trusted locations in CA !!

upvoted 1 times

⊟ **zerrowall** 2 years ago

Regarding User1 there is some confusion. The IP range of this user is in the "trusted ips" of the MFA service settings in the old MFA portal. That means that the MFA request has to be skipped. In this case, the answer has to be N.

At the same time, there is a description in Microsoft documentation, that if "Location condition" is set up as "All trusted locations" that applies to the following:

- All locations that have been marked as trusted location
- MFA Trusted IPs (if configured)

So, based on the eam task this condition is appropriate for the 1st string of table and User1 should meet with MFA, i.e. the answer is Y.

This is a weird situation.

https://learn.microsoft.com/en-us/azure/active-directory/conditional-access/location-condition#all-trusted-locations

upvoted 2 times

⊟ **doody** 2 years ago

answer is Y,N,N

All trusted locations

This option applies to:

'All locations that have been marked as trusted location

MFA Trusted IPs (if configured)'

https://learn.microsoft.com/en-us/azure/active-directory/conditional-access/location-condition#any-location

upvoted 1 times

⊟ **bac0n** 2 years, 1 month ago

TRIPLE NO. The IPs are Public. https://learn.microsoft.com/en-us/azure/active-directory/authentication/howto-mfa-mfasettings - The trusted IPs can include private IP ranges only when you use MFA Server. For cloud-based Azure AD Multi-Factor Authentication, you can use only public IP address ranges.

They don't mention anything about MFA server in this question.

upvoted 5 times

⊟ **bac0n** 2 years, 1 month ago

the IPs are private ***

upvoted 1 times

⊟ **Jawad1462** 2 years, 1 month ago

YNN first one is Y, because of this

You configure an Azure Multi-Factor Authentication (MFA) trusted IP address range of 192.168.1.0/27

upvoted 3 times

⊟ **zeeen** 2 years, 1 month ago

Private IP ranges can't be configured

https://learn.microsoft.com/en-us/azure/active-directory/conditional-access/location-condition#ip-address-ranges

upvoted 1 times

⊟ **zeeen** 2 years, 1 month ago

N,N,N

This question, all IPs are private, so

Doesn't it correspond to any conditional access?

upvoted 2 times

⊟ **Wedge34** 2 years, 2 months ago

Y,N,Y for me

upvoted 2 times

⊟ **mohamed_Saed** 2 years, 2 months ago

Yes , NO , No

1 IS TRUSTED

upvoted 1 times

⊟ **Tanasi** 1 year, 7 months ago

no, it is not

upvoted 1 times

⊟ **ariania** 2 years, 2 months ago

It dosent state if the Condition of the CA's are included or Excluded, should we just assume its excluded? Else they include the trusted locations to have MFA if accessing.

upvoted 1 times

⊟ **ariania** 2 years, 2 months ago

User 1 access through CA1 (forms) with Location:(included as nothing else is stated) trusted location = require MFA

YES

User 2 access through CA2 (planner) with Location:(included as nothing else is stated) NY = nothing

NO

User 3 access through CA1 (forms) with Location:(included as nothing else is stated) trusted location = require MFA, but NY is not a trusted location in the include, so no MFA will be promted.

NO

upvoted 3 times

⊟ **pipojede** 2 years, 2 months ago

Just note the order of IP Adress ranges in the first table it. The first line (trusted range) is number TWO.

.2 Trusted

.1 NOT TRUSTED

.3 NOT TRUSTED

upvoted 3 times

⊟ **yoton** 2 years, 3 months ago

I dont get why user3 won't be prompted for MFA. The policy applied to that user says "Grant Access: Require MFA." Can someone provide a little more explaining. To me it doesn't matter where they are logging in from, they will still be required to complete MFA.

upvoted 1 times

⊟ **yoton** 2 years, 3 months ago

Derp. Is it because they're logging in from an untrusted location so they will be barred access completely and thus not prompted for MFA?

upvoted 1 times

Question #71 *Topic 1*

Your network contains an on-premises Active Directory domain. The domain contains a domain controller named DC1.
You have a Microsoft 365 E5 subscription.
You install the Microsoft Defender for Identity sensor on DC1.
You need to configure enhanced threat detection in Defender for Identity. The solution must ensure that the following events are collected from DC1:
✑ 4726 - User Account Deleted
✑ 4728 - Member Added to Global Security Group
✑ 4776 - Domain Controller Attempted to Validate Credentials for an Account (NTLM)
What should you do on DC1?

A. Install the Azure Monitor agent.

B. Install System Monitor (SYSMON).

C. Configure the Windows Event Collector service.

D. Configure the Advanced Audit Policy Configuration policy.

Suggested Answer: *D*
Windows Event logs -
Defender for Identity detection relies on specific Windows Event logs that the sensor parses from your domain controllers. For the correct events to be audited and included in the Windows Event log, your domain controllers require accurate Advanced Audit Policy settings.
For the correct events to be audited and included in the Windows Event Log, your domain controllers require accurate Advanced Audit Policy settings. Incorrect
Advanced Audit Policy settings can lead to the required events not being recorded in the Event Log and result in incomplete Defender for Identity coverage.

Note: Relevant Windows Events -
For Active Directory Federation Services (AD FS) events
1202 - The Federation Service validated a new credential
1203 - The Federation Service failed to validate a new credential
4624 - An account was successfully logged on
4625 - An account failed to log on

For other events -
1644 - LDAP search
4662 - An operation was performed on an object
4726 - User Account Deleted
4728 - Member Added to Global Security Group
4729 - Member Removed from Global Security Group
4730 - Global Security Group Deleted
4732 - Member Added to Local Security Group
4733 - Member Removed from Local Security Group
4741 - Computer Account Added
4743 - Computer Account Deleted
4753 - Global Distribution Group Deleted
4756 - Member Added to Universal Security Group
4757 - Member Removed from Universal Security Group
4758 - Universal Security Group Deleted
4763 - Universal Distribution Group Deleted
4776 - Domain Controller Attempted to Validate Credentials for an Account (NTLM)
7045 - New Service Installed
8004 - NTLM Authentication
Reference:
https://docs.microsoft.com/en-us/defender-for-identity/prerequisites https://docs.microsoft.com/en-us/defender-for-identity/configure-windows-event-collection

Community vote distribution

D (100%)

pete26 Highly Voted 👍 2 years, 3 months ago

Selected Answer: D

D is correct.

https://docs.microsoft.com/en-us/defender-for-identity/configure-windows-event-collection

upvoted 7 times

pete26 Highly Voted 👍 2 years, 2 months ago

Valid on exam October 14, 2022

upvoted 7 times

RomanV Most Recent 🕓 1 year, 8 months ago

The correct answer is D: Configure the Advanced Audit Policy Configuration policy. Every system admin should know this.

upvoted 1 times

Question #72 Topic 1

You have a Microsoft 365 E5 subscription that uses Azure Active Directory (Azure AD) Privileged Identity Management (PIM).
A user named User1 is eligible for the User Account Administrator role.
You need User1 to request to activate the User Account Administrator role.
From where should User1 request to activate the role?

A. the My Access portal

B. the Microsoft 365 Defender portal

C. the Microsoft 365 admin center

D. the Azure Active Directory admin center

Suggested Answer: *A*
Activate a role -
When you need to assume an Azure AD role, you can request activation by opening My roles in Privileged Identity Management.
1. Sign in to the Azure portal.
2. Open Azure AD Privileged Identity Management
3. Select My roles, and then select Azure AD roles to see a list of your eligible Azure AD roles.
4. My roles page showing roles you can activate
5. In the Azure AD roles list, find the role you want to activate.
6. Azure AD roles - My eligible roles list
7. Select Activate to open the Activate pane.
Reference:
https://docs.microsoft.com/en-us/azure/active-directory/privileged-identity-management/pim-how-to-activate-role

Community vote distribution
D (90%) 10%

B0bacer Highly Voted 2 years, 3 months ago
D.the Azure Active Directory admin center -> Azure portal ->Privileged Identity Management

https://learn.microsoft.com/en-us/azure/active-directory/privileged-identity-management/pim-how-to-activate-role
upvoted 15 times

billo79152718 Highly Voted 2 years, 3 months ago
Correct is D
upvoted 7 times

Patesso Most Recent 1 year, 7 months ago
Etait a l'examen le 18/05/2023
upvoted 2 times

pid 1 year, 7 months ago
Selected Answer: A
If the user1 is just a standard user how would the user login to Azure Admin center. My Apps portal gives you list of eligible roles.
upvoted 2 times

AnonymousJhb 1 year, 8 months ago
Selected Answer: D
Azure Active Directory admin center -> Azure portal ->Privileged Identity Management
upvoted 1 times

RomanV 1 year, 8 months ago
The correct answer is D. The user should request to activate the User Account Administrator role from the Azure Active Directory admin center.
There is no longer a 'My Access portal'.
upvoted 2 times

yaza85 1 year, 11 months ago
Selected Answer: D

Please Change the selection. The description is already correct

upvoted 2 times

⊟ **formazionehs** 2 years ago

Selected Answer: D

Answer is D

upvoted 2 times

⊟ **examdog** 2 years ago

Selected Answer: D

My Access portal is for "Identity Governance". This question is about AAD PIM.

upvoted 2 times

⊟ **skycrap** 2 years ago

Selected Answer: D

answer is d for sure

upvoted 2 times

⊟ **doody** 2 years ago

Answer : D forsure

upvoted 2 times

⊟ **bighiller** 2 years ago

The URL for the My Access Portal: https://myaccess.microsoft.com/

upvoted 2 times

⊟ **Wedge34** 2 years, 2 months ago

Selected Answer: D

Answer is D

upvoted 2 times

⊟ **EzeQ** 2 years, 3 months ago

Selected Answer: D

Never heard of any "My Access Portal"

upvoted 2 times

⊟ **ewu** 2 years, 3 months ago

Selected Answer: D

Answer is D

upvoted 2 times

⊟ **JimboJones99** 2 years, 3 months ago

Selected Answer: D

Answer is D

upvoted 4 times

⊟ **MaartenC** 2 years, 3 months ago

I think this question is messed up and mixes "identity governance access packages" with eligible/assigned PIM AD roles. the "My Access Portal" is used for requesting access via an Access Package that contains some from of access to resources.

upvoted 4 times

Question #73 *Topic 1*

You have a Microsoft 365 E5 subscription.
You need to enable support for sensitivity labels in Microsoft SharePoint Online.
What should you use?

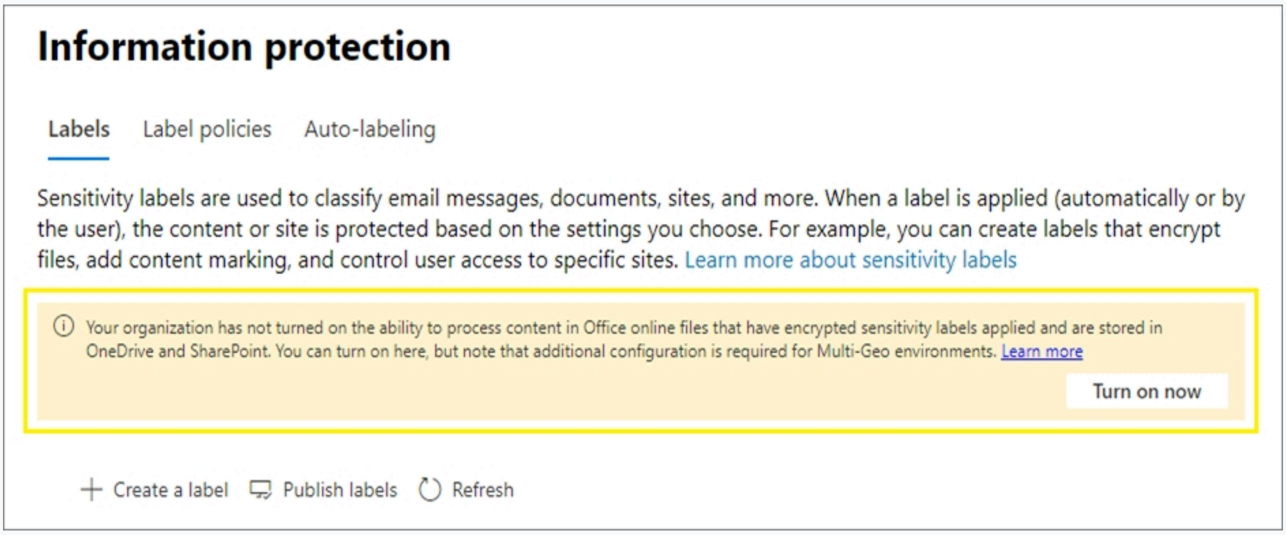
A. the SharePoint admin center

B. the Microsoft 365 admin center

C. the Microsoft 365 Compliance center

D. the Azure Active Directory admin center

Suggested Answer: *C*
Use the Microsoft Purview compliance portal to enable support for sensitivity labels
This option is the easiest way to enable sensitivity labels for SharePoint and OneDrive, but you must sign in as a global administrator for your tenant.
1. Sign in to the Microsoft Purview compliance portal as a global administrator, and navigate to Solutions > Information protection > Labels
2. If you see a message to turn on the ability to process content in Office online files, select Turn on now:



Information protection

Sensitivity labels are used to classify email messages, documents, sites, and more. When a label is applied (automatically or by the user), the content or site is protected based on the settings you choose. For example, you can create labels that encrypt files, add content marking, and control user access to specific sites. Learn more about sensitivity labels

ⓘ Your organization has not turned on the ability to process content in Office online files that have encrypted sensitivity labels applied and are stored in OneDrive and SharePoint. You can turn on here, but note that additional configuration is required for Multi-Geo environments. Learn more

Reference:
https://docs.microsoft.com/en-us/microsoft-365/compliance/sensitivity-labels-sharepoint-onedrive-files

Community vote distribution
C (100%)

billo79152718 Highly Voted 2 years, 3 months ago
correct
upvoted 6 times

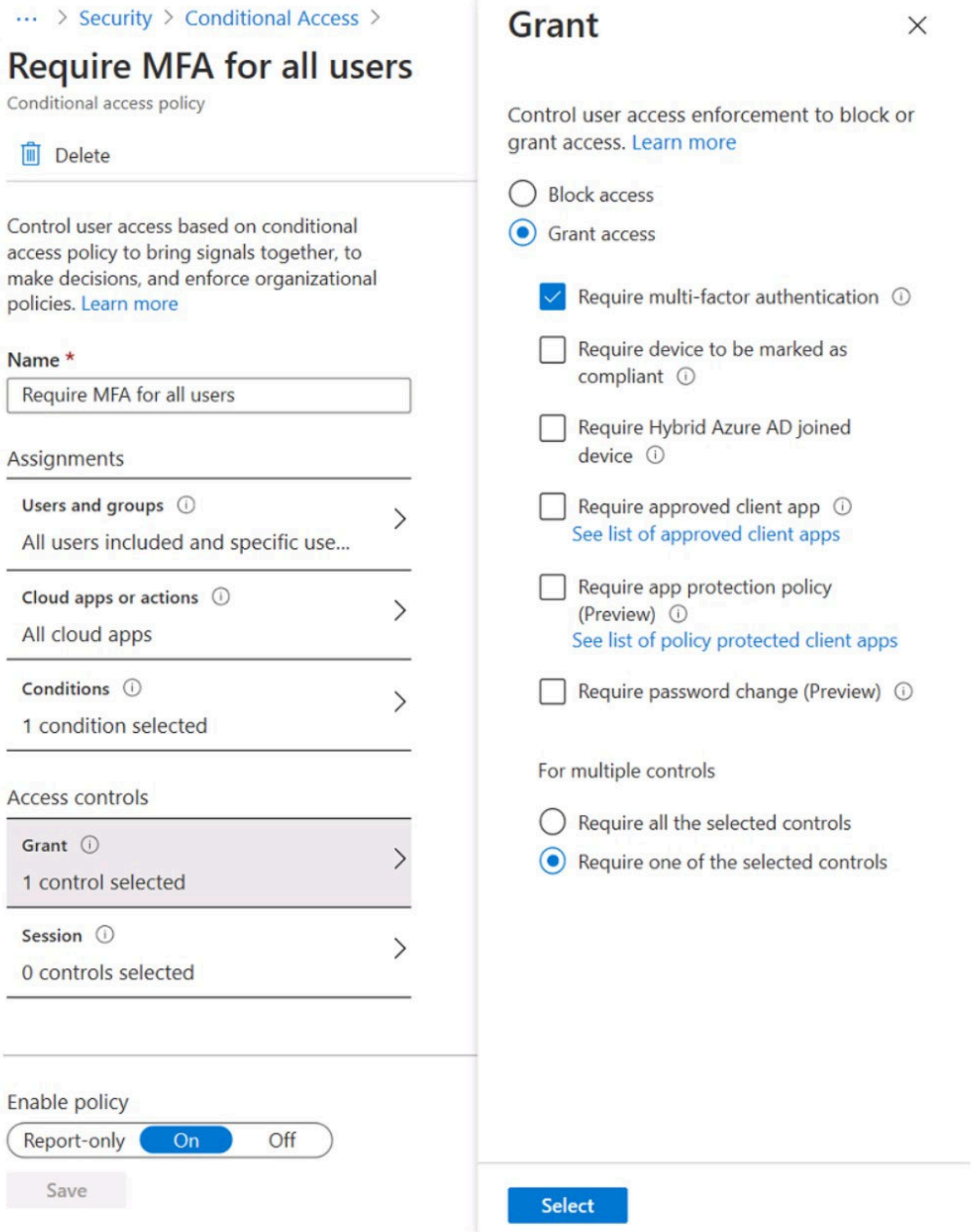
jspecht Most Recent 1 year, 11 months ago
Selected Answer: C
It is now called Microsoft Purview
upvoted 4 times

Question #74 *Topic 1*

HOTSPOT -

You have a Microsoft 365 tenant.

A conditional access policy is configured for the tenant as shown in the Policy exhibit. (Click the Policy tab.)



... > Security > Conditional Access >

Require MFA for all users

Conditional access policy

Delete

Control user access based on conditional access policy to bring signals together, to make decisions, and enforce organizational policies. Learn more

Name *

Require MFA for all users

Assignments

Users and groups: All users included and specific use...

Cloud apps or actions: All cloud apps

Conditions: 1 condition selected

Access controls

Grant: 1 control selected

Session: 0 controls selected

Enable policy: Report-only [✓ On] Off

Save

Grant

Control user access enforcement to block or grant access. Learn more

○ Block access

● Grant access

☑ Require multi-factor authentication

□ Require device to be marked as compliant

□ Require Hybrid Azure AD joined device

□ Require approved client app
See list of approved client apps

□ Require app protection policy (Preview)
See list of policy protected client apps

□ Require password change (Preview)

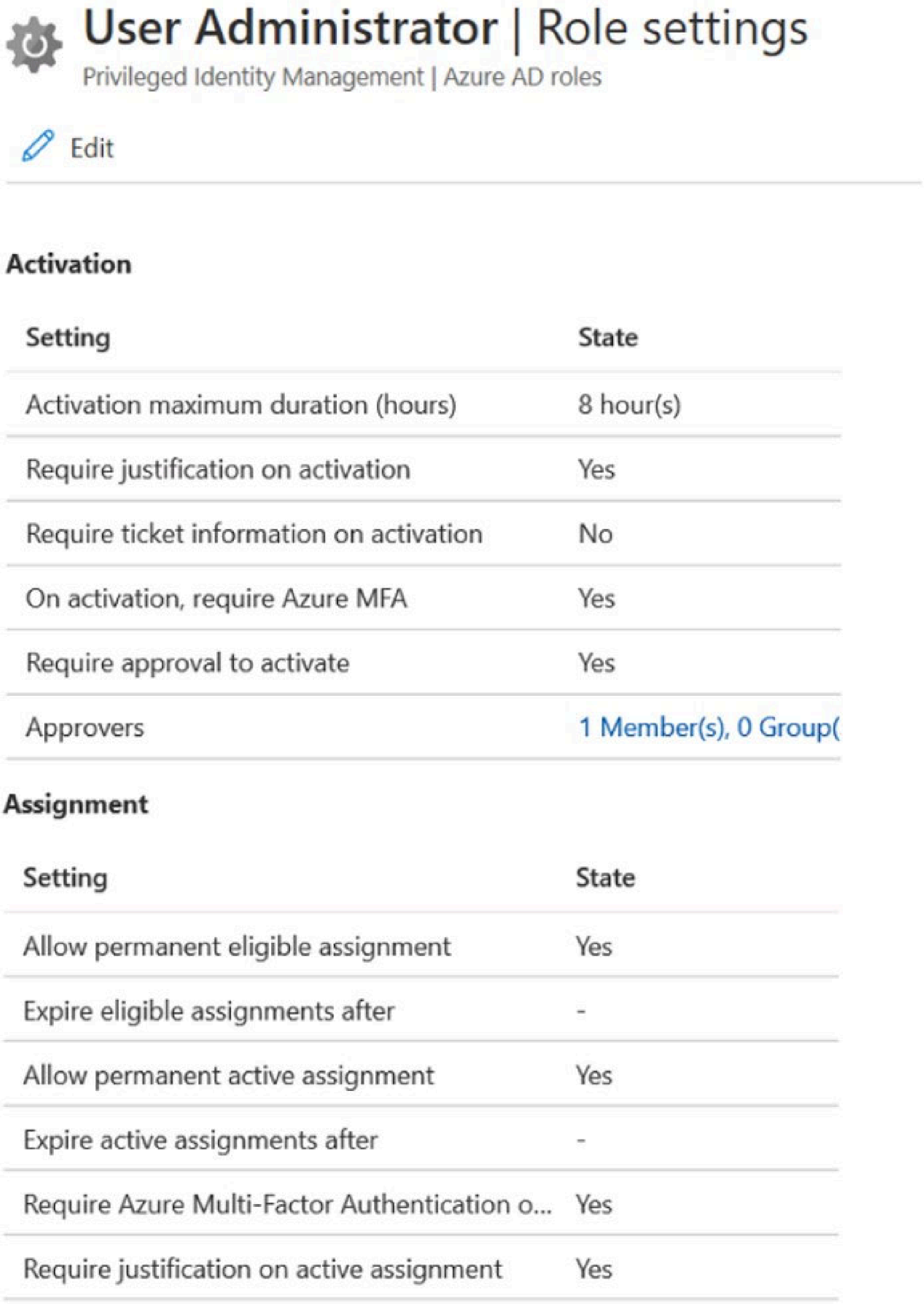
For multiple controls

○ Require all the selected controls

● Require one of the selected controls

Select

The User Administrator role is configured as shown in the Role setting exhibit. (Click the Role setting tab.)



User Administrator | Role settings

Privileged Identity Management | Azure AD roles

Edit

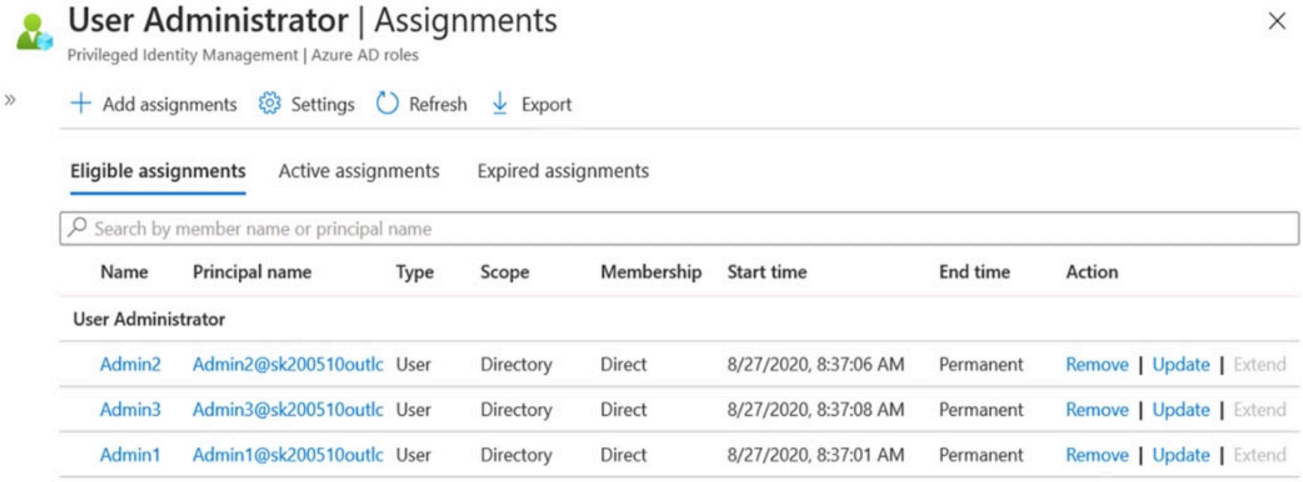
Activation

Setting	State
Activation maximum duration (hours)	8 hour(s)
Require justification on activation	Yes
Require ticket information on activation	No
On activation, require Azure MFA	Yes
Require approval to activate	Yes
Approvers	1 Member(s), 0 Group(

Assignment

Setting	State
Allow permanent eligible assignment	Yes
Expire eligible assignments after	-
Allow permanent active assignment	Yes
Expire active assignments after	-
Require Azure Multi-Factor Authentication o...	Yes
Require justification on active assignment	Yes

The User Administrator role has the assignments shown in the Assignments exhibit. (Click the Assignments tab.)



User Administrator | Assignments

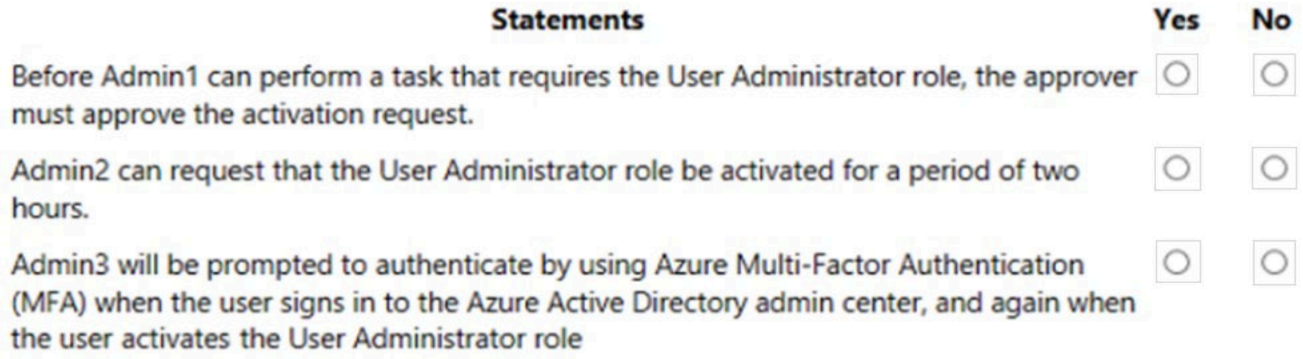
Privileged Identity Management | Azure AD roles

Name	Principal name	Type	Scope	Membership	Start time	End time	Action
User Administrator							
Admin2	Admin2@sk200510outlc	User	Directory	Direct	8/27/2020, 8:37:06 AM	Permanent	Remove | Update | Extend
Admin3	Admin3@sk200510outlc	User	Directory	Direct	8/27/2020, 8:37:08 AM	Permanent	Remove | Update | Extend
Admin1	Admin1@sk200510outlc	User	Directory	Direct	8/27/2020, 8:37:01 AM	Permanent	Remove | Update | Extend

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

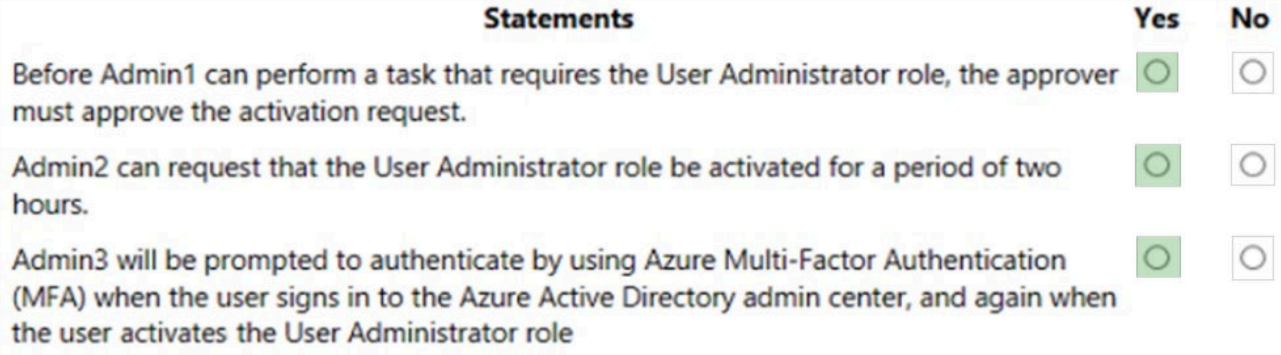
NOTE: Each correct selection is worth one point.

Hot Area:



Statements	Yes	No
Before Admin1 can perform a task that requires the User Administrator role, the approver must approve the activation request.	○	○
Admin2 can request that the User Administrator role be activated for a period of two hours.	○	○
Admin3 will be prompted to authenticate by using Azure Multi-Factor Authentication (MFA) when the user signs in to the Azure Active Directory admin center, and again when the user activates the User Administrator role	○	○

Suggested Answer:



Statements	Yes	No
Before Admin1 can perform a task that requires the User Administrator role, the approver must approve the activation request.	[✓ ○]	○
Admin2 can request that the User Administrator role be activated for a period of two hours.	[✓ ○]	○
Admin3 will be prompted to authenticate by using Azure Multi-Factor Authentication (MFA) when the user signs in to the Azure Active Directory admin center, and again when the user activates the User Administrator role	[✓ ○]	○

Box 1: Yes -

In this scenario the User Administrator role is require justification on active assignment.

Require justification -

You can require that users enter a business justification when they activate. To require justification, check the Require justification on active assignment box or the

Require justification on activation box.

Box 2: Yes -

Activation maximum duration is 8 hours.

Box 3: Yes -

Require multifactor authentication

Privileged Identity Management provides enforcement of Azure AD Multi-Factor Authentication on activation and on active assignment.

Reference:

https://docs.microsoft.com/en-us/azure/active-directory/privileged-identity-management/pim-how-to-change-default-settings

ariania Highly Voted 2 years, 2 months ago

I notice one small diffrence this time around, it should be

Y

Y

Y

As i first stated, this due to the "assignment" field, second from bottom: "require MFA on Activation of the role".

I cant edit or remove previously reply. sorry!

upvoted 7 times

ColmTheMeanie Most Recent 1 year, 10 months ago

User may not be prompted for multi-factor authentication if they authenticated with strong credential or provided multi-factor authentication earlier in this session.

upvoted 3 times

ChachaChatra 1 year, 11 months ago

Valid on28/01/23

upvoted 4 times

⊟ **IT_Nerd31** 1 year, 12 months ago

The answer is YYN, Just tested in my environment. It is NOT YYY.

upvoted 4 times

⊟ **ariania** 2 years, 3 months ago

I would belive

Y

Y

Y

But when i tested it in my lab, i was only prompted for MFA once in this chain - the only diffrence was i did not have an "All User MFA CA" active, only MFA via M365 admin center on the specific user. Can anyone confirm?

upvoted 1 times

⊟ **ariania** 2 years, 2 months ago

Ive done extensive testing, in lab it comes out as:

Y

Y

N - Its already satisfied from logging in to Azure Portal (all users - all app CA)

upvoted 12 times

⊟ **ariania** 2 years, 2 months ago

This is correct, after talking to Microsoft representative:

So you will not get promoted twice as you just got promted when logging in to Azure Portal (all users/all apps).

"you only get prompted per session and not activation."

upvoted 3 times

⊟ **billo79152718** 2 years, 3 months ago

No - Role is already activated.

Yes - Correct!

No - Role is already activated

upvoted 4 times

⊟ **xyz213** 2 years, 3 months ago

Careful. User Assignments is under "Eligible Assignments" so these Users are permantly allowed to activate the role. Role is not permanently active for them (Would be under "Active Assignments")

So Y/Y/Y is correct.

upvoted 14 times

⊟ **Daniel830** 2 years, 3 months ago

That's right. Thank you for clarifying it, I had the same doubt.c

upvoted 2 times

⊟ **yoton** 1 year, 12 months ago

really bro

upvoted 1 times

⊟ **Snoopy70** 2 years, 1 month ago

I agree here. All these roles are activated. The view is not from the end user with the admin role.

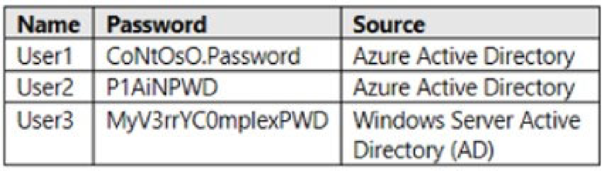
upvoted 1 times

Question #75 Topic 1

HOTSPOT -

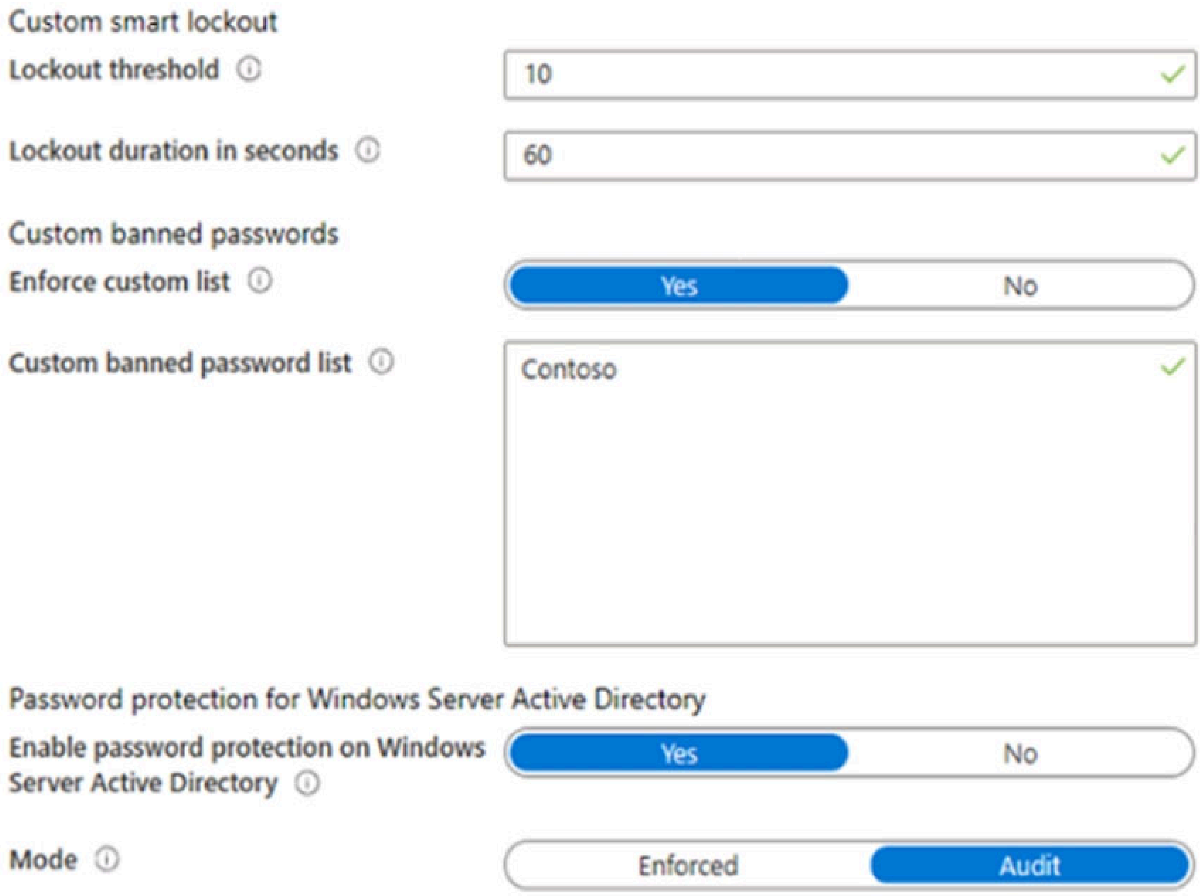
Your company has a Microsoft 365 E5 subscription and a hybrid Azure Active Directory named contoso.com.

Contoso.com includes the following users:



Name	Password	Source
User1	CoNtOsO.Password	Azure Active Directory
User2	P1AiNPWD	Azure Active Directory
User3	MyV3rrYC0mplexPWD	Windows Server Active Directory (AD)

You configure Password protection for Contoso.com as shown in the following exhibit.



Custom smart lockout

Lockout threshold: 10

Lockout duration in seconds: 60

Custom banned passwords

Enforce custom list: [✓ Yes] No

Custom banned password list: Contoso

Password protection for Windows Server Active Directory

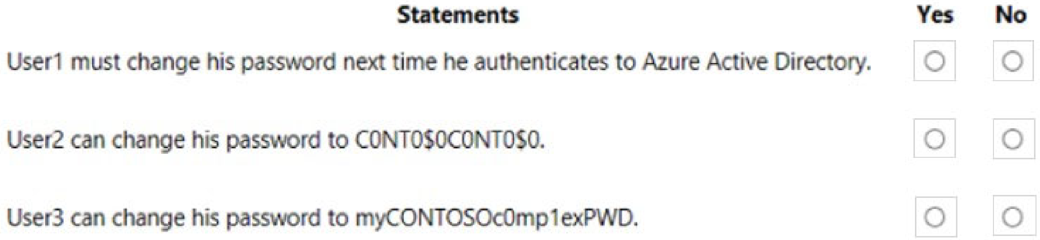
Enable password protection on Windows Server Active Directory: [✓ Yes] No

Mode: Enforced [✓ Audit]

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

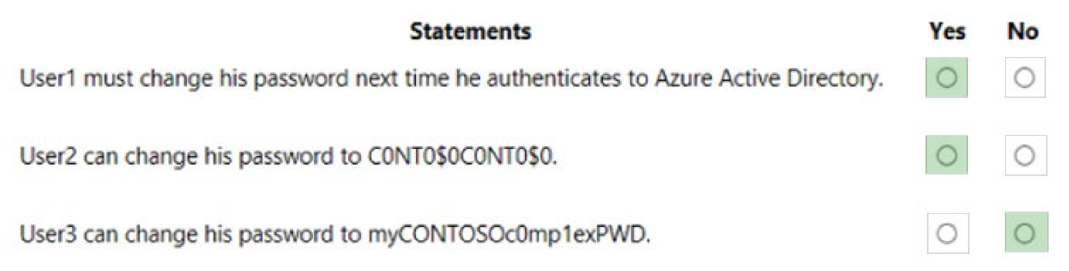
NOTE: Each correct selection is worth one point.

Hot Area:



Statements	Yes	No
User1 must change his password next time he authenticates to Azure Active Directory.	○	○
User2 can change his password to C0NT0$0C0NT0$0.	○	○
User3 can change his password to myCONTOSOc0mp1exPWD.	○	○

Suggested Answer:



Statements	Yes	No
User1 must change his password next time he authenticates to Azure Active Directory.	●	○
User2 can change his password to C0NT0$0C0NT0$0.	●	○
User3 can change his password to myCONTOSOc0mp1exPWD.	○	●

Box 1: Yes -

Note: The following considerations and limitations apply to the custom banned password list:

The custom banned password list can contain up to 1000 terms.
The custom banned password list is case-insensitive.
The custom banned password list considers common character substitution, such as "o" and "0", or "a" and "@".
The minimum string length is four characters, and the maximum is 16 characters.

Box 2: Yes -
The $ character is OK when it used instead of an S.

Box 3: No -
Reference:
https://docs.microsoft.com/en-us/azure/active-directory/authentication/tutorial-configure-custom-password-protection

dakasa Highly Voted 👍 2 years, 4 months ago

Here, the answer will be N, Y, Y
Audit mode is the default initial setting, where passwords can continue to be set. Passwords that would be blocked are recorded in the event log. After you deploy the proxy servers and DC agents in audit mode, monitor the impact that the password policy will have on users when the policy is enforced.
https://docs.microsoft.com/en-us/azure/active-directory/authentication/howto-password-ban-bad-on-premises-deploy

upvoted 42 times

MaartenC 2 years, 3 months ago

there's two enforce statements in this config: one for custom banned passwords and one for Windows Server Active Directory. I think it's Y,Y,N since the mode on Windows Server AD is set to audit.

upvoted 1 times

MaartenC 2 years, 3 months ago

If you disable "enable password protection on Windows Server AD", the "mode" option is greyed out.. To me that linked the "mode" option specifically to windows server ad

upvoted 2 times

EzeQ 2 years, 3 months ago

Voted for Best reply

upvoted 2 times

Just2a 2 years, 2 months ago

Agreed to N,Y,Y
First NO: Password protection only applies when the user changes his password, so in this case the user will not be prompted to change the password.

upvoted 1 times

msysadmin 1 year, 10 months ago

Agree, N,Y,Y. It is audit mode not yet enforced.

upvoted 2 times

Broesweelies Highly Voted 👍 2 years, 3 months ago

Pretty sure it is N N Y
Let me explain:
First NO: Password protection only applies when the user changes his password, so in this case the user will not be prompted to change the password.
Second NO: The banned word can not be used and Password protection will change the dollar symbol to an S. For people saying the policy is in audit mode: Audit mode only applies when you enable on prem password protection. When you click 'no' for on prem password, this audit mode will be greyed out. For Azure AD this policy will be applied.
Third YES: Password protection for on prem is in audit mode, so password can be changed to whatever.

upvoted 33 times

EM1234 1 year, 10 months ago

Do you have any documentation for you conclusion on user 2?
I added a custom banned word in audit mode to my lab tenant which is AAD only and it allowed me to reset a fake user with that word.

you say: Audit mode only applies when you enable on prem password protection.

audit mode is the default for this policy and I add words and save it is not enforced. Please add a citation for your analysis.

upvoted 2 times

EM1234 1 year, 10 months ago

I tested it again with an 8 letter banned custom word and only added !1 at the end which should only be three points if being evaluated. The password saved successfully.

upvoted 1 times

RomanV Most Recent 1 year, 6 months ago

Why is Azure AD still rejecting weak passwords even though I've configured the policy to be in Audit mode?

Audit mode is only supported in the on-premises Active Directory environment. Azure AD is implicitly always in "enforce" mode when it evaluates passwords.

Source: https://learn.microsoft.com/en-us/azure/active-directory/authentication/howto-password-ban-bad-on-premises-faq

upvoted 1 times

TrivediVivek78 1 year, 9 months ago

Correct Answer should be

1. No : as given policy applies when changing password not authenticating
2. No : tested in Lab environment and it fails to update the given password with this message ("Unfortunately, your password contains a word, phrase, or pattern that is banned by your organization. Please try again with a different password")
3. Yes : as the on-prem servers are not enforced

upvoted 1 times

lcaothu92 1 year, 9 months ago

The correct answer here should be N, Y, Y

The key point here Audit mode

"Audit mode

Audit mode is intended as a way to run the software in a "what if" mode. Each Azure AD Password Protection DC agent service evaluates an incoming password according to the currently active policy.

If the current policy is configured to be in audit mode, "bad" passwords result in event log messages but are processed and updated. This behavior is the only difference between audit and enforce mode. All other operations run the same."

- First NO: Password protection only applies when the user changes his password, so in this case the user will not be prompted to change the password.

upvoted 1 times

JoeP1 1 year, 10 months ago

Audit mode only applies to On Premises AD.

The documentation is here (under the question "Why is Azure AD still rejecting weak passwords even though I've configured the policy to be in Audit mode?"):

https://learn.microsoft.com/en-us/azure/active-directory/authentication/howto-password-ban-bad-on-premises-faq

upvoted 2 times

yeti2390 1 year, 10 months ago

Shouldn't it be N, Y, Y? It is set to audit mode, i.e it's not actually enabled so the settings aren't enforced?

upvoted 1 times

rick001 1 year, 11 months ago

its quite simple..

1 - only happens when he actually changes it.. not when authenticates.

2 - user2 is azure AD so policy is in effect but he changes it to C0NT0$0 - not contoso no effect there. So he can change it.

3 - User is on prem and the policy is in audit so he can do whatever.

TL;DR

1 - N

2 - Y

3 - Y

upvoted 1 times

zerrowall 2 years ago

N,N,Y

Regarding User2, it's not possible to use the suggested password, because the following:

1. The sign "$" will be substituted to "s" during the normalization step of password evaluation.

See here https://learn.microsoft.com/en-us/azure/active-directory/authentication/concept-password-ban-bad#step-1-normalization

2. In the normalized password "contosocontoso" there are two banned substrings "contoso", thus on the Score Calculation step the score will be 2. But for accepting a new password we need a score 5. So, User2 will not be able to change the password to suggested one. See here about scoring:

https://learn.microsoft.com/en-us/azure/active-directory/authentication/concept-password-ban-bad#score-calculation

upvoted 7 times

skycrap 2 years ago

I go for NNY. See explanation of Broesweelies

upvoted 3 times

Wedge34 2 years, 2 months ago

Answer is N, N, Y

upvoted 7 times

Acbrownit 2 years, 2 months ago

N, y, y due to audit mode. Regarding the statement in the posted answer on limitations, there is no limit to password length in custom banned password list, so answer 3 is fine regardless of whether audit mode is enabled or not.

upvoted 2 times

MrDribble 2 years, 3 months ago

I believe it's N/Y/Y

The key thing is (Audit) which will only monitor the passwords and thus will not use the banned password list.

While there is password protection on Windows Server Active Directory - it's will require an agent to run on the server, which has its own requirements.

You can't assume that this has been completed.

upvoted 7 times

Tanasi 1 year, 10 months ago

literally the only person that noticed that the policy is on audit mode only

upvoted 1 times

xyz213 2 years, 3 months ago

N/Y/Y

This is a helpful link. The banned list doesn't just ban passwords 1:1.

https://docs.microsoft.com/en-us/azure/active-directory/authentication/concept-password-ban-bad#how-are-passwords-evaluated

upvoted 3 times

xyz213 2 years, 3 months ago

Actually that makes it N/N/Y.

C0NT0$0C0NT0$0 would get normalized to contosocontoso and only get 2 points out of 5.

upvoted 3 times

xyz213 2 years, 3 months ago

Unfortunatly I can't edit my comments..

After going over it again i think it is Y/N/Y

But that assumes that "Password" is in the global banned password list.

CoNtOsO.Password would be normalized to contoso.password -> 3/5 required points.

upvoted 2 times

ashkins 2 years, 3 months ago

You are in audit mode not enforced mode- https://learn.microsoft.com/en-us/azure/active-directory/authentication/howto-password-ban-bad-on-premises-operations#modes-of-operation

upvoted 1 times

Trainee2244 2 years, 3 months ago

N,Y,Y is right. why should User1 change the Password next time he signs in ? is the Password in the List ? No it isnt and the other users CAN change the desired Password if they want to.

upvoted 4 times

Question #76 *Topic 1*

You have a Microsoft 365 E5 subscription that contains a user named User1.
You need to ensure that User1 can use the Microsoft 365 compliance center to search audit logs and identify which users were added to Microsoft 365 role groups. The solution must use the principle of least privilege.
To which role group should you add User1?

A. View-Only Organization Management

B. Security Reader

C. Organization Management

D. Compliance Management

Suggested Answer: *A*
View-Only Organization Management - Members can view the properties of any object in the Exchange Online organization.
Note: You have to be assigned the View-Only Audit Logs or Audit Logs role in Exchange Online to search the audit log. By default, these roles are assigned to the
Compliance Management and Organization Management role groups on the Permissions page in the Exchange admin center.
To give a user the ability to search the audit log with the minimum level of privileges, you can create a custom role group in Exchange Online, add the View-Only
Audit Logs or Audit Logs role, and then add the user as a member of the new role group.
Incorrect:
Not C: Organization Management - Members have administrative access to the entire Exchange Online organization and can perform almost any task in
Exchange Online.
Not D: Compliance Management - Members can configure and manage compliance settings within Exchange in accordance with their policies.
Reference:
https://docs.microsoft.com/en-us/microsoft-365/compliance/search-the-audit-log-in-security-and-compliance

Community vote distribution

D (73%) A (20%) 7%

Tanasi Highly Voted 1 year, 10 months ago

I hate this type of questions. Do I really have to remember them?!

You will probably never use it anyway.

upvoted 9 times

nsss 1 year, 8 months ago

Agreed, totally pointless to memorize this bs.

upvoted 3 times

ysm Most Recent 1 year, 8 months ago

Selected Answer: D

Compliance Management

You have to be assigned the View-Only Audit Logs or Audit Logs role in Exchange Online to search the audit log. By default, these roles are assigned to the Compliance Management and Organization Management role groups on the Permissions page in the Exchange admin center. Global administrators in Office 365 and Microsoft 365 are automatically added as members of the Organization Management role group in Exchange Online. To give a user the ability to search the audit log with the minimum level of privileges, you can create a custom role group in Exchange Online, add the View-Only Audit Logs or Audit Logs role, and then add the user as a member of the new role group. For more information, see Manage role groups in Exchange Online.

upvoted 1 times

Stig_88 1 year, 8 months ago

Selected Answer: D

View-Only Org Management got 2 permissions:
View-Only Config

View-Only Recipients

Security Reader got 1 permission

Answer is D: Got 11 permissions including what is required on the requirement.

upvoted 1 times

smiff 1 year, 8 months ago

Selected Answer: D

https://learn.microsoft.com/en-us/exchange/permissions-exo/permissions-exo

upvoted 1 times

RomanV 1 year, 8 months ago

To ensure that User1 can use the Microsoft 365 compliance center to search audit logs and identify which users were added to Microsoft 365 role groups, while adhering to the principle of least privilege, you should add User1 to the Security Reader role group.

Correct answer should be B. Security Reader

upvoted 2 times

Aleyah 1 year, 9 months ago

Selected Answer: D

D is correct

upvoted 1 times

abrub 1 year, 9 months ago

Selected Answer: B

If the only requirement is for User1 to identify which users were added to Microsoft 365 role groups, then the "View-Only Organization Management" role group could be considered as a valid option. This role group provides read-only access to most features in the Microsoft 365 admin center, including the ability to view role group membership.

However, if the requirement is specifically to use the Microsoft 365 Compliance Center to search audit logs and identify which users were added to Microsoft 365 role groups, then the "Security Reader" role group would be a more appropriate choice, as it provides access to the Compliance Center and associated workloads, including the ability to search audit logs.

upvoted 1 times

chickenroaster 1 year, 10 months ago

Answer is correct. https://learn.microsoft.com/en-us/exchange/view-only-organization-management-exchange-2013-help

upvoted 2 times

chickenroaster 1 year, 10 months ago

Correction: View-Only Organization Management role has no View-Only Audit Logs permissions. So answer is wrong.

upvoted 1 times

kkkk369 1 year, 10 months ago

The "Security Reader" role provides the least privilege necessary to search audit logs and view information about role groups, which meets the requirement of using the principle of least privilege. The "View-Only Organization Management" role provides similar permissions, but also allows for viewing other details such as service health, message trace, and reports.

Adding User1 to the "Organization Management" role would give them more permissions than necessary and would not follow the principle of least privilege. The "Compliance Management" role is focused on compliance-related tasks such as creating retention policies and doesn't provide the necessary permissions to search audit logs.

upvoted 2 times

shouro88 1 year, 11 months ago

Selected Answer: D

Compliance Management.
Assigned Roles
Audit Logs
Compliance Admin
Data Loss Prevention
Information Rights Management
Journaling
Message Tracking

Retention Management
Transport Rules
View-Only Audit Logs
View-Only Configuration
View-Only Recipients

View-Only Organization Management
Assigned Roles
View-Only Configuration
View-Only Recipients

correct Answer- D
upvoted 2 times

⊟ **shouro88** 1 year, 11 months ago

My bad, please ignore

Correct answer is A following least priviledged access
upvoted 1 times

⊟ **msysadmin** 1 year, 10 months ago

Actually your first decision is correct. Correct answer is D.

View-Only Organization Management: Members can view the properties of any object in the Exchange Online organization. #View-Only Configuration, View-Only Recipients

Compliance Management is correct
Organization Management is incorrect - Have a many of admin privileges
upvoted 1 times

⊟ **brotown22** 1 year, 12 months ago

Selected Answer: A

Principle of least privilege means View Only Org Mgmt with View-Only Audit Logs added achieves 'read-only' requirement. All other options have more permissions by default than required. Given answer is correct.
upvoted 3 times

⊟ **mcclane654** 2 years ago

Selected Answer: D

https://admin.exchange.microsoft.com/#/adminRoles click the roles and check permissions.
compliance management and org management have access. but compliance management is least priveliged.
not to be confused with ordinary audit logs those require reports reader.
upvoted 2 times

⊟ **EM1234** 1 year, 10 months ago

The answer is d. Mcclane654 tells you all how to see it. If you go into exchange admin and look at the roles, once you select it you can click on permissions tab.
view-only org management does not have the audit logs permission ticked so it does not have the requirements from the question. Please go and look for yourself, you will see.
upvoted 1 times

⊟ **Zimb** 2 years ago

https://learn.microsoft.com/en-us/exchange/view-only-audit-logs-role-exchange-2013-help
given answer is correct.
https://learn.microsoft.com/en-us/exchange/security-and-compliance/exchange-auditing-reports/search-role-group-changes
You need to be assigned permissions before you can perform this procedure or procedures. To see what permissions you need, see the "View-only administrator audit logging
upvoted 2 times

⊟ **Snoopy70** 2 years, 1 month ago

The answer is correct. I checked in my lab and the permissions for the view only organisation management have the least permissions in comparison with the compliance management.
upvoted 2 times

⊟ **Lomak** 2 years, 2 months ago

Selected Answer: D

https://learn.microsoft.com/en-us/exchange/permissions-exo/permissions-exo#role-based-permissions

upvoted 1 times

⊟ **pete26** 2 years, 2 months ago

Valid on exam October 14, 2022

upvoted 4 times

⊟ **wuzime** 2 years, 3 months ago

I think the given answer is correct.
Refer to: https://learn.microsoft.com/en-us/exchange/view-only-organization-management-exchange-2013-help

upvoted 2 times

⊟ **yoton** 2 years, 3 months ago

REEEE damn you Exchange Server 2013

upvoted 1 times

⊟ **RJ06** 2 years, 2 months ago

View-Only Organization Management only gives access to following sub-roles.
View-Only Configuration
View-Only Recipients

For audit logs, you require "view-only audit logs" which will be accomplished by going further to "Compliance Management" role. Security Reader wont fulfill all requirements and Organisation Management will be an overkill.

upvoted 3 times

Question #77 *Topic 1*

HOTSPOT
-

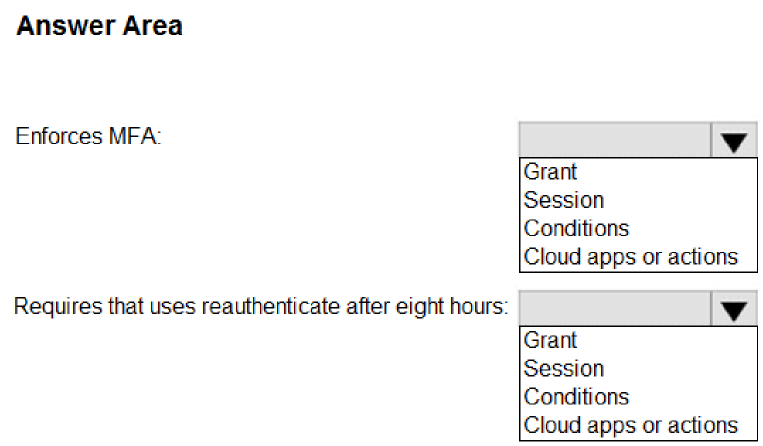
You have a Microsoft 365 E5 subscription.

You need to create a conditional access policy named Policy1 that meets the following requirements:

• Enforces multi-factor authentication (MFA)
• Requires that users reauthenticate after eight hours

Which settings should you configure in Policy1 for each requirement? To answer, select the appropriate options in the answer area.

NOTE: Each correct selection is worth one point.

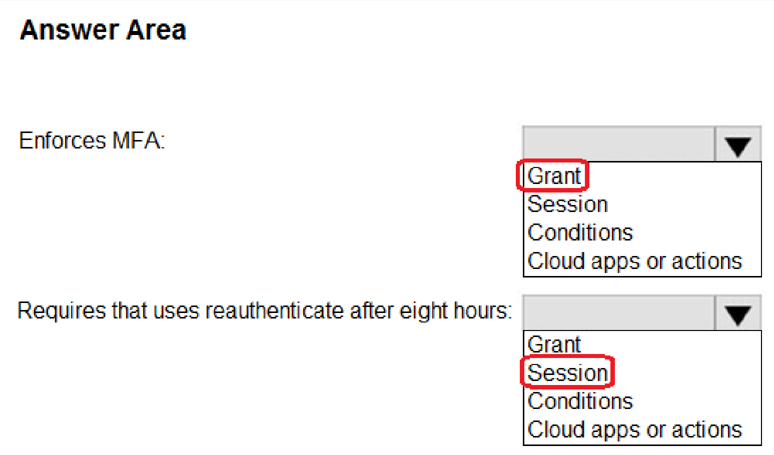


Answer Area

Enforces MFA:
- Grant
- Session
- Conditions
- Cloud apps or actions

Requires that uses reauthenticate after eight hours:
- Grant
- Session
- Conditions
- Cloud apps or actions

Suggested Answer:



Answer Area

Enforces MFA:
- [✓ Grant]
- Session
- Conditions
- Cloud apps or actions

Requires that uses reauthenticate after eight hours:
- Grant
- [✓ Session]
- Conditions
- Cloud apps or actions

EetswahBah 1 year, 7 months ago

1. Grant
2. Session

upvoted 1 times

T3st3r 1 year, 8 months ago

1. Grant
2. Session

upvoted 2 times

AnonymousJhb 1 year, 8 months ago

Grant as per https://learn.microsoft.com/en-us/azure/active-directory/conditional-access/howto-conditional-access-policy-all-users-mfa#create-a-conditional-access-policy

upvoted 1 times

⊟ **RomanV** 1 year, 8 months ago

1. Conditions
2. Session

Don't believe me? Try it out in the Azure admin portal.

upvoted 1 times

⊟ **RomanV** 1 year, 8 months ago

To prove my point for the disbelievers out here:

For answer 2 Session:

Sign-in frequency control

1. Browse to Azure Active Directory > Security > Conditional Access.
2. Select New policy.
3. Give your policy a name. We recommend that organizations create a meaningful standard for the names of their policies.
4. Choose all required conditions for customer’s environment, including the target cloud apps.
5. Under Access controls > Session.

- Select Sign-in frequency.
- Choose Periodic reauthentication and enter a value of hours or days or select Every time.

6.Save your policy.

upvoted 1 times

⊟ **MoritzW** 1 year, 10 months ago

I think the first answer should be Conditions

upvoted 2 times

⊟ **kmk_01** 1 year, 9 months ago

From https://learn.microsoft.com/en-us/azure/active-directory/conditional-access/howto-conditional-access-policy-all-users-mfa
Under Access controls > Grant, select Grant access, Require multifactor authentication, and select Select.

upvoted 1 times

⊟ **RomanV** 1 year, 8 months ago

Incorrect. "Grant" is for RISKY USERS as stated by Microsoft under "Sign-in frequency control every time risky user"

Source: https://learn.microsoft.com/en-us/azure/active-directory/conditional-access/howto-conditional-access-session-lifetime

upvoted 1 times

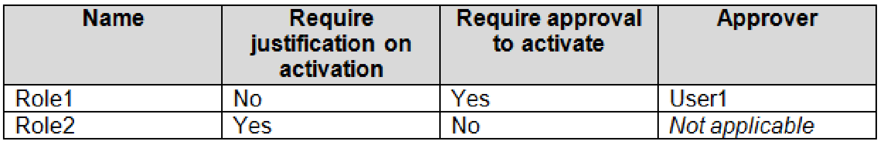
Question #78 *Topic 1*

HOTSPOT

-

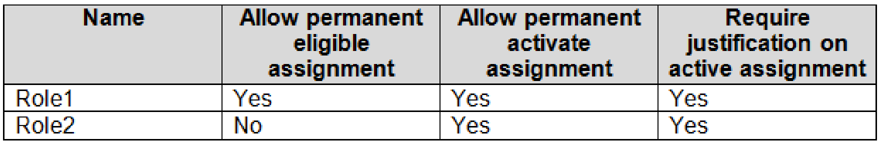
You have a Microsoft 365 E5 subscription that contains three users named Use1, User2, and User3.

You have Azure Active Directory (Azure AD) roles that have the role activation settings shown in the following table.



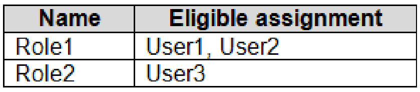
Name	Require justification on activation	Require approval to activate	Approver
Role1	No	Yes	User1
Role2	Yes	No	*Not applicable*

You have Azure AD roles that have the role assignment settings shown in the following table.



Name	Allow permanent eligible assignment	Allow permanent activate assignment	Require justification on active assignment
Role1	Yes	Yes	Yes
Role2	No	Yes	Yes

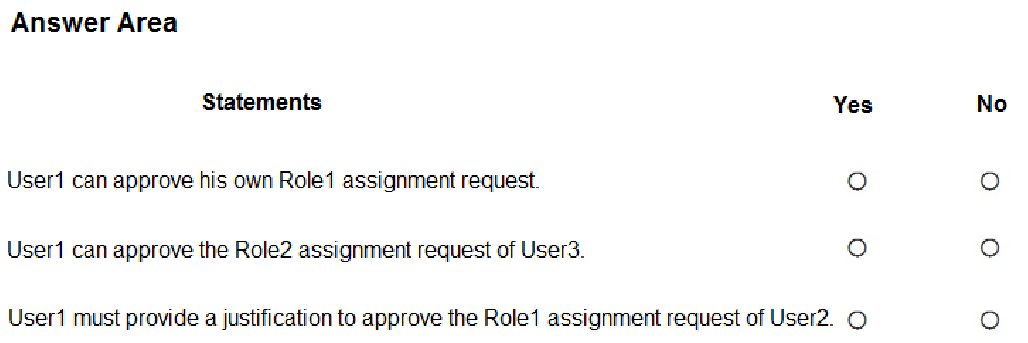
The Azure AD roles have eligible users assigned as shown in the following table.



Name	Eligible assignment
Role1	User1, User2
Role2	User3

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

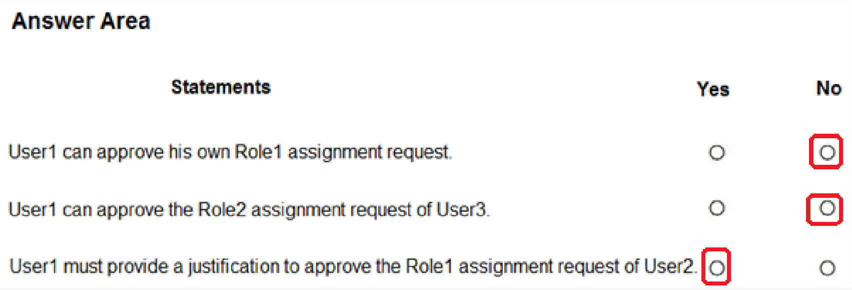
NOTE: Each correct selection is worth one point.



Answer Area

Statements	Yes	No
User1 can approve his own Role1 assignment request.	○	○
User1 can approve the Role2 assignment request of User3.	○	○
User1 must provide a justification to approve the Role1 assignment request of User2.	○	○

Suggested Answer:



Answer Area

Statements	Yes	No
User1 can approve his own Role1 assignment request.	○	[✓ ○]
User1 can approve the Role2 assignment request of User3.	○	[✓ ○]
User1 must provide a justification to approve the Role1 assignment request of User2.	[✓ ○]	○

JoeP1 Highly Voted 1 year, 10 months ago

I think the answers should be N/N/N.

1. (No) Approvers can't approve their own activation request.
2. (No) Role2 does not need approval to activate.
3. (No) Justification is not needed for activation approval of Role1. Justification is only needed when eligibility assignment is made with

activation included(ie permanent activation).

Use of the term 'Assignment Request' in the questions is confusing.

upvoted 12 times

formazionehs Most Recent 1 year, 9 months ago

Box 1: No

https://learn.microsoft.com/en-us/azure/active-directory/privileged-identity-management/azure-ad-pim-approval-workflow

Approvers are not able to approve their own role activation requests.

Box 2: No

Role 2 has Require approval to activate: No

Box 3: Yes

Require justification on active assignment: Yes

https://learn.microsoft.com/en-us/azure/active-directory/privileged-identity-management/pim-how-to-change-default-settings

You can require that users enter a business justification when they create an active (as opposed to eligible) assignment (activate a role for a user).

upvoted 2 times

examtopics11 1 year, 10 months ago

NNY

1. Approvers are not able to approve their own role activation requests

https://learn.microsoft.com/en-us/azure/active-directory/privileged-identity-management/azure-ad-pim-approval-workflow

2. Role2 "Require approval to activate" = No

3. I think the key word is "assignment request of User2.

upvoted 3 times

kmk_01 1 year, 9 months ago

But why and how would the approver User1 provide justification?

upvoted 1 times

Question #79 *Topic 1*

You have a hybrid Azure Active Directory (Azure AD) tenant that has pass-through authentication enabled.

You plan to implement Azure AD Identity Protection and enable the user risk policy.

You need to configure the environment to support the user risk policy.

What should you do first?

A. Enable the sign-in risk policy.

B. Enforce the multi-factor authentication (MFA) registration policy.

C. Configure a conditional access policy.

D. Enable password hash synchronization.

Suggested Answer: *D*

Community vote distribution

C (67%) D (33%)

⊟ **sleb** Highly Voted 1 year, 7 months ago

ChatGPT says it's C.

upvoted 7 times

⊟ **jamspurple** 1 year, 7 months ago

Funny, but it's wrong in case anyone else is wondering...

upvoted 1 times

⊟ **DavidBM** 1 year, 6 months ago

Nice, i think the same :-)

upvoted 2 times

⊟ **Citmerian** 1 year, 6 months ago

Once password hash synchronization is enabled, you can proceed with configuring a conditional access policy to further enhance security measures based on risk factors.

Therefore, option D is the correct answer for the first step in configuring the environment to support the user risk policy in Azure AD Identity Protection.

upvoted 4 times

⊟ **Tweety1972** Most Recent 1 year, 6 months ago

You have to create a Conditional Access first to configure the user risk policy.

upvoted 2 times

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

Selected Answer: C

Begin by creating a CAP = option C

https://learn.microsoft.com/en-us/azure/active-directory/identity-protection/howto-identity-protection-configure-risk-policies#enable-policies

upvoted 3 times

⊟ **Dhamus** 1 year, 8 months ago

Selected Answer: D

The organization has pass-through authentication enabled.

I'm going for option D.

upvoted 2 times

⊟ **RomanV** 1 year, 8 months ago

Incorrect. Enabling password hash synchronization is a prerequisite for implementing pass-through authentication, but if you read the question with 2 eyes instead of 1, you will read "...that has pass-through authentication enabled"

So the correct answer is A. Enable the sign-in risk policy.

upvoted 1 times

⊟ **RomanV** 1 year, 8 months ago

Source: https://learn.microsoft.com/en-us/defender-cloud-apps/aadip-integration

upvoted 2 times

⊟ **Tweety1972** 1 year, 6 months ago

Microsoft's recommendation:
Microsoft recommends the below risk policy configurations to protect your organization:
1. User risk policy
Require a secure password change when user risk level is High. Azure AD MFA is required before the user can create a new password with password writeback to remediate their risk.

https://learn.microsoft.com/en-us/azure/active-directory/identity-protection/howto-identity-protection-configure-risk-policies

upvoted 2 times

⊟ **Tanasi** 1 year, 7 months ago

dude, you just contradicted yourself so much. pass-through authentication is different from password hash synchronization. sign-in risk =/= user risk.
Answer is C. Use conditional access.
https://portal.azure.com/#view/Microsoft_AAD_IAM/IdentityProtectionMenuBlade/~/UserPolicy

upvoted 2 times

⊟ **RomanV** 1 year, 8 months ago

"For users to self-remediate risk though, they must register for Azure AD Multifactor Authentication before they become risky. For more information, see the article Plan an Azure Active Directory Multi-Factor Authentication deployment. Use the Identity Protection multifactor authentication registration policy to help get your users registered for Azure AD Multifactor Authentication before they need to use it. "

So Enable MFA will be the correct answer.

https://learn.microsoft.com/en-us/azure/active-directory/identity-protection/how-to-deploy-identity-protection

upvoted 6 times

⊟ **RomanV** 1 year, 8 months ago

To make the MFA point stronger:

"If organizations have a sign-in risk policy that requires multifactor authentication when the sign-in risk level is medium or high, their users must complete multifactor authentication when their sign-in risk is medium or high."

Source: https://learn.microsoft.com/en-us/azure/active-directory/identity-protection/concept-identity-protection-policies#azure-ad-mfa-registration-policy

upvoted 4 times

⊟ **josh_josh** 1 year, 9 months ago

Selected Answer: D

D is the answer

upvoted 1 times

⊟ **Aleyah** 1 year, 9 months ago

Selected Answer: C

......

upvoted 3 times

Question #80 *Topic 1*

You configure several Microsoft Defender for Office 365 policies in a Microsoft 365 subscription.

You need to allow a user named User1 to view Defender for Office 365 reports from the Threat management dashboard.

Which role provides User1 with the required role permissions?

A. Reports reader

B. Exchange administrator

C. Security administrators

D. Compliance administrator

Suggested Answer: *A*

Community vote distribution

C (100%)

Dhamus 1 year, 8 months ago

Selected Answer: C

Correct answer, Security Administrator can view Defender reports.

upvoted 2 times

Stig_88 1 year, 8 months ago

Selected Answer: C

Answer is C:
When you go to 365 Admin Center>Roles>Role Assignments
Search for Reports Reader
Permissions tab
Run As
It will open new tab running the Role you selected, which will show you that looking at the reports through MS 365 Defender Threat Reports dashboard is no an option.

upvoted 1 times

abrub 1 year, 9 months ago

Selected Answer: C

Sec Admin should be correct

upvoted 4 times

examtopics11 1 year, 10 months ago

Selected Answer: C

only Security Administrator role mentions Defender 365.

upvoted 4 times

> **JoeP1** 1 year, 10 months ago
>
> I agree that the only one listed with access is Security Administrator.
>
> The Reports Reader description says the role gives access to "view usage reporting data and the reports dashboard in Microsoft 365 admin center" as well as "all sign-in logs, audit logs, and activity reports in Azure AD" but can't "access the product-specific admin centers"
> These details are from: https://learn.microsoft.com/en-us/azure/active-directory/roles/permissions-reference#reports-reader
>
> upvoted 2 times

JBSacdalan 1 year, 10 months ago

I think there is a typo, it should be Security reader and Security Administrator

upvoted 4 times

yoton 1 year, 10 months ago

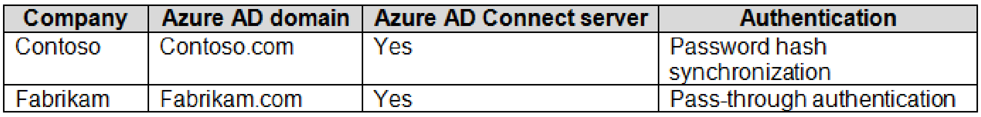
Should be security administrator

upvoted 1 times

Question #81 *Topic 1*

A company named Contoso, Ltd. acquires a company named Fabrikam, Inc.

Users at each company continue to use their company's Microsoft 365 tenant. Both companies have hybrid Azure Active Directory (Azure AD) tenants configured as shown in the following table.



Company	Azure AD domain	Azure AD Connect server	Authentication
Contoso	Contoso.com	Yes	Password hash synchronization
Fabrikam	Fabrikam.com	Yes	Pass-through authentication

In the Contoso tenant, you create a new Microsoft 365 group named FabrikamUsers, and you add FabrikamUsers as a member of a Microsoft Teams team named Corporate.

You need to add Fabrikam users to the FabrikamUsers group.

What should you do first?

A. Configure the Contoso tenant to use pass-through authentication as the authentication method.

B. In the Contoso tenant, create a new conditional access policy.

C. In the Contoso tenant, create guest accounts for all the Fabrikam users.

D. Configure the Fabrikam tenant to use federation as the authentication method.

Suggested Answer: *D*

Community vote distribution

C (89%) 11%

Clinson 1 year, 6 months ago

Selected Answer: D

ADFS is how organizations share access to resources with each other. Although, I think this questoin should say something more about how many users because ADFS is not easy to setup and for small organizations wouldn't be worth it.

ADFS can be used in the below scenarios:
Single Sign-On (SSO): ADFS can be used to provide Single Sign-On (SSO) authorization to users who want to access applications located in different networks or organizations. It provides seamless Single Sign-On (SSO) access to Internet-facing applications or services.
https://blog.miniorange.com/what-is-adfs/
https://learn.microsoft.com/en-us/azure/active-directory/hybrid/connect/plan-connect-user-signin#federation-that-uses-a-new-or-existing-farm-with-ad-fs-in-windows-server-2012-r2

upvoted 1 times

Dhamus 1 year, 8 months ago

Selected Answer: C

The answer is C, I have done it in my laboratory.

upvoted 3 times

josh_josh 1 year, 9 months ago

Selected Answer: C

C is the answer

upvoted 2 times

Pointless 1 year, 9 months ago

C

Since both companies have hybrid Azure AD tenants, creating guest accounts for Fabrikam users in the Contoso tenant would allow them to access the FabrikamUsers group in the Corporate Teams team. Option A is not necessary for this task. Option B is not relevant to adding Fabrikam users to a group. Option D is also not necessary as both companies already have hybrid Azure AD tenants.

upvoted 4 times

kmk_01 1 year, 9 months ago

Selected Answer: C

I would go for C too.

upvoted 2 times

MoritzW 1 year, 10 months ago

Selected Answer: C

I also think it should be C. There is no way to add users from another company with federation.

upvoted 1 times

microsoftbyomded 1 year, 10 months ago

ADSF or Cross-tenant access with Azure AD External Identities? Fédération does not appear in the ms docs regarding b2b guest access

upvoted 1 times

Question #82 *Topic 1*

You have a Microsoft 365 E5 subscription that contains a user named User1.

You need to ensure that User1 can configure an Azure Active Directory (Azure AD) Identity Protection user risk policy and receive Azure AD Identity Protection alerts. The solution must use the principle of least privilege.

Which role should you assign to User1?

A. Security Operator

B. Identity Governance Administrator

C. Security Administrator

D. Security Reader

Suggested Answer: *A*

Community vote distribution

C (88%) 13%

AVN1711 1 year, 3 months ago

Selected Answer: A

I think A-Security Operator is the right answer. in the Permissions>Manage all it has
-Create and delete all resources, and read and update standard properties in Azure AD Identity Protection

upvoted 1 times

Ndaiga 1 year, 6 months ago

Selected Answer: C

Security Admin is the correct answer. Security operator can't configure policies

upvoted 1 times

Jay_ITN 1 year, 7 months ago

The Identity Governance Administrator role in Microsoft 365 provides the necessary permissions to configure and manage identity-related policies and features, including Azure AD Identity Protection. This role allows User1 to configure user risk policies and receive alerts specifically related to Azure AD Identity Protection.

Assigning User1 the Identity Governance Administrator role ensures that they have the appropriate level of access and control over identity protection without granting them broader security administration privileges (such as the Security Administrator role) that may exceed their requirements.

upvoted 1 times

kmk_01 1 year, 9 months ago

Selected Answer: C

Yes it's C. Only Global Admins and Security Admins can configure Identity Protection policies. https://learn.microsoft.com/en-us/azure/active-directory/identity-protection/overview-identity-protection#required-roles

upvoted 2 times

rtis16 1 year, 10 months ago

Selected Answer: C

Agreed with EM1234, it should be C.

upvoted 2 times

msysadmin 1 year, 10 months ago

Selected Answer: C

Answer is C
https://learn.microsoft.com/en-us/azure/active-directory/roles/permissions-reference#security-operator

upvoted 2 times

EM1234 1 year, 10 months ago

I think it should be C.

This is from the docs on the security operator built in role:

All permissions of the Security Reader role
Perform all Identity Protection operations except for configuring or changing risk-based policies, resetting passwords, and configuring alert e-mails.

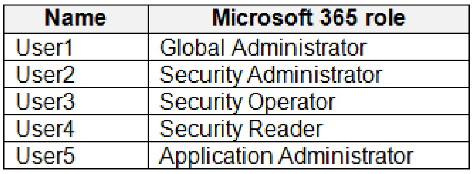
https://learn.microsoft.com/en-us/azure/active-directory/roles/permissions-reference#security-operator
upvoted 4 times

Question #83 *Topic 1*

HOTSPOT

-

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



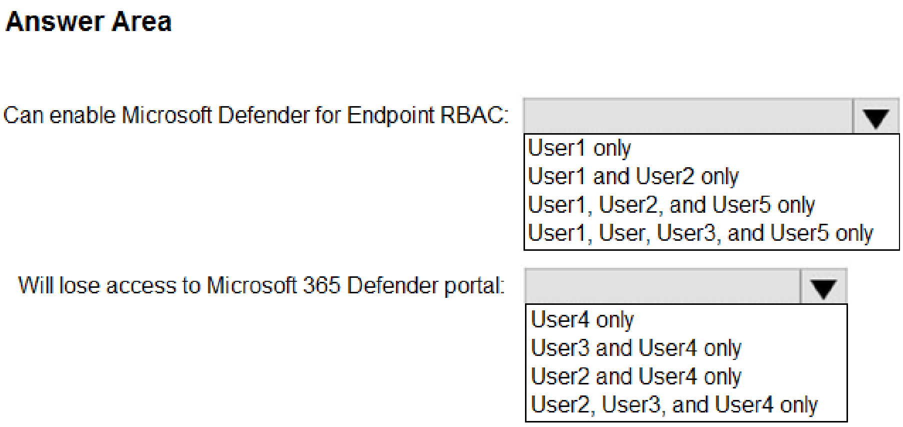
Name	Microsoft 365 role
User1	Global Administrator
User2	Security Administrator
User3	Security Operator
User4	Security Reader
User5	Application Administrator

You plan to enable Microsoft Defender for Endpoint role-based access control (RBAC).

You need to identify which users can enable RBAC in Microsoft Defender for Endpoint, and which users will lose access to Microsoft 365 Defender portal after RBAC in enabled.

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

NOTE: Each correct selection is worth one point.



Answer Area

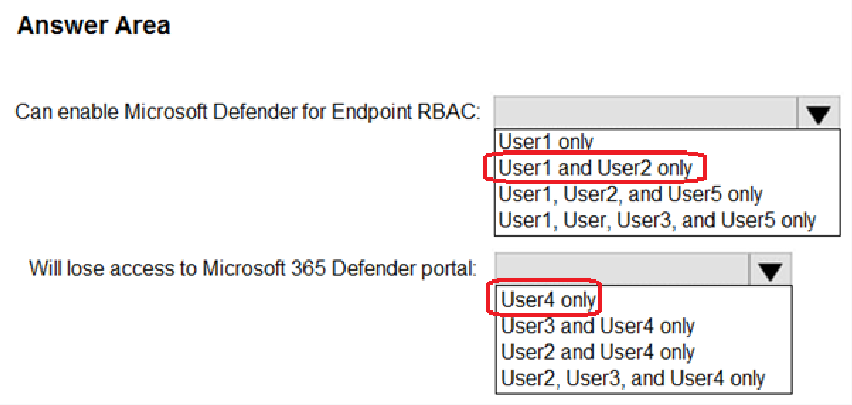
Can enable Microsoft Defender for Endpoint RBAC: ▼

User1 only
User1 and User2 only
User1, User2, and User5 only
User1, User, User3, and User5 only

Will lose access to Microsoft 365 Defender portal: ▼

User4 only
User3 and User4 only
User2 and User4 only
User2, User3, and User4 only

Suggested Answer:



Answer Area

Can enable Microsoft Defender for Endpoint RBAC: ▼

User1 only
[✓ User1 and User2 only]
User1, User2, and User5 only
User1, User, User3, and User5 only

Will lose access to Microsoft 365 Defender portal: ▼

[✓ User4 only]
User3 and User4 only
User2 and User4 only
User2, User3, and User4 only

⊟ **Kallely** 2 months, 3 weeks ago

https://learn.microsoft.com/en-us/defender-endpoint/assign-portal-access

upvoted 1 times

⊟ **RomanV** 1 year, 8 months ago

Correct answers:

- User1 and User2 only
- User4 only

I hear you ask, why?

"Initially, only those with Azure AD Global Administrator or Security Administrator rights will be able to create and assign roles in the Microsoft 365 Defender portal, therefore, having the right groups ready in Azure AD is important.

Turning on role-based access control will cause users with read-only permissions (for example, users assigned to Azure AD Security reader role) to lose access until they are assigned to a role."

Source: https://learn.microsoft.com/en-us/microsoft-365/security/defender-endpoint/rbac?view=o365-worldwide

upvoted 4 times

formazionehs 1 year, 9 months ago

Can enable Microsoft Defender for Endpoint RBAC: User1 and User2 only

https://learn.microsoft.com/en-us/microsoft-365/security/defender-endpoint/rbac?view=o365-worldwide

To enable the feature, you must have a Global Administrator role or Security Administrator role in Azure AD.

Will lose access to Microsoft 365 Defender portal: User4 only

Turning on role-based access control will cause users with read-only permissions (for example, users assigned to Azure AD Security reader role) to lose access until they are assigned to a role.

upvoted 1 times

JoeP1 1 year, 10 months ago

Can enable Microsoft Defender for Endpoint RBAC is correct for User1 and User2 only because Microsoft says: "When you first log in to the Microsoft 365 Defender portal, you're granted either full access or read only access. Full access rights are granted to users with Security Administrator or Global Administrator roles in Azure AD. "

The article is at: https://learn.microsoft.com/en-us/microsoft-365/security/defender-endpoint/rbac?view=o365-worldwide

upvoted 1 times

JoeP1 1 year, 10 months ago

User4(Security Reader) will definitely lose access to the Microsoft 365 Defender portal, but I am not sure about User3(Security Operator).

I found a Microsoft article that confirms the loss of access:"Turning on role-based access control will cause users with read-only permissions (for example, users assigned to Azure AD Security reader role) to lose access until they are assigned to a role."

The article is at: https://learn.microsoft.com/en-us/microsoft-365/security/defender-endpoint/rbac?view=o365-worldwide

upvoted 2 times

msysadmin 1 year, 10 months ago

This part unclear for me: which users will lose access to Microsoft 365 Defender portal after RBAC in enabled?

Not agree Security reader will lose access to Microsoft 365 Defender portal

https://learn.microsoft.com/en-us/microsoft-365/security/defender/custom-roles?view=o365-worldwide

upvoted 1 times

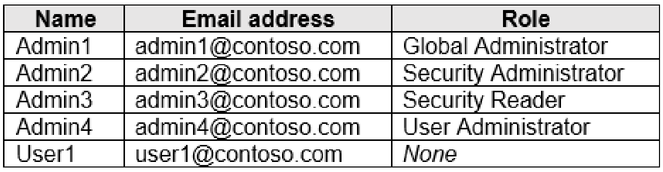
EM1234 1 year, 10 months ago

ET admins are not even citing their pages for their answers on this one... like a few others I have seen.

upvoted 1 times

Question #84 Topic 1

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



Name	Email address	Role
Admin1	admin1@contoso.com	Global Administrator
Admin2	admin2@contoso.com	Security Administrator
Admin3	admin3@contoso.com	Security Reader
Admin4	admin4@contoso.com	User Administrator
User1	user1@contoso.com	*None*

Azure AD Identity Protection detects that the account of User1 is at risk and generates an alert.

How many users will receive the alert?

A. 1

B. 2

C. 3

D. 4

E. 5

Suggested Answer: *C*

Community vote distribution

C (100%)

EM1234 Highly Voted 1 year, 10 months ago

I will do their job for them I guess:

It is 3.

https://learn.microsoft.com/en-us/azure/active-directory/identity-protection/howto-identity-protection-configure-notifications

upvoted 6 times

chickenroaster 1 year, 10 months ago

The recipients of this email - Users in the Global Administrator, Security Administrator, or Security Reader roles are automatically added to this list.

upvoted 2 times

RomanV Most Recent 1 year, 8 months ago

Correct answer: 3

Why?

"Users in the Global Administrator, Security Administrator, or Security Reader roles are automatically added to this list. We attempt to send emails to the first 20 members of each role. If a user is enrolled in PIM to elevate to one of these roles on demand, then they will only receive emails if they are elevated at the time the email is sent."

Source: https://learn.microsoft.com/en-us/azure/active-directory/identity-protection/howto-identity-protection-configure-notifications

upvoted 2 times

PhoenixSlasher 1 year, 9 months ago

Selected Answer: C

User admin, security administrator and global admin

upvoted 2 times

Jay_ITN 1 year, 8 months ago

Microsoft states the following - The recipients of this email - Users in the Global Administrator, Security Administrator, or Security Reader roles are automatically added to this list. We attempt to send emails to the first 20 members of each role. If a user is enrolled in PIM to elevate to one of these roles on demand, then they will only receive emails if they are elevated at the time the email is sent.

Optionally you can Add custom email here users defined must have the appropriate permissions to view the linked reports in the Azure portal.

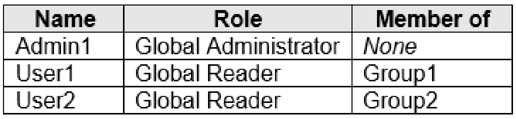
upvoted 1 times

Question #85 Topic 1

HOTSPOT

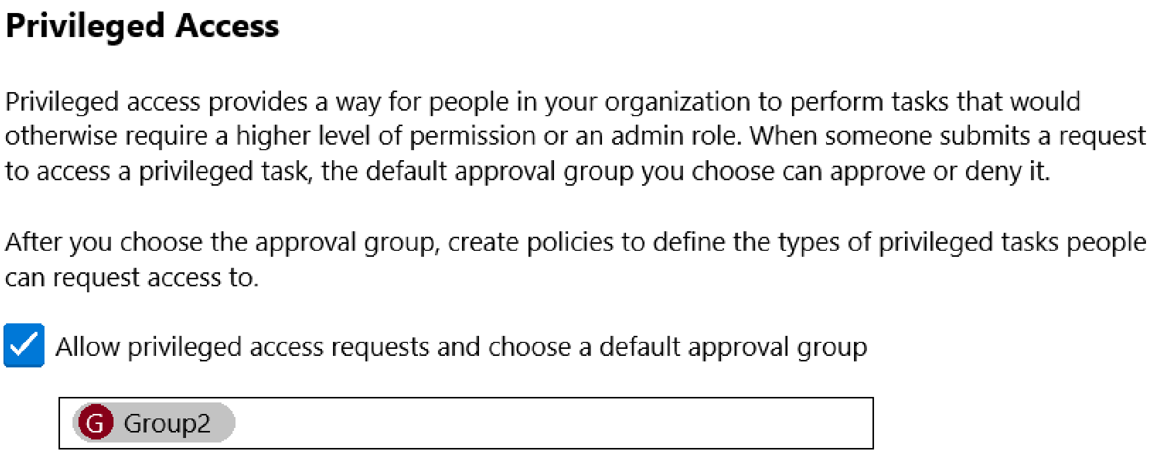
-

You have a Microsoft 365 E5 subscription that contains two groups named Group1 and Group2 and the users shown in the following table.



Name	Role	Member of
Admin1	Global Administrator	*None*
User1	Global Reader	Group1
User2	Global Reader	Group2

You have the Privileged Access settings configured as shown in the following exhibit.



Privileged Access

Privileged access provides a way for people in your organization to perform tasks that would otherwise require a higher level of permission or an admin role. When someone submits a request to access a privileged task, the default approval group you choose can approve or deny it.

After you choose the approval group, create policies to define the types of privileged tasks people can request access to.

☑ Allow privileged access requests and choose a default approval group

G Group2

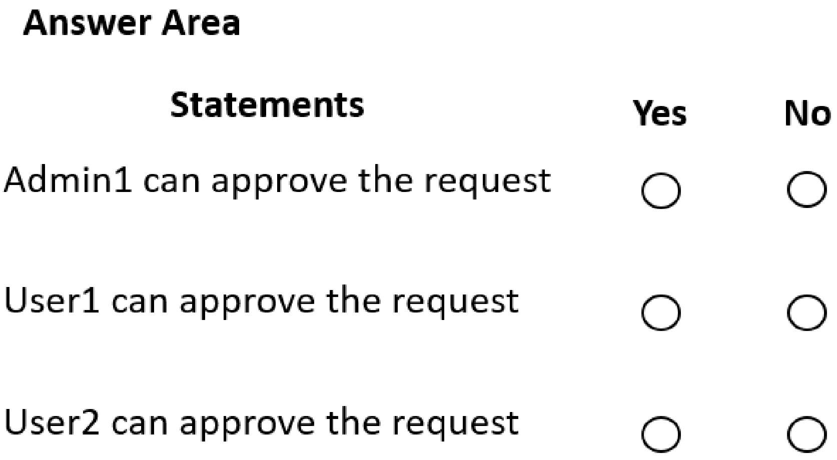
You have a privileged access policy that has the following settings:

- Policy name: New Transport Rule
- Policy type: Task
- Policy scope: Exchange
- Approval Type: Manual
- Approver group: Group1

User1 requests access to the New Transport Rule policy for a duration of two hours.

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

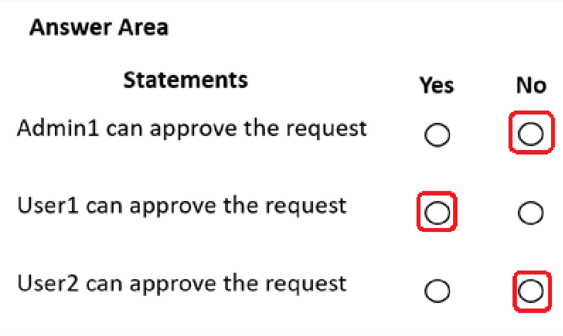
NOTE: Each correct selection is worth one point.



Answer Area

Statements	Yes	No
Admin1 can approve the request	○	○
User1 can approve the request	○	○
User2 can approve the request	○	○

Suggested Answer:



Answer Area

Statements	Yes	No
Admin1 can approve the request	○	[✓ ○]
User1 can approve the request	[✓ ○]	○
User2 can approve the request	○	[✓ ○]

GPerez73 1 year, 8 months ago

N/N/N Global reader cannot raise a request to PAM. Tested in lab

upvoted 2 times

Ahhallison 1 year, 8 months ago

I agree, this is the way.

upvoted 1 times

examdj101j 1 year, 8 months ago

Based on everything I read here and my own study Answers are correct...

N - Because A default approval group is assigned (Group 2) Tested by users below

Y - Because User 1 is in Group 1 which is defined in the policy as an Approver

N - Because User 2 is in Group 2 (Which would be able to approve as the default) But in this case the approver is defined as Group 1.

upvoted 2 times

Tweety1972 1 year, 6 months ago

You cannot approve request for your self

upvoted 1 times

Stig_88 1 year, 8 months ago

N-Admin1 is not member of Group2.

N-You cannot approve request for your self even if you are member of approver Group

Y-User2 is member of Group2 who is the approver.

upvoted 1 times

Stig_88 1 year, 8 months ago

N

N

N-Global Reader do not have access to "Privileged Access"

upvoted 2 times

GatesBill 1 year, 9 months ago

Tried the exact samen scenario; interestingly enough User1 was not able to create any access requests - "Couldn't create privileged access request." (although it has a E5 subscription and Global Reader role)

Please bear in mind that this question is about PAM, not PIM.

upvoted 1 times

Pointless 1 year, 9 months ago

N - If an approver is defined then Global/PIM admins can't approve

N - User cannot approver their own requests

N - approver defined is user group1 and user 2 is in group2 so they can't approve.

upvoted 4 times

JoeP1 1 year, 10 months ago

I don't think User1 can approve their own request, so the second statement should also be No.

I only found a Microsoft Techcommunity answer confirming someone can't approve their own PAM request:
https://techcommunity.microsoft.com/t5/microsoft-365/office365-privileged-access-approval-process-if-requester-is-in/m-p/282012

upvoted 3 times

tecnicosoffshoretech 1 year, 10 months ago

Just tested on my lab, and there is not anymore and opción to set Group 2 as a default approved for all the roles.
If not approved group is selected for a particular rol, de global admin or PIM administrator can approve the active rol. If a group is selected (on the example group 1) this is the new approval group and global admin and PIM admin cant approve anymore (only see and cancel)
https://learn.microsoft.com/en-us/azure/active-directory/privileged-identity-management/azure-ad-pim-approval-workflow
upvoted 1 times

⊟ **tecnicosoffshoretech** 1 year, 10 months ago
After further testing, the default approval group for all the roles is in Microsoft 365 Admin - Org Settings - Security and privacy - Privileged access.
upvoted 1 times

⊟ **tecnicosoffshoretech** 1 year, 10 months ago
But the approval group for priviledged access to perform taks in Purwiew (compliance center) doenst have anything to see with PIM therefore the answers are good.
¨Privileged access management is defined and scoped at the task level, while Azure AD Privileged Identity Management applies protection at the role level¨
https://learn.microsoft.com/en-US/microsoft-365/compliance/privileged-access-management?WT.mc_id=365AdminCSH_inproduct&view=o365-worldwide
upvoted 1 times

⊟ **rtis16** 1 year, 10 months ago
Global admins can manage this by default. Am I missing something?
https://learn.microsoft.com/en-us/microsoft-365/compliance/privileged-access-management?view=o365-worldwide#frequently-asked-questions
upvoted 1 times

Question #86 *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 contains a user named User1.

You need to ensure that User1 can review Conditional Access policies.

Solution: You assign User1 the Security Reader role.

Does that meet the goal?

A. Yes

B. No

Suggested Answer: *A*

Community vote distribution

A (100%)

Citmerian 1 year, 6 months ago

Check this: https://learn.microsoft.com/en-us/azure/active-directory/roles/delegate-by-task
read: Security - Conditional Access (Least privileged role - Security Reader) - (Additional roles - Conditional Access Administrator and Security Administrator)

upvoted 1 times

Citmerian 1 year, 6 months ago

I think YES

upvoted 1 times

DavidBM 1 year, 6 months ago

Selected Answer: A

Yes, assigning User1 the Security Reader role will allow them to review Conditional Access policies. The Security Reader role allows users to view security reports and dashboards in Azure Security Center and view security settings in Azure Active Directory (Azure AD) Identity Protection and Privileged Identity Management

Therefore, the answer is A. Yes.

upvoted 1 times

Lekso 1 year, 6 months ago

The answer is NO . This is no a security issue only a conditional access issue

upvoted 1 times

Anonism 1 year, 7 months ago

NO
The Security Reader role provides read-only access to security-related information in Azure AD and other Microsoft 365 security tools. While it allows User1 to view security-related data, it does not grant the necessary permissions to review or manage Conditional Access policies.

upvoted 1 times

RomanV 1 year, 6 months ago

Read between the lines my friend. The question is --> You need to ensure that User1 can REVIEW Conditional Access policies.

Reviewing is not the same as MANAGING CAP.

upvoted 1 times

⊟ **RomanV** 1 year, 6 months ago

Read this as well:

To see applied Conditional Access policies in the sign-in logs, administrators must have permissions to view both the logs and the policies. The least privileged built-in role that grants both permissions is Security Reader. As a best practice, your Global Administrator should add the Security Reader role to the related administrator accounts.

So answer is A: YES

Source: https://learn.microsoft.com/en-us/azure/active-directory/reports-monitoring/how-to-view-applied-conditional-access-policies
upvoted 1 times

Question #88 *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 contains a user named User1.

You need to ensure that User1 can review Conditional Access policies.

Solution: You assign User1 the Authentication Administrator role.

Does that meet the goal?

A. Yes

B. No

Suggested Answer: *A*

Community vote distribution

B (100%)

DavidBM 1 year, 6 months ago

Selected Answer: B

No, assigning User1 the Authentication Administrator role will not allow them to review Conditional Access policies. The Authentication Administrator role allows users to manage authentication features and settings for Azure Active Directory (Azure AD), such as password policies and multi-factor authentication

Therefore, the answer is B. No.

upvoted 2 times

AnonymousJhb 1 year, 8 months ago

Selected Answer: B

Assigning the Authentication Administrator role to User1 would not meet the goal of allowing them to review Conditional Access policies. The Authentication Administrator role is a high-privileged role in Azure AD that provides full access to manage authentication methods and passwords for all users in the directory. This role does not provide access to Conditional Access policies or any other security-related features.

upvoted 4 times

RomanV 1 year, 8 months ago

B. No.

Assigning the Authentication Administrator role to User1 would not meet the goal of allowing them to review Conditional Access policies. The Authentication Administrator role is a high-privileged role in Azure AD that provides full access to manage authentication methods and passwords for all users in the directory. This role does not provide access to Conditional Access policies or any other security-related features.

Therefore, assigning the Authentication Administrator role to User1 would not provide them with the necessary permissions to review Conditional Access policies. A more appropriate solution would be to assign them the Security Reader role, which provides read-only access to security-related information in Azure AD, including Conditional Access policies.

upvoted 1 times

RomanV 1 year, 8 months ago

To see applied Conditional Access policies in the sign-in logs, administrators must have permissions to view both the logs and the policies. The least privileged built-in role that grants both permissions is Security Reader. As a best practice, your Global Administrator should add the Security Reader role to the related administrator accounts.

The following built-in roles grant permissions to read Conditional Access policies:

Global Administrator
Global Reader
Security Administrator
Security Reader
Conditional Access Administrator
The following built-in roles grant permission to view sign-in logs:

Global Administrator
Security Administrator
Security Reader
Global Reader
Reports Reader

Source: https://learn.microsoft.com/en-us/azure/active-directory/reports-monitoring/how-to-view-applied-conditional-access-policies
upvoted 3 times

V1nc3n7 1 year, 8 months ago

Selected Answer: B

https://learn.microsoft.com/en-us/azure/active-directory/roles/permissions-reference#authentication-administrator does not list microsoft.directory/conditionalAccessPolicies/standard/read
upvoted 1 times

smiff 1 year, 8 months ago

Selected Answer: B

Answer: No

https://learn.microsoft.com/en-us/azure/active-directory/reports-monitoring/how-to-view-applied-conditional-access-policies
upvoted 2 times

Question #89 *Topic 1*

HOTSPOT

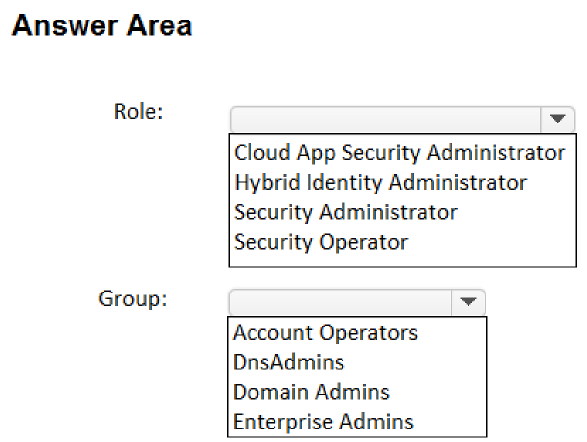
-

You have a hybrid Microsoft 365 E5 environment that contains a synced user named User1.

You need to ensure that User1 can configure Microsoft Defender for Identity and deploy a Defender for Identity sensor. The solution must use the principle of least privilege.

Which role should you assign to User1, and to which group should you add User1? To answer, select the appropriate options in the answer area.

NOTE: Each correct selection is worth one point.



Answer Area

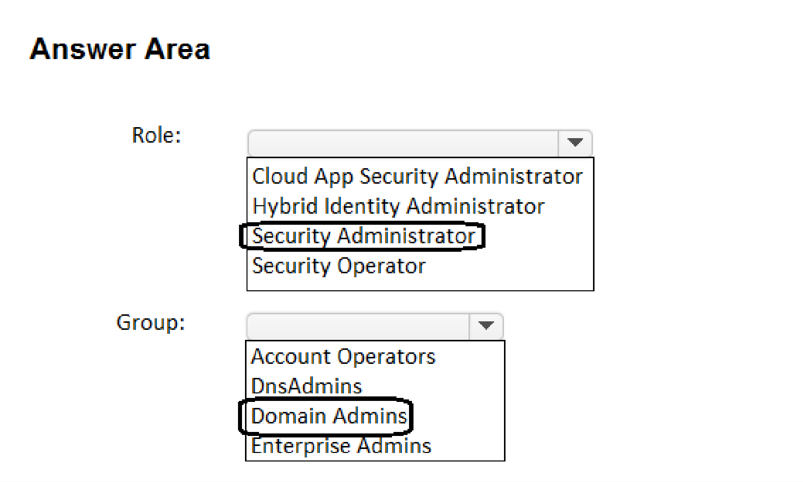
Role:

Cloud App Security Administrator
Hybrid Identity Administrator
Security Administrator
Security Operator

Group:

Account Operators
DnsAdmins
Domain Admins
Enterprise Admins

Suggested Answer:



Answer Area

Role:

Cloud App Security Administrator
Hybrid Identity Administrator
[✓ Security Administrator]
Security Operator

Group:

Account Operators
DnsAdmins
[✓ Domain Admins]
Enterprise Admins

DavidBM 1 year, 6 months ago

To ensure that User1 can configure Microsoft Defender for Identity and deploy a Defender for Identity sensor, you should assign the Security Administrator role to User1 and add User1 to the Security Admins group or Domain Admins group.

Therefore, the answer area should have the following options selected:

Role: Security Administrator
Group: Domain Admins
upvoted 3 times

Question #90 *Topic 1*

You plan to deploy a new Microsoft 365 subscription that will contain 500 users.

You need to ensure that the following actions are performed when the users sign in to the subscription:

• Evaluate the users' risk level based on their location and travel.
• Require high-risk users to sign in by using Azure Multi-Factor Authentication (Azure MFA).

The solution must minimize cost.

Which license should you assign to each user?

A. Enterprise Mobility + Security E3

B. Microsoft 365 Business Premium

C. Microsoft 365 E3

D. Microsoft 365 E5

Suggested Answer: *A*

Community vote distribution

D (86%) 14%

AVN1711 1 year, 3 months ago

Selected Answer: D

to have advanced user risk leveled capabilities you need to have Azure P2, which is included in M3656 E5 or E5 Security licenses, so the right answer is D. If I do remember right there is no Security E3 license, because of that answer - A. (Enterprise Mobility + Security E3) is incorrect

upvoted 1 times

Maxx4 1 year, 6 months ago

Selected Answer: A

To ensure that users' risk levels are evaluated based on their location and travel, and to require high-risk users to sign in using Azure Multi-Factor Authentication (Azure MFA), while minimizing cost, you should assign each user the A. Enterprise Mobility + Security E3 license.

The Enterprise Mobility + Security E3 license includes Azure Active Directory Identity Protection, which provides risk-based conditional access capabilities. It allows you to evaluate user risk levels based on factors like location and travel patterns. With this license, you can create conditional access policies to require Azure MFA for high-risk users while allowing low-risk users to sign in without additional authentication factors.

upvoted 1 times

Maxx4 1 year, 6 months ago

The Microsoft 365 Business Premium (option B) license does not include Azure Active Directory Identity Protection or the advanced risk-based conditional access capabilities required for evaluating user risk levels and enforcing Azure MFA for high-risk users.

The Microsoft 365 E3 (option C) and Microsoft 365 E5 (option D) licenses include Azure Active Directory Identity Protection and provide the necessary capabilities for evaluating user risk and enforcing Azure MFA. However, these licenses are more expensive than the Enterprise Mobility + Security E3 license, which can help minimize costs while still meeting the stated requirements.

Therefore, to meet the requirements while minimizing cost, you should assign each user the Enterprise Mobility + Security E3 license (option A).

upvoted 1 times

DavidBM 1 year, 6 months ago

Selected Answer: D

To evaluate the users' risk level based on their location and travel and require high-risk users to sign in by using Azure Multi-Factor Authentication (Azure MFA), you should assign the Azure AD Premium P2 license to each user

Azure AD Premium P2 provides risk-based Conditional Access policies that can be used to evaluate the risk level of a sign-in attempt based on the user’s location and travel

Therefore, the answer is D. Microsoft 365 E5.

upvoted 1 times

⊟ **dadmundur** 1 year, 8 months ago

Risk based conditional access requires an Azure AD Premium P2 license. It is included with Microsoft 365 E5 or it can be purchased additionally via the "Enterprise Mobility + Security E5" package.

"Organizations with Azure AD Premium P2 licenses can create Conditional Access policies incorporating Azure AD Identity Protection sign-in risk detections."
https://learn.microsoft.com/en-us/azure/active-directory/conditional-access/howto-conditional-access-policy-risk

Microsoft 365 feature matrix:
https://m365maps.com/matrix.htm

upvoted 2 times

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

Selected Answer: D

P2
https://learn.microsoft.com/en-us/azure/active-directory/authentication/concept-mfa-licensing#available-versions-of-azure-ad-multi-factor-authentication

upvoted 2 times

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

Selected Answer: D

D
https://learn.microsoft.com/en-us/azure/active-directory/authentication/concept-mfa-licensing#available-versions-of-azure-ad-multi-factor-authentication

upvoted 1 times

⊟ **V1nc3n7** 1 year, 8 months ago

Selected Answer: D

D

You need Azure AD P2 license with is included in M365 E5

upvoted 1 times

⊟ **smiff** 1 year, 8 months ago

D.

That feature requires AADP P2 license.

upvoted 3 times

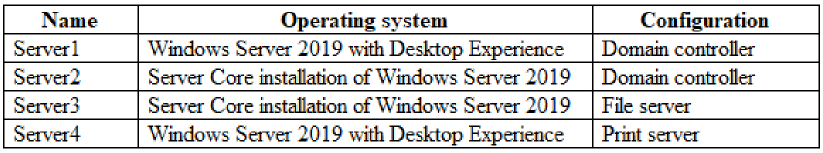
Question #91

Topic 1

HOTSPOT

-

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



Name	Operating system	Configuration
Server1	Windows Server 2019 with Desktop Experience	Domain controller
Server2	Server Core installation of Windows Server 2019	Domain controller
Server3	Server Core installation of Windows Server 2019	File server
Server4	Windows Server 2019 with Desktop Experience	Print server

You have Microsoft 365 subscription.

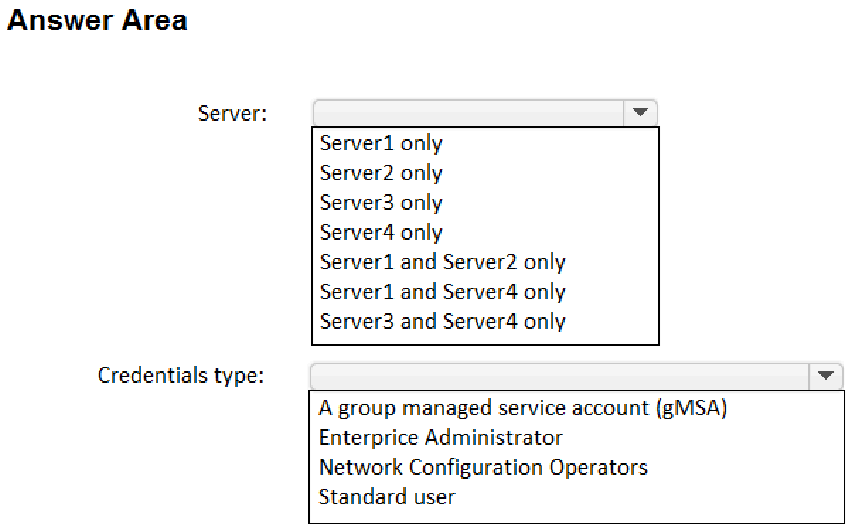
You plan to deploy Microsoft Defender for Identity.

You need to deploy the Defender for Identity sensor. The solution must meet the following requirements:

- Support the collection of Event Tracing for Windows (ETW) log entries.
- Use the principle of least privilege.
- Maximize security.

On which servers can you install the sensor, and which type of credentials is required for the sensor? To answer, select the appropriate options in the answer area.

NOTE: Each correct selection is worth one point.



Answer Area

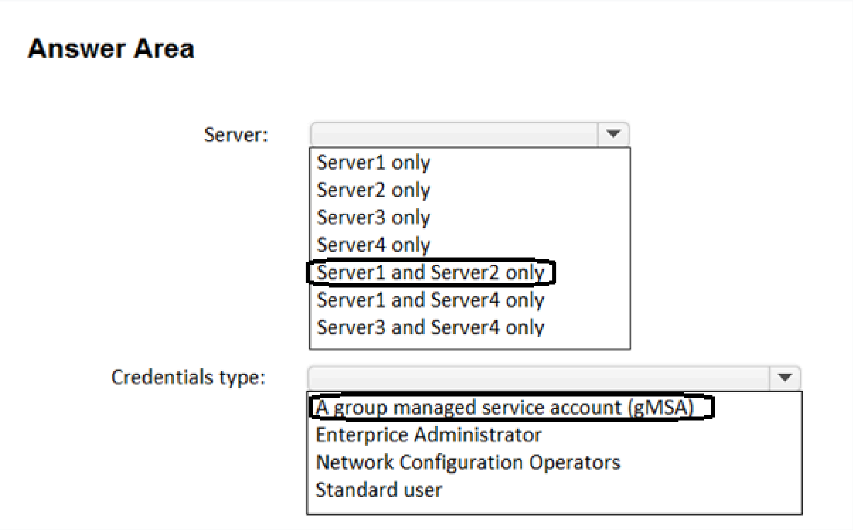
Server:

- Server1 only
- Server2 only
- Server3 only
- Server4 only
- Server1 and Server2 only
- Server1 and Server4 only
- Server3 and Server4 only

Credentials type:

- A group managed service account (gMSA)
- Enterprice Administrator
- Network Configuration Operators
- Standard user

Suggested Answer:



Answer Area

Server:

- Server1 only
- Server2 only
- Server3 only
- Server4 only
- [✓ Server1 and Server2 only]
- Server1 and Server4 only
- Server3 and Server4 only

Credentials type:

- [✓ A group managed service account (gMSA)]
- Enterprice Administrator
- Network Configuration Operators
- Standard user

⊟ **DavidBM** 1 year, 6 months ago

To deploy the Defender for Identity sensor that supports the collection of Event Tracing for Windows (ETW) log entries, uses the principle of least privilege and maximizes security, you should install the sensor on domain controllers and use a service account to run the sensor.

Therefore, the answer area should have the following options selected:

Servers: Domain controllers
Credentials: Service account

upvoted 1 times

⊟ **sleb** 1 year, 7 months ago

As of my knowledge cutoff in September 2021, it is not possible to deploy Microsoft Defender for Identity (formerly Azure Advanced Threat Protection) sensor on a Windows Server Core installation, including Windows Server 2019.

The Defender for Identity sensor requires a full installation of Windows Server with a graphical user interface (GUI) because it relies on components that are not available in the Server Core edition. The sensor installation process involves using the Azure ATP portal or PowerShell commands, both of which are not supported on Server Core. So server1 only it seems.

upvoted 2 times

⊟ **Tanasi** 1 year, 7 months ago

You can install on Core and Desktop Experience. Only on Nano you cannot.
See here:
https://learn.microsoft.com/en-us/defender-for-identity/prerequisites

upvoted 3 times

⊟ **GPerez73** 1 year, 7 months ago

Crystal clear. Thanks for the link Tanasi

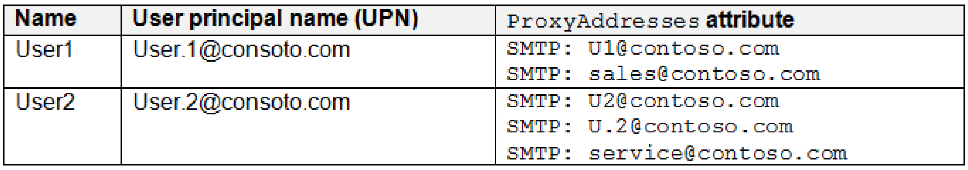
upvoted 1 times

Question #93 Topic 1

DRAG DROP

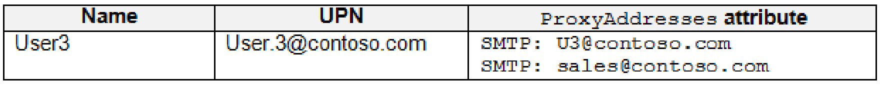
-

Your network contains an on-premises Active Directory domain named contoso.com that syncs to Azure AD by using Azure AD Connect. The domain contains the users shown in the following table.



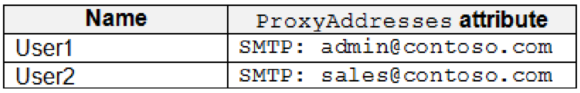
Name	User principal name (UPN)	ProxyAddresses attribute
User1	User.1@consoto.com	SMTP: U1@contoso.com SMTP: sales@contoso.com
User2	User.2@consoto.com	SMTP: U2@contoso.com SMTP: U.2@contoso.com SMTP: service@contoso.com

From Active Directory Users and Computers, you add the user shown in the following table.



Name	UPN	ProxyAddresses attribute
User3	User.3@contoso.com	SMTP: U3@contoso.com SMTP: sales@contoso.com

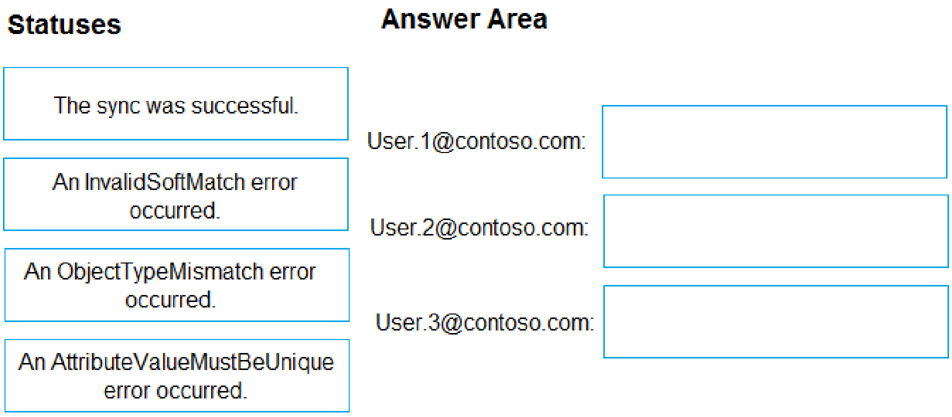
From Active Directory1 Users and Computers, you update the ProxyAddresses attributes as shown in the following table.



Name	ProxyAddresses attribute
User1	SMTP: admin@contoso.com
User2	SMTP: sales@contoso.com

Which status will Azure AD Connect sync return for each user after the next sync? To answer, drag the appropriate statuses to the correct users. Each status may be used once, more than once, or not at all. You may need to drag the split bar between panes or scroll to view content.

NOTE: Each correct selection is worth one point.



Statuses

- The sync was successful.
- An InvalidSoftMatch error occurred.
- An ObjectTypeMismatch error occurred.
- An AttributeValueMustBeUnique error occurred.

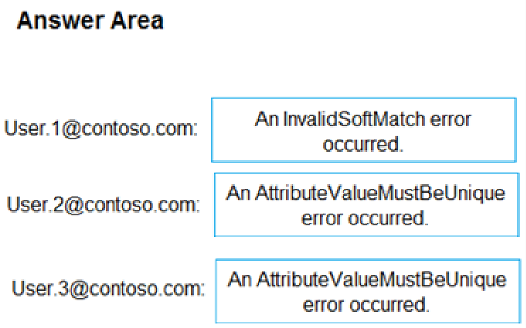
Answer Area

User.1@contoso.com:

User.2@contoso.com:

User.3@contoso.com:

Suggested Answer:



Answer Area

User.1@contoso.com: An InvalidSoftMatch error occurred.

User.2@contoso.com: An AttributeValueMustBeUnique error occurred.

User.3@contoso.com: An AttributeValueMustBeUnique error occurred.

darkschneider 1 year, 6 months ago

https://learn.microsoft.com/en-us/azure/active-directory/hybrid/connect/tshoot-connect-sync-errors

upvoted 3 times

⊟ **Clinson** 1 year, 6 months ago

Great link.

I take the answer to be
User 1 = Successful. There are no conflicts on the User 1 change.
User 2 = AttributeValueMustBeUnique. The proxy address conflicts with an existing synced user. The change will not be updated.
User 3 = InvalidSoftMatch. Conflicts with an existing synced user, but this is a user that is not yet synced and won't be until the error is resolved.

upvoted 1 times

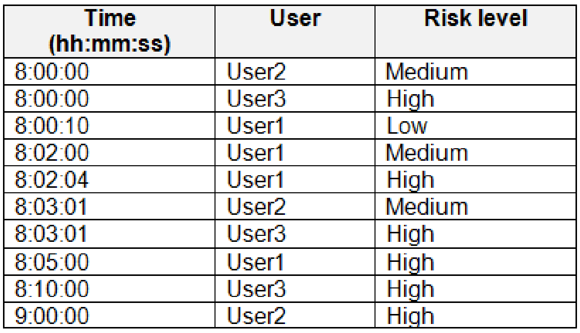
HOTSPOT

-

You have a Microsoft 365 E5 subscription that contains four users named User1, User2, User3, and User4.

In Azure AD Identity Protection, you configure User4 as the only recipient of Users at risk detected alerts. You set Alert on user risk level at or above to Low.

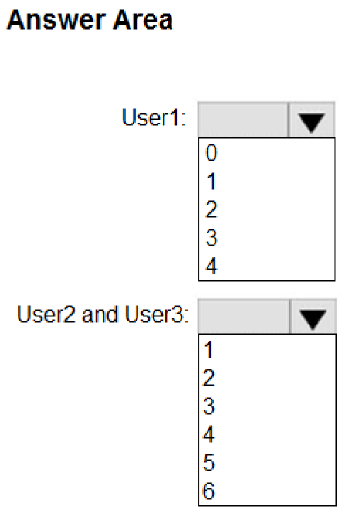
Azure AD Identity Protection detects the risk events shown in the following table.



Time (hh:mm:ss)	User	Risk level
8:00:00	User2	Medium
8:00:00	User3	High
8:00:10	User1	Low
8:02:00	User1	Medium
8:02:04	User1	High
8:03:01	User2	Medium
8:03:01	User3	High
8:05:00	User1	High
8:10:00	User3	High
9:00:00	User2	High

How many alerts will User4 receive that include User1, and how many alerts will User4 receive that include User2 and User3? To answer, select the appropriate options in the answer area.

NOTE: Each correct selection is worth one point.

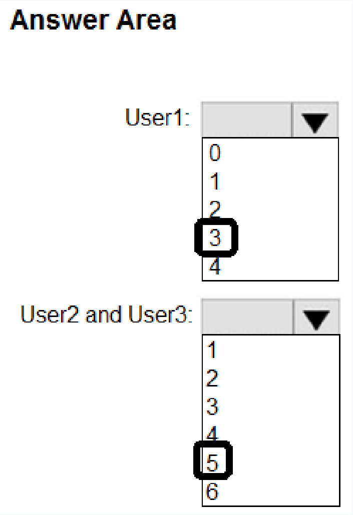


Answer Area

User1: 0, 1, 2, 3, 4

User2 and User3: 1, 2, 3, 4, 5, 6

Suggested Answer:



Answer Area

User1: 0, 1, 2, [✓ 3], 4

User2 and User3: 1, 2, 3, 4, [✓ 5], 6

darkschneider 1 year, 6 months ago

See https://learn.microsoft.com/en-us/azure/active-directory/identity-protection/howto-identity-protection-configure-notifications . Looks like there is a mechanism limiting the sending of alerts received less than 5 seconds from each other.

upvoted 1 times

Orion8575 1 year, 6 months ago

User1:4 , User2&3:6 it states you set Alert on user risk level "at" or "above to Low".

upvoted 1 times

Kodoi 1 year, 7 months ago

User1:3, User2&3:4

upvoted 4 times

> **Pkmn2901** 1 year, 6 months ago
>
> Why? Can you explain?
>
> upvoted 2 times
>
> > **tjitsen** 1 year, 6 months ago
> >
> > Kodio is right.
> > User1 : 3
> > User2&3 : 4
> >
> > Recalculations of the user risk level result in an email alert if the risk level matches the policy to send alerts (low and above in this case).
> > Even if the user risk level is the same as the previous level after recalculation, an alert will be send.
> > Alerts generated within a 5 second window, will be aggregated into one email.
> >
> > Reference: https://learn.microsoft.com/en-us/azure/active-directory/identity-protection/howto-identity-protection-configure-notifications#users-at-risk-detected-email
> >
> > upvoted 3 times
> >
> > > **Citmerian** 1 year, 6 months ago
> > >
> > > I'ts OK.
> > > User1 : 3
> > > User2&3 : 4
> > > Different users with 5 seconds between alarms, system only send one mail that include all users
> > >
> > > Exemple: user2 and user3 at 8:00 have and alarm but system only send one mail that include two users.
> > >
> > > upvoted 2 times
> > >
> > > > **Citmerian** 1 year, 6 months ago
> > > >
> > > > 5 or less seconds only one mail
> > > >
> > > > upvoted 1 times

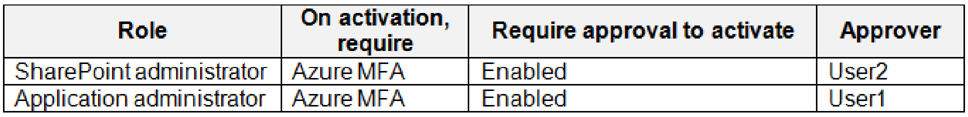
Question #95 *Topic 1*

HOTSPOT

-

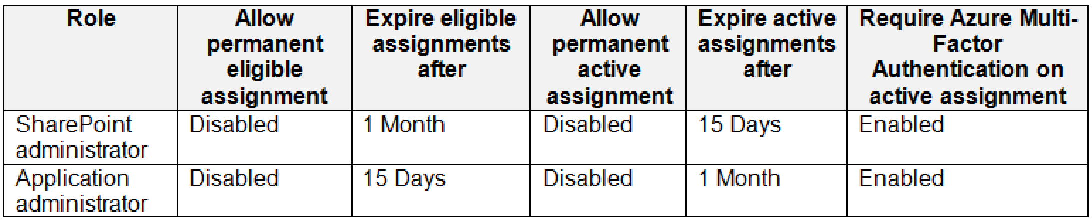
You have a Microsoft 365 subscription that uses Azure AD Privileged Identity Management (PIM).
You use PIM to manage access to the SharePoint administrator, the Application administrator, and the Global administrator roles.

The PIM Activation settings are configured as shown in the following table.



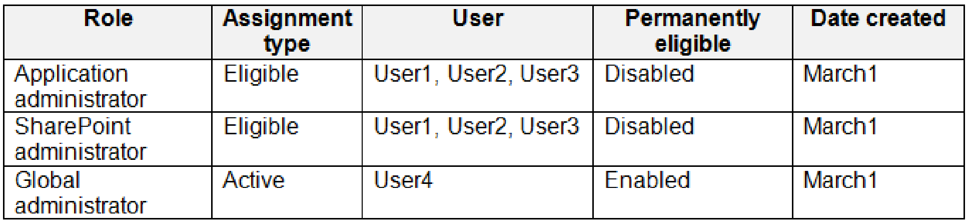
Role	On activation, require	Require approval to activate	Approver
SharePoint administrator	Azure MFA	Enabled	User2
Application administrator	Azure MFA	Enabled	User1

The PIM Assignment settings are configured as shown in the following table.



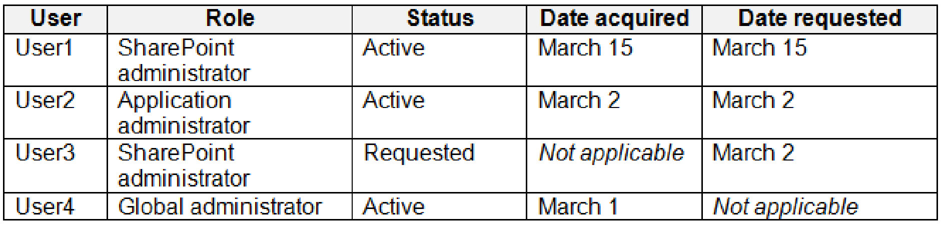
Role	Allow permanent eligible assignment	Expire eligible assignments after	Allow permanent active assignment	Expire active assignments after	Require Azure Multi-Factor Authentication on active assignment
SharePoint administrator	Disabled	1 Month	Disabled	15 Days	Enabled
Application administrator	Disabled	15 Days	Disabled	1 Month	Enabled

PIM has the role assignments shown in the following table.



Role	Assignment type	User	Permanently eligible	Date created
Application administrator	Eligible	User1, User2, User3	Disabled	March1
SharePoint administrator	Eligible	User1, User2, User3	Disabled	March1
Global administrator	Active	User4	Enabled	March1

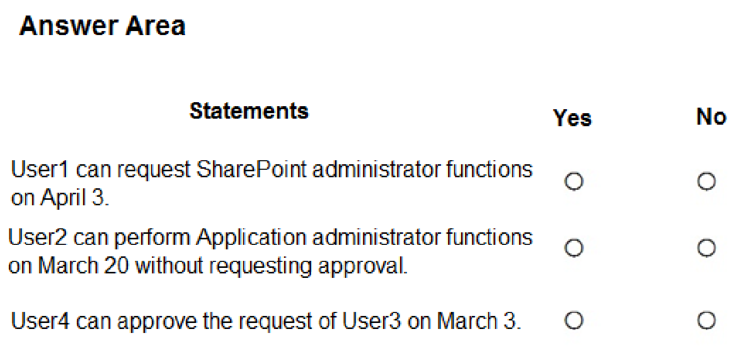
PIM has the user assignments shown in the following table.



User	Role	Status	Date acquired	Date requested
User1	SharePoint administrator	Active	March 15	March 15
User2	Application administrator	Active	March 2	March 2
User3	SharePoint administrator	Requested	*Not applicable*	March 2
User4	Global administrator	Active	March 1	*Not applicable*

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

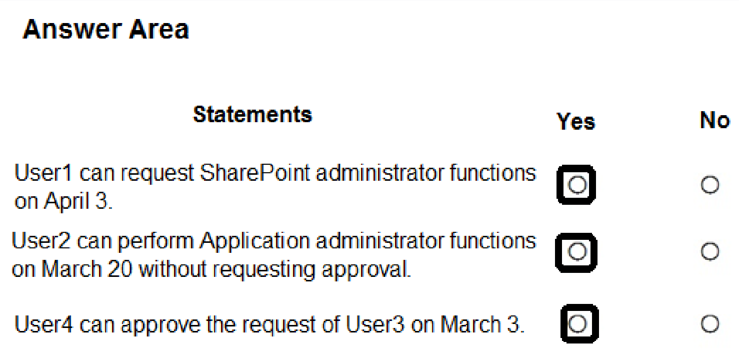
NOTE: Each correct selection is worth one point.



Answer Area

Statements	Yes	No
User1 can request SharePoint administrator functions on April 3.	○	○
User2 can perform Application administrator functions on March 20 without requesting approval.	○	○
User4 can approve the request of User3 on March 3.	○	○

Suggested Answer:



Answer Area

Statements	Yes	No
User1 can request SharePoint administrator functions on April 3.	[✓ ○]	○
User2 can perform Application administrator functions on March 20 without requesting approval.	[✓ ○]	○
User4 can approve the request of User3 on March 3.	[✓ ○]	○

KarimaMaf 1 year, 6 months ago

yes yes no

cause the user3 has an approver already set which is user2, if no approver set in this case global admin or privileged role administrator are the default approver

upvoted 4 times

Question #96 *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 contains a user named User1.

You need to ensure that User1 can review Conditional Access policies.

Solution: You assign User1 the Application Administrator role.

Does that meet the goal?

A. Yes

B. No

Suggested Answer: *B*

Community vote distribution

B (100%)

⊟ **Maxx4** 1 year, 6 months ago

Selected Answer: B

B. No

Assigning the Application Administrator role to User1 does not meet the goal of allowing User1 to review Conditional Access policies.

The Application Administrator role in Microsoft 365 primarily focuses on managing applications and their associated settings, such as configuring and managing Azure AD app registrations, managing application permissions, and handling application integrations. This role does not include specific permissions for reviewing or managing Conditional Access policies.

To allow User1 to review Conditional Access policies, you would need to assign them a role that specifically includes the necessary permissions for managing Conditional Access. The appropriate role for this requirement is the Conditional Access Administrator role. This role grants users the ability to create, view, and manage Conditional Access policies within the Microsoft 365 environment.

Therefore, assigning the Application Administrator role to User1 does not meet the goal of allowing them to review Conditional Access policies.
upvoted 1 times

Question #1 *Topic 2*

DRAG DROP -

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

You receive the following alerts:

✑ Suspected Netlogon privilege elevation attempt

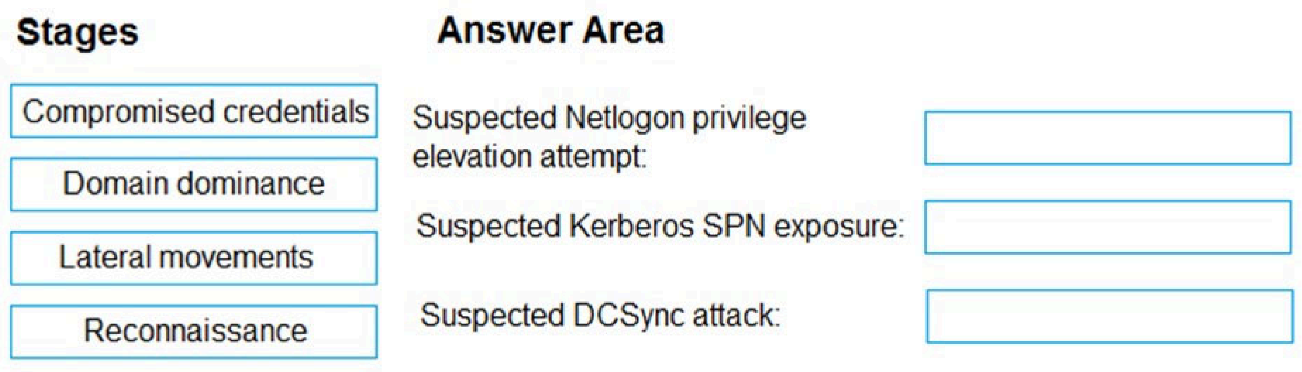
✑ Suspected Kerberos SPN exposure

✑ Suspected DCSync attack

To which stage of the cyber-attack kill chain does each alert map? To answer, drag the appropriate alerts to the correct stages. Each alert may be used once, more than once, or not at all. You may need to drag the split bar between panes or scroll to view content.

NOTE: Each correct selection is worth one point.

Select and Place:



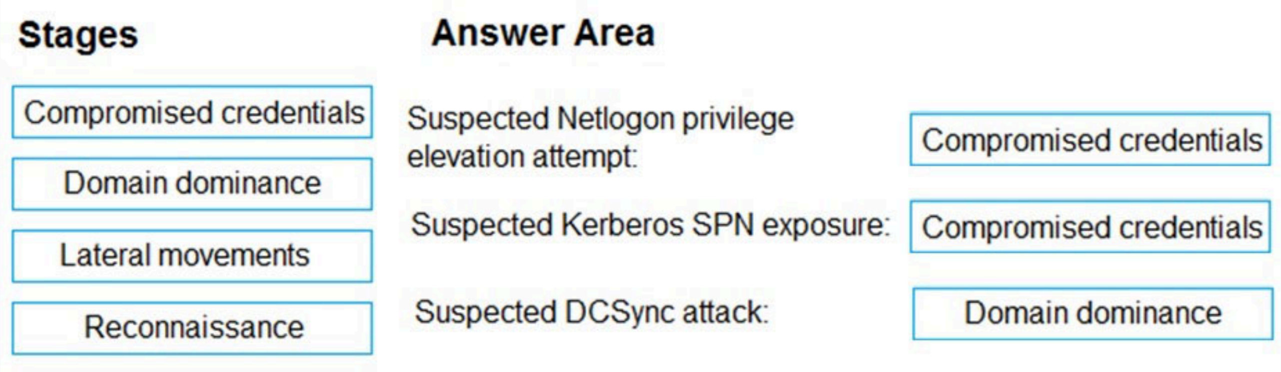
Stages

- Compromised credentials
- Domain dominance
- Lateral movements
- Reconnaissance

Answer Area

Suspected Netlogon privilege elevation attempt:	
Suspected Kerberos SPN exposure:	
Suspected DCSync attack:	

Suggested Answer:



Stages

- Compromised credentials
- Domain dominance
- Lateral movements
- Reconnaissance

Answer Area

Suspected Netlogon privilege elevation attempt:	Compromised credentials
Suspected Kerberos SPN exposure:	Compromised credentials
Suspected DCSync attack:	Domain dominance

Box 1: Compromised credential -

The following security alerts help you identify and remediate Compromised credential phase suspicious activities detected by Defender for Identity in your network.

In this tutorial, you'll learn how to understand, classify, remediate and prevent the following types of attacks:

Suspected Netlogon privilege elevation attempt (CVE-2020-1472 exploitation) (external ID 2411)

Suspected Kerberos SPN exposure (external ID 2410)

Etc.

Box 2: Compromised credential -

Box 3: Domain dominance -

The following security alerts help you identify and remediate Domain dominance phase suspicious activities detected by Defender for Identity in your network. In this tutorial, learn how to understand, classify, prevent, and remediate the following attacks:

Suspected DCSync attack (replication of directory services) (external ID 2006)

Etc.

Reference:

https://docs.microsoft.com/en-us/defender-for-identity/compromised-credentials-alerts https://docs.microsoft.com/en-us/defender-for-identity/domain-dominance-alerts

Tanasi 1 year, 7 months ago

Suspected Netlogon privilege elevation attempt is Privilege escalation, but we do not have that option so Compromised Credentials is better. See here:

https://learn.microsoft.com/en-us/defender-for-identity/alerts-overview

upvoted 1 times

Lomak 2 years, 2 months ago

Correct

https://learn.microsoft.com/en-us/defender-for-identity/alerts-overview

upvoted 3 times

pete26 2 years, 3 months ago

Answers appears to be correct.

Suspected DCSync attack (replication of directory services) (external ID 2006) is part of Domain Dominance.

Suspected Kerberos SPN exposure (external ID 2410) AND Suspected Netlogon privilege elevation attempt (CVE-2020-1472 exploitation) (external ID 2411) are part of Compromised credentials.

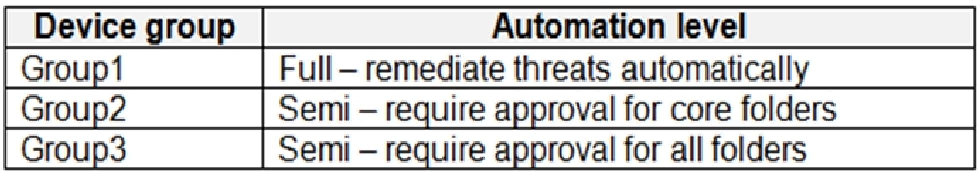
upvoted 3 times

Question #2 Topic 2

HOTSPOT -

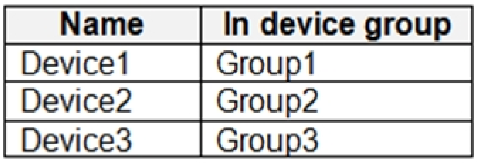
You have a Microsoft 365 subscription.

You configure Microsoft Defender for Endpoint as shown in the following table.



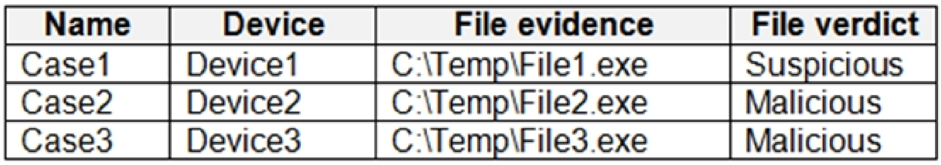
Device group	Automation level
Group1	Full – remediate threats automatically
Group2	Semi – require approval for core folders
Group3	Semi – require approval for all folders

You onboard devices to Microsoft Defender for Endpoint as shown in the following table.



Name	In device group
Device1	Group1
Device2	Group2
Device3	Group3

Microsoft Defender for Endpoint contains the incidents shown in the following table.

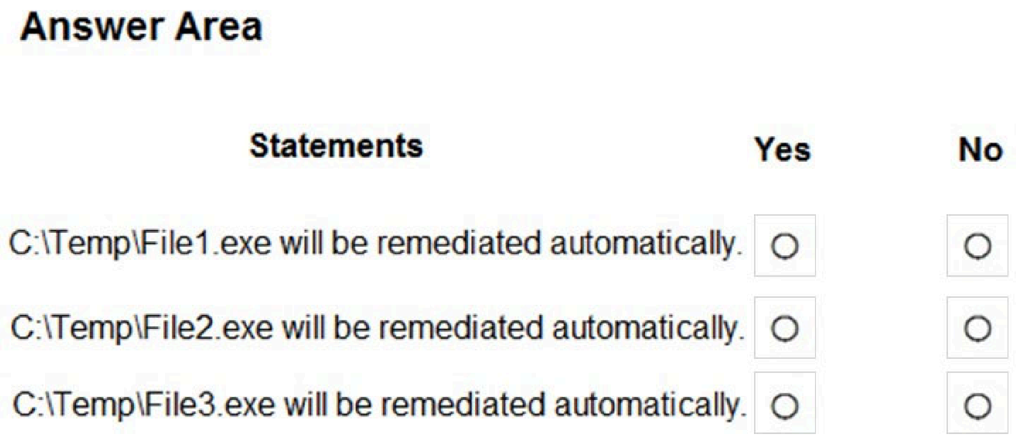


Name	Device	File evidence	File verdict
Case1	Device1	C:\Temp\File1.exe	Suspicious
Case2	Device2	C:\Temp\File2.exe	Malicious
Case3	Device3	C:\Temp\File3.exe	Malicious

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

NOTE: Each correct selection is worth one point.

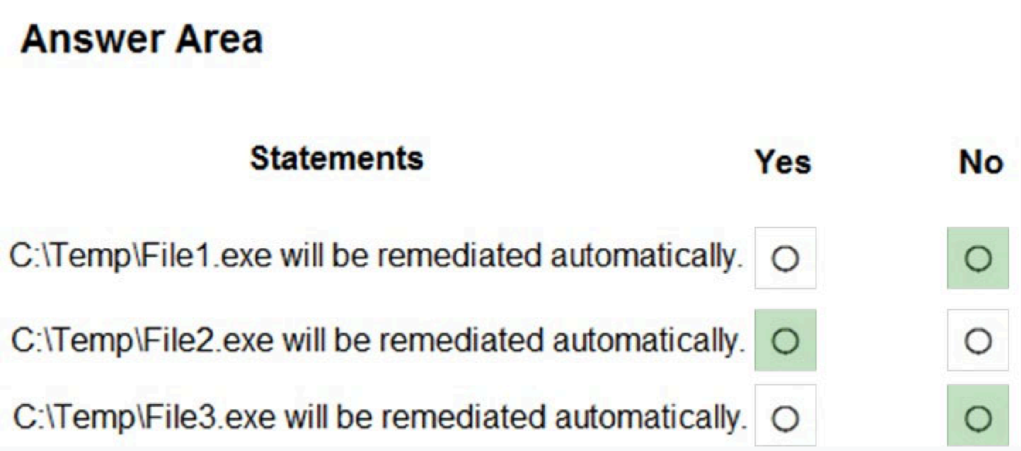
Hot Area:



Answer Area

Statements	Yes	No
C:\Temp\File1.exe will be remediated automatically.	○	○
C:\Temp\File2.exe will be remediated automatically.	○	○
C:\Temp\File3.exe will be remediated automatically.	○	○

Suggested Answer:



Answer Area

Statements	Yes	No
C:\Temp\File1.exe will be remediated automatically.	○	[✓ ○]
C:\Temp\File2.exe will be remediated automatically.	[✓ ○]	○
C:\Temp\File3.exe will be remediated automatically.	○	[✓ ○]

Box 1: No -

File1.exe on Device1 is suspicious. Device1 is in Group1. Group1 has automation level Full - remediate threats automatically.

Note: Full automation (recommended) means remediation actions are taken automatically on artifacts determined to be malicious.

Box 2: Yes -

File2 on Device2 is malicious. Device2 is in Group2. Group2 has automation level Semi - require approval for core folders.

Note: Semi-automation means some remediation actions are taken automatically, but other remediation actions await approval before

being taken.
Semi - require approval for core folders remediation:
With this level of semi-automation, approval is required for any remediation actions needed on files or executables that are in core folders.
Core folders include operating system directories, such as the Windows (\windows*).
Remediation actions can be taken automatically on files or executables that are in other (non-core) folders.

Box 3: No -
File3 on Device3 is malicious. Device3 is in Group3. Group3 has automation level Semi - require approval for all folders.
Reference:
https://docs.microsoft.com/en-us/microsoft-365/security/defender-endpoint/automation-levels

horseboxIRL Highly Voted 2 years, 1 month ago
N
Y
N

https://learn.microsoft.com/en-us/microsoft-365/security/defender-endpoint/manage-auto-investigation?view=o365-worldwide#review-completed-actions

Case 1: According to the doc - Full - remediate threats automatically: A verdict of Malicious is reached for a piece of evidence. This means the Suspicious file will not be auto-remediated.

Case 2: The file will be AR as it falls outside of the core folders.

Case 3: Approval for all folders.
upvoted 12 times

sarabjeet22 Most Recent 1 year, 7 months ago
N N N
https://learn.microsoft.com/en-us/microsoft-365/security/defender-endpoint/automation-levels?view=o365-worldwide
upvoted 2 times

tjitsen 1 year, 6 months ago
N Y N
Based on your same reference, my answer is N Y N
It states that C:\Temp is not considered a core folder, so automatic remediation in this case.
Reference: https://learn.microsoft.com/en-us/microsoft-365/security/defender-endpoint/automation-levels?view=o365-worldwide
upvoted 2 times

ChachaChatra 1 year, 11 months ago
Valid on28/01/23
upvoted 3 times

zik4 1 year, 11 months ago
Y-Y- N
upvoted 1 times

hans333 2 years ago
YYN,

@horseboxIRL, it also says: Appropriate remediation actions are taken automatically.
upvoted 1 times

tatdatpham 2 years, 2 months ago
I think the answer should be Y - Y - N
upvoted 2 times

billo79152718 2 years, 3 months ago
According to: https://docs.microsoft.com/en-us/microsoft-365/security/defender-endpoint/automation-levels?view=o365-worldwide
upvoted 3 times

billo79152718 2 years, 3 months ago

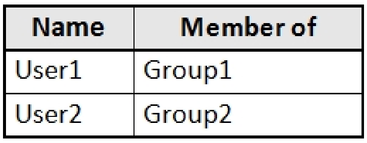
Correct!

upvoted 2 times

Question #3 *Topic 2*

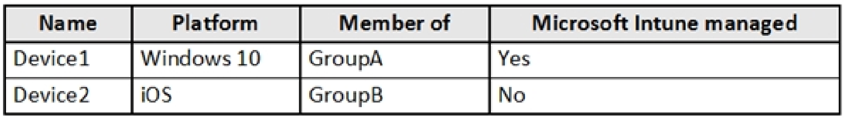
HOTSPOT -

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



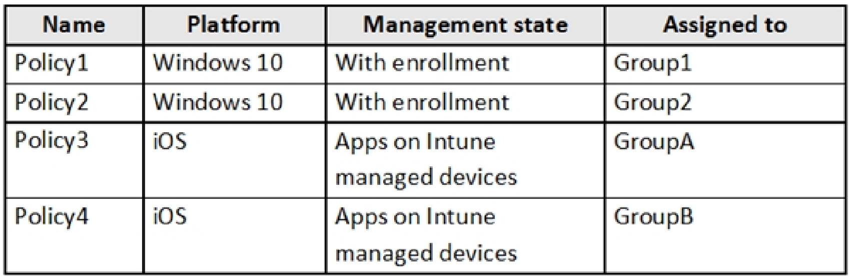
Name	Member of
User1	Group1
User2	Group2

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.

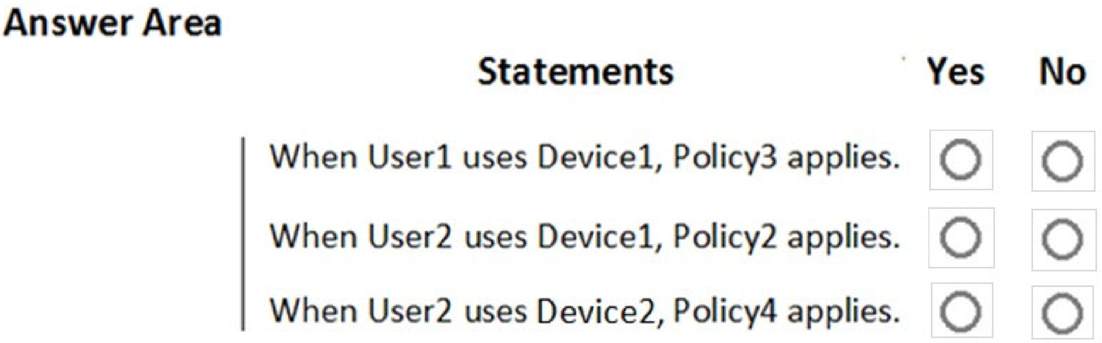


Name	Platform	Management state	Assigned to
Policy1	Windows 10	With enrollment	Group1
Policy2	Windows 10	With enrollment	Group2
Policy3	iOS	Apps on Intune managed devices	GroupA
Policy4	iOS	Apps on Intune managed devices	GroupB

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

NOTE: Each correct selection is worth one point.

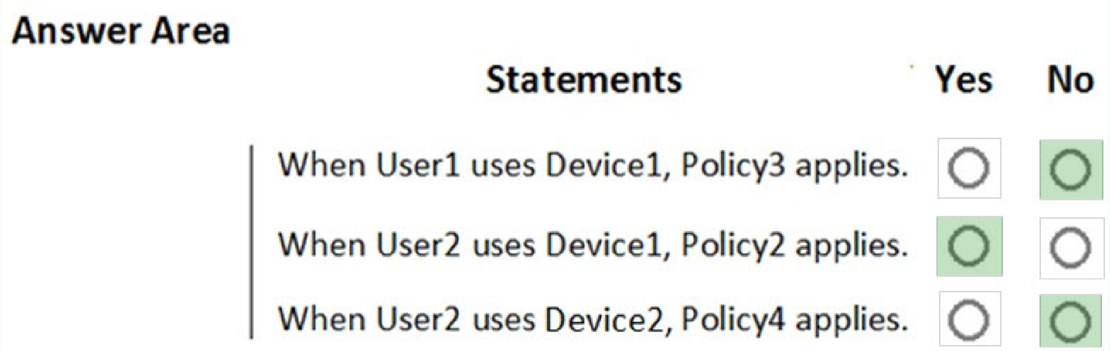
Hot Area:



Answer Area

Statements	Yes	No
When User1 uses Device1, Policy3 applies.	○	○
When User2 uses Device1, Policy2 applies.	○	○
When User2 uses Device2, Policy4 applies.	○	○

Suggested Answer:



Answer Area

Statements	Yes	No
When User1 uses Device1, Policy3 applies.	○	[✓ ○]
When User2 uses Device1, Policy2 applies.	[✓ ○]	○
When User2 uses Device2, Policy4 applies.	○	[✓ ○]

Reference:

https://docs.microsoft.com/en-us/intune/apps/app-protection-policy

DudleyYVR Highly Voted 3 years, 8 months ago

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

upvoted 29 times

kiketxu Highly Voted 3 years, 9 months ago

I would say here: NO, YES, "YES".

In the third, User2 w/Device2 matches with iOS Policy4 for GroupB.

upvoted 18 times

phatboi 2 years, 12 months ago

device 2 is not intune managed and the policy 4 is for intune app managed

upvoted 5 times

Jslei 3 years, 9 months ago

but Device2 is not intune managed?

upvoted 4 times

Sugar123 3 years, 9 months ago

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

upvoted 23 times

rkapoor8855 3 years, 9 months ago

Agreed

upvoted 5 times

kiketxu 3 years, 9 months ago

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

upvoted 11 times

cebularz 3 years, 6 months 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 years, 5 months 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 3 times

Wigoth Most Recent 1 year, 7 months ago

I go for NYN but in different way: user1->> GRP1 : GRP1->> POL1 = POL3 is not applied

user2->> GRP2 : GRP2->> POL2 = POL2 is applied

user2->> GRP2 : GRP2->> POL2 = POL4 is not applied

They don't ask if the devices are compliant or not but if the policies are applied or not

upvoted 1 times

Paul_white 1 year, 11 months ago

This question tests your understanding of app protection policies. App protection policies are applied to groups with users and not groups with devices. The device group is there as a distraction, you should only focus on the groups with users. This explains how app protection policies can protect organisation data on unmanaged/personal devices. The answer remains No Yes, No since the app protection policies are applied to the groups with the users and not groups with devices

upvoted 7 times

mcclane654 2 years ago

answer is correct, the managed state bugged me: https://learn.microsoft.com/en-us/mem/intune/apps/app-protection-policies?WT.mc_id=Portal-fx#target-app-protection-policies-based-on-device-management-state

upvoted 1 times

NarenKA 2 years, 4 months ago

Answer is: N Y N

Since Policy3 applies to iOS and Device1 is a Windows 10 device Policy3 does not apply.

Since User2 is a member of Group2 and Policy2 apply to Windows 10 devices, Policy2 applies to User2 on Device1.

User2 isn't a member of Group2 and since you need to have users as part of the protected group Policy4 does not apply to Device2 / User2.

upvoted 3 times

sliix 2 years, 8 months ago

Can anyone tell me what's the meaning of "Apps on intuned managed devices"?

upvoted 4 times

mkoprivnj 3 years, 1 month ago

N, Y, N

upvoted 6 times

⊟ **Nail** 3 years, 4 months ago

https://docs.microsoft.com/en-us/mem/intune/apps/quickstart-create-assign-app-policy

"App protection policies can only be applied to groups that contains users, not groups that contain devices."

upvoted 4 times

⊟ **theboywonder** 3 years, 6 months ago

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

upvoted 1 times

⊟ **Robert__Susin** 3 years, 5 months 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 6 times

⊟ **prats005** 3 years, 9 months ago

which one is correct?

upvoted 1 times

⊟ **w00t** 3 years, 9 months ago

Answer is correct:

Yes, No, Yes.

upvoted 1 times

Question #4 *Topic 2*

DRAG DROP -

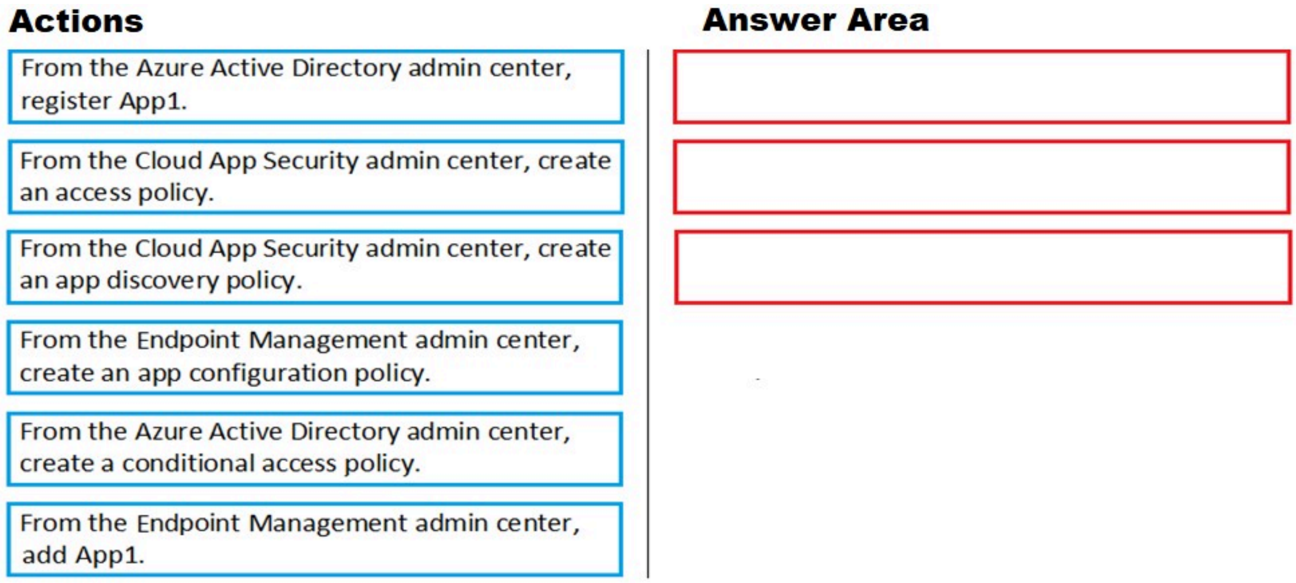
You have a Microsoft 365 subscription that uses an Azure Active Directory (Azure AD) tenant named contoso.com. All the devices in the tenant are managed by using Microsoft Endpoint Manager.

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:

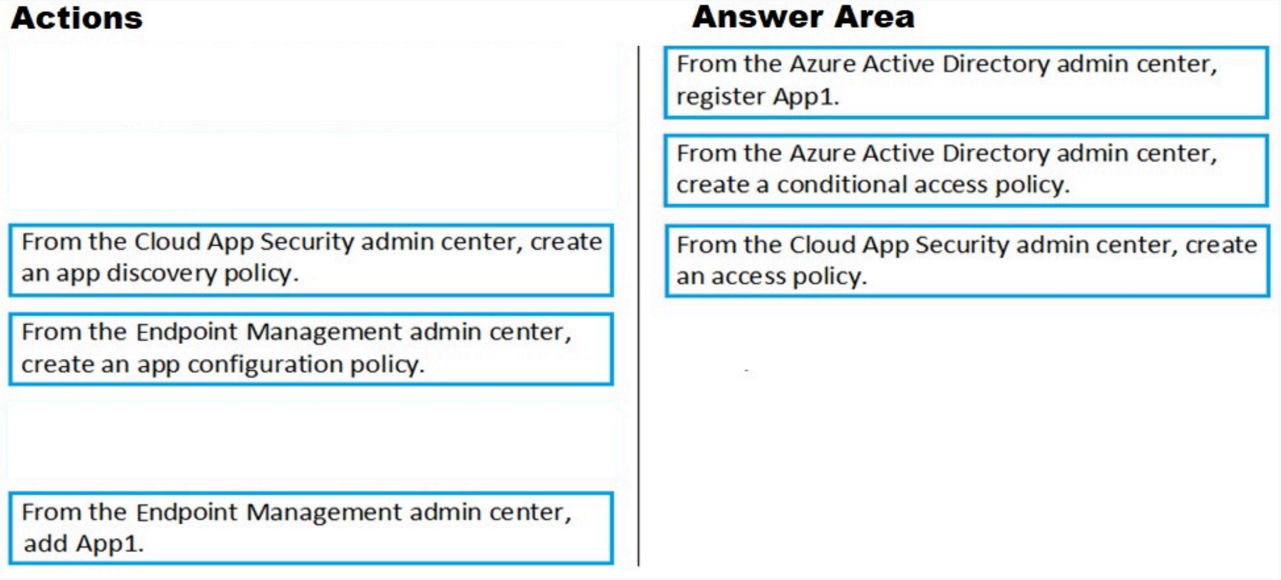


Actions

- From the Azure Active Directory admin center, register App1.
- From the Cloud App Security admin center, create an access policy.
- From the Cloud App Security admin center, create an app discovery policy.
- From the Endpoint Management admin center, create an app configuration policy.
- From the Azure Active Directory admin center, create a conditional access policy.
- From the Endpoint Management admin center, add App1.

Answer Area

Suggested Answer:



Actions

- From the Cloud App Security admin center, create an app discovery policy.
- From the Endpoint Management admin center, create an app configuration policy.
- From the Endpoint Management admin center, add App1.

Answer Area

1. From the Azure Active Directory admin center, register App1.
2. From the Azure Active Directory admin center, create a conditional access policy.
3. From the Cloud App Security admin center, create an access policy.

Reference:

https://docs.microsoft.com/en-us/cloud-app-security/access-policy-aad

DarkAndy Highly Voted 2 years, 6 months ago

Valid on exam. Jun 10, 2022

upvoted 11 times

WMG Highly Voted 3 years, 4 months ago

Answer is correct. Register App, configure CA policy for it, then review.

"access policies enable real-time monitoring and control over access to cloud apps based on user, location, device, and app."

ref:

https://docs.microsoft.com/en-us/cloud-app-security/access-policy-aad

upvoted 9 times

⊟ **mcclane654** Most Recent 1 year, 11 months ago

correct: https://learn.microsoft.com/en-us/defender-cloud-apps/proxy-deployment-aad

upvoted 1 times

⊟ **pete26** 2 years, 2 months ago

Valid on exam October 14, 2022

upvoted 2 times

⊟ **mkoprivnj** 3 years, 1 month ago

1,2,3 is correct! Register App, configure CA policy for it, then access review.

upvoted 3 times

⊟ **Sido1** 3 years, 9 months ago

correct

upvoted 4 times

⊟ **kiketxu** 3 years, 9 months ago

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

upvoted 10 times

Question #5 *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

Suggested Answer: *A*
In order to view and use the reports described in this article, you need to be a member of one of the following role groups in the Microsoft 365 Defender portal:
✑ Organization Management
✑ Security Administrator
✑ Security Reader
✑ Global Reader
Note:
There are several versions of this question in the exam. The question has two possible correct answers:
1. Security Administrator
2. Security Reader
Other incorrect answer options you may see on the exam include the following:
✑ Message center reader
✑ Service administrator
Reference:
https://docs.microsoft.com/en-us/microsoft-365/security/office-365-security/view-reports-for-mdo

Community vote distribution

A (100%)

⊟ **mkoprivnj** Highly Voted 👍 3 years, 1 month ago

Selected Answer: A

A is correct!

upvoted 7 times

⊟ **Maxx4** Most Recent 🕒 1 year, 6 months ago

The correct answer is A. Security reader.

To allow User1 to view Microsoft Defender for Office 365 reports in the Threat management dashboard, you should assign them the Security reader role.

The Security reader role provides users with read-only access to security-related features and settings in Microsoft 365. This role specifically includes permissions to view reports, including those in Microsoft Defender for Office 365. By assigning User1 the Security reader role, they will have the necessary permissions to access and review the reports in the Threat management dashboard.

upvoted 1 times

⊟ **Maxx4** 1 year, 6 months ago

The Compliance administrator role (option B) is focused on managing compliance-related features and settings, such as data retention, eDiscovery, and information protection. It does not directly grant permissions to view Defender for Office 365 reports.

The Information Protection administrator role (option C) is responsible for managing information protection and data classification features. While it may have some relevant permissions, it does not specifically provide access to view Defender for Office 365 reports.

The Exchange administrator role (option D) primarily focuses on managing Exchange Online features and settings. While it may have access to certain security-related configurations, it does not grant direct permissions to view Defender for Office 365 reports.

upvoted 1 times

⊟ **tempfreetenm** 2 years, 7 months ago

Information Protection administrator is a certification, it's not an existing role.

upvoted 1 times

⊟ **arska** 2 years, 9 months ago

Selected Answer: A

Security reader

upvoted 4 times

⊟ **webhav** 3 years, 5 months ago

"view" is the keyword

upvoted 4 times

⊟ **ZakS** 3 years, 7 months ago

Correct - Security Reader

upvoted 3 times

Question #6 *Topic 2*

You have a Microsoft 365 Enterprise E5 subscription.
You use Microsoft Defender for Endpoint.
You plan to use Microsoft 365 Attack simulator.
What is a prerequisite for running Attack simulator?

A. Enable multi-factor authentication (MFA).

B. Configure Microsoft Defender for Office 365.

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

D. Integrate Microsoft 365 Threat Intelligence and Microsoft Defender for Endpoint.

Suggested Answer: *A*
Reference:
https://docs.microsoft.com/en-us/office365/securitycompliance/attack-simulator

Community vote distribution
A (56%) D (33%) 11%

⊟ **zerrowall** Highly Voted 👍 2 years ago
There are two different MS 365 Attack Simulators. The first one was retired. The new version is called "Defender for Office 365 Attack simulation training". Probably some questions are about the previous version and are not appropriate for the new version. For example, I didn't find the requirements for MFA for the new version.
upvoted 6 times

⊟ **JoeP1** 1 year, 10 months ago
I see a number of 2018 references to the attack simulator that list MFA as a requirement. I do not see any for the new version.
upvoted 1 times

⊟ **Daniel830** Highly Voted 👍 2 years, 3 months ago
Selected Answer: D
I think It's D.

"If your organization has Microsoft 365 E5 or Microsoft Defender for Office 365 Plan 2, which includes Threat Investigation and Response capabilities, you can use Attack simulation training in the Microsoft 365 Defender portal"

See reference link: https://learn.microsoft.com/en-us/microsoft-365/security/office-365-security/attack-simulation-training-get-started?view=o365-worldwide
upvoted 5 times

⊟ **PhyMac** 2 years ago
I cannot find any mention of Defender for endpoint in the URL you indicated.
Defender for office 365(B) is the correct answer.
upvoted 3 times

⊟ **Tanasi** 1 year, 7 months ago
I run this on a tenant and this integration was not done. So it's not D
upvoted 1 times

⊟ **Maxx4** Most Recent ⊙ 1 year, 6 months ago
Selected Answer: D
The correct answer is D. Integrate Microsoft 365 Threat Intelligence and Microsoft Defender for Endpoint.

To run the Microsoft 365 Attack simulator, a prerequisite is to integrate Microsoft 365 Threat Intelligence and Microsoft Defender for Endpoint.

Microsoft 365 Threat Intelligence provides insights into global attack trends and threat intelligence data, while Microsoft Defender for Endpoint offers endpoint protection and threat detection capabilities. By integrating these two services, you can enhance your security posture and leverage the full functionality of the Attack simulator.

The Attack simulator allows you to simulate real-world attack scenarios to assess your organization's security defenses and identify potential vulnerabilities. It helps you evaluate the effectiveness of your security controls, educate users about potential threats, and improve your overall security readiness.

upvoted 1 times

Maxx4 1 year, 6 months ago

Enabling multi-factor authentication (MFA) (option A) is a recommended security practice but not a prerequisite specifically for running the Attack simulator.

Configuring Microsoft Defender for Office 365 (option B) and creating a Conditional Access App Control policy for accessing Microsoft 365 (option C) are not prerequisites for running the Attack simulator. These are separate configurations related to securing Office 365 applications and implementing access controls.

Therefore, the correct prerequisite for running the Microsoft 365 Attack simulator is option D, integrating Microsoft 365 Threat Intelligence and Microsoft Defender for Endpoint.

upvoted 1 times

RomanV 1 year, 8 months ago

Enabling multi-factor authentication (MFA), configuring Microsoft Defender for Office 365, or creating a Conditional Access App Control policy for accessing Microsoft 365 are not prerequisites for running Attack simulator, although they may be important security measures to implement in your environment.

Correct answer is D. Integrate Microsoft 365 Threat Intelligence and Microsoft Defender for Endpoint.

upvoted 3 times

Tanasi 1 year, 7 months ago

I was able to run the Attack simulator without the integration.

I think the question is just outdated and it probably wanted option A.

upvoted 1 times

GatesBill 1 year, 9 months ago

https://learn.microsoft.com/en-us/microsoft-365/security/office-365-security/attack-simulation-training-get-started?view=o365-worldwide#what-do-you-need-to-know-before-you-begin

- MFA is not listed as a requirement as it was before
- You'll use MDO for sure, but what do they mean by "Configuring"?
- No policy or whatsoever is needed
- Attack Simulation training falls under MDO and not MDE, so acquiring MDE licenses is not necessary at all

So guessing "configure" just means utilizing it; the correct answer would be B for the newer version of Attack Simulation...

upvoted 1 times

chickenroaster 1 year, 10 months ago

Selected Answer: A

MFA is required.

upvoted 1 times

amymay101 1 year, 11 months ago

Selected Answer: B

pre-req should be to config this in Defender for Office 365. Can find any reference to MFA as a pre-req

upvoted 1 times

shouro88 1 year, 11 months ago

An attack simulation is platform independent. What you are saying does not make any sense, please do not guess.

upvoted 2 times

zerrowall 2 years ago

Selected Answer: B

B

I think Defender for office 365 is the correct answer

upvoted 1 times

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

Very strange question.

It is correct that the admin account doing the simulation needs MFA enabled, but not the users who are targeted by the campaign. But anwer D can also be correct as you dont know which plan the company has. If they have E 5 licenses, then the correct answer is A, but if they have E3 for example, you need to include Threat Investigation and Response capabilities

upvoted 1 times

⊟ **Acbrownit** 2 years, 2 months ago

Question states it has e5 licenses, so that is a moot point.

upvoted 1 times

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

Selected Answer: A

https://connectioncloudsupport.zendesk.com/hc/en-us/articles/4403047001881-Introduction-to-Attack-Simulator-in-Microsoft-365. Read step 2!

upvoted 3 times

⊟ **Errr** 2 years, 3 months ago

Selected Answer: A

https://github.com/MicrosoftDocs/OfficeDocs-o365seccomp/issues/439

upvoted 2 times

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

I ALSO THINK ITS d

upvoted 2 times

⊟ **pete26** 2 years, 3 months ago

Selected Answer: A

100% A.

upvoted 4 times

Question #7 *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.
What should you do first?

A. From the Microsoft Defender for Identity portal, 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.

Suggested Answer: *C*
Reference:
https://docs.microsoft.com/en-us/office365/securitycompliance/attack-simulator

Community vote distribution
C (69%) D (31%)

pete26 Highly Voted 👍 2 years, 3 months ago
There is no correct answer here. You need MFA for the account you will be doing the simulation with.
upvoted 9 times

jeff1988 Highly Voted 👍 2 years, 3 months ago
Selected Answer: C
becuase the research group has alraedy an exchange online mailbox and you are only targetng the research department so you need to activate mfa for the research deparment
upvoted 7 times

Maxx4 Most Recent ⊙ 1 year, 6 months ago
Selected Answer: C
To model a spear-phishing attack that targets the Research group members using the Microsoft Office 365 Attack simulator, the first step you should take is:

C. Enable MFA for the Research group members.

Enabling multi-factor authentication (MFA) for the Research group members adds an extra layer of security to their mailbox accounts and helps protect against unauthorized access, including potential spear-phishing attacks. By enabling MFA, users are required to provide additional verification, such as a code sent to their mobile device or biometric authentication, when signing in to their accounts.

Before running the Attack simulator, it's important to ensure that the target users, in this case, the members of the Research group, have MFA enabled. This step enhances their security posture and helps evaluate the effectiveness of their MFA implementation in defending against spear-phishing attacks.
upvoted 1 times

chickenroaster 1 year, 10 months ago
Selected Answer: C
All others are wrong
upvoted 1 times

ChachaChatra 1 year, 11 months ago
Valid on28/01/23
upvoted 2 times

ariania 2 years, 3 months ago
C
Because a spearphising campaign. You want them to not only enter the creds, but MFA aswell. MFA is part of Speaphising built in campaign.
upvoted 4 times

chickenroaster 1 year, 10 months ago

MITM attacks trick the user into believing he is connecting to a real website when he is in fact providing his credentials to a fake, lookalike site. The trigger to the connection to the fake login is very often the result of spear-phishing campaigns. MITM attacks can bypass MFA protections because the credentials entered in the fake site are passed on automatically by the hackers into the real one. Any MFA authentication request will also unwittingly be passed on to the hackers. https://www.mantra.ms/blog/beating-mfa

upvoted 1 times

Broesweelies 2 years, 3 months ago

There is literally no correct answer for this.

MFA is only required for the admin when he wants to launch a campaign, not required for the users.

Attack simulator is only for the research group so no point in changing the exec mailboxes.

The rest of the answers is also incorrect...

Maybe this is an old question?

https://learn.microsoft.com/en-us/microsoft-365/security/office-365-security/attack-simulation-training-get-started?view=o365-worldwide

upvoted 5 times

mhzayt 2 years, 3 months ago

Selected Answer: D

The right answer is D. Attack Simulator can only be used for mailboxes in Exchange Online.

upvoted 4 times

EaaGleee 2 years, 3 months ago

The attack simulator is done on Reasearch group which is online. So C ?

upvoted 5 times

Question #8 *Topic 2*

You have a Microsoft 365 E5 subscription.

You implement Microsoft Defender for Office 365 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?

A. Set the action to Block

B. Add an exception

C. Add a condition

D. Set the action to Dynamic Delivery

Suggested Answer: *D*

Reference:

https://docs.microsoft.com/en-us/office365/securitycompliance/dynamic-delivery-and-previewing

Community vote distribution

D (100%)

⊟ **pete26** Highly Voted 👍 2 years, 3 months ago

Selected Answer: D

D is correct!

upvoted 7 times

⊟ **Maxx4** Most Recent ⊙ 1 year, 6 months ago

Selected Answer: D

To reduce the amount of time it takes to receive email messages that contain attachments while ensuring that all attachments are scanned for malware and blocking any attachments that have malware, you should:

D. Set the action to Dynamic Delivery.

By setting the action to Dynamic Delivery in the Microsoft Defender for Office 365 safe attachments policies, you can optimize the delivery process for email messages with attachments. Dynamic Delivery allows the email message to be delivered to the recipient's mailbox immediately, while the attachment is being scanned in the background. This way, users can access and read the email message without delay, even before the attachment scanning is completed.

upvoted 1 times

⊟ **heshmat2022** 1 year, 7 months ago

Introduction to Attack Simulator in Microsoft 365

1. Are you missing Attack Simulator? Attack Simulator requires Microsoft Defender for Office 365 Plan 2 or Office 365 Enterprise E5. Attack Simulator is not included in Microsoft Defender for Office 365 Plan 1, Office 365 Enterprise E3, or any Microsoft 365 Apps for business subscriptions.

2. The account you use to launch simulated attacks requires global administrator or security administrator permissions and multi-factor authentication (MFA). For more information about Attack Simulator requirements, see this topic. So A is the right answer.

upvoted 1 times

⊟ **Dinraj** 2 years, 3 months ago

Selected Answer: D

D is correct Answer

upvoted 3 times

Question #9 *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.

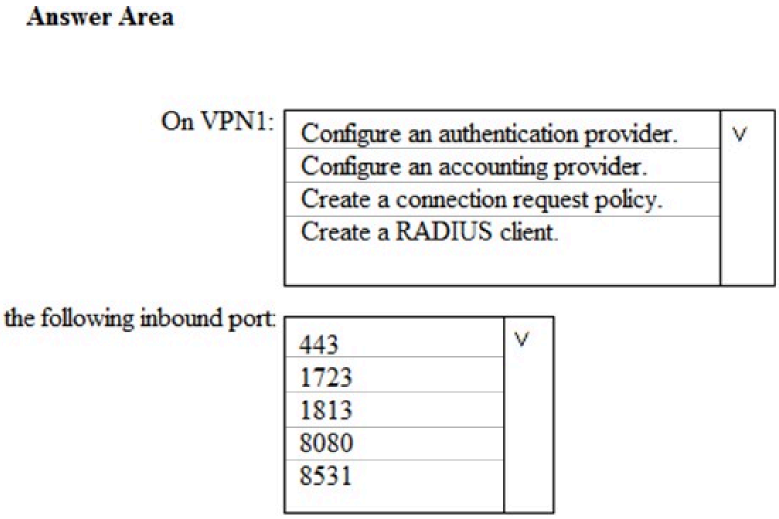
You install a Microsoft Defender for Identity standalone sensor on a server named Server1 that runs Windows Server 2016.

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:

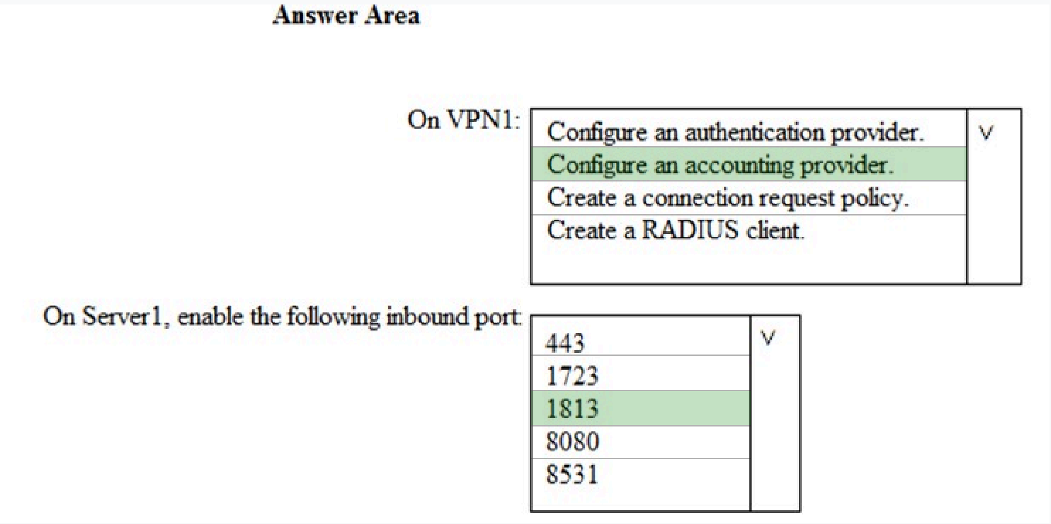


Answer Area

On VPN1:
- Configure an authentication provider.
- Configure an accounting provider.
- Create a connection request policy.
- Create a RADIUS client.

On Server1, enable the following inbound port:
- 443
- 1723
- 1813
- 8080
- 8531

Suggested Answer:



Answer Area

On VPN1:
- Configure an authentication provider.
- [✓ Configure an accounting provider.]
- Create a connection request policy.
- Create a RADIUS client.

On Server1, enable the following inbound port:
- 443
- 1723
- [✓ 1813]
- 8080
- 8531

Reference:

https://docs.microsoft.com/en-us/azure-advanced-threat-protection/install-atp-step6-vpn

Jamesbchz Highly Voted 3 years, 4 months ago

What the piss. I'm just gonna have to hope this stays in my brain somewhere for the test.

upvoted 57 times

Grudo 2 years, 11 months ago

Are you suggesting you have yet to deploy a Microsoft Defender for Identity solution for your Windows Server VPN?

upvoted 11 times

Ivkopivko12tka 2 years, 1 month ago

:-D ;-)

upvoted 1 times

WMG Highly Voted 3 years, 4 months ago

Defender for Identity only supports Radius events , and the default port is 1813. The only two things you need to remember.

upvoted 7 times

⊟ **horseboxIRL** Most Recent 2 years, 1 month ago

This is still on the exam as of 02 December 2022.

upvoted 3 times

⊟ **heshmat2022** 2 years, 3 months ago

In the Add RADIUS Server window, type the Server name of the closest Defender for Identity sensor (which has network connectivity). For high availability, you can add additional Defender for Identity sensors as RADIUS Servers. Under Port, make sure the default of 1813 is configured. Select Change and type a new shared secret string of alphanumeric characters. Take note of the new shared secret string as you'll need to fill it out later during Defender for Identity Configuration. Check the Send RADIUS Account On and Accounting Off messages box and select OK on all open dialog boxes.

upvoted 2 times

⊟ **NarenKA** 2 years, 4 months ago

The given answer is correct.

Three steps are required to set up VPN monitoring using Defender for Identity

1. Configure RADIUS Accounting on VPN1
2. Enable VPN / RADIUS Accounts in Defender for Identity
3. Enable inbound port 1813 on Server1

upvoted 6 times

⊟ **mkoprivnj** 3 years, 1 month ago

1st: configure an accounting provider

2nd: 1813

upvoted 7 times

⊟ **yoton** 1 year, 11 months ago

This does not help or contribute to the conversation.

upvoted 5 times

⊟ **Cepheid** 3 years, 1 month ago

So what do we need to do on VPN1? Is it RADIUS?

upvoted 1 times

⊟ **iwikneerg** 3 years, 7 months ago

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

upvoted 3 times

⊟ **arunjana** 3 years, 7 months ago

Given answer is correct.

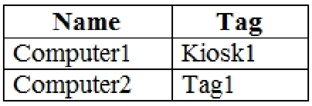
https://docs.microsoft.com/en-us/defender-for-identity/install-step6-vpn

upvoted 3 times

Question #10 | *Topic 2*

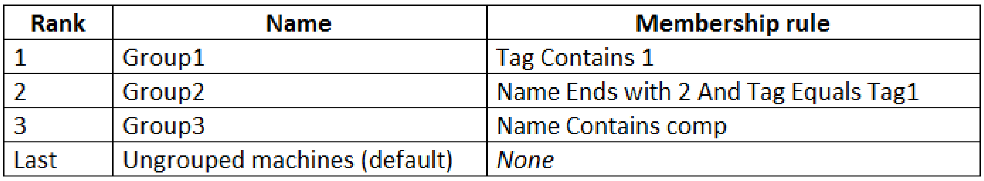
HOTSPOT -

You have a Microsoft Defender for Endpoint deployment that has the custom network indicators turned on. Microsoft Defender for Endpoint protects two computers that run Windows 10 as shown in the following table.



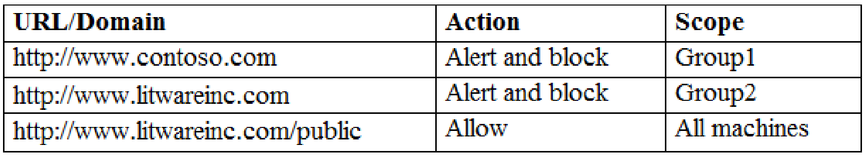
Name	Tag
Computer1	Kiosk1
Computer2	Tag1

Microsoft Defender for Endpoint has the device 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 turn on custom network indicators and create the URLs/Domain indicators shown in the following table.

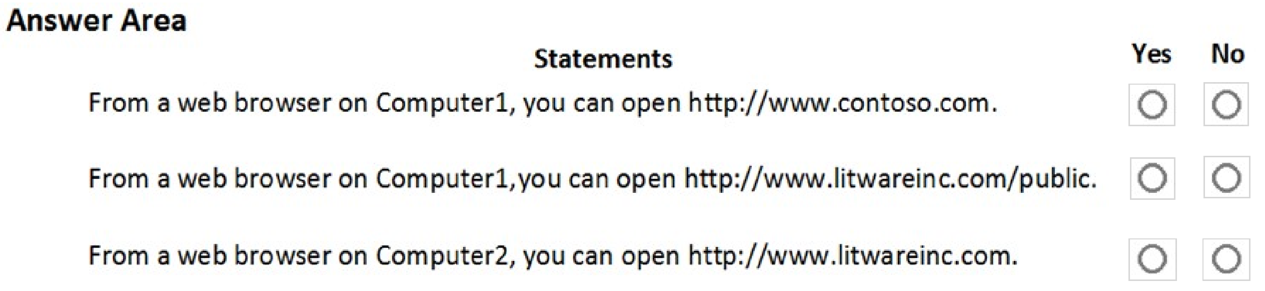


URL/Domain	Action	Scope
http://www.contoso.com	Alert and block	Group1
http://www.litwareinc.com	Alert and block	Group2
http://www.litwareinc.com/public	Allow	All machines

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

NOTE: Each correct selection is worth one point.

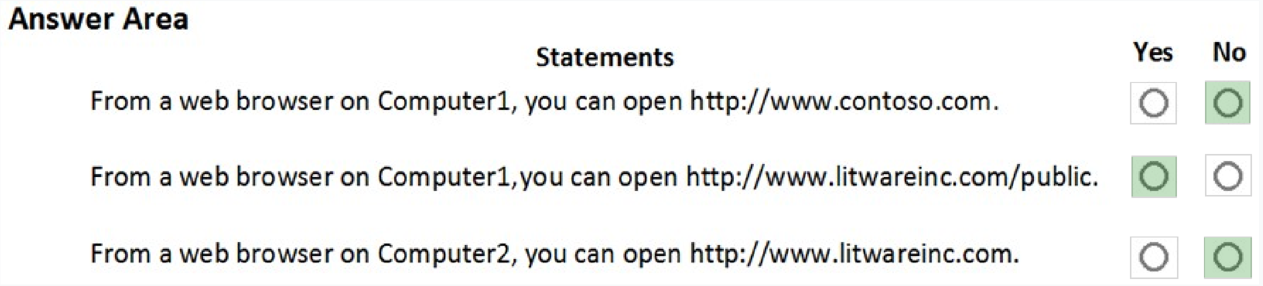
Hot Area:



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.	○	○

Suggested Answer:



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.	○	[✓ ○]

Dinraj Highly Voted 2 years, 3 months ago

Question is confusing, As per Rank condition both computer will be Group1, because Tag contains 1 and Rank is 1st, which is match higher rank and it will be assigned to that policy.

so Ans would be - N,Y<Y

upvoted 25 times

Tanasi 1 year, 10 months ago

You are correct.

upvoted 1 times

skycrap 2 years, 3 months ago

Agree with you.

upvoted 4 times

Sekoume 2 years, 3 months ago

True : "If a device is also matched to other groups, it's added only to the highest ranked device group." https://learn.microsoft.com/en-us/microsoft-365/security/defender-endpoint/machine-groups?view=o365-worldwide

upvoted 2 times

⊟ **Daniel830** Highly Voted 2 years, 3 months ago

It's N:Y:Y.

1. Computer1 is in Group 1 so It can't access the website --> N
2. All computers are allowed to access that site --> Y
3. Computer2 not a member of Group 2, so It has access to the website --> Y

upvoted 11 times

⊟ **Okadorium** Most Recent 1 year, 6 months ago

Agree with Daniel830. N:Y:Y

upvoted 1 times

⊟ **Perycles** 1 year, 8 months ago

2 computers are in group 1 because their tags match with "contains 1". so answers are N Y Y.

upvoted 2 times

⊟ **fuduran** 1 year, 12 months ago

Both computers are members of Group 1 only, NYY are the answers

upvoted 3 times

⊟ **tatdatpham** 2 years, 1 month ago

1. N
2.Y
3. Group 2: Name ends with 2 and tag equal Tag1, so Computer 2 in Group 2. Correct?
So my answer is N

upvoted 2 times

⊟ **kimble3k** 1 year, 12 months ago

Not correct, because: As per Rank condition both computer will be Group1, because Tag contains 1 and Rank is 1st, which is match higher rank and it will be assigned to that policy

upvoted 2 times

⊟ **kimble3k** 1 year, 11 months ago

Actually, forget my last post, I agree with you =D

upvoted 1 times

⊟ **Daniel830** 2 years, 3 months ago

Also, in the Group 2 description there is 'AND' operator, with means that both the conditions must be followed in order to be member of that group.

upvoted 2 times

⊟ **Sekoume** 2 years, 3 months ago

both conditions are met no ?

upvoted 1 times

⊟ **Lomak** 2 years, 2 months ago

but then out-ranked by Tag = Kiosk1

upvoted 2 times

Question #11 *Topic 2*

SIMULATION -

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

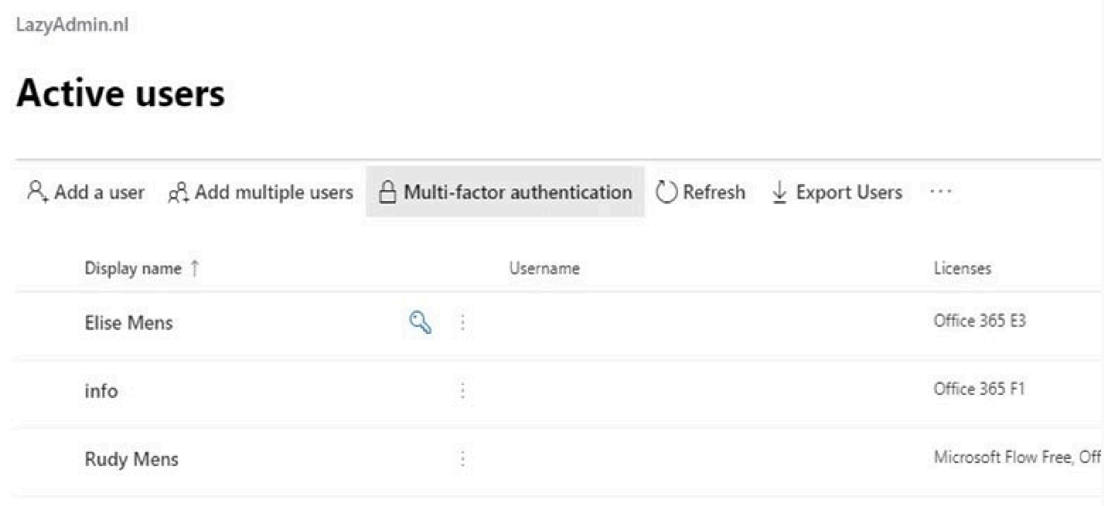
To complete this task, sign in to the Microsoft 365 admin center.

Suggested Answer: *See explanation below.*

1. Open the Admin Center and go to Users > Active Users

2. Open Multi-factor authentication

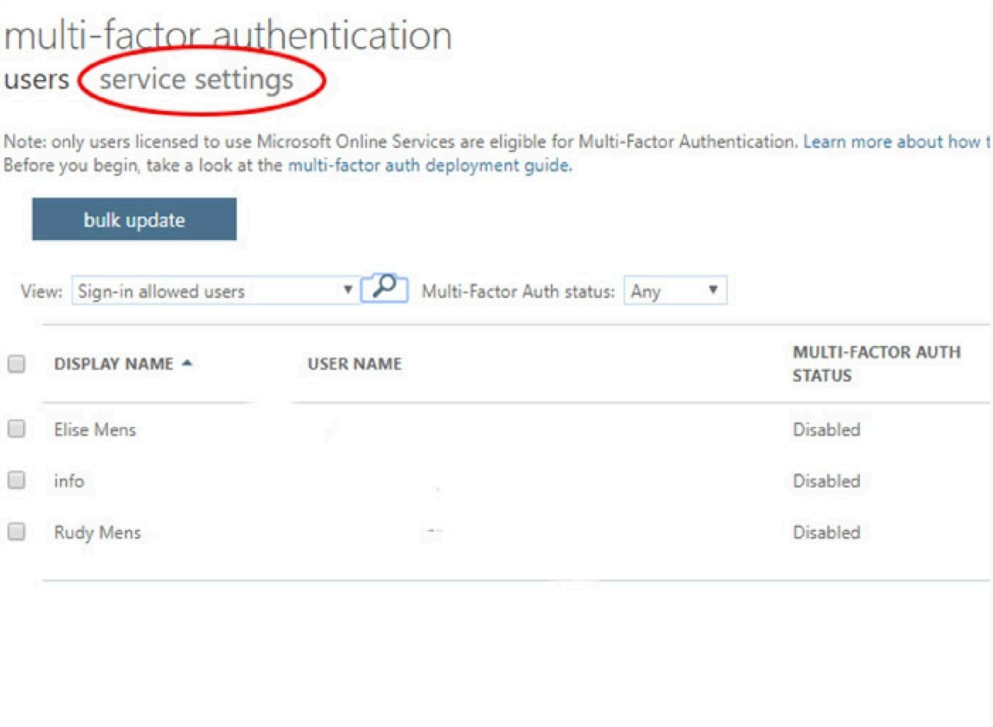
Don't select any user yet, just open the Multi-factor authentication screen. You will find the button in the toolbar.



Display name ↑	Username	Licenses
Elise Mens		Office 365 E3
info		Office 365 F1
Rudy Mens		Microsoft Flow Free, Off

3. Open the Service settings

Before we start enabling MFA for the users, we first go through the service settings. The button to the settings screen doesn't stand out, but it's just below the title



Note: only users licensed to use Microsoft Online Services are eligible for Multi-Factor Authentication. Learn more about how t
Before you begin, take a look at the multi-factor auth deployment guide.

View: Sign-in allowed users ▾ Multi-Factor Auth status: Any ▾

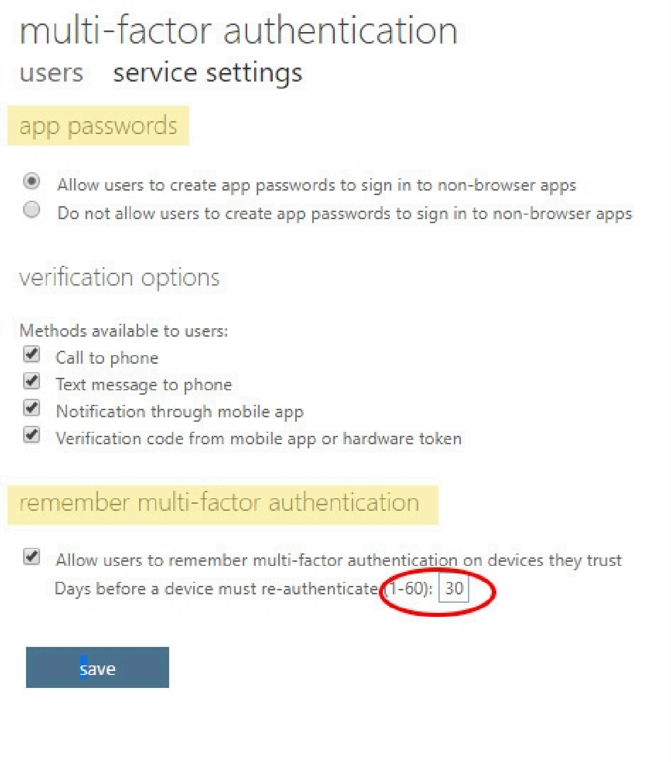
	DISPLAY NAME ▲	USER NAME	MULTI-FACTOR AUTH STATUS
□	Elise Mens		Disabled
□	info		Disabled
□	Rudy Mens		Disabled

4. Setup MFA Office 365

A few settings are important here:

➯ Make sure you check the App password. Otherwise, users can't authenticate in some applications (like the default mail app in Android). Also, take a look at the remember function. By default, it is set to 14 days.

▪



multi-factor authentication

users service settings

app passwords

● 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

verification options

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

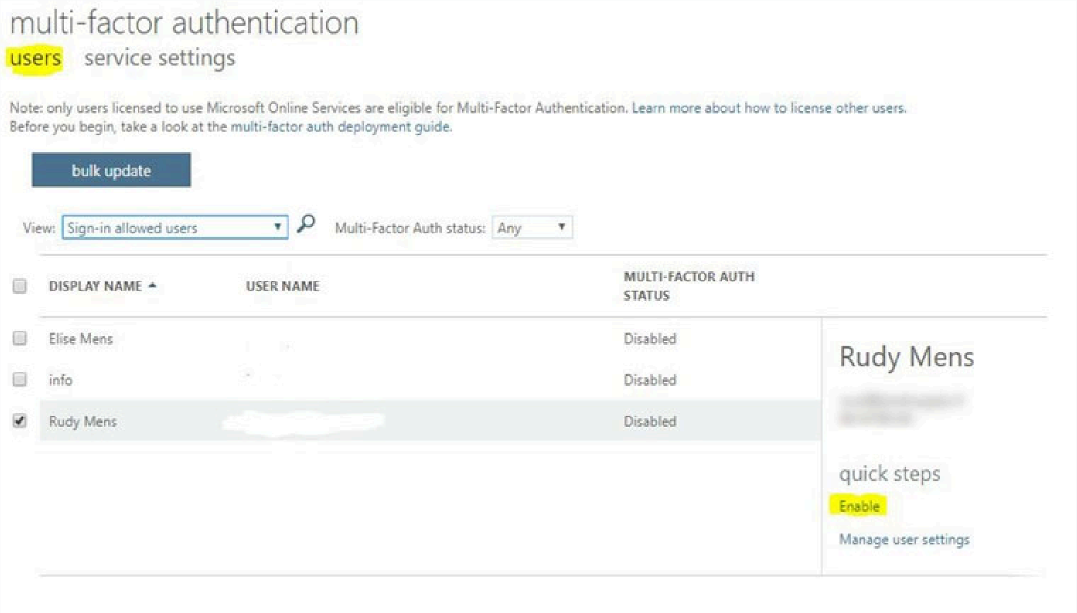
☑ Allow users to remember multi-factor authentication on devices they trust
Days before a device must re-authenticate (1-60): 30

5. Enable MFA for Office 365 users

After you have set the settings to your liking click on save and then on users (just below the title Multi-factor authentication).

You see the list of your users again. Here you can select single or multiple users to enable MFA.

At the moment you enable Office 365 MFA for a user it can get the setup screen as soon as the users browse to one of the Office 365 products.



multi-factor authentication

users service settings

Note: only users licensed to use Microsoft Online Services are eligible for Multi-Factor Authentication. Learn more about how to license other users.
Before you begin, take a look at the multi-factor auth deployment guide.

View: Sign-in allowed users ▾ Multi-Factor Auth status: Any ▾

	DISPLAY NAME ▲	USER NAME	MULTI-FACTOR AUTH STATUS
□	Elise Mens	[redacted]	Disabled
□	info	[redacted]	Disabled
☑	Rudy Mens	[redacted]	Disabled

Rudy Mens

[redacted]

quick steps

Enable

Manage user settings

Reference:

https://lazyadmin.nl/office-365/how-to-setup-mfa-in-office-365/

dlt_mate Highly Voted 3 years, 5 months 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 6 times

HnTer Highly Voted 3 years, 6 months 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 5 times

pitie110 Most Recent 2 years, 4 months ago

Cant we just enforce mfa for Allan ?

upvoted 2 times

skycrap 2 years ago

Agee, that is also the question. No reference to org settings or other users

upvoted 1 times

AzlearnRB 2 years, 5 months ago

Isnt it also possible to set a CA-Policy with this single user and require MFA?

upvoted 4 times

WMG 3 years, 4 months ago

If the question says "Use MFA for all authentication requests", enabling App Password breaks that (as you do not use MFA for that type of authentication).

upvoted 4 times

scar8 3 years, 4 months ago

yes, obviously answer was only copied from linked page for a more general description. so disable App Passwords and don't allow remembering

upvoted 5 times

MCPsince1999 3 years, 9 months 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 #12 Topic 2

SIMULATION -

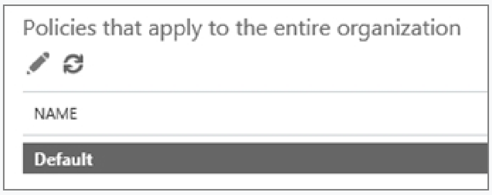
You need to ensure that all links to malware.contoso.com within documents stored in Microsoft Office 365 are blocked when the documents are accessed from

Office 365 ProPlus applications.

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

Suggested Answer: *See explanation below.*

1. After signing in to the Microsoft 365 admin center, navigate to Threat management, choose Policy > Safe Links.
2. In the Policies that apply to the entire organization section, select Default, and then choose Edit (the Edit button resembles a pencil).



Policies that apply to the entire organization

NAME
Default

3. In the Block the following URLs section, add the malware.contoso.com link.
4. In the Settings that apply to content except email section, select all the options.
5. Choose Save.

Reference:

https://docs.microsoft.com/en-us/microsoft-365/security/office-365-security/set-up-atp-safe-links-policies?view=o365-worldwide

⊟ **MSFTExamsPrep001** Highly Voted 2 years, 7 months ago

The answer has been moved to TABL. This means that you go to Security Admin Center -> Policies & rules -> Threat policies -> Tenant Allow/Block List -> Add Block URL/Email

https://docs.microsoft.com/en-us/microsoft-365/security/office-365-security/tenant-allow-block-list?view=o365-worldwide#use-the-microsoft-365-defender-portal

upvoted 17 times

⊟ **omiga** Highly Voted 3 years ago

From Admin center , go to Security Admin Center -> Policies & rules -> Threat policies.

Click on Safe Links -> Global settings.

Add the URL in the textbox under "Block the following URLs"

upvoted 13 times

⊟ **LillyLiver** 2 years, 9 months ago

I had this whole, long post to put in here. Then I read your reply and quickly deleted my reply. You are right.

upvoted 3 times

⊟ **stewie055** 2 years, 4 months ago

as sayed below, safe links is now in sec admin center in tenant allow/block list

upvoted 4 times

⊟ **GatesBill** Most Recent 1 year, 8 months ago

Go to security.microsoft.com > under Email & collaboration, select Policies & rules > Threat policies > Tenant Allow/Block List > URLs (not Domains & adresses as this only impacts email delivery and the questions states that it should block references to the given URL within documents sent by email)

upvoted 2 times

⊟ **Avaris** 2 years, 1 month ago

https://security.microsoft.com/tenantAllowBlockList?viewid=Sender&tid=9ea4dfb6-8781-4b96-ad1c-df69f6d55285

upvoted 2 times

⊟ **GatesBill** 1 year, 8 months ago

https://security.microsoft.com/tenantAllowBlockList?viewid=Sender

Don't put your tenant ID in it :)

upvoted 1 times

⊟ **marsonsing** 2 years, 4 months ago

as of this writing, Global settings under safe links has been retired. to accomplish the requested above user needs to go to security portal > policies and rules > threat policies > tenant Allow/Block List and add the url in there.

upvoted 6 times

[Removed] 3 years ago

From the admin center>>Security>>Policies & rules >> Threat policies >> Safe Links

upvoted 1 times

Nail 3 years, 4 months ago

From the M365 admin center: Go to Security admin center > Policies & rules (under Email & collaboration) > Threat policies > Safe Links > Global settings.

upvoted 8 times

mashaeg 3 years, 7 months ago

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

upvoted 5 times

Rhukey 3 years, 9 months ago

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

upvoted 1 times

Delli 3 years, 8 months ago

Then click on Global settings

upvoted 2 times

ellik 3 years, 8 months 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 3 years, 9 months ago

why remove email section ? office 365 proplus contain outlook

upvoted 1 times

Question #13 *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.

Suggested Answer: *See explanation below.*

1. After signing in to the Microsoft 365 admin center, select Security, Threat Management, Policy, then ATP Anti-phishing.
2. Select Default Policy to refine it.
3. In the Impersonation section, select Edit.
4. Go to Add domains to protect and select the toggle to automatically include the domains you own.
5. Go to Actions, open the drop-down If email is sent by an impersonated user, and choose the Quarantine message action.

Open the drop-down If email is sent by an impersonated domain and choose the Quarantine message action.

6. Select Turn on impersonation safety tips. Choose whether tips should be provided to users when the system detects impersonated users, domains, or unusual characters. Select Save.
7. Select Mailbox intelligence and verify that it's turned on. This allows your email to be more efficient by learning usage patterns.
8. Choose Add trusted senders and domains. Here you can add email addresses or domains that shouldn't be classified as an impersonation.
9. Choose Review your settings, make sure everything is correct, select Save, then Close.

Reference:

https://support.office.com/en-us/article/protect-against-phishing-attempts-in-microsoft-365-86c425e1-1686-430a-9151-f7176cce4f2c#ID0EAABAAA=Try_it

!

https://docs.microsoft.com/en-us/microsoft-365/security/office-365-security/set-up-anti-phishing-policies?view=o365-worldwide#example-anti-phishing-policy-to- protect-a-user-and-a-domain

Oz Highly Voted 4 years, 4 months 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 16 times

w00t Highly Voted 3 years, 9 months 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 16 times

BigDazza_111 Most Recent 2 years, 1 month ago

couldn't edit default phishing policy --> work around ? Go to Security admin --> policy and rules --> phishing policy --> new policy , add name /description, add users and select your own domain --> phishing email threshold ...max 4--> enable domains to protect , select your own --> enable mailox intelligence, enable intelligence for impersonaion, enable spoof intelligence, under ACTIONS if messge detected as spoof select quarantine, save policy, and then move it up as priority against other policies...would this work??

upvoted 2 times

Nail 3 years, 4 months ago

From the M365 admin center: Go to Security admin center > Policies & rules (under Email & collaboration) > Threat policies > Anti-phishing

upvoted 10 times

ThBEST 3 years, 6 months 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 2 times

WMG 3 years, 4 months ago

The question does not state anything about production or accuracy. Just that "as many as possible be identified." This means raising the threshold to max. In reality you would then review the quarantine and see if legit emails are being caught and why. If you have a lower setting, emails go through to your users and we all know how that goes.

Oz is correct, change to Most Aggressive.

upvoted 2 times

andreiiar 3 years, 8 months 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

DrMe 3 years, 12 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 3 years, 11 months ago

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

upvoted 2 times

Toyo1 4 years, 4 months 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

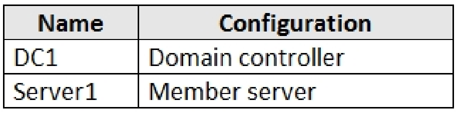
njeske 4 years, 3 months ago

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 #14 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 Microsoft Defender for Identity for the domain.

You install a Microsoft Defender for Identity standalone sensor on Server1.

You need to monitor the domain by using Microsoft Defender for Identity.

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.

Suggested Answer: *D*

Reference:

https://docs.microsoft.com/en-us/azure-advanced-threat-protection/configure-port-mirroring

Community vote distribution

D (67%) B (33%)

KarimaMaf 1 year, 6 months ago

https://learn.microsoft.com/en-us/defender-for-identity/configure-port-mirroring

upvoted 1 times

Maxx4 1 year, 6 months ago

Selected Answer: B

To monitor the domain using Microsoft Defender for Identity after installing the standalone sensor on Server1, you should:

B. Install the Microsoft Monitoring Agent on DC1.

Microsoft Defender for Identity requires the Microsoft Monitoring Agent to be installed on the domain controllers (DCs) in order to collect security-related events and data from the Active Directory environment.

In this scenario, since Server1 is a member server, installing the Microsoft Monitoring Agent on Server1 (option C) would not fulfill the requirement of monitoring the domain.

Configuring port mirroring for Server1 (option A) or configuring port mirroring for DC1 (option D) would not be the appropriate steps for monitoring the domain using Microsoft Defender for Identity. Port mirroring is typically used to capture network traffic and send it to a monitoring or security appliance for analysis, but it is not directly related to Microsoft Defender for Identity functionality.

Therefore, the correct action to monitor the domain using Microsoft Defender for Identity after installing the standalone sensor on Server1 is to install the Microsoft Monitoring Agent on DC1 (option B)

upvoted 2 times

Unicorn02 2 years, 1 month ago

D is correct.

Taken from: https://learn.microsoft.com/en-us/defender-for-identity/prerequisites

"The Defender for Identity standalone sensor is installed on a dedicated server and requires port mirroring to be configured on the domain controller to receive network traffic."

upvoted 2 times

Snaileyes 2 years, 3 months ago

It's tricky though, because Microsoft recommends deploying the "Defender for Identity" sensor on DC's

"For full coverage of your environment, we recommend deploying the Defender for Identity sensor."

This is from the note at the reference link...

Answer is D though, since question specifies the Standalone sensor...

upvoted 1 times

pete26 2 years, 3 months ago

Selected Answer: D

D is correct!

upvoted 4 times

JimboJones99 2 years, 3 months ago

Yes, the agent can't be installed on a DC

upvoted 3 times

Anonymousse 2 years, 3 months ago

uh, https://learn.microsoft.com/en-us/defender-for-identity/prerequisites

According to this, the sensor must be installed on a DC or AD FS server.

upvoted 2 times

Anonymousse 2 years, 3 months ago

However, the link in the original answer states installing on a standalone sensor. So it can be installed on a DC or Standalone server.

upvoted 1 times

Question #15 *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

Suggested Answer: *D*
Reference:
https://docs.microsoft.com/en-us/azure-advanced-threat-protection/workspace-portal

Community vote distribution

C (94%) 6%

⊟ **DTz** Highly Voted 👍 4 years, 6 months ago
Pretty sure this should be C
https://docs.microsoft.com/en-us/azure-advanced-threat-protection/install-atp-step4
upvoted 30 times

⊟ **mehnaz** 4 years, 5 months 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 7 times

⊟ **TDAC** 4 years, 3 months 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** 4 years, 6 months 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 4 times

⊟ **Marcelo72** 3 years, 10 months 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 6 times

⊟ **Maxx4** Most Recent ⊙ 1 year, 6 months ago
Selected Answer: C
o provide the administrator with the necessary Azure information required to deploy Azure Advanced Threat Protection (ATP) sensors, you should provide:

C. The access key.

The access key is a crucial piece of information required for deploying Azure ATP sensors. The access key acts as an authentication mechanism between the deployed sensors and the Azure ATP service. It allows the sensors to securely communicate with the Azure ATP cloud and send the collected security data for analysis.

The access key is generated within the Azure ATP portal or Azure ATP workspace. Once the administrator obtains the access key, they can use it during the sensor deployment process to establish the connection between the deployed sensors and the Azure ATP service.

The other options are not the required information for deploying Azure ATP sensors:
upvoted 2 times

JoeP1 1 year, 10 months ago

Selected Answer: C

According to the newest Microsoft documentation the sensor download and key are on the Identities part of the Microsoft 365 Defender portal. Since no special URL is needed I would says the answer is C.

Sensors documentation: https://learn.microsoft.com/en-us/defender-for-identity/download-sensor

upvoted 1 times

chickenroaster 1 year, 10 months ago

Selected Answer: C

Defender for Identity cloud service urls not admin center

upvoted 1 times

c95 2 years, 2 months ago

As the questions says "deploy" would that not mean that he already got the sensors downloaded and only needs the access key?

upvoted 1 times

> **BigDazza_111** 2 years, 1 month ago
>
> I thought this. It could also mean - 'remote push' 'Install' 'download'?. wording is difficult and vague
>
> upvoted 1 times

ciaphas 2 years, 3 months ago

Selected Answer: C

clearly is access key

upvoted 2 times

jore041 2 years, 3 months ago

Selected Answer: C

im pretty sure this is access key

upvoted 2 times

Whatsamattr81 2 years, 6 months ago

Access key is in the same place as the download (a custom package). Give them the URL (which can be guessed TBF and they can get both. Without the URL the access key is useless without the package. https://azurecloudai.blog/2020/04/15/deploy-azure-advanced-threat-protection-atp/

upvoted 3 times

> **BigDazza_111** 2 years, 1 month ago
>
> In fact this is correct. Need the URL to the ATP portal, access key and package download is there.
>
> Answer is D
>
> upvoted 1 times

Whatsamattr81 2 years, 6 months ago

Logically, the user can get the access key and the package from the ATP portal. Logically just giving them the URL (assuming they can access it) should be all you need to give them.

upvoted 1 times

sunilkms 2 years, 9 months ago

Selected Answer: C

it should be C, URL is nowhere needed in the sensor configuration.

upvoted 3 times

LillyLiver 2 years, 9 months ago

Selected Answer: C

At first I thought "the URL? Well I suppose they need to know how to get the sensor download." But now I'm convinced it's the Access Key. You need to provide that since there isn't an option to provide the sensor installation. So... yeah... C.

upvoted 2 times

> **LillyLiver** 2 years, 9 months ago
>
> Adding a bit more here, the question states "You need to provide the administrator with the Azure information required to deploy the sensors." I's not asking to provide the admin with the download of the sensor, but the information to deploy.
>
> I'm sticking with C...
>
> upvoted 2 times

⊟ **joergsi** 2 years, 10 months ago

Selected Answer: C

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

Prerequisites

- A Defender for Identity instance that's connected to Active Directory.
- A downloaded copy of your Defender for Identity sensor setup package and the
-=>ACCESS KEY.<=-
- Make sure Microsoft .NET Framework 4.7 or later is installed on the machine. If Microsoft .NET Framework 4.7 or later isn't installed, the Defender for Identity sensor setup package installs it, which may require a reboot of the server.
- For sensor installations on Active Directory Federation Services (AD FS) servers, see AD FS Prerequisites.
- Install the Npcap driver. For download and installation instructions, see How do I download and install the Npcap driver.

upvoted 3 times

⊟ **martinods** 3 years ago

Under Configure the sensor, enter the installation path and the access key that you copied from the previous step, based on your environment:
https://docs.microsoft.com/en-us/defender-for-identity/install-step4#install-the-sensor

upvoted 1 times

⊟ **mkoprivnj** 3 years, 1 month ago

Selected Answer: D

D is correct!

upvoted 1 times

⊟ **Cbruce** 3 years, 3 months ago

Doesn't it need C and D?
Access key
URL

upvoted 1 times

⊟ **MimeTalk** 3 years, 3 months ago

The answer seems correct as the administrator is not an azure administrator.
As per
https://practical365.com/azure-atp-intro/
To deploy the sensors, download the install package from the Azure ATP portal. You can use a software deployment tool to roll it out to your domain controllers, or just install it manually if you only have a few DCs in your environment. The access key displayed in the portal is used for initial registration of the sensors. They will then use certificates for ongoing authentication.
So providing the URL to the non Azure admin will help him to download the package and get the keys unless you work with him for each server.

upvoted 2 times

⊟ **Fcnet** 3 years, 3 months ago

The answer is correct,
The first step is to download the package, and later you need to configure and give the access key
6.Under Configure the sensor, enter the installation path and the access key that you copied from the previous step, based on your environment:

upvoted 1 times

⊟ **Fcnet** 3 years, 3 months ago

Which means the answer D. the URL of the Azure ATP admin center
is correct

upvoted 2 times

⊟ **jaber1986** 3 years, 3 months ago

@Fcent seriously!! you think providing link to ATP admin center is an answer! do you think other admins are having no idea accessing the portal!

upvoted 1 times

Question #16 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.

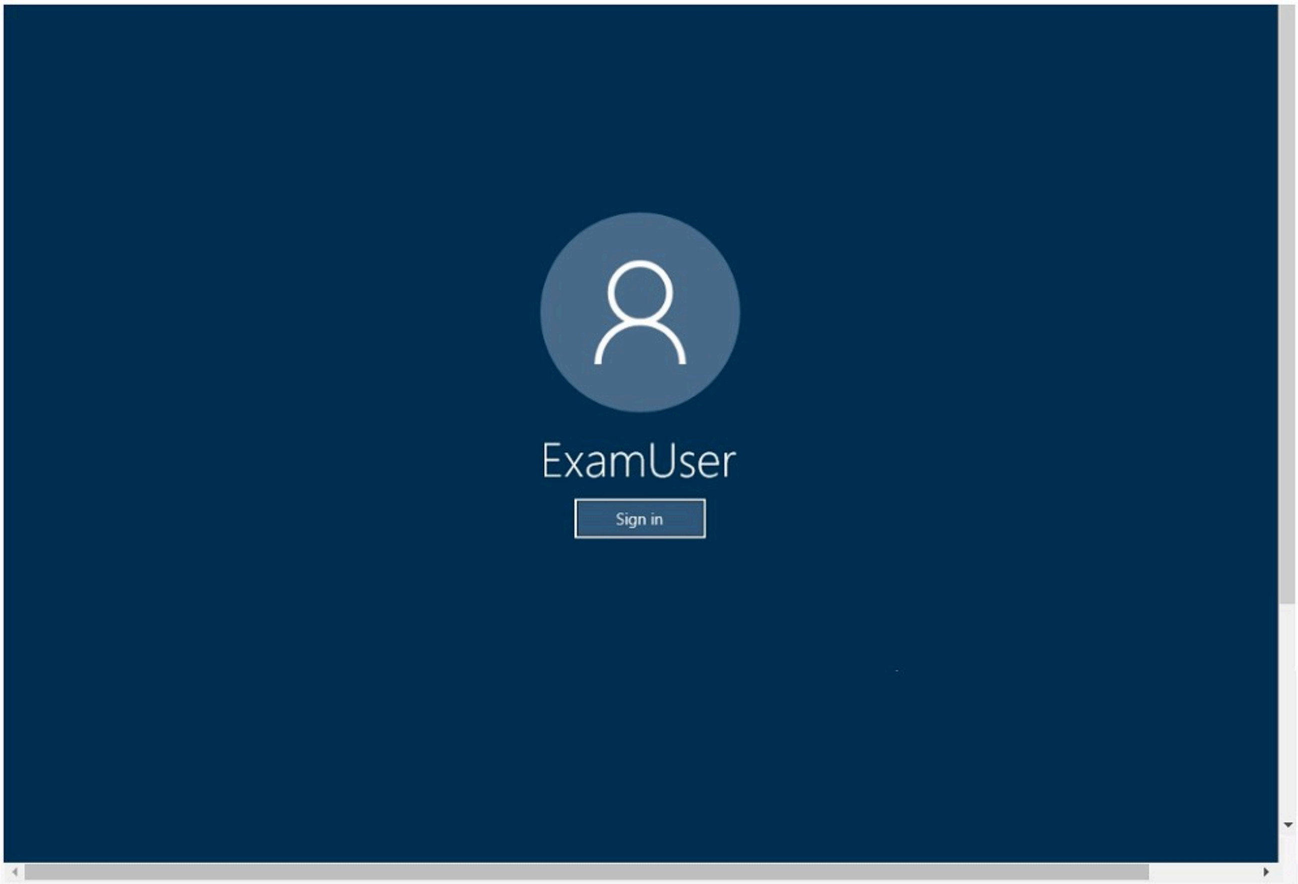
Scoring is based on the outcome of performing the tasks stated in the lab. In other words, it doesn't matter how you accomplish the task, if you successfully perform it, you will earn credit for that task.

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 -

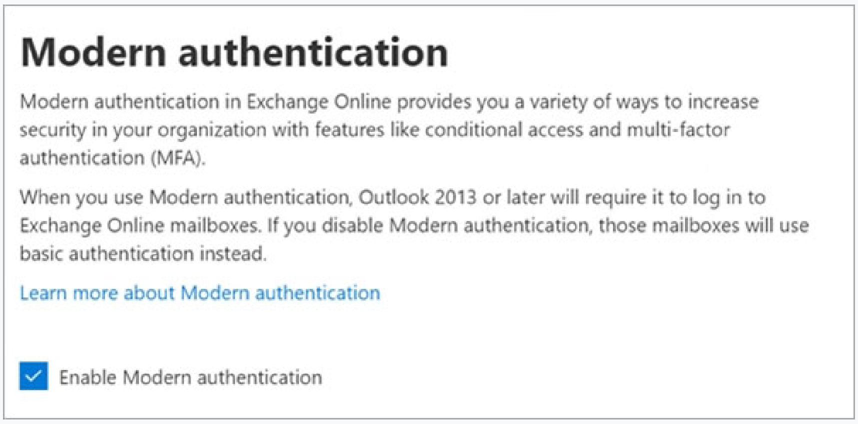
You need to ensure that a user named Alex Wilber can register for multifactor authentication (MFA).

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

Suggested Answer: *See explanation below.*

Enable Modern authentication for your organization

1. To enable modern authentication, from the admin center, select Settings > Settings and then in the Services tab, choose Modern authentication from the list.
2. Check the Enable modern authentication box in the Modern authentication panel.



Modern authentication

Modern authentication in Exchange Online provides you a variety of ways to increase security in your organization with features like conditional access and multi-factor authentication (MFA).

When you use Modern authentication, Outlook 2013 or later will require it to log in to Exchange Online mailboxes. If you disable Modern authentication, those mailboxes will use basic authentication instead.

Learn more about Modern authentication

☑ Enable Modern authentication

Enable multi-factor authentication for your organization
1. In the admin center, select Users and Active Users.
2. In the Active Users section, Click on multi-factor authentication.
3. On the Multi-factor authentication page, select user if you are enabling this for one user or select Bulk Update to enable multiple users.
4. Click on Enable under Quick Steps.
5. In the Pop-up window, Click on Enable Multi-Factor Authentication.

After you set up multi-factor authentication for your organization, your users will be required to set up two-step verification on their devices.
Reference:
https://docs.microsoft.com/en-us/microsoft-365/admin/security-and-compliance/set-up-multi-factor-authentication?view=o365-worldwide

⊟ **preeya** Highly Voted 2 years, 5 months ago
Had no labs at all in my exam july 27,2022
upvoted 8 times

⊟ **rtis16** Most Recent 1 year, 10 months ago
Pretty sure there's just multiple ways to do it now. I just go to AAD > Users > Per-user MFA (this is under the assumption that MFA is already enabled for the organization, since the question only asked to enable 1 user).
upvoted 1 times

⊟ **Madskillz13** 2 years, 3 months ago
Go to the Microsoft 365 admin center at https://admin.microsoft.com.
Go to users and locate the account.
Click on accounts and scroll down to multifactor authentication. Click on manage multifactor authentication. This takes you to this page:
https://account.activedirectory.windowsazure.com/UserManagement/MultifactorVerification.aspx?BrandContextID=O365
Here you can enable MFA for the individual user
upvoted 4 times

⊟ **leegend** 2 years, 9 months ago
The linked page now says:
Go to the Microsoft 365 admin center at https://admin.microsoft.com.
Select Show All, then choose the Azure Active Directory Admin Center.
Select Azure Active Directory, Properties, Manage Security defaults.
Under Enable Security defaults, select Yes and then Save.

So I'd be doing that now
upvoted 1 times

⊟ **derSchweiger** 2 years, 8 months ago
By enabling Security Defaults you will enable MFA for all users and that's not the scope of this question.
upvoted 6 times

⊟ **mbecile** 2 years, 11 months ago
Location for solution should be:
- Admin Portal > Settings: Org Settings > Services tab > Multi-Factor Authentication > Configure Multi-Factor Authentication
which will take you here:
https://account.activedirectory.windowsazure.com/UserManagement/MultifactorVerification.aspx?culture=en-US&BrandContextID=O365

The question and/or answer is a little dated.
- Modern Authentication used to not be enabled by default, and had to be enabled first before one could implement MFA in O365.

- Modern Auth is now enabled by default via the Security Defaults.

If you click on Modern Authentication, you will get this message:
"Modern authentication in Exchange Online provides you a variety of ways to increase security in your organization with features like conditional access and multi-factor authentication (MFA)."
upvoted 3 times

⊟ **oopspruu** 3 years, 4 months ago
I'm still not convinced if the Modern Authentication step is required. What is the Security Defaults is turned OFF? Modern Auth won't prompt for MFA then. The part 2 of the answer is what will force user to register for MFA.
upvoted 1 times

⊟ **Nail** 3 years, 4 months ago
I'm not sure where all this modern auth stuff is coming from. The question is requiring to enable registration of MFA for one user. Just do the second part of the answer and it meets the requirements.
upvoted 4 times

⊟ **Joshing** 3 years, 5 months 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 3 times

⊟ **Ahmed911** 3 years, 6 months ago
Wrong. Modern Authentication is for Exchange MFA only
upvoted 1 times

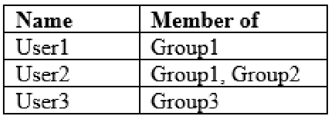
⊟ **mashaeg** 3 years, 7 months ago
Admin-Settings-Org Settings-Services/Modern Authentication
upvoted 1 times

Question #17 *Topic 2*

HOTSPOT -

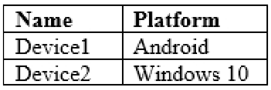
You have a Microsoft 365 subscription that uses a default domain name of contoso.com.

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

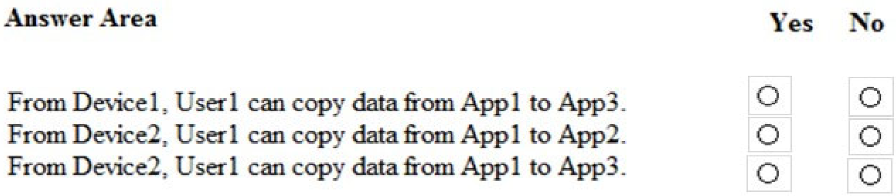
✑ Windows Information Protection mode: Block

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.

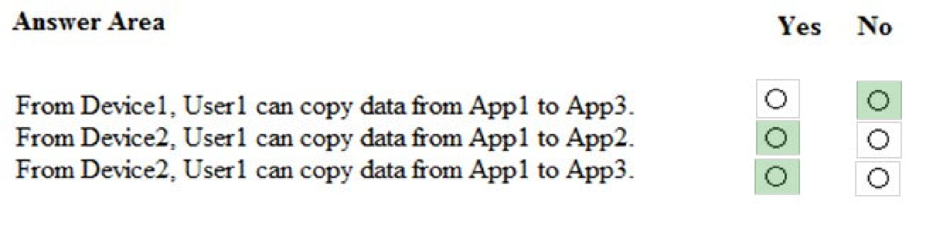
Hot Area:



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.	○	○

Suggested Answer:



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 4 years, 6 months 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 157 times

stromnessian 3 years, 4 months ago

IMHO DTz's answer is incorrect - try it yourself. To save time, try pasting from a protected app into Explorer, as it's a system process and therefore exempt.

upvoted 2 times

Joshing 3 years, 5 months 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 8 times

Joshing 3 years, 4 months ago

Clarity for question 2:

The reasoning why you can't Copy and Paste into App2 is due to the app being unenlightened so the Context this app runs will be "Personal". You can copy and paste out of it to another app but Copy and Pasting from App1 to App2 wouldn't work as App1 is enlightened and runs under the corporate context and wouldn't allow pasting into an app running in the personal context.

upvoted 1 times

STFN2019 4 years, 6 months ago

this makes more sense

upvoted 4 times

mehnaz 4 years, 5 months 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 9 times

mehnaz 4 years, 5 months ago

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

upvoted 1 times

mehnaz 4 years, 5 months ago

FINAL Correction: Its has to be Yes ,NO No

upvoted 2 times

Pitch09 3 years, 8 months ago

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

upvoted 1 times

ChrisBr Highly Voted 5 years, 2 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 64 times

madmouse256 4 years, 8 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

Toorop 5 years ago

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

upvoted 8 times

Sizz 4 years, 12 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

RonS 4 years, 8 months ago

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

upvoted 4 times

xofowi5140 4 years, 8 months ago

ProtectionPolicy1 have Windows Information Protection mode: Block

upvoted 6 times

Jhill777 4 years, 4 months 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

matthu 4 years, 8 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

dakasa 2 years, 4 months ago

Correct Y, Y, N. Here is information about the exemption of the app.
An exception allows you to specifically choose which unmanaged apps can transfer data to and FROM managed apps.
https://docs.microsoft.com/en-us/mem/intune/apps/app-protection-policies-exception

upvoted 1 times

McMac Most Recent 1 year, 6 months ago

This is clearly about App Protection Policies, so should be N, N, N ?

upvoted 1 times

Msleizaktest1 1 year, 10 months ago

On exam 24/02/2023

upvoted 3 times

beer32 1 year, 9 months ago

answer is correct ??

upvoted 1 times

ColmTheMeanie 1 year, 11 months ago

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

Microsoft Endpoint Manager has discontinued future investments in managing and deploying Windows Information Protection.

You can expunge this from your memories now

upvoted 1 times

pete26 2 years, 3 months ago

Starting in July 2022, Microsoft is deprecating Windows Information Protection. Microsoft Endpoint Manager is discontinuing future investments in managing and deploying Windows Information Protection (WIP). Just move on to the next question. The process of deprecation is to be completed by December 2022.

upvoted 4 times

Whatsamattr81 2 years, 6 months ago

You learn something every day. Been obsessing on this question. WIP will not work on android (I was getting confused between WIP and AIP). Device 1 is android.

upvoted 2 times

DarkAndy 2 years, 6 months ago

Valid on exam. Jun 10, 2022

upvoted 7 times

MK500 2 years, 7 months ago

The question does not specify which platform the policy is created for. The is only one policy which can either be for Android or for Windows 10. If the policy is for Android, the answer would be NO, YES, YES. If it is for Windows 10, answer is YES, YES, NO.

upvoted 1 times

cinziasun 2 years, 7 months ago

Correct answer is YNN.
1. Yes because device 1 is an Adroid Device and it's not included in policy;

2. No becasue App1 and device windows are included in policy;
3. No for the same reason of Q2.
upvoted 2 times

⊟ **LillyLiver** 2 years, 9 months ago
Well... I'm torn. I want to believe everyone saying that Q1 is Yes. It makes sense that WIP doesn't apply to Android devices so you can copy the data all day if you want. But I'm reading what the block mode does, and I don't know that I truly believe that theory.

From: https://docs.microsoft.com/en-us/windows/security/information-protection/windows-information-protection/create-wip-policy-using-intune-azure#:~:text=Table%202%20%20%20%20Mode%20%20,off%20and%20doesn%27t%20help%20to%20pr%20...%20

Block: WIP looks for inappropriate data sharing practices and stops the employee from completing the action. This can include sharing info across non-enterprise-protected apps in addition to sharing enterprise data between other people and devices outside of your enterprise.

I don't think that WIP is going to allow the ability to copy the data from App1 to App3. Also App3 isn't included in the policy anywhere. Every time I've read something about WIP if an app isn't a part of the policy, it's unenlightened and you can't do anything with it.

So I say it's N/Y/N.
upvoted 1 times

⊟ **LillyLiver** 2 years, 8 months ago
I'm coming back to this problem-child of a question a couple weeks later. I've changed my mind a little after looking at this some more.

Q1: N - The WIP is only going to apply to Win 10. And it's also protecting App1. So since App1 is protected with the block, meaning "...This can include sharing info across non-enterprise-protected apps in addition to sharing enterprise data between other people and devices outside of your enterprise." So Android can't even get to App1 to copy anything in the first place.

Q2: N - True, Device2 is a Windows 10 box, but App2 is excluded from the policy so it can't copy to App2 either.

Q3: N - Same as Q2, only you have App3. App3 isn't protected so it can't have App1 data copied to it.

So my answer has changed slightly to N,N,N.
upvoted 2 times

⊟ **martinods** 2 years, 11 months ago
YNN- You can use Windows Information Protection (WIP) policies with Windows 10 apps to protect apps without device enrollment.
https://docs.microsoft.com/en-us/mem/intune/apps/windows-information-protection-policy-create
upvoted 1 times

⊟ **martinods** 2 years, 12 months ago
app protection policy works on Android

1. Device 1 is an Android Device and app protection policy works on it -> Answer NO
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 2 times

⊟ **mkoprivnj** 3 years, 1 month ago
Y, N, N
upvoted 1 times

⊟ **Rstilekar** 3 years, 1 month ago
Corrected ans in short is # YES NO NO
1. Device 1 is an Android Device and WIP won't work at all -> Answer YES
2. App 2 is an exempt App but not App1 -> Answer NO....
The reasoning why you can't Copy and Paste into App2 is due to the app being unenlightened so the Context this app runs will be "Personal". You can copy and paste out of App2 to another app but Copy and Pasting from App1 to App2 wouldn't work as App1 is enlightened and runs under the corporate context and wouldn't allow pasting into an app running in the personal context
3. APP 3 is neither a protected nor an excempt app. WIP should Block -> Answer NO
upvoted 1 times

⊟ **Fcnet** 3 years, 3 months ago

Just to clarify.

What is the goal here ?

You want to block the copy feature from any app.

Except from app1 and app2 as app2 is exempted from the policy and app1 can copy from and to itself.

Wich means if you try to copy from app3 it won't work (from any device).

So the answer is

No - Yes - No

You won't be able to copy from App3 what ever device it is.

To reach this goal, you have to create at least 2 app protection policies : one for android and one for Windows.

upvoted 1 times

⊟ **Fcnet** 3 years, 3 months ago

When you click the "Create Policy" menu in MEM / Intune in App Protection Policies you get a drop-down to choose between Windows10 and later or iOS / iPadOS or Android

(from endpoint.microsoft.com / home / apps / app protection policies / create policy choose one from ios/android/windows)

How to create an app policy for Windows : (wip)

https://docs.microsoft.com/en-us/mem/intune/apps/quickstart-create-assign-app-policy

How to create an app policy for Android : (wip)

https://docs.microsoft.com/en-us/mem/intune/apps/app-protection-policies

upvoted 1 times

⊟ **Fcnet** 3 years, 3 months ago

If only one policy has been created

then the answer should be No - Yes - Yes if the policy for android only has been created,

but nothing tells us only one android policy has been created except the name protectionPolicy1 but it is not clear if it's a policy for android or for Windows....

In summary

if we wan't to gain the goal : avoid the copy paste from any appx except app2 and app1 from any device / android and Windows we have to create 2 policies : one for android and one for windows

And the answer would be

No - Yes - No

upvoted 1 times

⊟ **stromnessian** 3 years, 4 months ago

The answer is... ...it depends! The question does not provide enough information. Are the apps enlightened? Is the data work or personal? If we assume that the data is being copied from a work context in App1:

YES - This is WIP, so nothing to do with Android, i.e. the policy will not be applied.

YES - Exempt apps can interact with any work or personal data.

NO - The app is not included in the policy so will have the enterprise context of personal, so can only interact with personal data.

I read with interest the explanation from DTz, but in my humble opinion it is wrong. "Block" does not prevent enterprise data from leaving protected apps. If you think about it, that would be silly as users have to be able to copy and paste between enterprise apps. What "block" does is prevent copying from a work context to a personal one.

upvoted 2 times

Question #18 *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 Intune.
You need to ensure that the computers connect to Microsoft Defender for Endpoint.
What should you do in Microsoft Endpoint Manager admin center?

A. Configure an enrollment restriction

B. Create a device configuration profile

C. Create a conditional access policy

D. Create a Windows Autopilot deployment profile

Suggested Answer: *B*
Reference:
https://docs.microsoft.com/en-us/intune/advanced-threat-protection

Community vote distribution

B (100%)

pete26 Highly Voted 2 years, 3 months ago

Selected Answer: B

B is correct! I work all day long in Intune. :)

upvoted 9 times

Maxx4 Most Recent 1 year, 6 months ago

Selected Answer: B

To ensure that the computers connect to Microsoft Defender for Endpoint after they are enrolled in Microsoft Intune, you should:

B. Create a device configuration profile.

In the Microsoft Endpoint Manager admin center, you can create a device configuration profile to configure settings and policies for the enrolled Windows 10 computers. This includes configuring the connection to Microsoft Defender for Endpoint.

By creating a device configuration profile, you can specify the necessary settings and configurations to ensure that the computers connect to Microsoft Defender for Endpoint and establish the required communication for monitoring and protection.

Options A, C, and D are not directly related to configuring the connection to Microsoft Defender for Endpoint:

upvoted 1 times

Daniel830 2 years, 3 months ago

Correct. A configuration profile is needed in order to deploy Intune computer's into Defender for Endpoint.

upvoted 4 times

msysadmin 1 year, 10 months ago

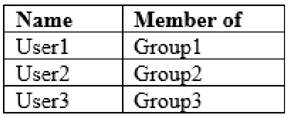
It saying to configure an "enrollment restriction". A is not correct

upvoted 1 times

Question #19 Topic 2

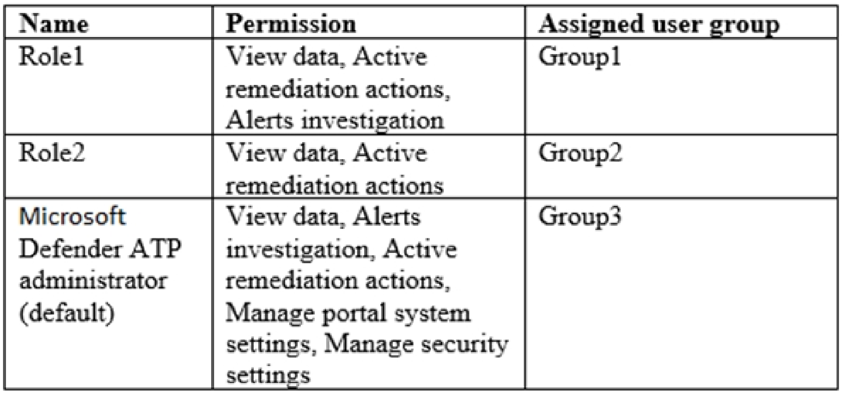
HOTSPOT -

Your company has a Microsoft 365 subscription that contains the users shown in the following table.



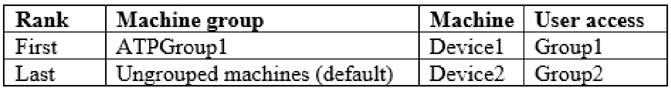
Name	Member of
User1	Group1
User2	Group2
User3	Group3

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:

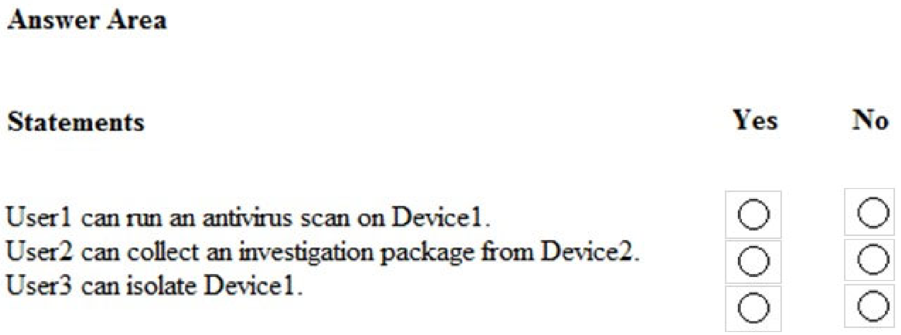


Rank	Machine group	Machine	User access
First	ATPGroup1	Device1	Group1
Last	Ungrouped machines (default)	Device2	Group2

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

NOTE: Each correct selection is worth one point.

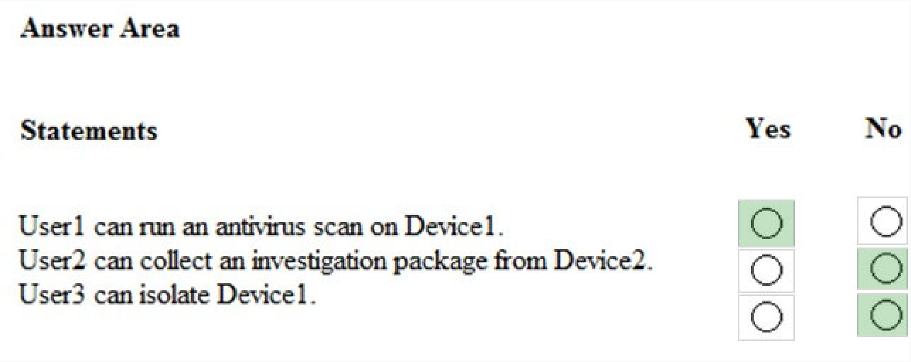
Hot Area:



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.	○	○

Suggested Answer:



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 Highly Voted 3 years, 5 months 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 28 times

WMG 3 years, 4 months ago

Correct, the built in admin role gives you access to all devices, so no assignment needed.

upvoted 3 times

stromnessian Highly Voted 3 years, 4 months ago

Despite MS making this information super hard to find, it's YNY.

Y - "Alerts investigation" permission required to run scans.

N - "Alerts investigation" permission required to download investigation package.

Y - At least "Active remediation actions" required to isolate device. Admin has full permissions and access to all machines regardless of group.

upvoted 13 times

zerrowall Most Recent 2 years ago

Regarding User2 see here:

https://learn.microsoft.com/en-us/microsoft-365/security/defender-endpoint/user-roles?view=o365-worldwide#permission-options

He doesn't have "Alerts investigation" permission, so the answer User is "N".

upvoted 1 times

Avaris 2 years, 1 month ago

it's a tricky question User3 doesn't have access to anything this is a silly one :)

upvoted 2 times

Trainee2244 2 years, 3 months ago

Y,N,Y is the right Answer

upvoted 3 times

Dom1nation 2 years, 8 months ago

Y-N-N is correct I think. Read all comments.

upvoted 1 times

Fernando001 2 years, 11 months ago

User 3 has no access to device 2, it should be no.

upvoted 1 times

mkoprivnj 3 years, 1 month ago

Correct answer is Y/N/Y.

upvoted 3 times

Rstilekar 3 years, 1 month ago

Y - "Alerts investigation" permission required to run scans.

N - "Alerts investigation" permission required to download investigation package.

Y - At least "Active remediation actions" required to isolate device. Admin has full permissions and access to all machines regardless of group.

upvoted 4 times

laugz92 3 years, 7 months 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 3 years, 6 months 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 9 times

weabey 3 years, 7 months 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 3 years, 9 months 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 3 times

Sugar123 3 years, 9 months 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 3 times

kiketxu 3 years, 9 months 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 6 times

Sugar123 3 years, 9 months 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 4 times

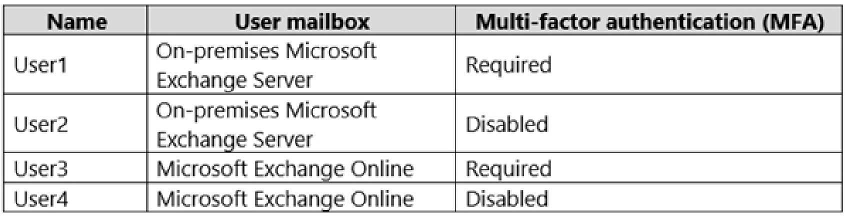
⊟ **JoelB** 3 years, 6 months ago

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 #20 *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

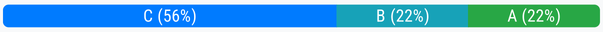
Suggested Answer: *C*

Each targeted recipient must have an Exchange Online mailbox.

Reference:

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

Community vote distribution



kiketxu Highly Voted 3 years, 9 months ago

C for sure. Only supported on EXO. Btw, MFA is to create and manage campaings.

upvoted 30 times

ffffffffdeeeeeeeeeeee 3 years, 7 months ago

ANS: A

Attack Simulator only works on cloud-based mailboxes and with MFA enabled.

upvoted 9 times

WMG 3 years, 4 months ago

No, answer is C. MFa is only required for the admins. Try it out. The targeted mailboxes need to be cloud mailboxes, not on-premise. The MFA status of the user who has full access and owner of a mailbox object is not relevant.

upvoted 6 times

Dhamus 1 year, 7 months ago

You are right.

upvoted 1 times

belyo Highly Voted 3 years, 9 months 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 12 times

kiketxu 3 years, 9 months ago

MFA is to create and manage campaings. In the statements says "against"

upvoted 11 times

chaoscreater 3 years, 6 months 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

WMG 3 years, 4 months ago

A user with a mailbox does not need MFA in order to be targeted by attack simulator. The user mailbox must however be in the cloud. so User 3 and User 4 fulfil that requirement.

This you can verify by just testing it in your lab environment. In no way does any documentation state that you need MFA for users, because it is not needed when you configure an attack simulation.

upvoted 4 times

Okadorium Most Recent 1 year, 6 months ago

MFA (Multi-Factor Authentication) is not a requirement to use Attack Simulator in Microsoft Defender for Office 365. Attack Simulator can be used to simulate phishing and spear-phishing attacks regardless of whether MFA is enabled or disabled for user accounts. Thus, the Answer is C.

upvoted 2 times

Maxx4 1 year, 6 months ago

Selected Answer: A

A. User3 only.

Microsoft 365 Attack Simulator can be used to simulate phishing and other attacks against users in order to assess their security awareness and resilience. However, Attack Simulator requires certain prerequisites to be met, specifically the availability of Exchange Online mailboxes and the user's MFA status.

In this scenario, User3 is the only user who meets both prerequisites. User3 has a mailbox in Microsoft Exchange Online, and MFA is enabled for this user. Therefore, you can use Attack Simulator against User3 to assess their response to simulated attacks.

User1 is an on-premises Exchange Server user with MFA enabled, which does not meet the requirement of having a mailbox in Exchange Online.

User2 is an on-premises Exchange Server user with MFA disabled, which does not meet the requirement of having MFA enabled.

User4 is a Microsoft Exchange Online user, but MFA is disabled for this user, which does not meet the requirement of having MFA enabled.

upvoted 1 times

clazmaz 1 year, 7 months ago

Selected Answer: B

It could be B, as per documentation:
"Attack simulation training supports on-premises mailboxes, but with reduced reporting functionality. "

-> https://learn.microsoft.com/en-us/microsoft-365/security/office-365-security/attack-simulation-training-get-started?view=o365-worldwide#what-do-you-need-to-know-before-you-begin

upvoted 2 times

TheABC 2 years, 4 months ago

The links posted don't give any requirements, I thought MFA was a requirement and only that, mailbox AI is online only, for me even B woudl be correct, as it seems to not mention MFA/Mailbox type online anywhere!

upvoted 1 times

[Removed] 2 years, 7 months ago

Selected Answer: A

I thought it was A but after some research C is correct. It used to be A.

upvoted 1 times

arska 2 years, 9 months ago

Selected Answer: C

Attack Simulator requires Exchange Online. It doesn't require MFA for the users.

upvoted 2 times

JCast20 2 years, 11 months ago

Requirements for Attack simulator
Your organization has Office 365 Threat Intelligence, with Attack simulator visible in the Security & Compliance Center (go to Threat management > Attack simulator)

Your organization's email is hosted in Exchange Online. (Attack simulator is not available for on-premises email servers.)

You are an Office 365 global administrator

Your organization is using Multi-factor authentication for Office 365 users

ANS:A

upvoted 3 times

⊟ **mkoprivnj** 3 years, 1 month ago

Selected Answer: C

C is correct!

upvoted 3 times

⊟ **Rstilekar** 3 years, 1 month ago

Only supported on EXO. MFA is to create and manage attack campaings.

upvoted 1 times

⊟ **jaketeek** 3 years, 3 months ago

It's most definitely C.

upvoted 2 times

⊟ **Nail** 3 years, 4 months ago

Definitely C. It is not asking about who is running Attack Simulator but who that admin is running it AGAINST. Those users need EXO.

upvoted 2 times

⊟ **MikeMatt2020** 3 years, 4 months ago

ANSWER IS C

1) "MFA is only required for the admin who initiates the Attack Simulator"
2) "Attack Simulator only works on CLOUD-BASED mailboxes"

The question clearly asks us to "identify the users against which you can use Attack Simulator". Hate the phrashing but they're asking who are our targeted users? Who are our victims? To be our test dummies, the user mailboxes MUST be cloud based. Regarding MFA, this is only relevant to the admins who CREATE/MANAGE the simulations.

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

upvoted 4 times

⊟ **Joshing** 3 years, 5 months 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 5 times

⊟ **Joshing** 3 years, 5 months ago

Clarity: The requirement is EXO to be targeted for the campaign. MFA is not required.

upvoted 1 times

⊟ **ViniciusVidal** 3 years, 9 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** 3 years, 7 months ago

C is correct. MFA is only required for the admin who initiates the 'Attack Simulator'

upvoted 4 times

Question #21 *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.

Suggested Answer: *See explanation below.*

You need to configure a Safe Links policy.

1. Go to the Office 365 Microsoft 365 Compliance center.
2. Navigate to Threat Management > Policy > Safe Links.
3. In the Policies that apply to the entire organization section, select Default, and then click the Edit icon.
4. In the Block the following URLs section, type in *.fabrikam.com. This meets the first requirement in the question.
5. In the Settings that apply to content except email section, untick the checkbox labelled Do not track when users click safe links. This meets the second requirement in the question.
6. Click Save to save the changes.

Reference:

https://docs.microsoft.com/en-us/microsoft-365/security/office-365-security/set-up-atp-safe-links-policies?view=o365-worldwide

hyve Highly Voted 3 years, 2 months ago

1. Go to Security.microsoft.com
2. Navigate to Policies and Rules > Threat Policies > Safe Links.
3. In Global Settings
4. In the Block the following URLs section, type in *.fabrikam.com.
5. untick the checkbox labelled Do not track when users click safe links.
6. Click Save to save the changes.

upvoted 14 times

AzlearnRB Highly Voted 2 years, 5 months ago

Seems like you cant use Safe Linnks for this anymore. Microsoft moved this functionality to the Tenant Allow/Block List.

upvoted 10 times

Maxx4 Most Recent 1 year, 6 months ago

To implement a solution to manage when users select links in documents or email messages from Microsoft Office 365 ProPlus applications or Android devices and meet the specified requirements, you can use the Microsoft Defender for Office 365 service. Here are the steps to follow:

Sign in to the Microsoft 365 portal (portal.office.com) using your administrator credentials.

Navigate to the Microsoft Defender Security Center.

In the Microsoft Defender Security Center, go to the "Threat management" or "Threat & Vulnerability Management" section, depending on your subscription.

Configure Safe Links policies:

a. In the appropriate section (e.g., Safe Links), create a new policy or edit an existing policy.

b. Configure the policy to block access to the domain named "fabrikam.com". This will prevent users from accessing any links to that domain.

c. Enable the option to store information when users select links. This will allow you to track and review user interactions with the links.

Save and apply the policy.

upvoted 1 times

skycrap 2 years, 4 months ago

In Microsoft 365 Defender

Email & Collaboration

Policies & Rules

Threat policies

Tenant Allow/Block Lists

upvoted 9 times

⊟ **itstudy369** 3 years, 11 months 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

⊟ **dzampar** 4 years, 2 months 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

⊟ **mitchg** 4 years, 2 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 8 times

Question #22 *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.

Suggested Answer: *See explanation below.*

You need to edit the Anti-Phishing policy.

1. Go to the Office 365 Microsoft 365 Compliance center.
2. Navigate to Threat Management > Policy > ATP Anti-Phishing.
3. Click on Default Policy.
4. In the Impersonation section, click Edit.
5. Go to the Actions section.
6. In the If email is sent by an impersonated user: box, select Quarantine the message from the drop-down list.
7. In the If email is sent by an impersonated domain: box, select Quarantine the message from the drop-down list.
8. Click Save to save the changes.
9. Click Close to close the anti-phishing policy window.

techstudent Highly Voted 👍 4 years, 1 month 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 8 times

GatesBill Most Recent ⊙ 1 year, 8 months ago

Security Admin Center (security.microsoft.com) > Policies & rules > Threat policies > Anti-phishing

Edit default policy or create new policy and set 'Phishing email threshold' to '4 - Most Aggressive'. This will do as follows: "Messages that are identified as phishing with a low, medium, or high degree of confidence are treated as if they were identified with a very high degree of confidence."

upvoted 2 times

doody 2 years ago

done from Anti-spam policy AND anti-phishing policy

upvoted 1 times

mbecile 2 years, 11 months ago

> https://security.microsoft.com/antiphishing

(Security Admin Center > Policies & Rules > Threat Policies > Anti-Phishing)

> Office365 AntiPhish Default (Default)

> Edit Protection Settings & Actions as needed to quarantine messages

> Save

(If it won't let you save, you need to run the command: Enable-OrganizationCustomization)

upvoted 3 times

mbecile 2 years, 11 months ago

There is also a setting in https://security.microsoft.com/antispam that could need to be changed.

> Security Admin Center > Policies & Rules > Threat Policies > Anti-Spam

> Anti-Spam inbound policy

> Phishing > change from "Move to Junk" to "Quarantine"

(High Confidence Phishing should already be set to "Quarantine")

upvoted 6 times

examTaker3 3 years, 4 months ago

Impersonation/spoofing do not equal phishing. This answer tells you how to change impersonation settings, not how to quarantine messages classified as phishing.

Security & Compliance Center, Threat Management > Policy > Anti-spam
Set the Actions for 'Phishing' and "High confidence phishing" to Quarantine.
upvoted 4 times

Fluffhead 3 years, 3 months ago
Phishing = Impersonation/Spoofing.
upvoted 2 times

Question #23 *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

Suggested Answer: *A*
Reference:
https://docs.microsoft.com/en-us/office365/securitycompliance/view-reports-for-atp#what-permissions-are-needed-to-view-the-atp-reports

Community vote distribution
A (100%)

joergsi Highly Voted 2 years, 10 months ago
Selected Answer: A
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?
In order to view and use the reports described in this article, you need to be a member of one of the following role groups in the Microsoft 365 Defender portal:

-Organization Management
-Security Administrator
-Security Reader
-Global Reader
upvoted 7 times

kiketxu Highly Voted 3 years, 9 months ago
A for sure!
upvoted 5 times

Maxx4 Most Recent 1 year, 6 months ago
Selected Answer: A
To allow User1 to view Advanced Threat Protection (ATP) reports in the Threat management dashboard, you should assign User1 the following role:

A. Security administrators.

The Security administrators role in Microsoft 365 provides the necessary permissions to view ATP reports and manage security-related configurations and policies. By assigning User1 the Security administrators role, they will have the required role permissions to access and review ATP reports in the Threat management dashboard.

The other roles mentioned do not specifically provide the necessary permissions for ATP reports:
upvoted 1 times

Dhamus 1 year, 7 months ago
It is correct, although the role is too much.
upvoted 1 times

arska 2 years, 9 months ago
Selected Answer: A
See joergsi
upvoted 1 times

⊟ **mbecile** 2 years, 11 months ago

A is Correct,

Although you should note that the "Security Reader" role will allow them to do the same, but since it was not an available answer, it should be "Security Administrator"

upvoted 3 times

⊟ **mkoprivnj** 3 years, 1 month ago

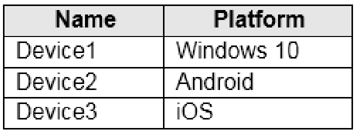
Selected Answer: A

A is correct!

upvoted 1 times

Question #24 *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

Suggested Answer: *D*
Microsoft Defender ATP (now known as Microsoft Defender for Endpoint) now supports Windows 7 SP1 and above, Windows Server 2008 SP1 and above, the three most recent major releases of macOS, iOS 11.0 and above, Android 6.0 and above and Red Hat Enterprise Linux 7.2 or higher, CentOS 7.2 or higher,
Ubuntu 16.04 LTS or higher LTS, Debian 9 or higher, SUSE Linux Enterprise Server 12 or higher, and Oracle Linux 7.2 or higher.
Reference:
https://docs.microsoft.com/en-us/windows/security/threat-protection/microsoft-defender-atp/evaluation-lab https://docs.microsoft.com/en-us/windows/security/threat-protection/microsoft-defender-atp/minimum-requirements

Community vote distribution

D (100%)

vijayvasisht Highly Voted 3 years, 9 months 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 24 times

ed_ma Most Recent 2 years ago

Selected Answer: D

https://learn.microsoft.com/en-us/mem/intune/protect/advanced-threat-protection-configure#create-and-assign-compliance-policy-to-set-device-risk-level

upvoted 1 times

TheABC 2 years, 4 months ago

Selected Answer: D

See vijayvasisht

upvoted 1 times

arska 2 years, 9 months ago

Selected Answer: D

See vijayvasisht

upvoted 1 times

mkoprivnj 3 years, 1 month ago

Selected Answer: D

D is correct!

upvoted 3 times

Nounna 3 years, 7 months 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 years, 8 months 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 4 times

DudleyYVR 3 years, 8 months ago

MD ATP is not fully integrated with Android.
iOS is NOT macOS. There's a difference.

upvoted 1 times

MCPsince1999 3 years, 9 months ago

Answer is A, W10 and Android is supported (not iOS)

upvoted 2 times

bingomutant 3 years, 9 months ago

see vijay below which is now correct

upvoted 1 times

kiketxu 3 years, 9 months 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 3 years, 9 months ago

latest 3 versions of iOS are now supported.

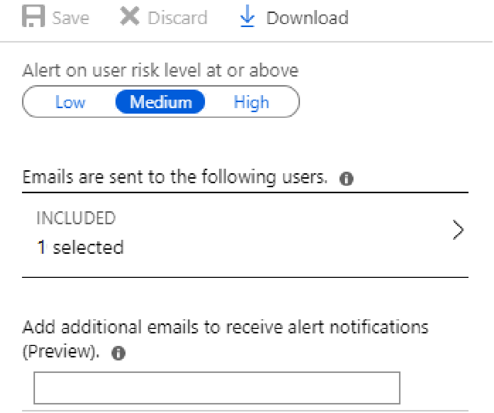
upvoted 2 times

Question #25 *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.



Alert on user risk level at or above

Low | **Medium** | High

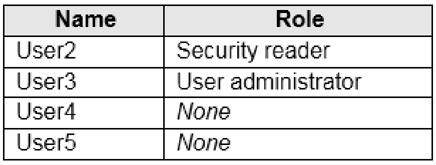
Emails are sent to the following users.

INCLUDED
1 selected

Add additional emails to receive alert notifications (Preview).

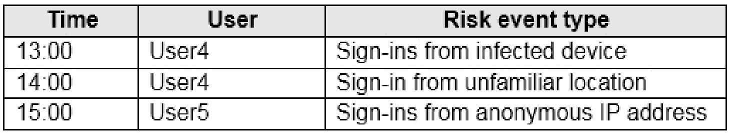
A user named User1 is configured to receive alerts from Azure AD Identity Protection.

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.

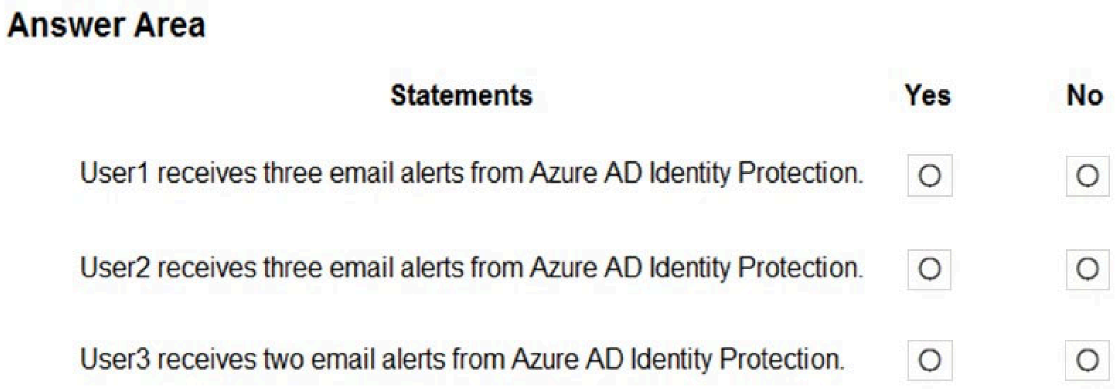


Time	User	Risk event type
13:00	User4	Sign-ins from infected device
14:00	User4	Sign-in from unfamiliar location
15:00	User5	Sign-ins from anonymous IP address

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

NOTE: Each correct selection is worth one point.

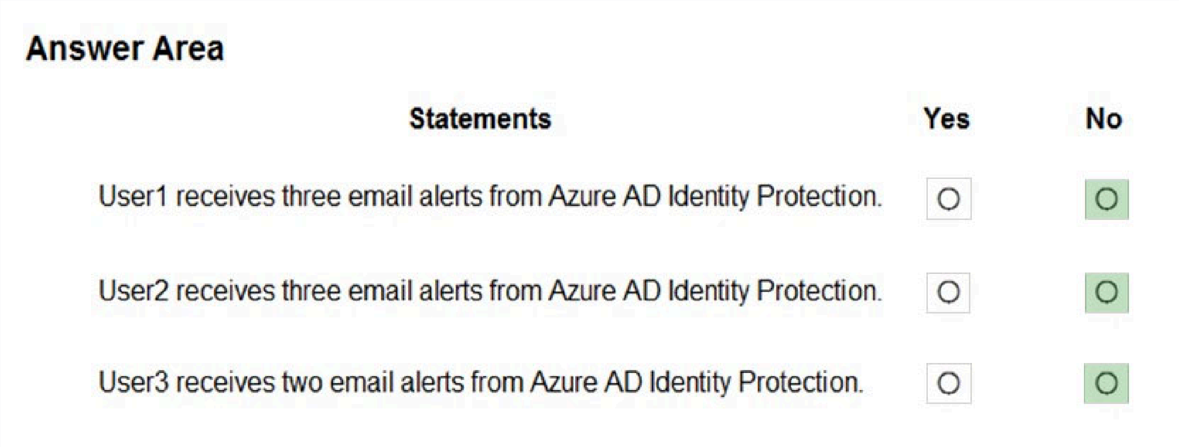
Hot Area:



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.	○	○

Suggested Answer:



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.	○	[✓ ○]

Box 1: No -
User1 will receive the two alerts classified as medium or higher.
Sign-ins from infected device is classified as low. This risk detection identifies IP addresses, not user devices. If several devices are behind a single IP address, and only some are controlled by a bot network, sign-ins from other devices my trigger this event unnecessarily, which is why this risk detection is classified as
Low.

Box 2: No -
User2 will receive the two alerts classified as medium or higher.
Email alerts are sent to all global admins, security admins and security readers
Sign-ins from infected device is classified as low. This risk detection identifies IP addresses, not user devices. If several devices are behind a single IP address, and only some are controlled by a bot network, sign-ins from other devices my trigger this event unnecessarily, which is why this risk detection is classified as
Low.

Box 3: No -
User3 will not receive alters.
Email alerts are sent to all global admins, security admins and security readers.
Reference:
https://docs.microsoft.com/en-us/azure/active-directory/identity-protection/overview-identity-protection https://docs.microsoft.com/en-us/azure/active-directory/identity-protection/howto-identity-protection-configure-risk-policies

kiketxu Highly Voted 3 years, 9 months 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 31 times

Sethoo 3 years, 9 months 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 4 times

TheGuy 3 years, 9 months 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 3 times

Kalzonee3611 3 years, 7 months ago

How do you which activity falls under which category of threat?

upvoted 3 times

Jhill777 2 years, 7 months ago

Sign-ins from infected devices is low

upvoted 3 times

Yetijo 3 years, 6 months 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 2 times

MrAce Highly Voted 3 years, 4 months ago

Maybe I think too simple. But the screenshot is User risk level and not Sign-in risk level. So answer is No No No.

upvoted 22 times

kidney83 3 years, 3 months ago

Very subtle, but I think you are right

upvoted 3 times

Grudo 2 years, 11 months ago

Everyone missed this except you and adamsca

upvoted 2 times

RVR 2 years, 3 months ago

I think you're right. The given answer appears to be correct.

upvoted 1 times

GatesBill Most Recent 1 year, 8 months ago

A user risk represents the probability that a given identity or account is compromised.
A sign-in risk represents the probability that a given authentication request isn't authorized by the identity owner.

Microsoft doesn't provide specific details about how risk is calculated. Each level of risk brings higher confidence that the user or sign-in is compromised.
> Reference: https://learn.microsoft.com/en-us/azure/active-directory/identity-protection/concept-identity-protection-risks#risk-levels

Yet again an invalid question where the given policy does not match the given scenario and even if it did, no concrete info is known as Microsoft did not provide it (yet?).

upvoted 1 times

SKam22 2 years, 5 months ago

User risk vs sign-in risk. Answer, N,N,N. Policy doesn't apply to the Sign-ins. See below for User vs Sign-in risk: https://docs.microsoft.com/en-us/azure/active-directory/identity-protection/concept-identity-protection-risks

upvoted 2 times

Whatsamattr81 2 years, 6 months ago

Its sneaky, but those risks are sign in risks, and the picture is of a user risk policy. Unless the Q is wrong, the answer would be NNN... If the picture is wrong, and it should be a sign in risk policy, the answer would be YYN. Either way, you'll get one mark for this lol

upvoted 1 times

mbecile 2 years, 11 months ago

Per Microsoft Docs

- Users with Leaked Credentials = High
- Sign-ins from Anonymous IP Addresses = Medium
- Impossible Travels to atypical locations = Medium
- Sign-in from unfamiliar location = Medium
- Sign-ins from IP Addresses with suspicious activity = Low
- Sign-ins from infected devices = Low

Source:
https://docs.microsoft.com/en-us/learn/modules/introduction-to-azure-identity-protection/4-explore-vulnerabilities-risk-events

upvoted 2 times

mkoprivnj 3 years, 1 month ago

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.

upvoted 1 times

Rstilekar 3 years, 1 month ago

At present scenerios there are name changes to Azure Sentinel role to Microsoft Sentinel Role. Right ans is B & E.
E. Logic App Contributor # Create and run playbooks.
Microsoft Sentinel uses playbooks for automated threat response. Playbooks are built on Azure Logic Apps, and are a separate Azure resource. You can use the Logic App Contributor role to assign explicit permission for using playbooks.

B. *Azure (now Microsoft) Sentinel responder # Manage incidents.
Can can view data, incidents, workbooks, and other Microsoft Sentinel resources (like Microsoft Sentinel Responder) ++ manage incidents (assign, dismiss, etc.)

Ref # https://docs.microsoft.com/en-us/azure/sentinel/roles#roles-and-allowed-actions

upvoted 1 times

adamsca 3 years, 2 months ago

So, I am a little confused as I came up with No No No Because the exhibit show user risk policy but the risk event types were sign in risk events. They should not get emails based on user risk policy because we are talking about sign in risk events. Isn't "sign in risk" different from user risk? There are separate policies for these. Terrible question in my opinion. Let me know what u think.

upvoted 6 times

gkp_br 3 years, 2 months ago

N - N - N
Sign-ins from infected devices - Low

https://docs.microsoft.com/pt-br/learn/modules/introduction-to-azure-identity-protection/4-explore-vulnerabilities-risk-events

upvoted 9 times

AlexanderSaad 3 years, 3 months ago

Configure users at risk detected alerts
As an administrator, you can set:
The user risk level that triggers the generation of this email - By default, the risk level is set to “High” risk.
The recipients of this email - Users in the Global administrator, Security administrator, or Security reader roles are automatically added to this list. We attempt to send emails to the first 20 members of each role. If a user is enrolled in PIM to elevate to one of these roles on demand, then they will only receive emails if they are elevated at the time the email is sent.

upvoted 1 times

Hami3191 3 years, 3 months ago

https://docs.microsoft.com/en-us/azure/active-directory/identity-protection/howto-identity-protection-configure-notifications#:~:text=The%20recipients%20of,email%20is%20sent.

upvoted 1 times

The_Poet 3 years, 5 months 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 years, 5 months 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 3 years, 7 months ago

Definitely YYN

upvoted 2 times

Pitch09 3 years, 8 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%20user

upvoted 2 times

ismossss 3 years, 8 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 3 times

Question #26 *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

Suggested Answer: *DE*
Reference:
https://docs.microsoft.com/en-us/azure/sentinel/roles

Community vote distribution

DE (55%) BE (36%) 9%

⊟ **xyzzy** Highly Voted 4 years, 3 months ago
Azure Sentinel Contributor + Logic App Contributor is correct
upvoted 21 times

⊟ **TDAC** 4 years, 3 months 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

⊟ **dakasa** 2 years, 4 months ago
In the question there is no two different users with different roles, it is for use user you need to assign two roles to be able to create and run playbooks (see the table)
https://docs.microsoft.com/en-us/azure/sentinel/roles#roles-and-allowed-actions
upvoted 1 times

⊟ **JaBe** 4 years, 1 month 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 12 times

⊟ **FumerLaMoquette** 4 years, 1 month ago
I agree.
Azure sentinel responder
Logic app contributor
upvoted 10 times

⊟ **MrGarak1** 4 years, 1 month 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 5 times

MrGarak1 4 years, 1 month ago

so the answer is correct.

upvoted 1 times

EM1234 1 year, 10 months ago

Not that someone who wrote this 2 years ago would ever come back to read this but I will say it anyway.

I thought it DE but it is BE.

The requirements from the question are:
✑ Create and run playbooks.
✑ Manage incidents.

According to the link everyone keeps adding:
https://learn.microsoft.com/en-us/azure/sentinel/roles#microsoft-sentinel-roles-and-allowed-actions
"Logic App Contributor role to create and edit playbooks."

So that takes care of requirement 1

Then we see further up on the page (I linked above)

"Microsoft Sentinel Responder can, in addition to the above, manage incidents (assign, dismiss, etc.)."

So that takes care of requirement 2 with fewer privileges than Sentinel Contributor.

So, IMO, it doesn't really matter that "Microsoft Sentinel Contributor can, in addition to the above, create and edit workbooks, analytics rules, and other Microsoft Sentinel resources."

Also, I want to point out workbooks are not playbooks, for those of you that may be confused on that.

upvoted 3 times

GatesBill 1 year, 8 months ago

To further confirm BE is correct, here is the reference to it:
https://learn.microsoft.com/en-us/azure/sentinel/roles#microsoft-sentinel-roles-permissions-and-allowed-actions

upvoted 3 times

GatesBill 1 year, 8 months ago

In addition:

Workbooks provide a flexible canvas for data analysis and the creation of rich visual reports within the Azure portal. They allow you to tap into multiple data sources from across Azure, and combine them into unified interactive experiences.

Workbooks can be found under log analytics workspace resource or Azure Sentinel itself. It is like a custom dashboard which lets a user create graphs and other visuals using Kusto query language.

Playbooks are related to Azure Sentinel. They are basically Logic Apps with a trigger that activates the Log App/Playbook when an Azure Sentinel query rule is matched.

Reference: https://www.bettercoder.io/job-interview-questions/2192/what-is-a-difference-between-a-playbook-and-a-workbook-in-azure

upvoted 2 times

naren49 Highly Voted 👍 3 years, 11 months 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 9 times

kiketxu 3 years, 9 months ago

Pretty clear!

https://docs.microsoft.com/en-us/azure/sentinel/roles#roles-and-allowed-actions

upvoted 9 times

Fala_Fel 3 years, 5 months ago

Yes, section "Azure Sentinel roles and allowed actions" clearly shows answer is correct.

D. Azure Sentinel contributor

E. Logic App contributor

upvoted 2 times

Anonymousse 2 years, 2 months ago

Microsoft Sentinel Responder can, in addition to the above, manage incidents (assign, dismiss, etc.).

upvoted 1 times

subhuman Most Recent 1 year, 6 months ago

The highlighted answers are wrong.

correct answer is B & E

Azure sentinel contributor does not satisfy the requirement in the question " Least privilege "

upvoted 1 times

Maxx4 1 year, 6 months ago

Selected Answer: AC

To achieve the tasks of creating and running playbooks, as well as managing incidents in Azure Sentinel while following the principle of least privilege, you should assign the following built-in RBAC roles:

A. Automation Operator

C. Automation Runbook Operator

The Automation Operator role provides the necessary permissions to create and run playbooks in Azure Sentinel. This role allows users to design and execute automation logic using playbooks without granting excessive privileges.

The Automation Runbook Operator role specifically grants permissions to run automation runbooks. While playbooks in Azure Sentinel are implemented using Logic Apps, the Automation Runbook Operator role is designed for Azure Automation and can be used to execute runbooks associated with playbooks.

Assigning only the Automation Operator and Automation Runbook Operator roles ensures that users have the necessary permissions to create and run playbooks while minimizing their access to other sensitive Azure Sentinel resources.

upvoted 1 times

Maxx4 1 year, 6 months ago

The other role options are not directly related to the specified tasks:

B. Azure Sentinel responder: This role is focused on responding to incidents and investigating security alerts but does not provide the necessary permissions for creating and running playbooks.

D. Azure Sentinel contributor: This role provides broader access to Azure Sentinel resources, including managing incidents and playbooks. However, assigning this role would exceed the principle of least privilege as it grants more permissions than required.

E. Logic App contributor: This role provides permissions specifically for managing Logic Apps, but it does not include the necessary permissions for creating and running playbooks in Azure Sentinel.

Therefore, the correct roles to assign are Automation Operator (option A) and Automation Runbook Operator (option C).

upvoted 1 times

tjitsen 1 year, 6 months ago

Selected Answer: BE

B E

Azure Sentinel Responder: manage incidents

Logic App Contributor: create and run playbooks

Azure Sentinel Contributor is correct too but because of principle of least privilege, this is incorrect.

Reference: https://learn.microsoft.com/en-us/azure/sentinel/roles#microsoft-sentinel-roles-permissions-and-allowed-actions

upvoted 1 times

Luc043 1 year, 8 months ago

Selected Answer: BE

Correction

upvoted 1 times

V1nc3n7 1 year, 8 months ago

Selected Answer: BE

BE responder can manage incidents

upvoted 1 times

shouro88 1 year, 11 months ago

Microsoft Sentinel Reader can view data, incidents, workbooks, and other Microsoft Sentinel resources.

Microsoft Sentinel Responder can, in addition to the above, manage incidents (assign, dismiss, etc.).

Option B

You can use the Microsoft Sentinel Playbook Operator role to assign explicit, limited permission for running playbooks, and the Logic App Contributor role to create and edit playbooks.

Option E

upvoted 1 times

fjfg 1 year, 11 months ago

Selected Answer: BE

Considering Least Privilege, the roles should be B (Microsoft Sentinel Responder) to Manage Incidents and E (Logic App Contributor) to create and run playbooks.

https://learn.microsoft.com/en-us/azure/sentinel/roles#roles-and-allowed-actions

upvoted 1 times

Bob27745 2 years, 3 months ago

Valid on exam as of 9/21/2022

upvoted 4 times

Whatsamattr81 2 years, 6 months ago

Badly worded… Microsoft Sentinel Contributor role lets you attach a playbook to an analytics rule. Microsoft Sentinel Responder role lets you run an already attached playbook. Logic App contributor is a given, but there's not enough info in this question - you can't make assumptions. However, LAC role can create as many playbooks as they want, unless they are MSC they can't attach any… I'd go DE to be safe but BE does fall within the parameters of the question.

upvoted 3 times

arska 2 years, 9 months ago

Selected Answer: DE

See naren49 and the table here: https://docs.microsoft.com/en-us/azure/sentinel/roles#microsoft-sentinel-roles-and-allowed-actions

upvoted 2 times

mbecile 2 years, 11 months ago

Selected Answer: DE

You need to have BOTH Azure Sentinel Contributor and Logic App Contributor in order to fulfill the requirement of being able to "Create and Run Playbooks"

See Microsoft's chart specifically showing this, here:

https://docs.microsoft.com/en-us/azure/sentinel/roles#microsoft-sentinel-roles-and-allowed-actions

upvoted 2 times

mkoprivnj 3 years, 1 month ago

Selected Answer: DE

D & E are correct!

upvoted 2 times

⊟ **mkoprivnj** 3 years, 1 month ago

Azure Sentinel Contributor + Logic App Contributor is correct

upvoted 2 times

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

You can use the Logic App Contributor role to assign explicit permission for using playbooks.

Microsoft Sentinel Responder can, in addition to the above, manage incidents (assign, dismiss, etc.)

https://docs.microsoft.com/en-us/azure/sentinel/roles#roles-and-allowed-actions

upvoted 1 times

⊟ **Fearless90** 3 years, 1 month ago

D. Azure Sentinel contributor

E. Logic App contributor

https://docs.microsoft.com/en-us/azure/sentinel/roles

Refer to the table

Microsoft Sentinel Contributor + Logic App Contributor

Create and run playbooks

Manage incidents (dismiss, assign, etc.)

Microsoft Sentinel roles and allowed actions

The following table summarizes the Microsoft Sentinel roles and their allowed actions in Microsoft Sentinel.

upvoted 2 times

Question #27

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

Suggested Answer: *B*
Note: The delay period was 24 hours. In ATP release 2.62, the 24 hour delay period has been increased to 72 hours.

Community vote distribution

B (75%) D (25%)

mnak Highly Voted 4 years, 6 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 26 times

WMG 3 years, 4 months ago
It is still 72 hours. Double check before taking exam, just in case:
https://docs.microsoft.com/en-us/defender-for-identity/sensor-update
upvoted 11 times

btd2020 Highly Voted 4 years, 7 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 14 times

ginsahec 4 years, 7 months ago
Yes , the answer is 72 hrs.
https://docs.microsoft.com/es-es/azure-advanced-threat-protection/sensor-update
upvoted 8 times

Metasploit 4 years, 4 months 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

VTHAR 4 years, 3 months 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 4 years, 3 months 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 3 times

Davidf 4 years, 2 months ago
Did 101 very recently (which has recently been updated) and got 20 and 72 hours as option, went with 72 (and passed)
upvoted 5 times

Maxx4 Most Recent 1 year, 6 months ago
Selected Answer: D

When enabling the delayed deployment of updates for an Azure ATP sensor, the sensor named Sensor1 will be updated approximately 48 hours after the Azure ATP cloud service is updated.

Therefore, the correct option is:

D. 48 hours.

upvoted 2 times

Maxx4 1 year, 6 months ago

A quick search shows 72 hrs. but given that there is no 72 hrs to select. 48 hrs will be the closest.

upvoted 1 times

RomanV 1 year, 8 months ago

Sensors set to Delayed update are updated on a delay of 72 hours, following the official release of each service update.

upvoted 1 times

heyhey12345 2 years, 4 months ago

72 hours

upvoted 2 times

Vikram365 2 years, 7 months ago

72 Hrs

https://docs.microsoft.com/en-us/defender-for-identity/sensor-update

upvoted 3 times

LillyLiver 2 years, 9 months ago

Sensors set to Delayed update are updated on a delay of 72 hours, following the official release of each service update.

upvoted 2 times

mkoprivnj 3 years, 1 month ago

Selected Answer: B

now 72 h.

upvoted 6 times

mkoprivnj 3 years, 1 month ago

72hours

upvoted 2 times

Fearless90 3 years, 1 month ago

It is still 72 hours.
It was 24 hours, but was updated to 72 hours in Azure ATP release 2.62
Double check before taking exam, just in case:
https://docs.microsoft.com/en-us/azure-advanced-threat-protection/atp-whats-new#azure-atp-release-262
https://docs.microsoft.com/en-us/defender-for-identity/sensor-update

upvoted 2 times

Turd1 3 years, 3 months ago

Answers are correct

Straight 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 and high confidence phishing messages, and deliver spam, high confidence spam, and bulk email messages to the user's Junk Email folder. But, you can also create and customize anti-spam policies to quarantine spam, high confidence spam, and bulk-email messages. For more information, see Configure anti-spam policies in EOP.

upvoted 1 times

kiketxu 3 years, 9 months 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 4 years ago

answer would be 72

upvoted 6 times

Question #28 *Topic 2*

DRAG DROP -

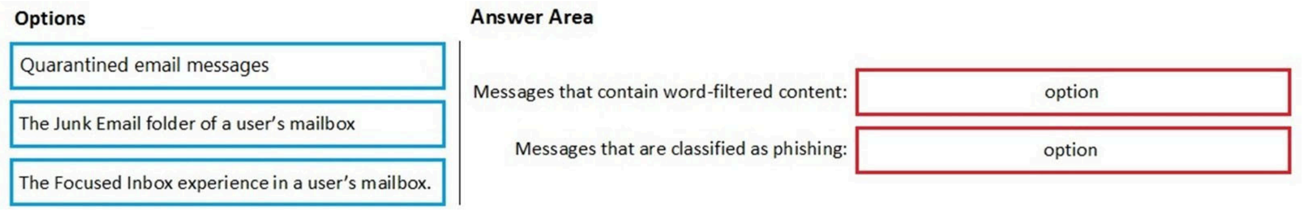
You have a Microsoft 365 E5 subscription. All users use Microsoft Exchange Online.

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:



Options

Quarantined email messages

The Junk Email folder of a user's mailbox

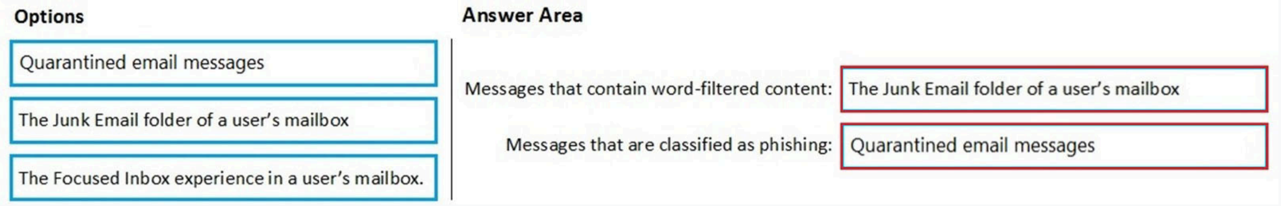
The Focused Inbox experience in a user's mailbox.

Answer Area

Messages that contain word-filtered content: option

Messages that are classified as phishing: option

Suggested Answer:



Options

Quarantined email messages

The Junk Email folder of a user's mailbox

The Focused Inbox experience in a user's mailbox.

Answer Area

Messages that contain word-filtered content: The Junk Email folder of a user's mailbox

Messages that are classified as phishing: Quarantined email messages

asquante Highly Voted 3 years, 8 months ago

This is incorrect. By default both go to Junk Mail, only high confidence phishing goes to Quarantine.

upvoted 17 times

WMG 3 years, 4 months ago

This is correct, both go to Junk.

Current 365 tenants get preset security policies. Standard and Strict. Standard is default for users. The Standard policy for EOP Anti-Phishing sends phishing emails to Junk-email.

upvoted 4 times

JR20 2 years, 11 months ago

This is not true. Phishing messages go to quarantine by default. Phishing messages are quarantined by default:

https://docs.microsoft.com/en-us/microsoft-365/security/office-365-security/configure-your-spam-filter-policies?view=o365-worldwide

upvoted 5 times

Jhill777 2 years, 10 months ago

JR 20 keeps perpetuating a lie. Straight from the default policy in the portal: "If message is detected as spoof

Move message to the recipients' Junk Email folders"

upvoted 5 times

tnagy 2 years, 5 months ago

Wrong. JR is right. Check the default actions.

https://docs.microsoft.com/en-us/microsoft-365/security/office-365-security/configure-your-spam-filter-policies?view=o365-worldwide

upvoted 2 times

TheABC 2 years, 4 months ago

Seems like that page has * move to quar and in my experience thats where I have gone to get stuff out of !

upvoted 2 times

TheABC 2 years, 4 months ago

Looking at my tenant, the default for phishing is to move to junk so I am absolutely confussed, doc says one thing tenant is doing antoher !

upvoted 2 times

JR20 2 years, 3 months ago

If I'm giving you a lie, it's straight from Microsoft's documentation. We all know MS functionality changes and can be wrong over time. I gave you a link, it's right there in black and white, and still is. In addition to that, who said anything about Spoofing? The question is about Phishing. I'm more than happy to admit that the dropdown in the anti-spam policy defaults to junk for Phishing unless they are high confidence. I guess the question is, which source do you use to answer this question? How it functions today or how Microsoft tells you it does?

upvoted 3 times

⊟ **MikeLab** 2 years ago

Documentation seems to have been updated last week. I don't see that phishing email are quarantined in there... I read Move message to Junk Email folder is checked in the table.

upvoted 1 times

⊟ **MikeLab** 2 years ago

And I read again after posting my above reply, there's an * stating that the default action for the spam filtering verdict next to quarantine. The documentation is confused itself
I agree that the default action in a vanilla M365 tenant set the default antispam policy to move the phishing emails to the junk mail folder...

upvoted 1 times

⊟ **chaoscreater** Highly Voted 👍 3 years, 6 months 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 10 times

⊟ **JR20** 2 years, 11 months ago

It's possible it changed in the last 6 months. But this is incorrect. Phishing messages go to quarantine by default:
https://docs.microsoft.com/en-us/microsoft-365/security/office-365-security/configure-your-spam-filter-policies?view=o365-worldwide

upvoted 3 times

⊟ **kanag1** 3 years, 5 months 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 3 times

⊟ **RomanV** Most Recent 🕐 1 year, 8 months ago

Guys relax, this is correct.

" By default, messages that are classified as spam or bulk are delivered to the recipient's Junk Email folder, while messages classified as phishing are quarantined."

Source: https://learn.microsoft.com/en-us/microsoft-365/security/office-365-security/anti-spam-protection-faq?view=o365-worldwide#by-default--what-happens-to-a-spam-detected-message-

upvoted 3 times

⊟ **GatesBill** 1 year, 8 months ago

"By default, messages that are classified as spam or bulk are delivered to the recipient's Junk Email folder, while messages classified as phishing are quarantined."
- Reference: https://learn.microsoft.com/en-us/microsoft-365/security/office-365-security/anti-spam-protection-faq?view=o365-worldwide#by-default--what-happens-to-a-spam-detected-message-

upvoted 1 times

⊟ **thehighlandcow** 1 year, 9 months ago

In the Anti-spam policy, default for phishing messages is to go to quarantine.
In Anti-phishing policy, default for 'spoof' is junk

Question doesn't clearly state what policy we are creating?

upvoted 1 times

⊟ **Santini** 1 year, 11 months ago

Email from spoofed senders (the From address of the message doesn't match the source of the message) is classified as phishing in Defender for Office 365. Sometimes spoofing is benign, and sometimes users don't want messages from specific spoofed sender to be quarantined. To minimize the impact to users, periodically review the spoof intelligence insight, the Spoofed senders tab in the Tenant Allow/Block List, and the

Spoof detections report. Once you have reviewed allowed and blocked spoofed senders and made any necessary overrides, you can be confident to configure spoof intelligence in anti-phishing policies to Quarantine suspicious messages instead of delivering them to the user's Junk Email folder.
https://learn.microsoft.com/en-us/microsoft-365/security/office-365-security/anti-phishing-protection-tuning?view=o365-worldwide

upvoted 1 times

rivetting 2 years ago

Copied from Anti spam inbound policy

Actions

Spam message action
Move message to Junk Email folder
High confidence spam message action
Move message to Junk Email folder
Phishing message action
Move message to Junk Email folder

upvoted 1 times

Lomak 2 years, 2 months ago

Just double check most recent table - and note the (*)
As of today, Phishing is Quarantined by default
https://learn.microsoft.com/en-us/microsoft-365/security/office-365-security/configure-your-spam-filter-policies?view=o365-worldwide

upvoted 2 times

patryk2402 2 years, 1 month ago

@Lomak you are 1000% correct. It clearly states that "An asterisk (*) after the check mark indicates the default action for the spam filtering verdict". Great catch!!!

upvoted 1 times

muc5 2 years, 2 months ago

"By default, messages that are classified as spam or bulk are delivered to the recipient's Junk Email folder, while messages classified as phishing are quarantined." ->https://learn.microsoft.com/en-us/microsoft-365/security/office-365-security/anti-spam-protection-faq?view=o365-worldwide

upvoted 2 times

patryk2402 2 years, 1 month ago

@muc5 that is wrong...

https://learn.microsoft.com/en-us/microsoft-365/security/office-365-security/configure-your-spam-filter-policies?view=o365-worldwide

look at what it states regarding the asterisk

upvoted 1 times

pete26 2 years, 3 months ago

Both go to Junk!

upvoted 2 times

Whatsamattr81 2 years, 6 months ago

as of today - By default, anti-spam polices quarantine phishing and high confidence phishing messages, and deliver spam, high confidence spam, and bulk email messages to the user's Junk Email folder

upvoted 2 times

mxcasarini 2 years, 3 months ago

Wrong, Phishing and High confidence phishing go in Quarantine for default

upvoted 2 times

patryk2402 2 years, 1 month ago

@mxcasarini...you are 1000% right.

upvoted 1 times

Whatsamattr81 2 years, 6 months ago

Move to Junk is the default. Quarantine has to be configured - https://docs.microsoft.com/en-us/microsoft-365/security/office-365-security/set-up-anti-phishing-policies?view=o365-worldwide

upvoted 1 times

galindyl 2 years, 9 months ago

An asterisk (*) after the check mark indicates the default action for the spam filtering verdict.
Action
Move message to Junk Email folder: The message is delivered to the mailbox and moved to the Junk Email folder.
Spam Highconfidencespam Phishing Highconfidencephishing Bulk
Check mark.* Check mark.* Check mark. Check mark Check mark*

Quarantine message: Sends the message to quarantine instead of the intended recipients.
Spam Highconfidencespam Phishing Highconfidencephishing Bulk
Check mark. Check mark Check mark* Check mark* Check mark

See: https://docs.microsoft.com/en-us/microsoft-365/security/office-365-security/configure-your-spam-filter-policies?view=o365-worldwide

upvoted 3 times

patryk2402 2 years, 1 month ago

You are correct

upvoted 1 times

mkoprivnj 3 years, 1 month ago

Both go to JUNK.

upvoted 3 times

JR20 2 years, 11 months ago

I believe this is incorrect. Phishing messages are quarantined by default:
https://docs.microsoft.com/en-us/microsoft-365/security/office-365-security/configure-your-spam-filter-policies?view=o365-worldwide

upvoted 2 times

Fearless90 3 years, 1 month ago

messages that contain word filtered content > Junk
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." So by default anti-spam policy it would go to users Junk folder.

messages that are classified as phishing > Quarantine
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 and high confidence phishing messages, and deliver spam, high confidence spam, and bulk email messages to the user's Junk Email folder. You need to customize anti-spam policies if you need to quarantine them.

upvoted 2 times

Rstilekar 3 years, 1 month ago

https://docs.microsoft.com/en-us/microsoft-365/security/office-365-security/quarantine-email-messages?view=o365-worldwide
Both ans are JUNK, JUNK

Q1 : Messages that are classified as Phishing: Correct Ans. JUNK
By default, anti-spam polices quarantine phishing and high confidence phishing messages, and deliver spam, high confidence spam, and bulk email messages to the user's Junk Email folder. You need to customize anti-spam policies if you need to quarantine them.

Q1 : Messages that contain word-filtered content: Correct Ans. JUNK
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." So by default anti-spam policy it would go to users Junk folder.

upvoted 1 times

_T 3 years ago

Your comment literally contains the opposite of what you just stated. "By default, anti-spam polices quarantine phishing and high confidence phishing messages" . So be default phish is quarantined according to this.

upvoted 2 times

Hami3191 3 years, 3 months ago

Junk , Junk : By default, anti-spam polices quarantine phishing and high confidence phishing messages, and deliver spam, high confidence spam, and bulk email messages to the user's Junk Email folder.

upvoted 1 times

Question #29 *Topic 2*

You have a Microsoft 365 subscription.
You create a Microsoft Defender for Office 365 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

Suggested Answer: *C*
Reference:
https://docs.microsoft.com/en-us/microsoft-365/security/office-365-security/manage-quarantined-messages-and-files#BKMK_ModQuarantineTime

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

Maxx4 1 year, 6 months ago
Selected Answer: D
The answer is D, Anti-malware.

Anti-malware policies are used to scan email attachments for malicious content. They can also be used to quarantine attachments that are suspected to be malicious. The retention duration for attachments in quarantine can be configured in the anti-malware policy.

The other options are incorrect. Anti-phishing policies are used to protect against phishing attacks. DKIM is a domain-based message authentication, reporting, and conformance standard that helps to prevent email spoofing. Anti-spam policies are used to protect against spam.

Here is a table that summarizes the different types of threat management policies in Microsoft Defender for Office 365:

Type of policy Description
Anti-malware Scans email attachments for malicious content and quarantines attachments that are suspected to be malicious.
Anti-phishing Protects against phishing attacks.
DKIM Helps to prevent email spoofing.
Anti-spam Protects against spam.
upvoted 1 times

Dhamus 1 year, 9 months ago
Es correcto, esto únicamente se puede configurar en la directiva de correo no deseado entrante.
upvoted 1 times

EM1234 1 year, 10 months ago
For those of you (like me that expected the answer to involve quarantine policies. Here is something explaining why it is in the anti-spam policy even though the question is asking about safe-attachments.

https://learn.microsoft.com/en-us/microsoft-365/security/office-365-security/quarantine-policies?view=o365-worldwide

" Note

How long quarantined messages are held in quarantine before they expire is controlled by the Retain spam in quarantine for this many days (QuarantineRetentionPeriod) in anti-spam policies. For more information, see Configure anti-spam policies in EOP."

It is like they are testing us on what the devs did that is not intuitive.
upvoted 2 times

Tommy0000 1 year, 10 months ago

Selected Answer: C

"The default value is 15 days in the default anti-spam policy and in new anti-spam policies that you create in PowerShell. The default value is 30 days in new anti-spam policies that you create in the Microsoft 365 Defender portal.A valid value is from 1 to 30 days."

https://learn.microsoft.com/en-us/microsoft-365/security/office-365-security/anti-spam-policies-configure?view=o365-worldwide

upvoted 1 times

⊟ **NishBlade** 1 year, 12 months ago

Anti-spam

upvoted 1 times

⊟ **pete26** 2 years, 3 months ago

Selected Answer: C

C is correct!

upvoted 3 times

⊟ **skycrap** 2 years, 3 months ago

Agree with you

upvoted 1 times

Question #30 *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

Suggested Answer: *D*
Reference:
https://docs.microsoft.com/en-us/windows/security/threat-protection/windows-defender-atp/machine-groups-windows-defender-advanced-threat-protection

Community vote distribution

D (100%)

Maxx4 1 year, 6 months ago

Selected Answer: D

The answer is D, Create two machine groups.

Machine groups in Microsoft Defender Security Center allow you to group computers together based on specific criteria. In this case, you can create two machine groups: one for the executives and one for all other users. You can then configure different remediation settings for each machine group.

For the executives, you can configure the remediation settings to require manual approval by a Microsoft Defender for Endpoint administrator. For all other users, you can configure the remediation settings to occur automatically.

Here are the steps on how to create two machine groups in Microsoft Defender Security Center:

Go to the Machine groups page in the Microsoft Defender Security Center console.
Click Create machine group.
Enter a name and description for the machine group.
Select the Executives check box.
Click Create.
Repeat steps 3-5 to create the Other users machine group.
Once the machine groups are created, you can configure the remediation settings for each machine group.
upvoted 2 times

heshmat2022 2 years, 3 months ago

In Microsoft Defender for Endpoint, you can create device groups and use them to:

Limit access to related alerts and data to specific Azure AD user groups with assigned RBAC roles
Configure different auto-remediation settings for different sets of devices
Assign specific remediation levels to apply during automated investigations
In an investigation, filter the Devices list to specific device groups by using the Group filter.
upvoted 2 times

arska 2 years, 9 months ago

Selected Answer: D

Simple is good.
upvoted 3 times

mbecile 2 years, 11 months ago

D - Keep it simple!

upvoted 1 times

mkoprivnj 3 years, 1 month ago

Selected Answer: D

D is correct!

upvoted 1 times

WMG 3 years, 4 months ago

Create two device groups, one for the rest and one group for the 20 computers that needs these specific settings. Groups are used to manage access to alerts, auto-remediation, remediation levels etc.

https://docs.microsoft.com/en-us/microsoft-365/security/defender-endpoint/machine-groups?view=o365-worldwide

upvoted 4 times

SlimBoy 3 years, 7 months ago

The answer is correct

upvoted 1 times

Question #31 *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.

Suggested Answer: *B*
Reference:
https://docs.microsoft.com/en-us/microsoft-365/security/office-365-security/integrate-office-365-ti-with-mde?view=o365-worldwide

Community vote distribution

B (100%)

mbecile Highly Voted 2 years, 11 months ago

Selected Answer: B

B is Correct, but it's now in the new Security Admin Center (Defender portal)

> Go to the Microsoft 365 Defender portal > Email & collaboration: Explorer
(https://security.microsoft.com/threatexplorer)
> MDE Settings (Top-right Corner)
> Toggle-On "Connect to Defender for Endpoint"
(It's the only option, you can't miss it.)

upvoted 14 times

MallonoX_111 2 years, 9 months ago

https://docs.microsoft.com/en-us/microsoft-365/security/office-365-security/integrate-office-365-ti-with-mde?view=o365-worldwide

upvoted 3 times

kanag1 Highly Voted 3 years, 5 months ago

M365--> Security Portal --> Settings -->EndPoints -->General --> Advanced features -->Microsoft Intune connection

upvoted 10 times

tecnicosoffshoretech 1 year, 10 months ago

This is for intune, not for Office 365

upvoted 1 times

Maxx4 Most Recent 1 year, 6 months ago

Selected Answer: B

The answer is B, From the Microsoft 365 security admin center, select Threat management, and then select Explorer.

The Microsoft 365 security admin center is the central location for managing security settings and features in Microsoft 365. The Threat management page in the security admin center provides a unified view of threats across your organization.
The Explorer page in the Threat management page allows you to view and investigate threats that have been detected by Microsoft Defender for Office 365 and Microsoft Defender for Endpoint. You can also use the Explorer page to configure the integration between these two products.
To configure the integration between Microsoft Defender for Office 365 and Microsoft Defender for Endpoint, follow these steps:
In the Microsoft 365 security admin center, select Threat management.
Select Explorer.
In the MDE Settings section, select the Enable integration with Microsoft Defender for Endpoint check box.
Click Save.

upvoted 1 times

JoeP1 1 year, 10 months ago

Selected Answer: B

The Answer is B, but now(3/4/2023) the site to use is called Microsoft 365 Defender Portal.

The full steps are:
To integrate Microsoft Defender for Office 365 and Microsoft Defender for EndpointL

1. Go into the Microsoft 365 Defender Portal
2. Choose Email & Collaboration
3. Go into Explorer
4. Select MD Settings
5. In the Microsoft Defender for Endpoint connection flyout turn on Connect to Microsoft Defender for Endpoint and click Close
6. Choose settings in the navigation pane
7. On the Settings page choose Endpoints and go into Advanced Features
8. Turn on Office 365 Threat Intelligence connection
9. Click Save Preferences

Updated documentation can be found at: https://learn.microsoft.com/en-us/microsoft-365/security/office-365-security/integrate-office-365-ti-with-mde?view=o365-worldwide

upvoted 3 times

⊟ **spysot** 2 years, 4 months ago

Selected Answer: B

The settings have changed since then. The right answer is B.
Go to Security center > Email & Collaboration > Explorer > MDE settings up right in the screen.

upvoted 4 times

⊟ **Jhill777** 2 years, 7 months ago

Selected Answer: B

Explorer

upvoted 3 times

⊟ **tatendazw** 2 years, 8 months ago

https://docs.microsoft.com/en-us/microsoft-365/security/office-365-security/integrate-office-365-ti-with-mde?view=o365-worldwide#to-integrate-microsoft-defender-for-office-365-with-microsoft-defender-for-endpoint

upvoted 2 times

⊟ **mkoprivnj** 3 years, 1 month ago

Selected Answer: B

B is correct!

upvoted 2 times

⊟ **Rstilekar** 3 years, 1 month ago

Correct ans.
Name change - MS Defender Sec ADmin Center is now MS Defender portal.

Integrating Microsoft Defender for Office 365 with Microsoft Defender for Endpoint is set up in both Defender for Endpoint and Defender for Office 365.

1. For O365 to Endpoint integration#
Go to the Microsoft 365 Defender portal and sign in.
Go to Email & collaboration > Explorer.
On the Explorer page, in the upper right corner of the screen, select MDE Settings.
In the Microsoft Defender for Endpoint connection flyout that appears, turn on Connect to Microsoft Defender for Endpoint (Toggle on.) and then select Close.

2. For Endpoint to O365 integration#
In the navigation pane, choose Settings. On the Settings page, choose Endpoints
On the Endpoints page that opens, choose Advanced features.
Scroll down to Office 365 Threat Intelligence connection, and turn it on (Toggle on.).

When you're finished, select Save preferences.

upvoted 4 times

Rstilekar 3 years, 1 month ago

Correct answer.

Correct ans.

Go to the Microsoft 365 Defender portal and sign in.
Go to Email & collaboration > Explorer.
On the Explorer page, in the upper right corner of the screen, select MDE Settings.
In the Microsoft Defender for Endpoint connection flyout that appears, turn on Connect to Microsoft Defender for Endpoint (Toggle on.) and then select Close.

upvoted 1 times

vinut 3 years, 3 months ago

https://docs.microsoft.com/en-us/microsoft-365/security/office-365-security/integrate-office-365-ti-with-mde?view=o365-worldwide

upvoted 1 times

arunjana 3 years, 7 months 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 7 times

Question #32 *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 Microsoft Defender for Identity 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 Microsoft Defender for Identity sensors.

B. Configure auditing in the Microsoft 365 Compliance center.

C. Turn on Delayed updates for the Microsoft Defender for Identity sensors.

D. Integrate SIEM and Microsoft Defender for Identity.

Suggested Answer: *D*
Note:
There are several versions of this question in the exam. The questions in the exam have two different correct answers:
✑ Integrate SIEM and Microsoft Defender for Identity
Configure Event Forwarding on the domain controllers
▪
Other incorrect answer options you may see on the exam include the following:
✑ Configure Microsoft Defender for Identity notifications
✑ Modify the Domain synchronizer candidate settings on the Microsoft Defender for Identity sensors
✑ Enable the Audit account management Group Policy setting for the servers
✑ Configure auditing in the Microsoft 365 Defender portal
Reference:
https://docs.microsoft.com/en-us/azure-advanced-threat-protection/configure-event-forwarding

Community vote distribution
D (100%)

Bob27745 Highly Voted 2 years, 3 months ago
Valid on exam 9/21/2022
upvoted 5 times

Maxx4 Most Recent 1 year, 6 months ago
Selected Answer: D
The answer is D, Integrate SIEM and Microsoft Defender for Identity.

Microsoft Defender for Identity can be integrated with a third-party SIEM solution to collect and analyze security logs from your on-premises Active Directory domain. This integration allows you to detect when sensitive groups are modified and when malicious services are created.

To integrate SIEM and Microsoft Defender for Identity, you will need to:

Configure the SIEM solution to collect security logs from your on-premises Active Directory domain.
Configure Microsoft Defender for Identity to export security logs to the SIEM solution.
Configure the SIEM solution to analyze the security logs from Microsoft Defender for Identity.
Once the integration is configured, you will be able to view and investigate security events in Microsoft Defender for Identity from the SIEM solution. This will allow you to get a unified view of security events across your on-premises and cloud environments.
upvoted 1 times

Question #33 *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.

Suggested Answer: *B*
Reference:
https://docs.microsoft.com/en-gb/azure/azure-monitor/platform/workbooks-overview

Community vote distribution

B (68%) C (32%)

mbecile Highly Voted 2 years, 11 months ago

The given answer, B, is correct.

If you have Microsoft Sentinel (via Azure AD Premium P1 or P2), you should have the Fusion-based rule with all available connectors enabled by default.

> Azure Portal > Microsoft Sentinel > Configuration: Analytics > Advanced Multistage Attack Detection (Rule Type: Fusion, Status: Enabled)
Source:
https://docs.microsoft.com/en-us/azure/sentinel/configure-fusion-rules

The scenario given in the question is already able to be detected by this default rule.
Source:
https://docs.microsoft.com/en-us/azure/sentinel/fusion-scenario-reference#mass-file-deletion-following-suspicious-azure-ad-sign-in

If you are wanting to see a history of this type of event taking place in the organization, you only need to create a Microsoft Sentinel Workbook for it.
https://docs.microsoft.com/en-us/azure/sentinel/monitor-your-data
upvoted 10 times

EzeQ 2 years, 4 months ago

I did upvote this question, but in my view the correct option is B, because from the same source you "In order to enable these Fusion-powered attack detection scenarios, any data sources listed must be ingested to your Log Analytics workspace."
https://docs.microsoft.com/en-us/azure/sentinel/fusion-scenario-reference
upvoted 2 times

pete26 Highly Voted 2 years, 5 months ago

Selected Answer: B

MeasureUp prep test states it is a workbook. They are the official Microsoft Test Partner.
upvoted 7 times

Maxx4 Most Recent 1 year, 6 months ago

Selected Answer: C

The answer is C, Add a playbook.

A playbook is a collection of tasks that can be automated to respond to a security incident. In this case, you can create a playbook that will:

Investigate the incident by gathering information from Azure AD and Microsoft OneDrive.

Notify the appropriate personnel of the incident.
Take steps to mitigate the incident, such as blocking the compromised account.
By adding a playbook to your active rule, you can ensure that your organization is prepared to respond to multistage attacks in a timely and effective manner.

The other options are incorrect. Adding data connectors will not help you to detect multistage attacks. Adding a workbook will allow you to visualize the data that is collected by your active rule, but it will not help you to respond to incidents. Creating a custom rule template is not necessary in this case, as you can use the default settings of the Fusion rule template.

upvoted 1 times

GPerez73 1 year, 8 months ago

Selected Answer: C

It is C for me.Question is about automation, so playbook

upvoted 2 times

abrub 1 year, 10 months ago

Selected Answer: B

Just says 'detect'. B

upvoted 1 times

mcclane654 1 year, 11 months ago

Selected Answer: B

They way I understand it after some research is that everything is already enabled. so nothing more has to be done. for example the question starts by telling us that the connectors are already set up. However a workbook makes it easier to monitor and therefore has to be the right answer.

Video from Microsoft security showing a demo:
https://www.youtube.com/watch?v=2QGN34n6mSo&ab_channel=MicrosoftSecurity

upvoted 1 times

ARYMBS 2 years, 7 months ago

Selected Answer: C

C? PLAYbook is the automation which you create not the WORKbook...

upvoted 4 times

Hei 2 years, 9 months ago

The question did mention it is using a template. I did a lookup it seems all the data sources are added in a rule template so probably no need to add data connector.

https://docs.microsoft.com/en-us/azure/sentinel/configure-fusion-rules

upvoted 4 times

kakakayayaya 3 years ago

A - the answer.
Azure AD and Office 365 connectors do not provide OneDrive logs.

upvoted 1 times

mkoprivnj 3 years, 1 month ago

Selected Answer: B

B is correct!

upvoted 6 times

AlexanderSaad 3 years, 1 month ago

Create an automation rule
Create a playbook
Add actions to a playbook
Attach a playbook to an automation rule or an analytics rule to automate threat response
https://docs.microsoft.com/en-us/azure/sentinel/tutorial-respond-threats-playbook

upvoted 5 times

Rstilekar 3 years, 1 month ago

You don’t need to have connected all the data sources listed above in order to make Fusion for emerging threats work. However, the more data sources you have connected, the broader the coverage, and the more threats Fusion will find. So A is more correct. The doc doenst mention anything on playbook and workbook (https://docs.microsoft.com/en-us/azure/sentinel/fusion#configure-scheduled-analytics-rules-for-fusion-detections)

upvoted 2 times

⊟ **Brandon_2319** 3 years, 1 month ago

I believe A is correct based off this doc.

https://docs.microsoft.com/en-us/azure/sentinel/connect-data-sources

upvoted 1 times

⊟ **Fluffhead** 3 years, 3 months ago

A is correct. The next step in using the Fusion rule template is to create data connections

upvoted 2 times

⊟ **saeedsaf** 3 years, 3 months ago

The link provided points towards creating a workbook, but does not relate to Fusion detections. The answer is most likely A since Fusion detection relies on multiple data sources and we only have Azure AD/Office 365 connected, but nothing from on-prem.

https://docs.microsoft.com/en-us/azure/sentinel/fusion#configure-scheduled-analytics-rules-for-fusion-detections

upvoted 2 times

⊟ **kiketxu** 3 years, 9 months ago

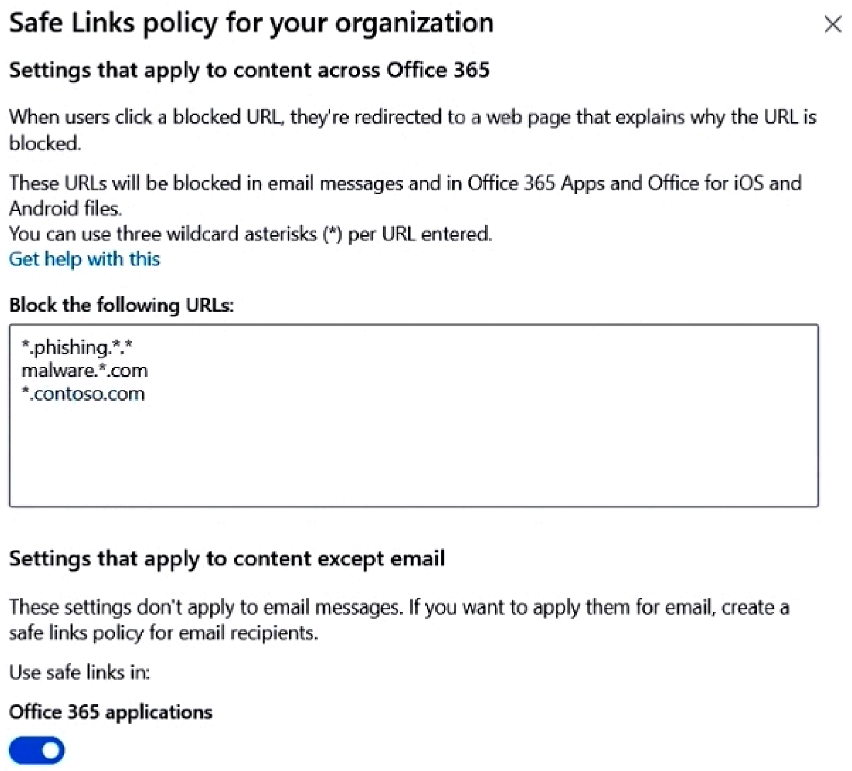
Agree with B.

upvoted 2 times

Question #34 *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.

These URLs will be blocked in email messages and in Office 365 Apps and Office for iOS and Android files.
You can use three wildcard asterisks (*) per URL entered.
Get help with this

Block the following URLs:

```
*.phishing.*.*
malware.*.com
*.contoso.com
```

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 recipients.

Use safe links in:

Office 365 applications

●

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

Suggested Answer: *D*

Reference:

https://docs.microsoft.com/en-us/microsoft-365/security/office-365-security/configure-global-settings-for-safe-links

Community vote distribution

A (67%) D (33%)

Bob27745 Highly Voted 2 years, 3 months ago

Valid on exam 9/21/2022

upvoted 11 times

geecr07 Most Recent 1 year, 7 months ago

Selected Answer: D

So why is the correct answer guys? Is a paint this exam :(

upvoted 1 times

thehighlandcow 1 year, 9 months ago

Still unsure on the answer, but based on my testing, the only entry allowed in the block URL list would be *.contoso.com. All other entries are invalid, test yourself. Also it no longer exists in the safe links policy, it's under Tenant allow/block list | URLs

upvoted 1 times

tecnicosoffshoretech 1 year, 10 months ago

Selected Answer: A

Missing or invalid domain values:

contoso
.contoso.
*.com
*.pdf

The A entry is incorrect configured

Entry: *.contoso.com

Block match:

www.contoso.com
xyz.abc.contoso.com

The D entry is blocked since everything on the left of * is blocked.

Therefore the correct answer should be A
upvoted 2 times

⊟ **tecnicosoffshoretech** 1 year, 10 months ago
https://learn.microsoft.com/en-us/microsoft-365/security/office-365-security/tenant-allow-block-list-urls-configure?view=o365-worldwide
upvoted 1 times

⊟ **VJO** 2 years, 1 month ago
Examples of invalid entries The following entries are invalid:
Missing or invalid domain values:
contoso
.contoso.
*.com
*.pdf
https://learn.microsoft.com/en-us/microsoft-365/security/office-365-security/allow-block-urls?view=o365-worldwide
This article implies that *.phishing.*.* is an invalid entry since it is missing the required domain value of .com
upvoted 2 times

⊟ **Ginaglia** 2 years, 1 month ago
So the correct answer would be A?
B and D look the same to me
upvoted 1 times

⊟ **Chris7910** 2 years, 3 months ago
Why is d correct? Is there any explanation?
upvoted 1 times

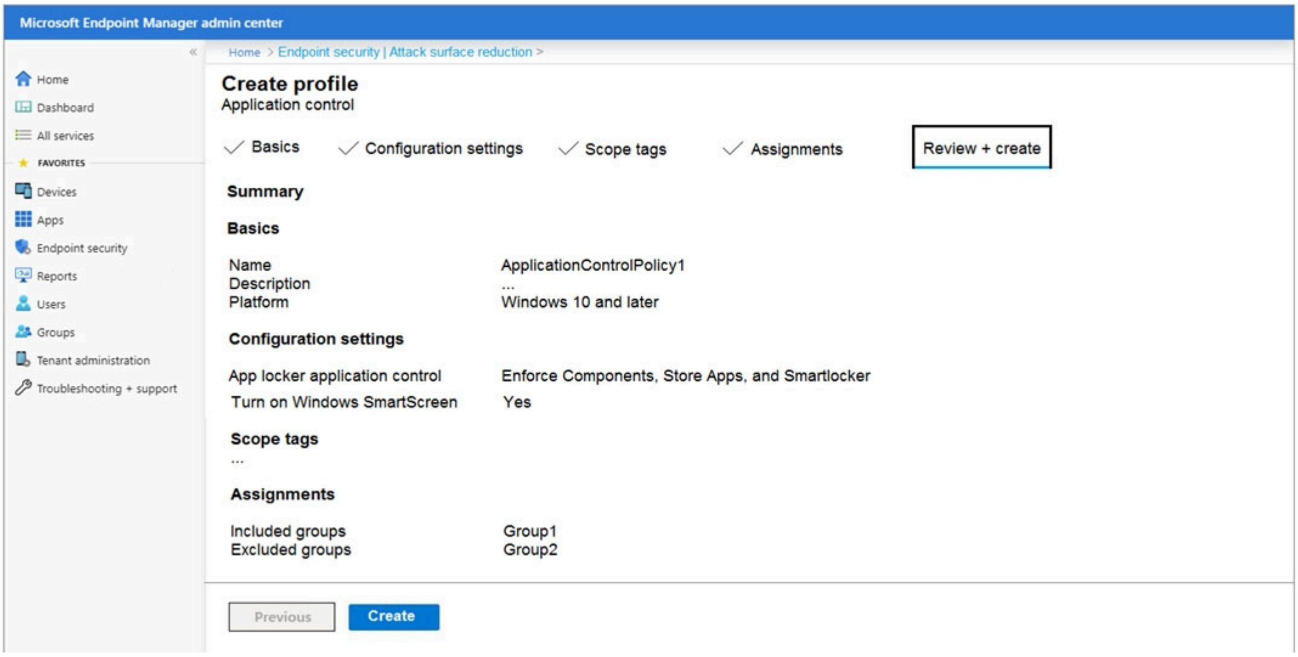
⊟ **pete26** 2 years, 3 months ago
Based on the way Blocked URLs are presented in the screenshot: malware.fabrikam.com will be blocked, but not www.malware.fabrikam.com.
There is no '*' in front of 'malware'
upvoted 5 times

Question #35 *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.



Create profile
Application control

Summary

Basics

Name	ApplicationControlPolicy1
Description	...
Platform	Windows 10 and later

Configuration settings

App locker application control	Enforce Components, Store Apps, and Smartlocker
Turn on Windows SmartScreen	Yes

Scope tags
...

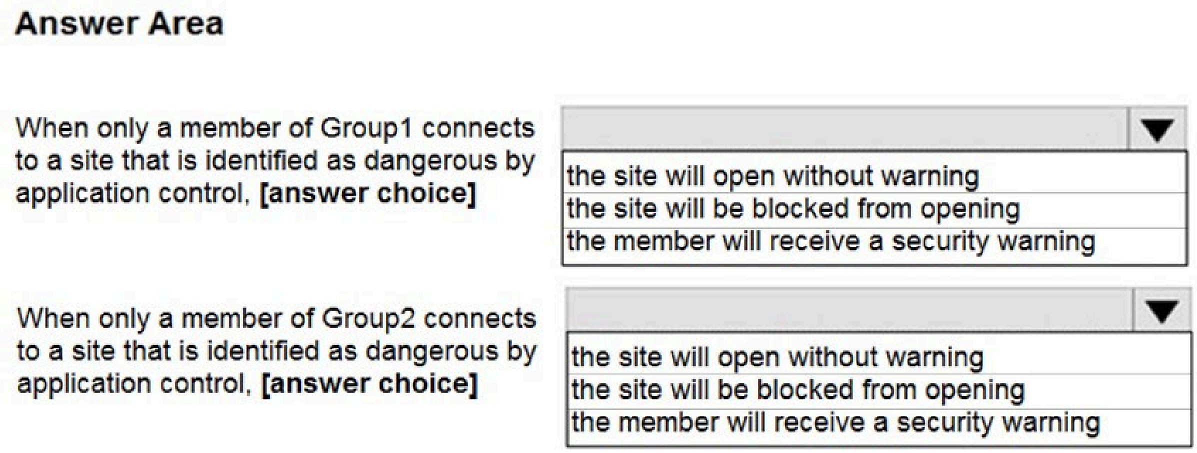
Assignments

Included groups	Group1
Excluded groups	Group2

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

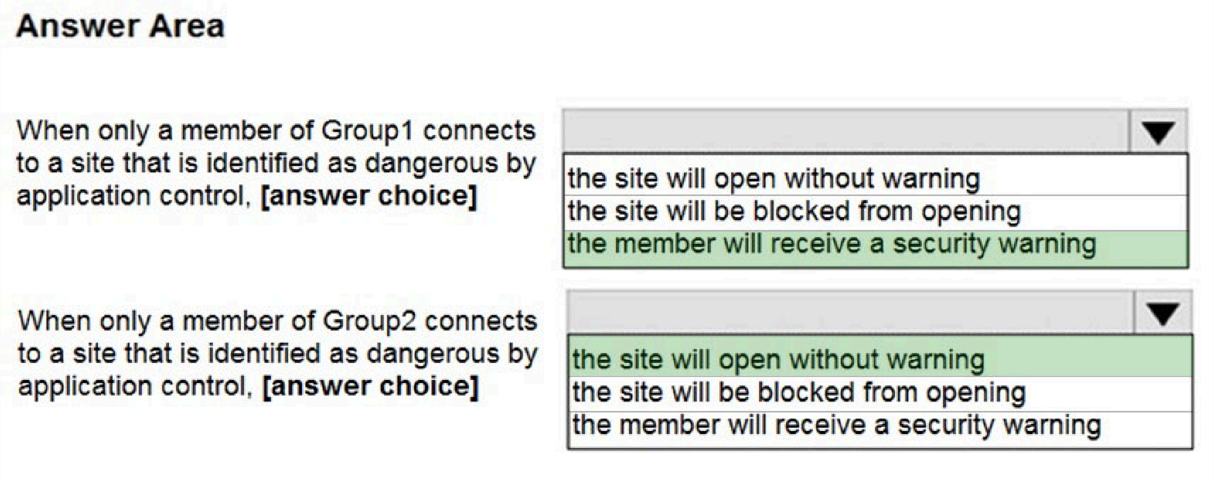
When only a member of Group1 connects to a site that is identified as dangerous by application control, **[answer choice]**

- 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

Suggested Answer:



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

Box 1: the member will receive a security warning.

Group1 is included in the policy so SmartScreen will be enabled. SmartScreen will display a warning.

Box 2: the site will open without warning.
Group2 is excluded from the policy so SmartScreen will not be enabled. Therefore, no warning will be displayed.

Bob27745 Highly Voted 👍 2 years, 3 months ago

Valid on Exam 9/21/2022

upvoted 7 times

DarkAndy Highly Voted 👍 2 years, 6 months ago

Valid on exam. Jun 10, 2022

upvoted 5 times

mcclane654 Most Recent 🕓 1 year, 11 months ago

there is a third setting on this policy:
Block users from ignoring SmartScreen warnings
Setting this to Yes, SmartScreen will not present an option for the user to disregard the warning and run the app. The warning will be presented, but the user will be able to bypass it. Setting this to Not configured will return the setting to Windows default which is to allow the user override. This setting requires the 'Turn on Windows SmartScreen' setting be enabled.

Since this is not enabled, only a warning would occur on included groups

upvoted 3 times

stewie055 2 years, 4 months ago

"smartscreen" is reall a exemple of microsoft marketing wording that makes no sens at all when you read it as is. It's not a screen. It might be smart but the entire word say nothing about what it actually do

upvoted 1 times

kakakayayaya 3 years ago

Profile has not been created, just validated :-)

upvoted 1 times

> **tempfreetenm** 2 years, 7 months ago
>
> "You create a profile as shown in the given example", implies the creation has taken place.
>
> upvoted 2 times

mkoprivnj 3 years, 1 month ago

3 & 1 is correct!

upvoted 1 times

Hami3191 3 years, 3 months ago

Microsoft Defender SmartScreen determines whether a site is potentially malicious by:

Analyzing visited webpages looking for indications of suspicious behavior. If Microsoft Defender SmartScreen determines that a page is suspicious, it will show a warning page to advise caution.

upvoted 1 times

kiketxu 3 years, 9 months 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 #36 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

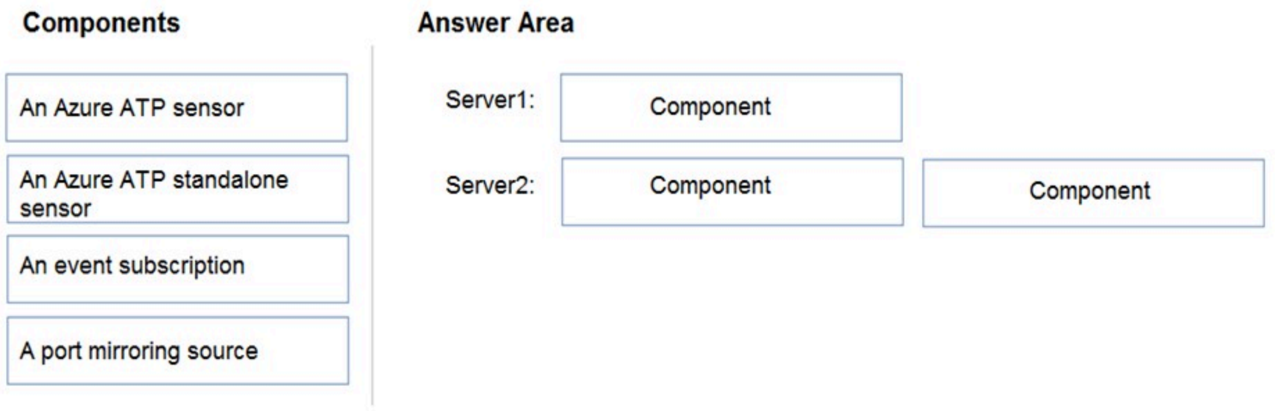
A security policy specifies that Server1 cannot connect to the Internet. Server2 can connect to the Internet.

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:



Components

An Azure ATP sensor

An Azure ATP standalone sensor

An event subscription

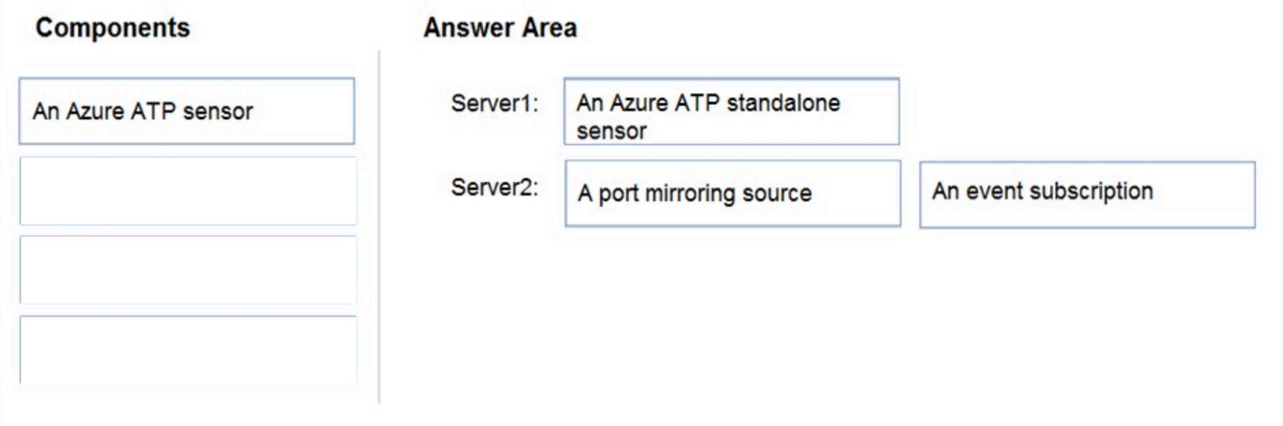
A port mirroring source

Answer Area

Server1: Component

Server2: Component Component

Suggested Answer:



Components

An Azure ATP sensor

Answer Area

Server1: An Azure ATP standalone sensor

Server2: A port mirroring source An event subscription

PeterC Highly Voted 3 years, 9 months 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 86 times

kiketxu 3 years, 9 months ago

Agree, thank you for sharing dude!

upvoted 4 times

hhaywood 3 years, 9 months ago

Agreed

upvoted 3 times

TimurKazan 3 years, 8 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 2 times

Joshing 3 years, 5 months 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

moutaz1983 Highly Voted 3 years, 4 months ago

Provided answer is wrong, I will go in the following:

Server1 - a port mirroring Source
Server2 - an Azure ATP Standalone sensor & an Event subscription

upvoted 6 times

Shadowankh Most Recent 2 years ago

.You install a Azure ATP sensor on domain controllers. Azure ATP standalone Sensor is installed on a dedicated server to monitor multiple domain controllers.
As the DC has no internet connection, the standalone sensor needs to be installed on Server2.
so
Server1 - a port mirroring Source
Server2 - an Azure ATP Standalone sensor & an Event subscription

upvoted 4 times

cluocal 2 years, 9 months ago

Server 1 (DC): Port mirroring SOURCE
--> Mirroring network-traffic from DC as source to Server 2 with ATP standalone sensor!

upvoted 2 times

mbecile 2 years, 11 months ago

Everyone seems to be overlooking that the Domain Controller is in a Hyper-V environment.
The given answer is correct.

"If a virtual domain controller can't be covered by the Defender for Identity sensor, you can have either a virtual or physical Defender for Identity standalone sensor as described in Configure port mirroring."
Source:
https://docs.microsoft.com/en-us/defender-for-identity/technical-faq#how-do-i-monitor-a-virtual-domain-controller-using-defender-for-identity

Port-Mirroring is supported for Virtual Defender for Standalone Identity Sensors with the Virtual Domain Controller on the same host.
Source:
https://docs.microsoft.com/en-us/defender-for-identity/configure-port-mirroring

upvoted 3 times

Jhill777 2 years, 10 months ago

The easiest way is to have a virtual Defender for Identity standalone sensor on every host where a virtual domain controller exists.
Since they don't mention the host as an option, using server 2 is your only option.

upvoted 1 times

EzeQ 2 years, 2 months ago

Sorry but the source says in the beginning "Most virtual domain controllers can be covered by the Defender for Identity sensor" the remaining of the document is for the exceptions.
The focus should be on the "can't connect to the internet"

upvoted 1 times

mkoprivnj 3 years, 1 month ago

Server1 - a port mirroring Source
Server2 - an Azure ATP Standalone sensor & an Event subscription

upvoted 4 times

Rstilekar 3 years, 1 month ago

Azure ATP (now MS Defender for Identity) Sensor vs Standalone Sensor
Azure ATP or MS Defender for Identity Sensor is installed directly on DC -
It monitor the domain controller network traffic for signs of malicious activity, as well as other security risks such as connections made with weak or insecure protocols. ...

The ATP standalone sensor monitors traffic that you direct to it by using port mirroring on your network switches. (Standalone sensor is not directly installed on DCs)

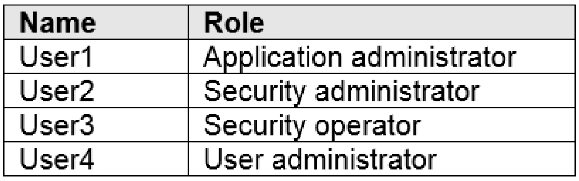
So right answers are
Server1 - a port mirroring Source
Server2 - an Azure ATP (*name change - MS Defender for Identity) Standalone sensor & an Event subscription
upvoted 4 times

⊟ **msjpman** 3 years, 2 months ago
https://docs.microsoft.com/ja-jp/defender-for-identity/configure-port-mirroring
upvoted 1 times

⊟ **jdemii** 3 years, 3 months ago
https://docs.microsoft.com/en-us/defender-for-identity/technical-faq#deployment "The easiest way is to have a virtual Defender for Identity standalone sensor on every host where a virtual domain controller exists" I think the hint for this Q is the hyper-v host
upvoted 2 times

Question #37 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 for Endpoint roles.

Which user should you identify?

A. User1

B. User4

C. User3

D. User2

Suggested Answer: *D*

Reference:

https://docs.microsoft.com/en-us/windows/security/threat-protection/microsoft-defender-atp/rbac

Community vote distribution

D (100%)

Bob27745 Highly Voted 2 years, 3 months ago

Vaild on exam 9/21/2022

upvoted 7 times

Maxx4 Most Recent 1 year, 6 months ago

Selected Answer: D

The answer is D, User2.

Only users with the Security Administrator role in Azure AD can enable Microsoft Defender for Endpoint roles. The other roles, such as Application Administrator, Security Operator, and User Administrator, do not have the necessary permissions.

Here is a table of the permissions for each role:

Role Permissions

Security Administrator Can enable Microsoft Defender for Endpoint roles

Security Operator Can view and manage Microsoft Defender for Endpoint data

Application Administrator Can manage applications and users

User Administrator Can manage user accounts

upvoted 1 times

JoeP1 1 year, 10 months ago

Selected Answer: D

The Security Administrator and the Global Administrator can enable roles in the Microsoft Defender portal.

upvoted 1 times

pete26 2 years, 3 months ago

Selected Answer: D

When you first log in to the Microsoft 365 Defender portal, you're granted either full access or read only access. Full access rights are granted to users with Security Administrator or Global Administrator roles in Azure AD. Read only access is granted to users with a Security Reader role in Azure AD.

upvoted 4 times

heshmat2022 2 years, 3 months ago

Before enabling the feature, it's important that you have a Global Administrator role or Security Administrator role in Azure AD and that you have your Azure AD groups ready to reduce the risk of being locked out of the portal.

upvoted 1 times

Question #38 *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 portal, configure security extensions.

B. From the Cloud App Security portal, configure app connectors.

C. From the Cloud App Security portal, configure log collectors.

D. From the Microsoft 365 compliance center, add and configure a data connector.

Suggested Answer: *A*
Reference:
https://docs.microsoft.com/en-us/cloud-app-security/siem-sentinel

Community vote distribution
A (100%)

pete26 Highly Voted 2 years, 2 months ago
Valid on exam October 14, 2022
upvoted 5 times

msysadmin Most Recent 1 year, 10 months ago
Selected Answer: A
https://www.youtube.com/watch?v=NsgpvNRsscg
upvoted 1 times

VJO 2 years, 1 month ago
This question is outdated. Microsoft Cloud App was replaced with Microsoft Defender for Cloud Apps. Please remove.
upvoted 2 times

Armored5772 2 years, 3 months ago
the same question as 4.80, but different answer
upvoted 1 times

pete26 2 years, 3 months ago
Well, they are asking the question slightly differently – it should be the same though
4.80: You need to manage incidents based on alerts generated by Microsoft Defender for Cloud Apps
2.38: You need to manage incidents based on alerts generated by Microsoft Cloud App Security.
upvoted 2 times

heshmat2022 2 years, 3 months ago
Integrating with Microsoft Sentinel
In the Defender for Cloud Apps portal, under the Settings cog, select Security extensions.

On the SIEM agents tab, select add (+), and then choose Microsoft Sentinel.
upvoted 4 times

xyz213 2 years, 3 months ago
Correct - A:
https://docs.microsoft.com/en-us/defender-cloud-apps/siem-sentinel
upvoted 2 times

Question #39 *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 Microsoft Defender for Identity 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 Microsoft Defender for Identity sensors.

D. Enable the Audit account management Group Policy setting for the servers.

Suggested Answer: *A*
Note:
There are several versions of this question in the exam. The questions in the exam have two different correct answers:
✑ Integrate SIEM and Microsoft Defender for Identity
✑ Configure Event Forwarding on the domain controllers
Other incorrect answer options you may see on the exam include the following:
✑ Configure Microsoft Defender for Identity notifications
✑ Modify the Domain synchronizer candidate settings on the Microsoft Defender for Identity sensors
✑ Configure auditing in the Microsoft 365 Defender portal
Reference:
https://docs.microsoft.com/en-us/azure-advanced-threat-protection/configure-event-forwarding

Community vote distribution

A (67%) D (33%)

Maxx4 1 year, 6 months ago

Selected Answer: D

The answer is D, From the Microsoft 365 compliance center, add and configure a data connector.

To manage incidents based on alerts generated by Microsoft Cloud App Security, you need to first configure a data connector in the Microsoft 365 compliance center. This will allow Microsoft Cloud App Security to send its data to Azure Sentinel. Once the data connector is configured, you can create rules in Azure Sentinel to create incidents based on the alerts from Microsoft Cloud App Security.

The other options are not necessary to manage incidents based on alerts generated by Microsoft Cloud App Security.

Option A, configuring security extensions in the Cloud App Security portal, is used to extend the capabilities of Cloud App Security. It is not necessary to manage incidents.
Option B, configuring app connectors in the Cloud App Security portal, is used to connect Cloud App Security to cloud applications. It is not necessary to manage incidents.
Option C, configuring log collectors in the Cloud App Security portal, is used to collect logs from cloud applications. It is not necessary to manage incidents.
upvoted 1 times

Maxx4 1 year, 6 months ago

Sorry guys this answer was for the previous question related to the "ou need to manage incidents based on alerts generated by Microsoft Cloud App Security.
What should you do first?". please ignore the answer for this question/ if the mod can delete this would be great. Thanks
upvoted 1 times

pete26 2 years, 3 months ago

Selected Answer: A

A is correct!
upvoted 2 times

Bob27745 2 years, 3 months ago

Valid on exam 9/21/2022

upvoted 3 times

heshmat2022 2 years, 3 months ago

To enhance detection capabilities, Defender for Identity needs the Windows events listed in Configure event collection. These can either be read automatically by the Defender for Identity sensor or in case the Defender for Identity sensor is not deployed, it can be forwarded to the Defender for Identity standalone sensor in one of two ways, by configuring the Defender for Identity standalone sensor to listen for SIEM events or by configuring Windows Event Forwarding.

upvoted 1 times

Question #40 *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. Azure Defender for Servers

C. Outlook on the web

D. the Microsoft 365 Compliance center.

E. Microsoft Defender for Identity admin center

Suggested Answer: *AD*
Reference:
https://docs.microsoft.com/en-us/office365/securitycompliance/manage-quarantined-messages-and-files

Community vote distribution

AD (100%)

skycrap Highly Voted 👍 2 years, 3 months ago
I think that this question is outdated. At the moment you can check quarantine in Microsoft 365 Defender under Email & Collaboration --> Review. As far as I know there is no quarantine option in the compliance center (Ms Purview).
upvoted 12 times

Maxx4 Most Recent 1 year, 6 months ago
Selected Answer: AD
The correct answers are D, the Microsoft 365 Compliance center, and A, the Exchange admin center.

The Microsoft 365 Compliance center allows you to view and manage quarantined messages and files. You can use the search bar to search for messages that were sent without attachments. The Exchange admin center allows you to view the message headers of quarantined messages. This can help you to identify the reason why the attachments were removed.

The other options are not necessary to review the attachments that were removed from the messages.

Option B, Azure Defender for Servers, is used to protect on-premises servers from malware and other threats. It is not used to manage quarantined messages and files.
Option C, Outlook on the web, is a web-based email client. It is not used to manage quarantined messages and files.
Option E, Microsoft Defender for Identity admin center, is used to manage Microsoft Defender for Identity, which is a cloud-based solution that protects on-premises Active Directory from threats. It is not used to manage quarantined messages and files.
upvoted 1 times

RomanV 1 year, 8 months ago
In organizations with Defender for Office 365, admins can manage files that were quarantined by Safe Attachments for SharePoint, OneDrive, and Microsoft Teams.
upvoted 1 times

Dzuljzebari 1 year, 10 months ago
You can get there from Compliance portal by selecting more resources > Office 365 Security & Compliance. Message will say that portal is deprecated but will offer a direct link to Quarantined messages. Very sneaky!
upvoted 1 times

Anonymousse 2 years, 2 months ago
See https://www.examtopics.com/discussions/microsoft/view/83292-exam-ms-500-topic-4-question-83-discussion/
upvoted 4 times

judyz 2 years, 3 months ago
should that be A&E?

upvoted 4 times

⊟ **iammjm** 2 years, 3 months ago

The .doc linked in the answer points to https://security.microsoft.com/quarantine and Exchange commandlets. Exchange admin portal points to security.ms as well. As for Compliance Center, where would I be able to view them?

upvoted 1 times

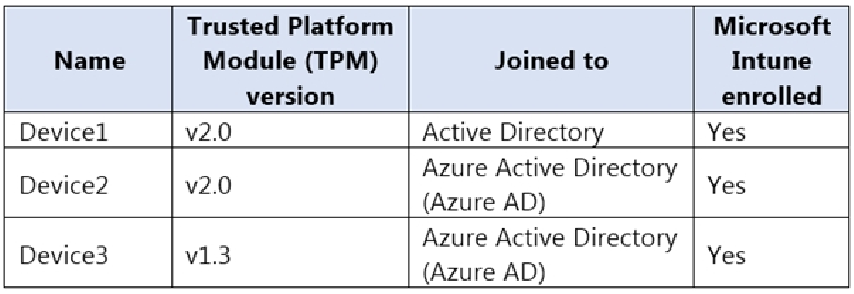
⊟ **EzeQ** 2 years, 2 months ago

Compliance doesn't make any sense in this question. Exchange it could be possible, I do not see a 2nd option, it could be security - not sure.

upvoted 1 times

Question #41 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

Suggested Answer: *B*

To silently enable BitLocker, the device must be Azure AD Joined or Hybrid Azure AD Joined and the device must contain TPM (Trusted Platform Module) 2.0.

Incorrect Answers:

A: Device1 is not Azure AD Joined or Hybrid Azure AD Joined, and the TPM version on Device3 is only 1.3. To silently enable BitLocker, the device must be Azure

AD Joined or Hybrid Azure AD Joined and the device must contain TPM (Trusted Platform Module) 2.0.

C: Device1 is not Azure AD Joined or Hybrid Azure AD Joined. To silently enable BitLocker, the device must be Azure AD Joined or Hybrid Azure AD Joined.

D: The TPM version on Device3 is only 1.3. To silently enable BitLocker, the device must contain TPM (Trusted Platform Module) 2.0.

Reference:

https://docs.microsoft.com/en-us/mem/intune/protect/encrypt-devices

Community vote distribution

D (63%) A (20%) B (17%)

Fcnet Highly Voted 3 years, 3 months ago

May be the documentation has changed but TPM 1.2 is supported for bitlocker

https://docs.microsoft.com/en-us/mem/intune/protect/encrypt-devices#silently-enable-bitlocker-on-devices

You can configure a BitLocker policy that automatically and silently enables BitLocker on a device.

Device must contain at least TPM (Trusted Platform Module) 1.2.

The answer should be

->D. Device2 and Device3 only

upvoted 32 times

Bob27745 Highly Voted 2 years, 3 months ago

Valid on exam 9/21/2022

upvoted 7 times

Jeetu4u Most Recent 1 year, 7 months ago

Selected Answer: D

It should be D.

Device Prerequisites

A device must meet the following conditions to be eligible for silently enabling BitLocker:

If end users sign in to the devices as Administrators, the device must run Windows 10 version 1803 or later, or Windows 11.
If end users sign in to the devices as Standard Users, the device must run Windows 10 version 1809 or later, or Windows 11.
The device must be Azure AD Joined or Hybrid Azure AD Joined.
Device must contain at least TPM (Trusted Platform Module) 1.2.
The BIOS mode must be set to Native UEFI only.
upvoted 1 times

Erez2023 1 year, 9 months ago
D
"BitLocker supports TPM version 1.2 or higher" :
https://learn.microsoft.com/en-us/windows/security/information-protection/bitlocker/bitlocker-overview-and-requirements-faq
upvoted 1 times

pid 1 year, 7 months ago
Question is weird too, how is a device 1 being managed by Intune if its only in Local AD? You need to be Hybrid or Azure AD joined to be in Intune
upvoted 1 times

msysadmin 1 year, 10 months ago
Selected Answer: D
I chose D option. Technically A correct. Question is unclear.

In practice, the correct answer is A.

Device Prerequisites

A device must meet the following conditions to be eligible for silently enabling BitLocker:

If end users sign in to the devices as Administrators, the device must run Windows 10 version 1803 or later, or Windows 11.
If end users sign in to the devices as Standard Users, the device must run Windows 10 version 1809 or later, or Windows 11.
The device must be Azure AD Joined or Hybrid Azure AD Joined.
Device must contain at least TPM (Trusted Platform Module) 1.2.
The BIOS mode must be set to Native UEFI only.
upvoted 1 times

mcclane654 1 year, 11 months ago
Selected Answer: D
I got confused by device 1. but its probably azure ad registrered. and therefore can't be silently enabled.

TPM 1.3 is also a BS option. but guess since its higher than 1.2 it should be possible in fantasy land where 1.3 exists.
upvoted 2 times

mhh 2 years ago
Selected Answer: B
There ist no TPM 1.3. So B is correct
upvoted 2 times

Erez2023 1 year, 9 months ago
D
"BitLocker supports TPM version 1.2 or higher" :
https://learn.microsoft.com/en-us/windows/security/information-protection/bitlocker/bitlocker-overview-and-requirements-faq
upvoted 1 times

Just2a 2 years, 1 month ago
Answer is 2 and 3 The device must be Azure AD Joined or Hybrid Azure AD Joined and
Device must contain at least TPM (Trusted Platform Module) 1.2. #3 is TPM 1.3
as per Microsoft - https://learn.microsoft.com/en-us/mem/intune/protect/encrypt-devices#device-prerequisites
upvoted 1 times

Kaneshiro 2 years, 2 months ago
Solo existen las versiones 1.2 y 2.0, no existe ninguna version 1.3 por lo que esta pregunta tiene trampa.

https://www.xatakawindows.com/windows/asi-puedes-comprobar-tu-ordenador-posee-chip-tpm-puedes-instalar-windows-11-tu-equipo

upvoted 1 times

pete26 2 years, 2 months ago

Valid on exam October 14, 2022

upvoted 3 times

Broesweelies 2 years, 3 months ago

Selected Answer: D

The prerequisites changed a few months ago: 1.2 TPM or 2.0 TPM, before that only 2.0 was compatible to silently enable Bitlocker. So Device 2 and 3.

Device 1 is a tricky one: You can Intune enroll devices without Azure AD join, but then again they say its a hybrid environment. Very naughty question from Microsoft!

upvoted 1 times

yoton 2 years, 3 months ago

Selected Answer: D

Link provided by exam topics states "Device must contain at least TPM (Trusted Platform Module) 1.2." Thus Device2 & Device3 are supported.

upvoted 1 times

RVR 2 years, 3 months ago

Selected Answer: D

" The device must also be Azure AD joined or hybrid Azure AD joined. The device must also contain at least TPM version 1.2 or the Trusted Platform Module."

Reference: https://cloudacademy.com/course/microsoft-365-device-application-protection-2923/configuring-and-managing-windows-device-encryption/

upvoted 1 times

pete26 2 years, 3 months ago

If it is true that in order to silently enable BitLocker, the device must contain TPM (Trusted Platform Module) 2.0. than only option would be B. Device1 is not AAD joined and Device3 is lacking the needed TPM version. However, it is cruel by Microsoft to put a TPM version that does not exist. So much confusion because of it.

upvoted 1 times

pete26 2 years, 3 months ago

TPM 1.2 is enough to silently enable Bitlocker. I still would go with B as 1.3 does not exist.

upvoted 2 times

yoton 1 year, 10 months ago

Uh https://trustedcomputinggroup.org/resource/tpm-library-specification/

upvoted 1 times

heshmat2022 2 years, 3 months ago

Windows 11, Windows 10, Windows Server 2016, and Windows Server 2019 support Device Health Attestation with TPM 2.0. Support for TPM 1.2 was added beginning with Windows version 1607 (RS1). TPM 2.0 requires UEFI firmware. A computer with legacy BIOS and TPM 2.0 won't work as expected.

upvoted 1 times

xyz213 2 years, 3 months ago

Selected Answer: B

B is only correct answer, TPM 1.3 doesn't exist, it is more catch me answer

upvoted 3 times

TheABC 2 years, 4 months ago

I think all them can be enrolled, join the dots, 1.3v is over 1.2v so thats fine, there is no such thing as Active Directory joined in AAD its Hybird or AAD joined, so by fact it states Hybrid we assume its joined, there for all are acceptable

upvoted 1 times

Question #42 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:

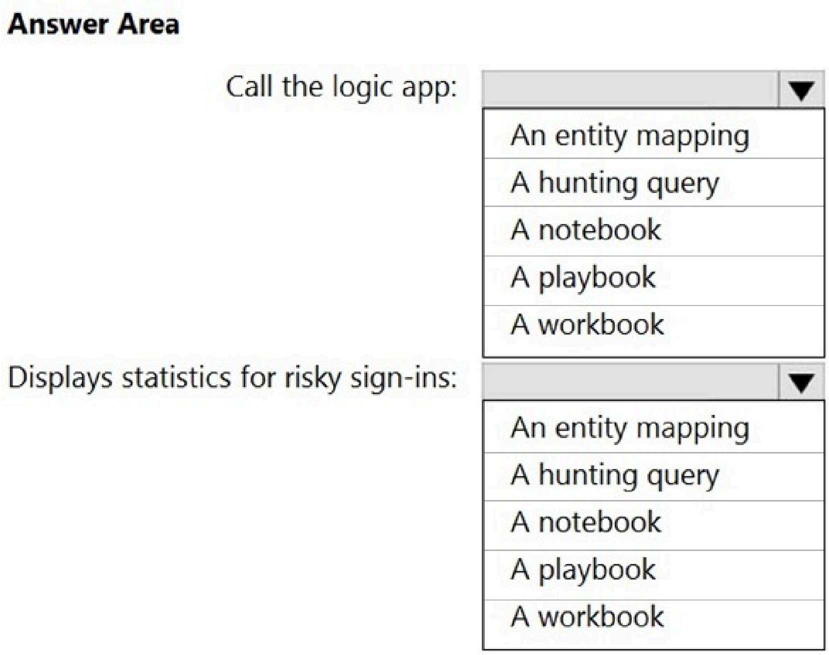
✑ Call the Azure logic app when an alert is triggered for a risky sign-in.

✑ 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:

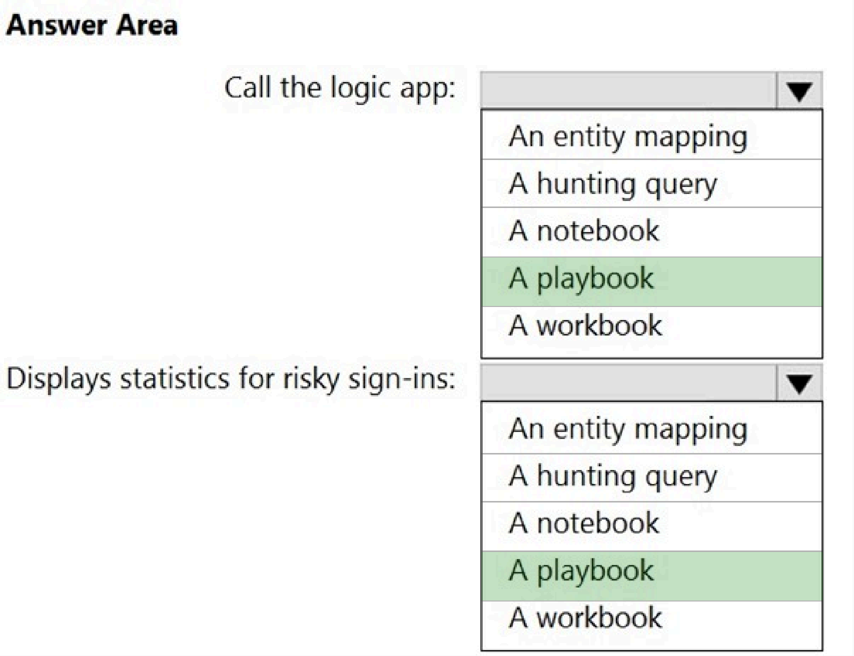


Answer Area

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

Suggested Answer:



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

Reference:

https://docs.microsoft.com/en-us/azure/sentinel/tutorial-respond-threats-playbook

⊟ **fred99** Highly Voted 3 years, 8 months ago

to display stats, should not it be Workbook instead of playbook?

upvoted 47 times

arunjana 3 years, 7 months ago

Absolutely right. Answers should be 1) Playbook, 2) Workbook

upvoted 29 times

prabhjot 3 years, 5 months ago

playbook (logic app) is for integration only so therefor to display reports and sats- Workbook shines

upvoted 4 times

M1crsoftPro Highly Voted 👍 3 years, 7 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 14 times

kmk_01 Most Recent ⏱ 1 year, 9 months ago

Playbooks are basically Logic Apps with a trigger that activates the Log App/Playbook when an Azure Sentinel query rule is matched). Workbooks provide a flexible canvas for data analysis and the creation of rich visual reports within the Azure portal.

https://www.bettercoder.io/job-interview-questions/2192/what-is-a-difference-between-a-playbook-and-a-workbook-in-azure

upvoted 1 times

ChachaChatra 1 year, 11 months ago

Valid on28/01/23

upvoted 2 times

yoton 2 years, 3 months ago

I dont think the second answer displayed is correct. A workbook, NOT a playbook, will display stats.

upvoted 2 times

cluocal 2 years, 9 months ago

Playbook --> Actions

Workbook --> Monitoring

upvoted 12 times

mkoprivnj 3 years, 1 month ago

1) Playbook, 2) Workbook

upvoted 6 times

Fearless90 3 years, 1 month ago

Call the Azure logic app when an alert is triggered for a risky sign-in > a playbook

https://docs.microsoft.com/en-us/azure/sentinel/automate-responses-with-playbooks

displays statistics for risky sign-ins that are detected and resolved > a workbook

https://docs.microsoft.com/en-gb/azure/azure-monitor/visualize/workbooks-overview

upvoted 3 times

Fcnet 3 years, 3 months ago

i agree with M1crsoftPro

the answer should be

call the logic app : playbook

display the risky sing in logs : workbook

upvoted 3 times

MimeTalk 3 years, 3 months ago

Calling the logic app is playbook

https://docs.microsoft.com/en-us/azure/sentinel/automate-responses-with-playbooks

The second one is workbook

https://docs.microsoft.com/en-gb/azure/azure-monitor/visualize/workbooks-overview

upvoted 1 times

saregi 3 years, 7 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

Question #43 *Topic 2*

DRAG DROP -

You have an Azure subscription and a Microsoft 365 subscription.

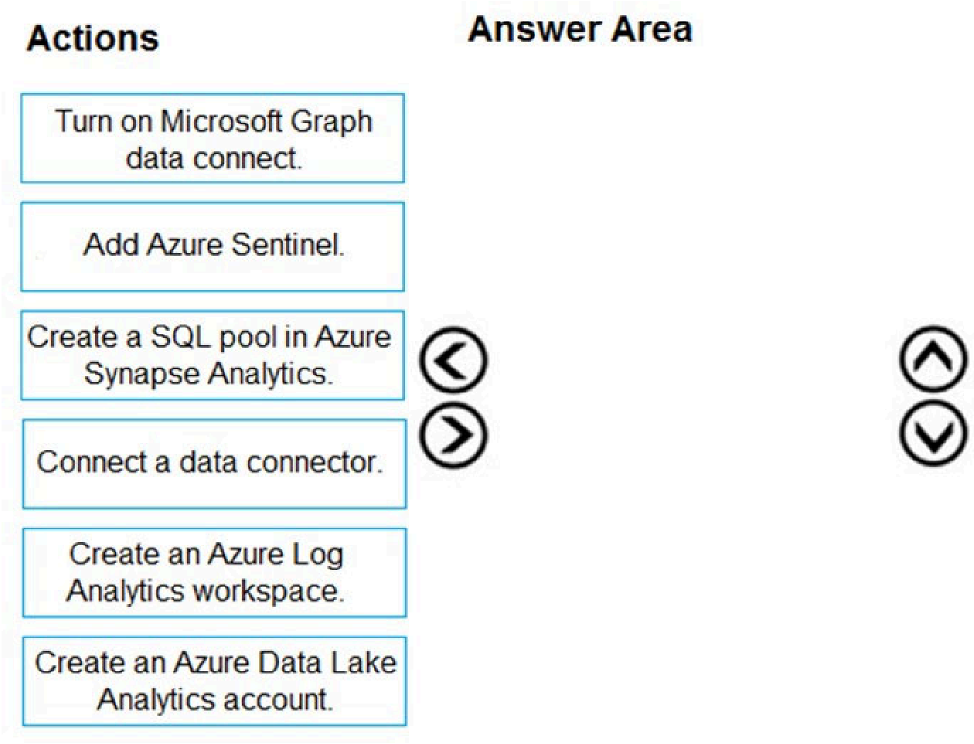
You need to perform the following actions:

✑ Deploy Microsoft Sentinel.

✑ Collect the Office 365 activity log by using Microsoft Sentinel.

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:

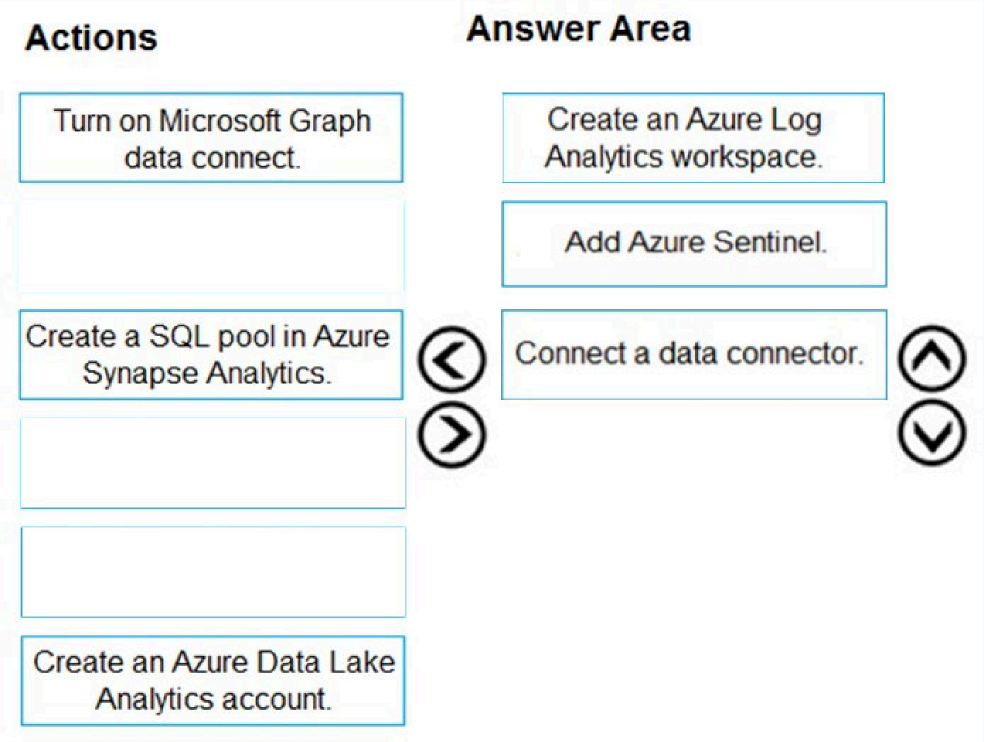


Actions

- Turn on Microsoft Graph data connect.
- Add Azure Sentinel.
- Create a SQL pool in Azure Synapse Analytics.
- Connect a data connector.
- Create an Azure Log Analytics workspace.
- Create an Azure Data Lake Analytics account.

Answer Area

Suggested Answer:



Actions

- Turn on Microsoft Graph data connect.
- Create a SQL pool in Azure Synapse Analytics.
- Create an Azure Data Lake Analytics account.

Answer Area

1. Create an Azure Log Analytics workspace.
2. Add Azure Sentinel.
3. Connect a data connector.

Reference:

https://docs.microsoft.com/en-us/azure/sentinel/quickstart-onboard https://docs.microsoft.com/en-us/azure/sentinel/connect-office-365

RomanV 1 year, 8 months ago

Given answers are correct. A prereq for Sentinel is Log Analytics.

"A Log Analytics workspace is required to house all of the data that Microsoft Sentinel will be ingesting and using for its detections, analytics, and other features. For more information, see Microsoft Sentinel workspace architecture best practices. Microsoft Sentinel doesn't support Log Analytics workspaces with a resource lock applied."

Source: https://learn.microsoft.com/en-us/azure/sentinel/prerequisites

Ps: If you don't pass the exam I will never talk to you again. I put time and brains in the comments to educate you in order for you to pass the d*mn exam. Success!

upvoted 3 times

⊟ **examdog** 2 years ago

When you add Sentinal, you have to add it to a log analytics workspace. So the answer is correct.

upvoted 3 times

⊟ **Just2a** 2 years, 1 month ago

Answer is Add Sentinel
Create workspace
Add connector

The question didnt see pre-requisite. So i think this is the other that needs to be done

upvoted 2 times

⊟ **Tanasi** 1 year, 7 months ago

you add Sentinel on a Workspace. But you can directly create Workspace when you want to create a Sentinel; I guess you are right too :D

upvoted 1 times

⊟ **EzeQ** 2 years, 2 months ago

from my reading of the referenced source, the only thing needed after installing Sentinel is to turn on the connector, but if you need to have 3 actions the Microsoft graph activation is the one that makes sense (as step 2).
Sentinel requires a Log Analytics workspace, but it does not appear in the options.

upvoted 1 times

⊟ **pete26** 2 years, 3 months ago

Answer is correct!

upvoted 2 times

⊟ **pete26** 2 years, 3 months ago

It is a re-worded question with the new terminology:
https://www.examtopics.com/discussions/microsoft/view/10311-exam-ms-500-topic-2-question-20-discussion/

upvoted 2 times

⊟ **billo79152718** 2 years, 3 months ago

correct!

upvoted 2 times

⊟ **emon8972** 2 years, 3 months ago

How many questions repeated from here?

upvoted 1 times

Question #44 *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 Microsoft Defender Exploit Guard (Microsoft Defender EG) on the devices.
Which type of device configuration profile should you use?

A. Endpoint protection

B. Device restrictions

C. Identity protection

D. Microsoft Defender for Endpoint

Suggested Answer: *A*
Reference:
https://docs.microsoft.com/en-us/mem/intune/protect/endpoint-protection-windows-10

Community vote distribution
A (100%)

⊟ **Maxx4** 1 year, 6 months ago
Selected Answer: A
The answer is A, Endpoint protection.

Microsoft Defender Exploit Guard (Microsoft Defender EG) is a set of security features that can be enabled on Windows 10 devices to help protect them from malware and other threats. These features can be enabled by using a device configuration profile in Microsoft Endpoint Manager.

The Endpoint protection device configuration profile contains settings for a variety of security features, including Microsoft Defender EG. To enable Microsoft Defender EG, you need to select the Exploit protection setting and then choose the desired settings.

The other options are not correct.

Option B, Device restrictions, is used to configure device-level restrictions, such as screen time limits and application blocking.
Option C, Identity protection, is used to configure identity-based security features, such as multi-factor authentication and passwordless login.
Option D, Microsoft Defender for Endpoint, is a comprehensive endpoint security solution that includes Microsoft Defender EG. However, you cannot enable Microsoft Defender EG using a Microsoft Defender for Endpoint device configuration profile.
upvoted 1 times

⊟ **King_Khong** 1 year, 9 months ago
in my exam 02/03/23
upvoted 4 times

⊟ **pete26** 2 years, 3 months ago
Selected Answer: A
A is correct!
https://learn.microsoft.com/en-us/mem/configmgr/protect/deploy-use/create-deploy-exploit-guard-policy
upvoted 3 times

Question #45 *Topic 2*

DRAG DROP -

You have a Microsoft 365 E5 subscription.

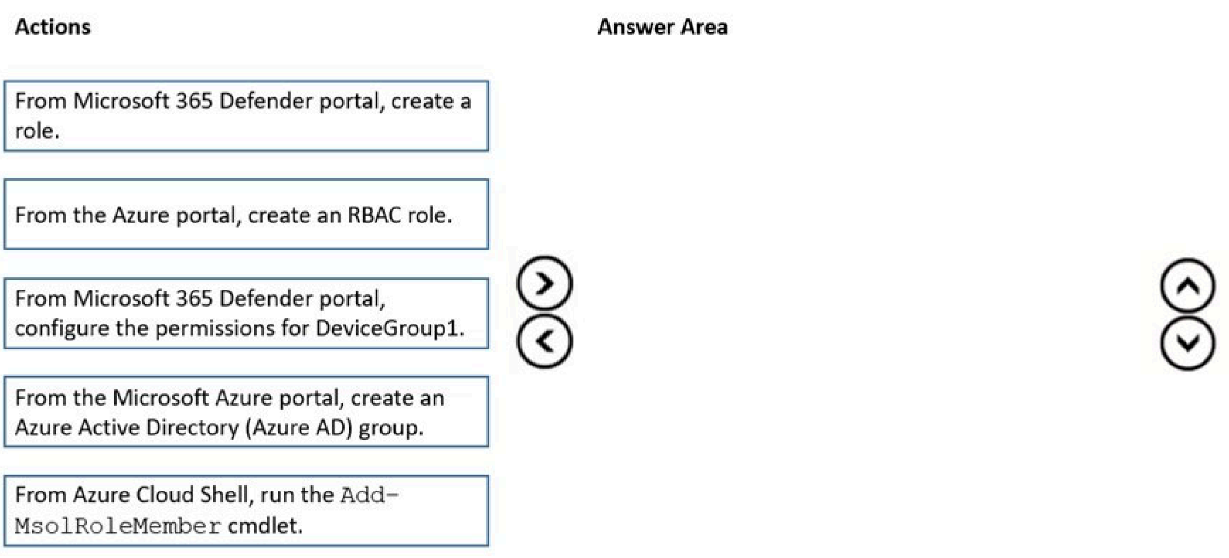
All computers run Windows 10 and are onboarded to Microsoft Defender for Endpoint.

You create a Microsoft Defender for Endpoint device group named DeviceGroup1.

You need to enable delegation for the security settings of the computers in DeviceGroup1.

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:

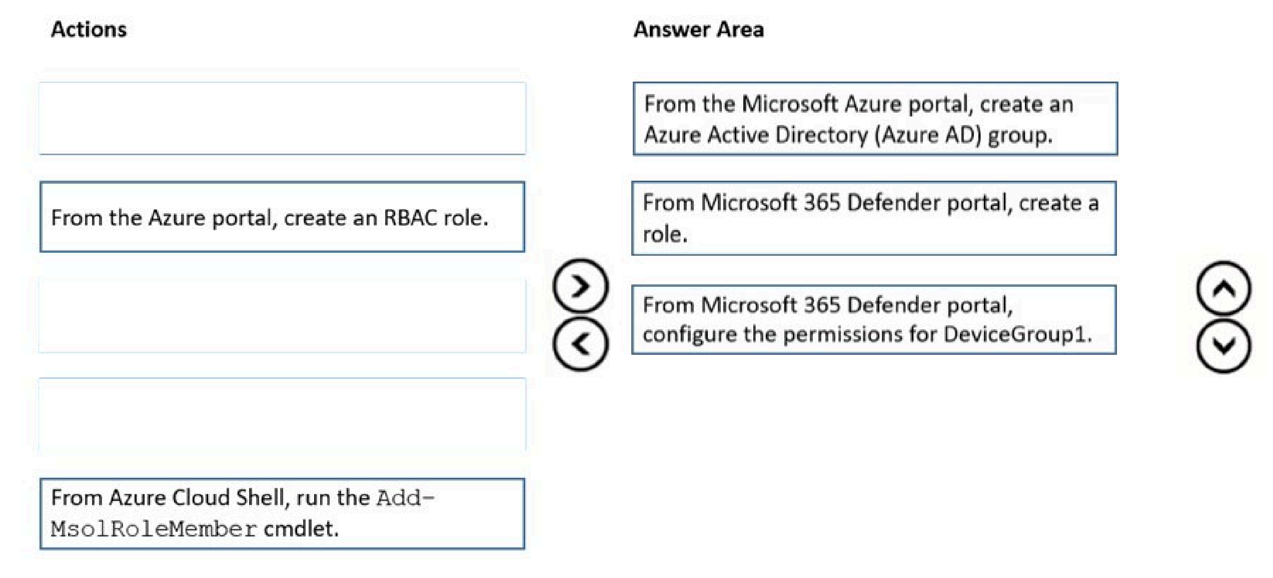


Actions

- From Microsoft 365 Defender portal, create a role.
- From the Azure portal, create an RBAC role.
- From Microsoft 365 Defender portal, configure the permissions for DeviceGroup1.
- From the Microsoft Azure portal, create an Azure Active Directory (Azure AD) group.
- From Azure Cloud Shell, run the `Add-MsolRoleMember` cmdlet.

Answer Area

Suggested Answer:



Actions

- From the Azure portal, create an RBAC role.
- From Azure Cloud Shell, run the `Add-MsolRoleMember` cmdlet.

Answer Area

1. From the Microsoft Azure portal, create an Azure Active Directory (Azure AD) group.
2. From Microsoft 365 Defender portal, create a role.
3. From Microsoft 365 Defender portal, configure the permissions for DeviceGroup1.

fjfg Highly Voted 1 year, 11 months ago

Very similar to another question, see discussion on:

https://www.examtopics.com/discussions/microsoft/view/10311-exam-ms-500-topic-2-question-20-discussion/

upvoted 5 times

Maxx4 Most Recent 1 year, 6 months ago

The three actions you need to perform in sequence to enable delegation for the security settings of the computers in DeviceGroup1:

Create a security group in Azure Active Directory (Azure AD) and add the users who will be delegated with the permissions to manage the security settings of the computers in DeviceGroup1.

Assign the Microsoft Defender for Endpoint Security Administrator role to the security group in Azure AD.
Enable delegation for the security settings of DeviceGroup1 in the Microsoft Defender for Endpoint portal.
upvoted 1 times

⊟ **RomanV** 1 year, 8 months ago

The correct answers are:

1. Create a role
2. Create a group
3. Configure the permissions for devicegroup1

"Create roles and assign the role to an Azure Active Directory group
After creating roles, you'll need to create a device group and provide access to the device group by assigning it to a role that you just created."

Source: https://learn.microsoft.com/en-us/microsoft-365/security/defender-endpoint/user-roles?view=o365-worldwide
upvoted 3 times

Question #46 *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

Suggested Answer: *D*
Reference:
https://docs.microsoft.com/en-us/office365/securitycompliance/set-up-anti-phishing-policies

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

⊟ **Joshing** Highly Voted 3 years, 5 months 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 10 times

⊟ **WMG** 3 years, 4 months ago
This is the correct answer and explanation. (they never said the mailboxes were migrated, did they now?)
upvoted 3 times

⊟ **KarimaMaf** Most Recent 1 year, 6 months ago
Note: For Mailbox Intelligence to work, recipient mailboxes must be hosted in Exchange Online
https://practical365.com/getting-the-most-out-of-microsoft-defender-for-office-365-policies/
upvoted 1 times

⊟ **Maxx4** 1 year, 6 months ago
Selected Answer: C
The answer is C. Select Directory extension attribute sync in Microsoft Azure Active Directory Connect (Azure AD Connect).

Mailbox intelligence is a feature of Microsoft Defender for Office 365 that uses the contact history learned from mailboxes to help protect users from impersonation attacks. In order to enable mailbox intelligence, you need to select Directory extension attribute sync in Microsoft Azure Active Directory Connect (Azure AD Connect). This will ensure that the contact history from on-premises mailboxes is synced to the cloud.

The other options are incorrect.

Option A is incorrect because attribute filtering is used to control which attributes are synced from on-premises to the cloud. It is not required to enable mailbox intelligence.
Option B is incorrect because the Microsoft Defender for Office 365 add-on is not required to enable mailbox intelligence. It is only required if you want to use the advanced features of Microsoft Defender for Office 365.
Option D is incorrect because migrating the on-premises mailboxes to Exchange Online is not required to enable mailbox intelligence.
Therefore, the correct answer is C.
upvoted 1 times

⊟ **arska** 2 years, 9 months ago
Selected Answer: D

See Joshing and hyve

upvoted 1 times

mkoprivnj 3 years, 1 month ago

Selected Answer: D

D is correct!

upvoted 1 times

hyve 3 years, 2 months ago

Mailbox intelligence is only available for Exchange Online mailboxes.

upvoted 2 times

mahtab 3 years, 6 months 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 3 times

JoeExam 3 years, 6 months 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 years, 5 months 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 3 years, 6 months 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 2 times

JoelB 3 years, 6 months 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 3 years, 6 months ago

Wrong Xtian is right, read the doc

upvoted 1 times

Xtian_ar 3 years, 6 months ago

E5 licenses already have antiphishing policies capability

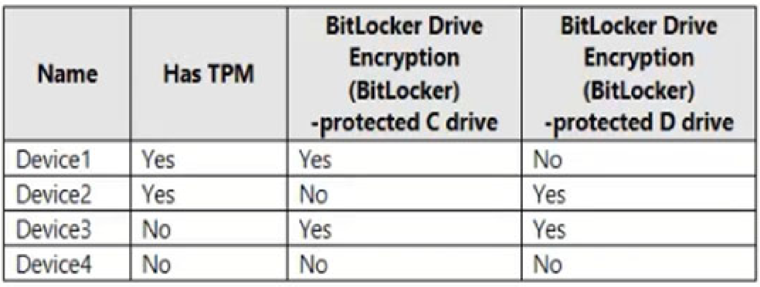
upvoted 3 times

Question #47 — *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.

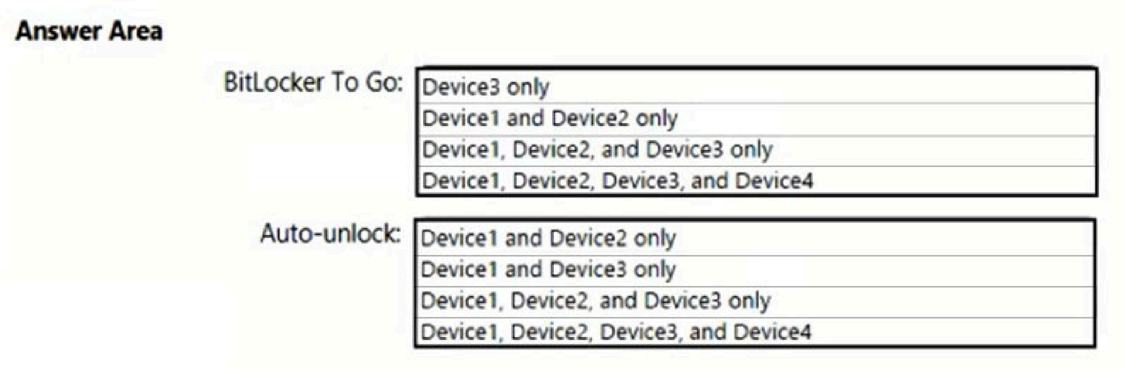


Name	Has TPM	BitLocker Drive Encryption (BitLocker) -protected C drive	BitLocker Drive Encryption (BitLocker) -protected D drive
Device1	Yes	Yes	No
Device2	Yes	No	Yes
Device3	No	Yes	Yes
Device4	No	No	No

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

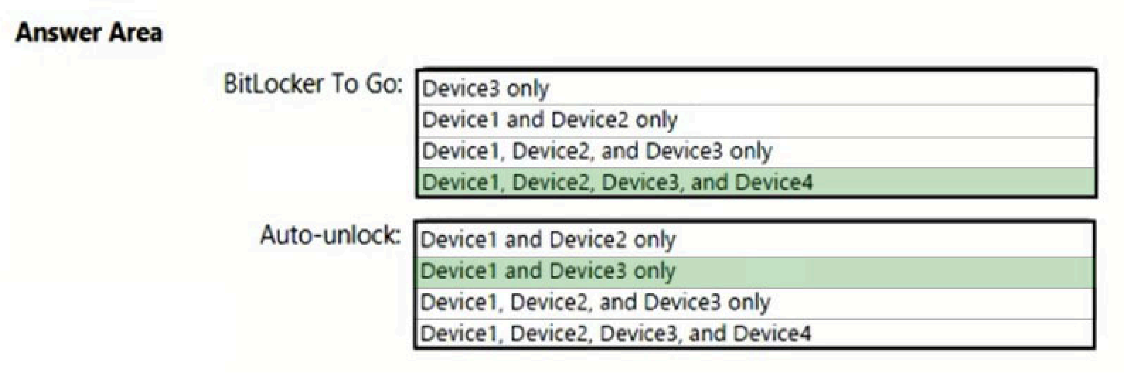
BitLocker To Go:

- 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

Suggested Answer:



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 4 years, 6 months 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 46 times

TimurKazan 3 years, 8 months 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 2 times

TimurKazan 3 years, 8 months 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 3 times

JiDu 4 years, 5 months ago

Good solid answer.

upvoted 6 times

kiketxu 3 years, 10 months ago

Absolutely agree, thumbs-up!

upvoted 2 times

msysadmin 1 year, 9 months ago

Your feedback is correct, but given question answer for auto-unlock: Device1,2,3. It is a correct answer.
Even your link which you provide: It is clearly explaining:

Enable-BitLockerAutoUnlock -MountPoint "E:"

upvoted 1 times

GatesBill 1 year, 8 months ago

"If BitLocker has been turned on for the operating system drive, you can set BitLocker to automatically unlock fixed data drives and removable data drives encrypted by BitLocker when you sign in to Windows. BitLocker uses encrypted information stored in the registry and volume metadata to unlock any drives that use automatic unlocking."
- ref: https://www.elevenforum.com/t/turn-on-or-off-auto-unlock-for-bitlocker-drive-in-windows-11.2804/

As long as the OS-disk isn't "unlocked", other drives won't unlock also. Even if you could turn on auto-unlock on drive D, it won't auto-unlock as drive C isn't encrypted thus not "unlockedable".

upvoted 1 times

jayze Highly Voted 👍 4 years, 7 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 14 times

msysadmin 1 year, 9 months ago

"It is only valid when using BitLocker to encrypt OS drives" - This is incorrect, all disk supporting auto unlock. I just checked my PC which I have a 3 different dirver and for all of them auto unlock active.

upvoted 1 times

cosmindv Most Recent ⏲ 1 year, 7 months ago

so it's correct because device 1 can use auto-unlock for D drive only after you unlock C drive with a password or other method,,,,, The computer requires a form of unlock but the data drive does not, and i am writing this comment to remember this because these people at microsoft are the worst kind of psychopaths

upvoted 2 times

ChachaChatra 1 year, 11 months ago

Valid on28/01/23

upvoted 3 times

preeya 2 years, 5 months ago

100% valid on exam july 27,2022

upvoted 6 times

⊟ **LillyLiver** 2 years, 9 months ago

I admit, this one had me stumped. I think I have it figured out.

Bitlocker To Go (BTG) can be used on all four devices because they are all Windows 10. At first I was thinking "if there isn't a TPM and we don't know what the BIOS or UEFI firmware is, how do we know?" Well, I think it has to do with the fact that BTG doesn't require a TPM or a certain BIOS/UEFI version. You are encrypting REMOVABLE disks. That's why all of the devices can use BTG.

Auto Unlock requires a Bitlocker'ed system disk. Those we know have compatible TPM/BIOS/UEFI. The D: drive in this question is NOT removeable. It is a secondary disk. So, the systems that have an encrypted system drive, can use Auto-Unlock.

Given all my research and asking "WTF!?", I think the given answers are correct.

upvoted 4 times

⊟ **mkoprivnj** 3 years, 1 month ago

1st: 1,2,3,4

2nd: 1,3 -- OS

upvoted 3 times

⊟ **Fearless90** 3 years, 1 month ago

On computers that do not have a TPM version 1.2, you can still use BitLocker to encrypt the Windows operating system drive. However, this implementation will require the user to insert a USB startup key to start the computer or resume from hibernation, and it does not provide the pre-startup system integrity verification offered by BitLocker with a TPM.

https://docs.microsoft.com/en-us/previous-versions/windows/it-pro/windows-server-2008-R2-and-2008/cc732774(v=ws.11)?redirectedfrom=MSDN

upvoted 1 times

⊟ **stewie055** 2 years, 5 months ago

"require USB startup key " or just a strong password that is hard to force (like it's done on linux). Not having TPM = no recovery key nor pin code secured inside, AND nothing to protect against cracking (TPM has a counter that would wipe out the pin code after too many failed attempts).

upvoted 1 times

⊟ **theboywonder** 3 years, 6 months 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** 3 years, 10 months 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** 4 years, 2 months 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 3 times

⊟ **Morne** 4 years, 3 months 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** 4 years, 3 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** 4 years, 3 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 4 years, 6 months 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 4 years, 7 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 4 times

The_Master 4 years, 6 months ago
Auto-unlock answer is correct, it requires bitlocker on the OS drive only.
upvoted 6 times

upstrem 4 years, 9 months ago
What is TPM?
upvoted 1 times

gbabes 4 years, 9 months ago
https://www.microsoft.com/en-US/windows/windows-10-specifications?SilentAuth=1&wa=wsignin1.0
Trusted Platform Module
upvoted 2 times

jasscomp 4 years, 8 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

stewie055 2 years, 5 months ago
Bitlocker can be enable without TPM (that's the ambiguous part).
No TPM = bitlocker does a simple encryption of the volume (you input a password that unlock the volume). This approch has limitation 1- difficulty to manage those passwords in big organisations resulting in volumes being lost 2- Password can be cracked (unless it's a usb device which is hard to implement)

With TPM = Volume is now unlockable by two things : 1- a 4 digit pin code (locally stored in the TPM) 2- A recovery Key (very long unckracable pwd stored in TPM AND in Azure AD if you allow it). TPM counts the number of failed attempts and wipe out the pin code after too many attempts, thus forcing you to go with its recovery key.

Side note, I think some pentester told me TPM provides protection against attackers trying to prob the microchip but I m not sure about it
upvoted 1 times

tosanede 4 years, 2 months 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

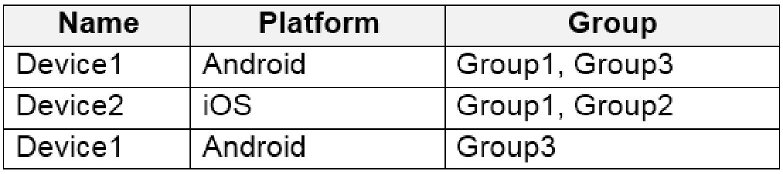
upvoted 1 times

Question #48 *Topic 2*

HOTSPOT -

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

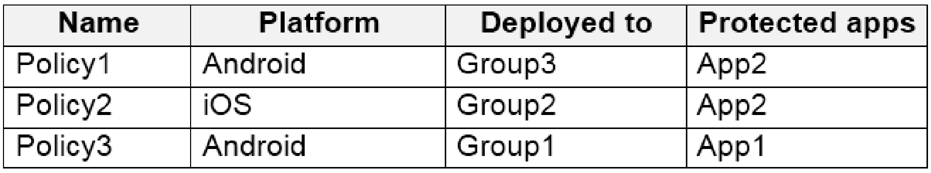
You enroll devices in Microsoft Intune as shown in the following table.



Name	Platform	Group
Device1	Android	Group1, Group3
Device2	iOS	Group1, Group2
Device1	Android	Group3

Each device has two line-of-business apps named App1 and App2 installed.

You create application control policies targeted to all the app types in Microsoft Endpoint Manager as shown in the following table.

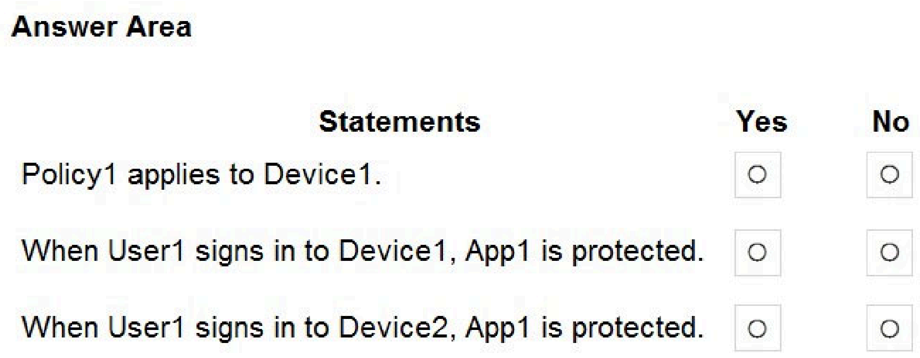


Name	Platform	Deployed to	Protected apps
Policy1	Android	Group3	App2
Policy2	iOS	Group2	App2
Policy3	Android	Group1	App1

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

NOTE: Each correct selection is worth one point.

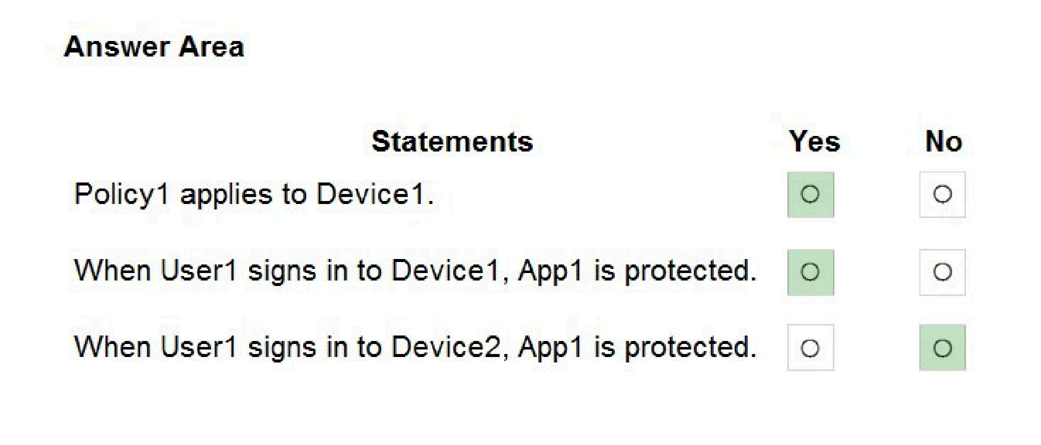
Hot Area:



Answer Area

Statements	Yes	No
Policy1 applies to Device1.	○	○
When User1 signs in to Device1, App1 is protected.	○	○
When User1 signs in to Device2, App1 is protected.	○	○

Suggested Answer:



Answer Area

Statements	Yes	No
Policy1 applies to Device1.	[✓ ○]	○
When User1 signs in to Device1, App1 is protected.	[✓ ○]	○
When User1 signs in to Device2, App1 is protected.	○	[✓ ○]

Box 1: Yes -

Device1 is an Android device in Group3 (and Group1). Policy1 applies to Android devices in Group3. Therefore, Policy1 does apply to Device1.

Box 2: Yes -

Policy3 protects App1 for Android devices in Group1. Device1 is in Group1 (and Group3). Therefore, App1 is protected on Device1.

Box 3: No -

Device2 is an iOS device in Group1 and Group2. Policy2 applies to iOS devices in Group2. However, Policy2 only protects App2. It does not protect App1.

Policy3 applies to Group1 and protects App1. However, Policy3 only applies to Android devices in Group1. It does not apply to iOS devices. Therefore, Policy3 does not apply to Device2 so App1 is not protected on Device2.

mcclane654 1 year, 11 months ago

why is device1 mentioned twice? spelling error or do they mean you reenroll device1 and only apply assign group 3?

upvoted 1 times

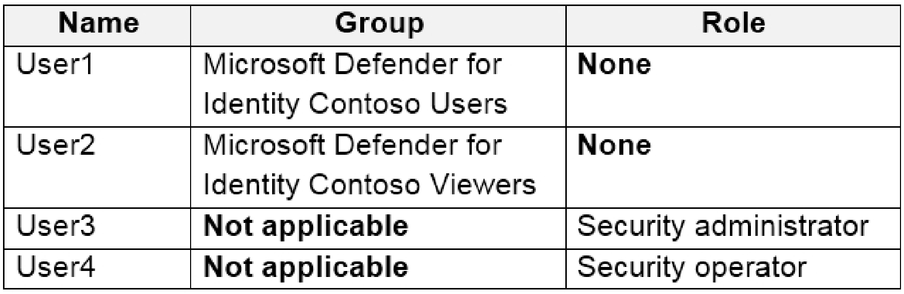
Dinraj 2 years, 3 months ago

Given Ans is correct

upvoted 4 times

Question #49 Topic 2

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



Name	Group	Role
User1	Microsoft Defender for Identity Contoso Users	**None**
User2	Microsoft Defender for Identity Contoso Viewers	**None**
User3	**Not applicable**	Security administrator
User4	**Not applicable**	Security operator

You discover that several security alerts are visible from the Microsoft Defender for Identity portal.

You need to identify which users in contoso.com can close the security alerts.

Which users should you identify?

A. User4 only

B. User1 and User2 only

C. User3 and User4 only

D. User1 and User3 only

E. User1 only

Suggested Answer: *D*

Community vote distribution

C (86%) 14%

⊟ **Dan91** Highly Voted 2 years, 3 months ago

According to this link, answers are correct.

https://docs.microsoft.com/en-us/defender-for-identity/role-groups

upvoted 9 times

⊟ **skycrap** 2 years, 3 months ago

You are right, thx for the link

upvoted 2 times

⊟ **kmk_01** 1 year, 9 months ago

Microsoft defender for identity Contoso Users and Microsoft defender for identity Contoso Viewers don't have any roles or permissions. Correct answer is D.

upvoted 1 times

⊟ **kmk_01** 1 year, 9 months ago

I mean C

upvoted 1 times

⊟ **TavoGC** 1 year, 7 months ago

MDI Viewers as shown in the exhibit do not have roles however, as shown in the link provided by Dan91, they do have permissions including manage security alerts.

upvoted 1 times

⊟ **TavoGC** 1 year, 7 months ago

I meant to say MDI Users, NOT viewers.

upvoted 1 times

⊟ **Maxx4** Most Recent 1 year, 6 months ago

Selected Answer: C

The two roles:

Security Operator has the ability to view and manage security alerts, investigate security incidents, and manage security policies. However, they do not have the ability to create or modify security policies.

Security Administrator has all of the permissions of a Security Operator, plus the ability to create and modify security policies. They also have the ability to manage security features that are not available to Security Operators, such as Privileged Identity Management and Identity Protection.

upvoted 1 times

⊟ **Dhamus** 1 year, 8 months ago

Selected Answer: C

The roles that can manage alerts in this question are security administrators and security operators.

upvoted 2 times

⊟ **GatesBill** 1 year, 8 months ago

People who voted for D are right based on this article: "Defender for Identity uses Azure AD security groups as a basis for role groups." - ref: https://learn.microsoft.com/en-us/defender-for-identity/role-groups#add-and-remove-users

...BUT, choosing this would exclude the Security Operator role, which has the necessary permissions also to achieve this assignment. And assuming groups have roles/permissions assigned to them without it being mentioned in the question would be naïve I agree

...SO people who voted for C are right (also?) based on this article: https://learn.microsoft.com/en-us/azure/active-directory/roles/permissions-reference#security-operator
+ confirmed by forum also: https://learn.microsoft.com/en-us/answers/questions/967525/security-alerts

upvoted 1 times

⊟ **kmk_01** 1 year, 9 months ago

Selected Answer: C

Microsoft defender for identity Contoso Users and Microsoft defender for identity Contoso Viewers don't have any roles or permissions. Correct answer is C.

upvoted 1 times

⊟ **EM1234** 1 year, 10 months ago

There seems to be no consensus. I choose C for reasons below.

When you read this link that Unicorn02 added about security operator permissions you see that they can manage security alerts from Identity portal.

https://learn.microsoft.com/en-us/azure/active-directory/roles/permissions-reference#security-operator
"Users with this role can manage alerts and have global read-only access on security-related features, including all information in Microsoft 365 Defender portal, Azure Active Directory, Identity Protection, Privileged Identity Management and Microsoft Purview compliance portal."

So the security operator can close the alerts and they are not included in answer choice D.

The answer D is problematic to me anyway as I am not sure how the name of a group is enough evidence as to the permissions of the group.

Dan91 provided this link:
https://docs.microsoft.com/en-us/defender-for-identity/role-groups

But as I read it, this shows the MDI roles that can be assigned. I do not see anything in the question to show that assignment of those roles to the groups. I am going to go with C. If anyone can see a flaw in my analysis please reply and help me to understand this more. Maybe I have missed something.

upvoted 2 times

⊟ **keithtemplin** 1 year, 10 months ago

Selected Answer: C

User1 and User 2 have no roles assigned to them or there is no reference to group membership, so we have to assume there are no permissions.

User3 and User4 are the only ones that have permissions:

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

https://learn.microsoft.com/en-us/microsoft-365/security/office-365-security/scc-permissions?view=o365-worldwide#:~:text=Security%20Operator,of%20security%20features.

upvoted 2 times

⊟ **formazionehs** 1 year, 11 months ago

Selected Answer: D

D is correct

upvoted 1 times

⊟ **Owen66** 2 years, 1 month ago

Correct answer should be C.

upvoted 3 times

⊟ **billo79152718** 2 years, 3 months ago

I would also suggest the security operator can close security alerts?

upvoted 3 times

⊟ **formazionehs** 1 year, 11 months ago

security operator can manage alert only in the Defender for Cloud Apps portal. He doesn't have privilege in Microsoft Defender for Identity

upvoted 1 times

⊟ **Unicorn02** 2 years, 1 month ago

Yes it seems so: See:

https://learn.microsoft.com/en-us/azure/active-directory/roles/permissions-reference#security-operator

upvoted 2 times

Question #50 *Topic 2*

You have a Microsoft 365 E5 subscription that contains 1,000 Windows 10 devices. The devices are onboarded to Microsoft Defender for Endpoint.

You need to view a consolidated list of the common vulnerabilities and exposures (CVE) that affect the devices. The solution must minimize administrative effort.

Which Threat & Vulnerability Management page should you use?

A. Software inventory

B. Event timeline

C. Weaknesses

D. Security recommendations

Suggested Answer: *C*

Reference:

https://docs.microsoft.com/en-us/microsoft-365/security/defender-endpoint/tvm-weaknesses?view=o365-worldwide

Community vote distribution

C (100%)

heshmat2022 Highly Voted 👍 2 years, 3 months ago

Weaknesses See the list of common vulnerabilities and exposures (CVEs) in your organization.

upvoted 8 times

Maxx4 Most Recent 1 year, 6 months ago

Selected Answer: C

The answer is C. Weaknesses.

The Weaknesses page in the Threat & Vulnerability Management (T&VM) portal provides a consolidated list of the CVEs that affect your devices. The list is sorted by severity, so you can quickly see which vulnerabilities are the most critical. You can also filter the list by device, asset, or vulnerability type.

The other options are incorrect.

Option A, Software inventory, provides a list of all the software installed on your devices. This can be helpful for identifying vulnerabilities, but it is not as consolidated as the Weaknesses page.

Option B, Event timeline, provides a chronological list of all the security events that have occurred on your devices. This can be helpful for investigating security incidents, but it is not as focused on vulnerabilities as the Weaknesses page.

Option D, Security recommendations, provides a list of security recommendations that you can implement to improve the security of your devices. This can be helpful, but it does not provide a consolidated list of the CVEs that affect your devices.

Therefore, the correct answer is C.

upvoted 1 times

Patesso 1 year, 7 months ago

etait a l'examen le 18/05/2023

upvoted 2 times

King_Khong 1 year, 9 months ago

answer is correct, in my exam 01/03/23

upvoted 4 times

Question #51 *Topic 2*

You have an Azure Sentinel workspace that has an Azure Active Directory (Azure AD) connector and an Office 365 connector.
From the workspace, you plan to create a scheduled query rule that will use a custom query. The rule will be used to generate alerts when inbound access to
Office 365 from specific user accounts is detected.
You need to ensure that when multiple alerts are generated by the rule, the alerts are consolidated as a single incident per user account.
What should you do?

A. From Set rule logic, map the entities.

B. From Analytic rule details, configure Severity.

C. From Set rule logic, set Suppression to Off.

D. From Analytic rule details, configure Tactics.

Suggested Answer: *A*
Reference:
https://docs.microsoft.com/en-us/azure/sentinel/map-data-fields-to-entities

Community vote distribution
C (100%)

heshmat2022 Highly Voted 2 years, 3 months ago
Entity mapping is an integral part of the configuration of scheduled query analytics rules. It enriches the rules' output (alerts and incidents) with essential information that serves as the building blocks of any investigative processes and remedial actions that follow.

The procedure detailed below is part of the analytics rule creation wizard. It's treated here independently to address the scenario of adding or changing entity mappings in an existing analytics rule.
upvoted 8 times

KarimaMaf Most Recent 1 year, 6 months ago
correct answer : You have the flexibility to group alerts into a single incident per the following logic:

Grouping alerts into a single incident if all the entities match (recommended)
Grouping all alerts triggered by this rule into a single incident
Grouping alerts into a single incident if the selected entities match (Account, Host, IP, URL)
link to group mapping :https://techcommunity.microsoft.com/t5/microsoft-sentinel-blog/what-s-new-reduce-alert-noise-with-incident-settings-and-alert/ba-p/1187940
upvoted 1 times

Maxx4 1 year, 6 months ago
Selected Answer: C
I would go for C: confusing
If you are creating a scheduled query rule in Azure Sentinel, you should select option A, From Set rule logic, map the entities. This is the more specific and correct answer for this question.

Option C, From Set rule logic, set Suppression to Off, is also a correct answer, but it is more general and can be used to consolidate alerts from any type of rule.

Once you have mapped the entities, Azure Sentinel will recognize alerts generated by the rule that share the same entity as part of the same incident. This consolidation allows for better management and analysis of the alerts, simplifying incident response and reducing duplication.
upvoted 1 times

ChachaChatra 1 year, 11 months ago
Valid on28/01/23
upvoted 3 times

Brigg5 1 year, 11 months ago

From the docs, "Entities enrich the rules' output (alerts and incidents) with essential information... They are also the criteria by which you can group alerts together into incidents in the Incident settings tab." 'A' is correct

upvoted 2 times

Question #52 *Topic 2*

DRAG DROP -

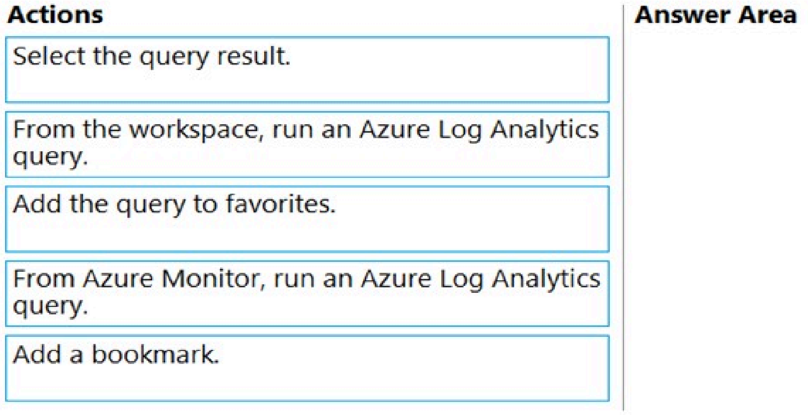
You have an Azure Sentinel workspace that has an Office 365 connector.

You are threat hunting events that have suspicious traffic from specific IP addresses.

You need to save the events and the relevant query results for future reference.

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:

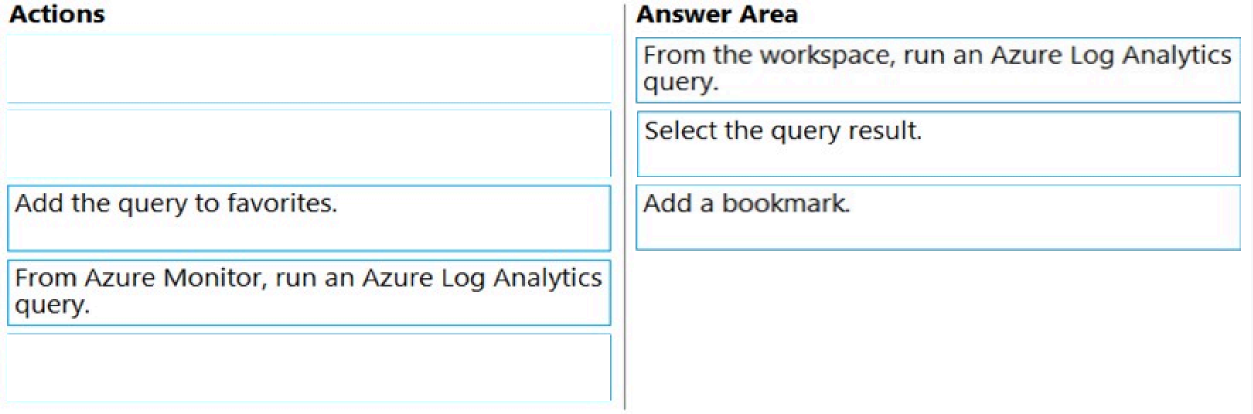


Actions

- Select the query result.
- From the workspace, run an Azure Log Analytics query.
- Add the query to favorites.
- From Azure Monitor, run an Azure Log Analytics query.
- Add a bookmark.

Answer Area

Suggested Answer:



Actions

- Add the query to favorites.
- From Azure Monitor, run an Azure Log Analytics query.

Answer Area

- From the workspace, run an Azure Log Analytics query.
- Select the query result.
- Add a bookmark.

Reference:

https://docs.microsoft.com/en-us/azure/sentinel/bookmarks

Just2a 2 years, 1 month ago

Answer is correct

upvoted 2 times

Ginaglia 2 years, 1 month ago

Should it be from Azure Monitor?

upvoted 1 times

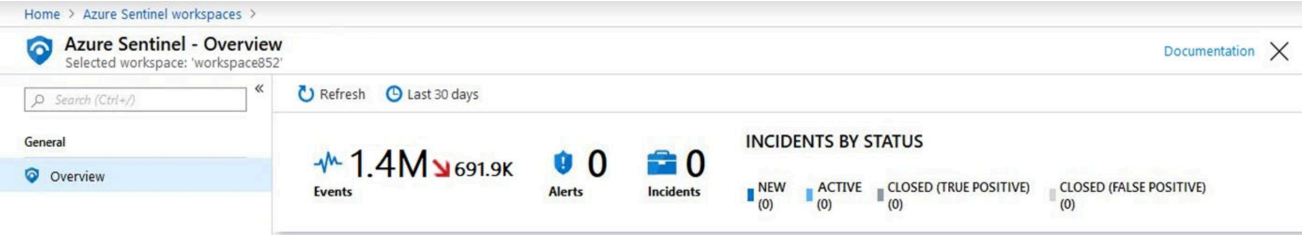
EM1234 1 year, 10 months ago

No, you run the query from the LAW. Go to monitor and try to do it.

upvoted 1 times

Question #53 *Topic 2*

You create an Azure Sentinel workspace.
You configure Azure Sentinel to ingest data from Azure Active Directory (Azure AD).
In the Azure Active Directory admin center, you discover Azure AD Identity Protection alerts. The Azure Sentinel workspace shows the status as shown in the following exhibit.



Home > Azure Sentinel workspaces >

Azure Sentinel - Overview
Selected workspace: 'workspace852'

1.4M 691.9K Events

0 Alerts

0 Incidents

INCIDENTS BY STATUS

NEW (0)
ACTIVE (0)
CLOSED (TRUE POSITIVE) (0)
CLOSED (FALSE POSITIVE) (0)

In Azure Log Analytics, you can see Azure AD data in the Azure Sentinel workspace.
What should you configure in Azure Sentinel to ensure that incidents are created for detected threats?

A. data connectors

B. rules

C. workbooks

D. hunting queries

Suggested Answer: *B*
Reference:
https://docs.microsoft.com/en-us/azure/sentinel/detect-threats-custom

Community vote distribution
B (71%) A (29%)

heshmat2022 Highly Voted 2 years, 3 months ago
SOrry, the answer is B :
create custom analytics rules to help discover threats and anomalous behaviors in your environment.
upvoted 9 times

King_Khong Most Recent 1 year, 9 months ago
B is correct, in my exam 01/03/23
upvoted 2 times

shouro88 1 year, 11 months ago
Selected Answer: B
Instance is already up and running, no point in choosing a "data connector"

After connecting your data sources to Microsoft Sentinel, create custom analytics RULES to help discover threats and anomalous behaviors in your environment.
upvoted 2 times

Wedge34 2 years, 2 months ago
Selected Answer: A
To get Identity Protection Alerts, you must have Identity Protection Connectors (defender for identity soon) and Azure AD premium P2 licence
upvoted 1 times

Acbrownit 1 year, 11 months ago
The question states that the alerts are already showing in Sentinel, so the connectors are there. Just needs a rule to parse the events
upvoted 2 times

RVR 2 years, 3 months ago
Selected Answer: B
Rules
Step 3: https://learn.microsoft.com/en-us/azure/sentinel/create-incidents-from-alerts
upvoted 3 times

⊟ **heshmat2022** 2 years, 3 months ago

Selected Answer: A

create custom analytics rules to help discover threats and anomalous behaviors in your environment.

upvoted 1 times

Question #54

Topic 2

You have a Microsoft 365 E5 subscription that has Microsoft 365 Defender enabled.
You plan to deploy a third-party app named App1 that will receive alert data from Microsoft 365 Defender.
Which format will Microsoft 365 Defender use to send the alert data to App1?

A. JSON

B. ZIP

C. XML

D. CSV

Suggested Answer: *A*
Reference:
https://docs.microsoft.com/en-us/microsoft-365/security/defender-endpoint/alerts?view=o365-worldwide

Bob27745 Highly Voted 2 years, 3 months ago

Valid on exam 9/21/2022

upvoted 5 times

Question #55

Topic 2

DRAG DROP -

You have a Microsoft 365 E5 subscription.

You plan to implement Azure Sentinel to create incidents based on:

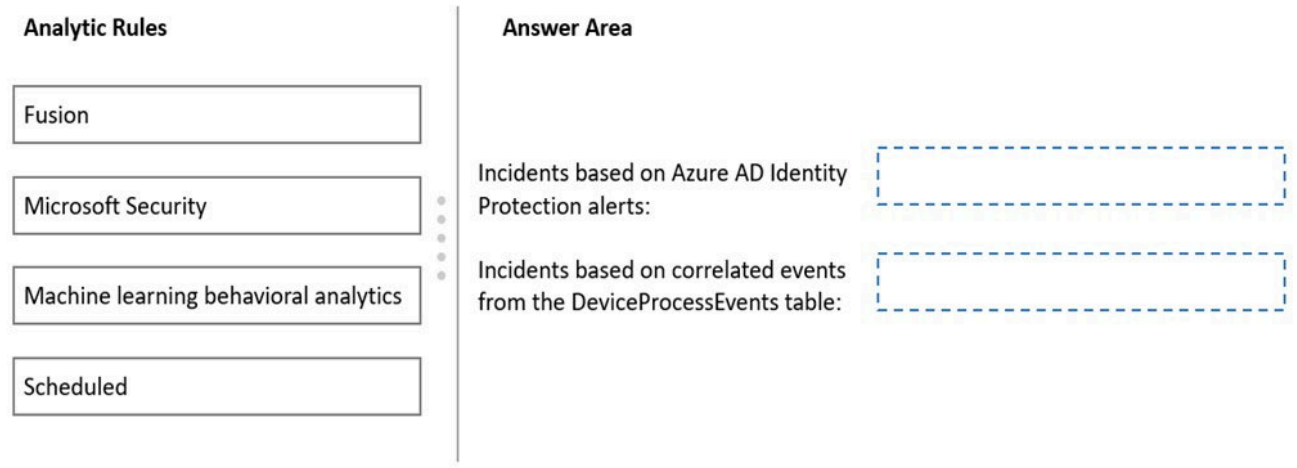
✑ Azure Active Directory (Azure AD) Identity Protection alerts

✑ Correlated events from the DeviceProcessEvents table

Which analytic rule types should you use for each incident type? To answer, drag the appropriate rule types to the correct incident types. Each rule type may be used once, more than once, or not at all. You may need to drag the split bar between panes or scroll to view content.

NOTE: Each correct selection is worth one point.

Select and Place:



Analytic Rules

Fusion

Microsoft Security

Machine learning behavioral analytics

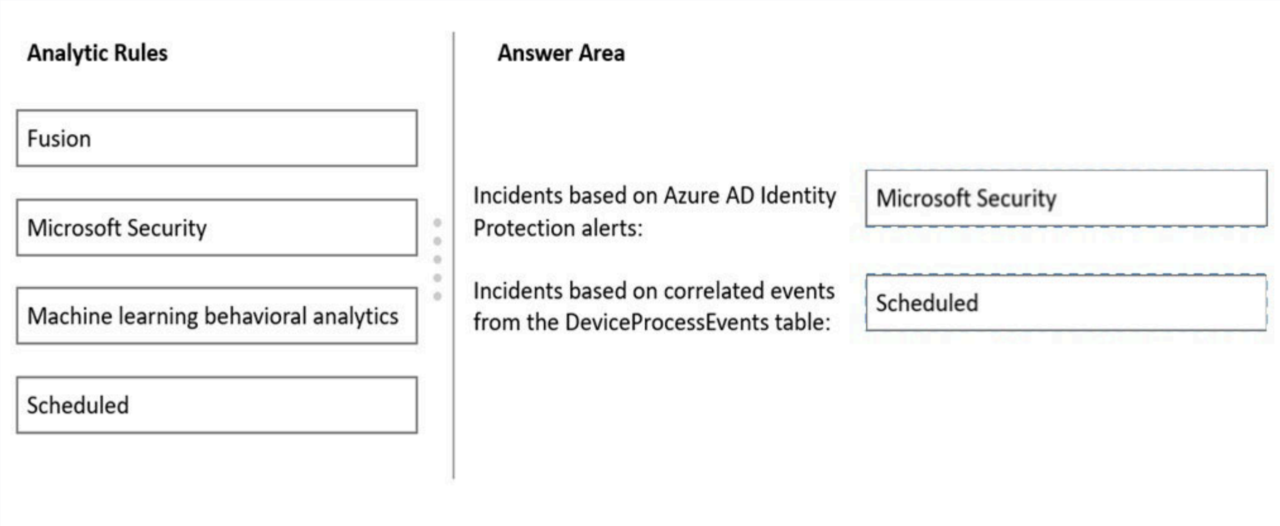
Scheduled

Answer Area

Incidents based on Azure AD Identity Protection alerts:

Incidents based on correlated events from the DeviceProcessEvents table:

Suggested Answer:



Analytic Rules

Fusion

Microsoft Security

Machine learning behavioral analytics

Scheduled

Answer Area

Incidents based on Azure AD Identity Protection alerts: Microsoft Security

Incidents based on correlated events from the DeviceProcessEvents table: Scheduled

Reference:

https://docs.microsoft.com/en-us/azure/sentinel/create-incidents-from-alerts https://docs.microsoft.com/en-us/azure/sentinel/detect-threats-custom

Nobal 2 years, 2 months ago

Answer is correct.

upvoted 2 times

Question #56 *Topic 2*

You have a Microsoft 365 E5 subscription.
You need to use Attack simulation training to launch a credential harvest simulation.
For which Microsoft 365 workloads can you create a payload?

A. Microsoft Exchange Online only

B. Microsoft Teams, Exchange Online, SharePoint Online, and OneDrive

C. Microsoft Teams and Exchange Online only

D. Microsoft SharePoint Online and OneDrive only

Suggested Answer: *A*
Create a payload, select a payload type.
On the Select type page, the only value that you can currently select is Email.
Incorrect:
Not A, Not B, Not C: Payloads cannot be created for Microsoft Exchange Online.
Reference:
https://docs.microsoft.com/en-us/microsoft-365/security/office-365-security/attack-simulation-training-payloads

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

Okadorium 1 year, 6 months ago
The answer is B: Microsoft Teams, Exchange Online, SharePoint Online, and OneDrive. With a Microsoft 365 E5 subscription, you can create payloads for credential harvest simulations in all of these workloads. Attack Simulator allows you to launch simulated phishing attacks and conduct security awareness training across these Microsoft 365 services.
upvoted 1 times

Maxx4 1 year, 6 months ago
Selected Answer: B
The correct answer is B. Microsoft Teams, Exchange Online, SharePoint Online, and OneDrive.

With a Microsoft 365 E5 subscription, you can create a payload for the following Microsoft 365 workloads:

Microsoft Teams: Attack simulation training allows you to simulate a credential harvest attack within the Teams environment.
Exchange Online: Attack simulation training enables you to launch a credential harvest simulation in Exchange Online, simulating an attack against email accounts.
SharePoint Online: You can create a payload for attack simulation training to launch a credential harvest simulation in SharePoint Online, testing the security of SharePoint sites and document libraries.
OneDrive: Attack simulation training allows you to simulate a credential harvest attack in OneDrive, testing the security of individual user's cloud storage and files.
By creating payloads for these Microsoft 365 workloads, you can effectively simulate and assess the security posture of your organization against credential harvest attacks.

Therefore, the correct answer is B. Microsoft Teams, Exchange Online, SharePoint Online, and OneDrive.
upvoted 1 times

Tanasi 1 year, 7 months ago
Selected Answer: A
valid 18 may 2023
upvoted 3 times

JoeP1 1 year, 10 months ago
Selected Answer: A
Since payloads must be by email, the only answer that makes sense is A - Exchange online
upvoted 1 times

Zimb 2 years ago

To remove one or more columns that are displayed, click Customize columns icon. Customize columns. By default, the only column that's not shown is Platform, and that value is currently always Email.

https://learn.microsoft.com/en-us/microsoft-365/security/office-365-security/attack-simulation-training-payloads?view=o365-worldwide

upvoted 1 times

NickBoq 2 years, 3 months ago

In Attack simulation training, a payload is the phishing email message and links or attachment content that's are presented to users in simulations.

upvoted 1 times

skycrap 2 years, 3 months ago

I think it's correct as the link in the answer: On the Select type page, the only value that you can currently select is Email

upvoted 3 times

heshmat2022 2 years, 3 months ago

In the Microsoft 365 Defender portal at https://security.microsoft.com, go to Email & collaboration > Attack simulation training > Simulation content library tab > Payloads > Tenant payloads tab. To go directly to the Simulation content library tab where you can select Payloads and the Tenant payloads tab, use https://security.microsoft.com/attacksimulator?viewid=simulationcontentlibrary.

upvoted 1 times

Dinraj 2 years, 3 months ago

YEs that is correct,
Just tested in lab, it is showing Email and Teams

upvoted 2 times

Dinraj 2 years, 3 months ago

But Teams is unable to select payloads, So Email only, Exchange is right option

upvoted 3 times

JimboJones99 2 years, 3 months ago

The solution contradicts the answer!

upvoted 2 times

Question #57 *Topic 2*

HOTSPOT -

You have a Microsoft Sentinel workspace that has an Azure Active Directory (Azure AD) connector and an Office 365 connector.

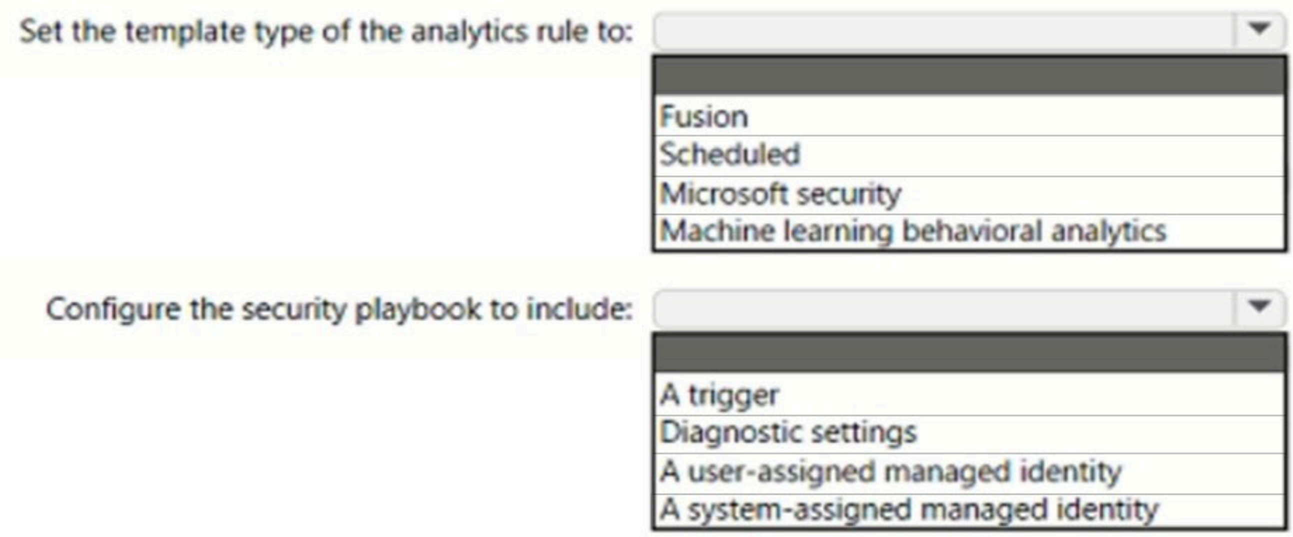
From the workspace, you plan to create an analytics rule that will be based on a custom query and will run a security playbook.

You need to ensure that you can add the security playbook and the custom query to the rule.

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

NOTE: Each correct selection is worth one point.

Hot Area:



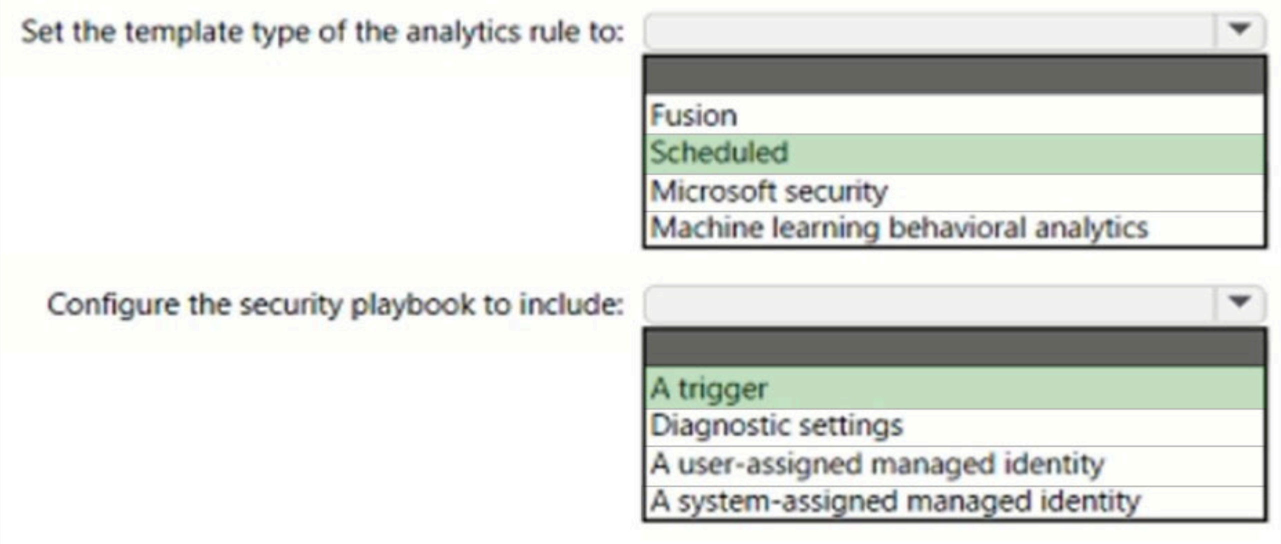
Set the template type of the analytics rule to:

- Fusion
- Scheduled
- Microsoft security
- Machine learning behavioral analytics

Configure the security playbook to include:

- A trigger
- Diagnostic settings
- A user-assigned managed identity
- A system-assigned managed identity

Suggested Answer:



Set the template type of the analytics rule to:

- Fusion
- [✓ Scheduled]
- Microsoft security
- Machine learning behavioral analytics

Configure the security playbook to include:

- [✓ A trigger]
- Diagnostic settings
- A user-assigned managed identity
- A system-assigned managed identity

Box 1: Scheduled -

Create a custom analytics rule with a scheduled query

1. From the Microsoft Sentinel navigation menu, select Analytics.
2. In the action bar at the top, select +Create and select Scheduled query rule. This opens the Analytics rule wizard.
3. Etc.

Box 2: A trigger -

Use triggers and actions in Microsoft Sentinel playbooks.

Reference:

https://docs.microsoft.com/en-us/azure/sentinel/detect-threats-custom https://docs.microsoft.com/en-us/azure/sentinel/playbook-triggers-actions#microsoft-sentinel-triggers-summary

EM1234 1 year, 10 months ago

The explanation should not say "etc" unless they are teaching us how to draw an owl. The answer does seem right to me though.

upvoted 1 times

⊟ **Jawad1462** 2 years, 1 month ago

Answer is correct

upvoted 1 times

Question #58 *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 admin center, select Reports and then select Security & Compliance.

C. From the Microsoft 365 Defender portal, select Settings and then select Security center.

D. From the Microsoft 365 Defender portal, select Explorer and then select MDE Settings.

Suggested Answer: *D*
To integrate Microsoft Defender for Office 365 with Microsoft Defender for Endpoint
Integrating Microsoft Defender for Office 365 with Microsoft Defender for Endpoint is set up in both Defender for Endpoint and Defender for Office 365.
1. Go to the Microsoft 365 Defender portal (https://security.microsoft.com) and sign in.
2. Go to Email & collaboration > Explorer.
3. On the Explorer page, in the upper right corner of the screen, select MDE Settings.
4. In the Microsoft Defender for Endpoint connection flyout that appears, turn on Connect to Microsoft Defender for Endpoint (Toggle on.) and then select Close.
Reference:
https://docs.microsoft.com/en-us/microsoft-365/security/office-365-security/integrate-office-365-ti-with-mde?view=o365-worldwide

Community vote distribution

D (100%)

Dinraj Highly Voted 2 years, 3 months ago

Selected Answer: D

D is correct Ans

upvoted 8 times

Maxx4 Most Recent 1 year, 6 months ago

Selected Answer: D

The answer is D. From the Microsoft 365 Defender portal, select Explorer and then select MDE Settings.

To integrate Microsoft Defender for Office 365 and Microsoft Defender for Endpoint, you need to configure the integration in the Microsoft 365 Defender portal. In the Microsoft 365 Defender portal, select Explorer and then select MDE Settings. On the MDE Settings page, select the Enable integration with Microsoft Defender for Endpoint check box.

The other options are incorrect.

Option A, From the Microsoft 365 admin center, select Settings, and then select Services & add-ins, is incorrect because you cannot configure the integration from the Microsoft 365 admin center.
Option B, From the Microsoft 365 admin center, select Reports and then select Security & Compliance, is incorrect because you cannot configure the integration from the Microsoft 365 admin center.
Option C, From the Microsoft 365 Defender portal, select Settings and then select Security center, is incorrect because you cannot configure the integration from the Security center page.
Therefore, the correct answer is D.

upvoted 1 times

bda92b3 1 year, 10 months ago

Correct

upvoted 1 times

mhh 2 years ago

agree, D is correct.

upvoted 1 times

Question #59 *Topic 2*

You have a Microsoft 365 E5 subscription that has Microsoft Defender for Cloud Apps enabled.
You need to create an alert in Defender for Cloud Apps when source code is shared externally.
Which type of policy should you create?

A. activity

B. Cloud Discovery anomaly detection

C. access

D. file

Suggested Answer: *D*
Detect externally shared source code
Detect when files that contain content that might be source code are shared publicly or are shared with users outside of your organization.

Prerequisites -
You must have at least one app connected using app connectors.

Steps -
1. On the Policies page, create a new File policy.
2. Select and apply the policy template Externally shared source code
3. Optional: Customize the list of file Extensions to match your organization's source code file extensions.
4. Optional: Set the Governance actions to be taken on files when a violation is detected. The governance actions available vary between services. For example, in Box, Send policy-match digest to file owner and Put in admin quarantine.
5. Select and apply the policy template

Reference:
https://docs.microsoft.com/en-us/defender-cloud-apps/policies-information-protection#detect-externally-shared-source-code

Community vote distribution

D (100%)

Maxx4 1 year, 6 months ago

Selected Answer: D

The answer is D. file.

To create an alert in Defender for Cloud Apps when source code is shared externally, you should create a file policy. A file policy allows you to specify the types of files that you want to monitor, and the actions that you want to take when a file is detected. In this case, you would want to specify the file extensions that are associated with source code, and you would want to take the action of creating an alert when a file with one of these extensions is shared externally.

The other options are incorrect.

Option A, activity, is incorrect because activity policies are used to monitor user activity, not file activity.
Option B, Cloud Discovery anomaly detection, is incorrect because Cloud Discovery anomaly detection is used to detect anomalous activity in Cloud Discovery, not in Defender for Cloud Apps.
Option C, access, is incorrect because access policies are used to control access to files, not to monitor file activity.
Therefore, the correct answer is D.
upvoted 1 times

shouro88 1 year, 11 months ago

Detect when files that contain content that might be source code are shared publicly or are shared with users outside of your organization.

Prerequisites
You must have at least one app connected using app connectors.

Steps

On the Policies page, create a new "File policy"

upvoted 3 times

Question #60 *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 365 Attack simulation training 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 Microsoft Azure portal, configure the user risk policy settings in Azure AD Identity Protection.

B. Migrate the Executive group members to Exchange Online.

C. Enable MFA for the Research group members.

D. Enable MFA for your account.

E. From the Microsoft Defender for Identity portal, configure the primary workspace settings.

Suggested Answer: *D*
Module 6 - Lab 1 - Exercise 1 - Conduct a Spear phishing attack
Holly Dickson is concerned that some users in her organization may require education about phishing attacks. In this lab you will use the Microsoft 365 Attack simulator to determine your users' susceptibility to phishing attacks.
Task 1: Enable Mulit-factor authentication for Holly Dickson
1. On LON-CL1, Go to the Office 365 Security & Compliance center https://protection.office.com and login as Holly Dickson.
2. Click Threat management, and then click Attack simulator.
3. Notice the warning that you must enable multi-factor authentication (MFA). You are about to do a simulated attack and the system wants to confirm your credentials. This is a requirement of the attack simulator. Let's enable MFA for Holly Dickson.
4. Etc.
Reference:
https://microsoftlearning.github.io/MS-500-Microsoft-365-Security/Instructions/Labs/MS500T00/LAB_AK_06_Lab1_Ex1_Phishing_attack.html

Community vote distribution
D (69%) B (23%) 8%

⊟ **Just2a** Highly Voted 👍 2 years, 1 month ago
D is wrong.
Each member of a group named Executive has an on-premises mailbox.
The Executive group members have multi-factor authentication (MFA) enabled.
Each member of a group named Research has a mailbox in Exchange Online.
Need to targets the Research group members which is in Exchange online.
The email addresses that you intend to spoof belong to the Executive group members which is on prem and already has MFA enable

Migrate them to Exxchange online should be the answer
upvoted 12 times

⊟ **Pointless** 1 year, 9 months ago
Executive group members are not targeted. Research group is targeted and they'll get spoofed emails that would look like coming from Executive group members. So Research group members need MFA enabled. Whether Executive members have MFA enabled or not is irrelevant here.
upvoted 1 times

⊟ **Pointless** 1 year, 9 months ago
Sorry, research group doesn't need MFA enabled but whoever is conducting the simulation should have MFA
upvoted 2 times

⊟ **BoxGhost** 2 years ago
Can we get a source for this please? I'm unable to find this within Microsoft's documentation:

https://techcommunity.microsoft.com/t5/microsoft-defender-for-office/mdo-attack-simulation-hybrid-on-prem/m-p/2832662
upvoted 1 times

pete26 Highly Voted 👍 2 years, 3 months ago

Selected Answer: D

D is correct!

upvoted 6 times

Maxx4 Most Recent 🕒 1 year, 6 months ago

Selected Answer: D

The answer is D. Enable MFA for your account.

Before you can use Microsoft 365 Attack simulation training to model a spear-phishing attack, you need to enable MFA for your account. This is because MFA will help to protect your account from being compromised, which could allow an attacker to impersonate you and send the spear-phishing emails.

upvoted 1 times

jimmyjose 1 year, 6 months ago

What does it even mean by stating "Enable MFA for your account"?

upvoted 1 times

andreane 1 year, 7 months ago

Attack Simulator is now available for On-Prem Mailboxes

https://learn.microsoft.com/en-us/microsoft-365/security/office-365-security/attack-simulation-training-get-started?view=o365-worldwide

upvoted 2 times

RomanV 1 year, 8 months ago

Few other important requirements must be met. First of all, Attack Simulator is currently only available for users with mailboxes in Exchange Online, as part of the feature relies on direct access to the mailbox store. In addition, an attack can only be launched by an administrator that has passed a Multi-factor authentication challenge, meaning that in order to access the feature your organization must have configured MFA.

So first we migrate them to EXO.

upvoted 1 times

> **RomanV** 1 year, 8 months ago
>
> 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.
>
> So I will go for answer D.
>
> upvoted 2 times

shouro88 1 year, 11 months ago

I did an Attack Simulation today and it did not ask me to do MFA. MFA is disabled in my test tenant

upvoted 1 times

Romke_en_Tomke 2 years ago

Selected Answer: C

As JosephMang is saying I believe C is the answer. You need to have MFA enabled for targeted users.
Sorry, the target group is "Research Group" and it's already "Exchange Online". Just need to enable MFA for the "Research Group" instead.

upvoted 1 times

examdog 2 years ago

Selected Answer: D

D is correct. The target is Research group only. Executive group emails are spoofed, but NOT attached.

upvoted 1 times

Daniel_Perez 2 years ago

Selected Answer: B

Simular ataques con licencia E5 requiere que los objetivos tengan MFA habilitado, como ya tiene el grupo Ejecutivo, además de que los buzones sean Exchange Online, no locales (on-prem).

Attack simulation along E5 requires MFA enabled on the targets. Executive group have already MFA enabled also the mailboxes need to be Exchange Online, not local (on-prem).

upvoted 1 times

⊟ **imjoe** 2 years, 1 month ago

Selected Answer: B

All the members of the Executive Group need to migrate from On-prem to Exchange Online.

upvoted 2 times

⊟ **imjoe** 2 years ago

Sorry, the target group is "Research Group" and it's already "Exchange Online". Just need to enable MFA for the "Research Group" instead.

upvoted 2 times

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

Selected Answer: D

D is correct

upvoted 1 times

⊟ **skycrap** 2 years, 3 months ago

Not sure this is actual. It used to require MFA but on this link https://learn.microsoft.com/en-us/microsoft-365/security/office-365-security/attack-simulation-training-get-started?view=o365-worldwide no mention of mfa

upvoted 3 times

Question #61 *Topic 2*

DRAG DROP -

You have a Microsoft 365 E5 subscription that uses Microsoft Defender for Endpoint and contains a Windows 10 device named Device1.

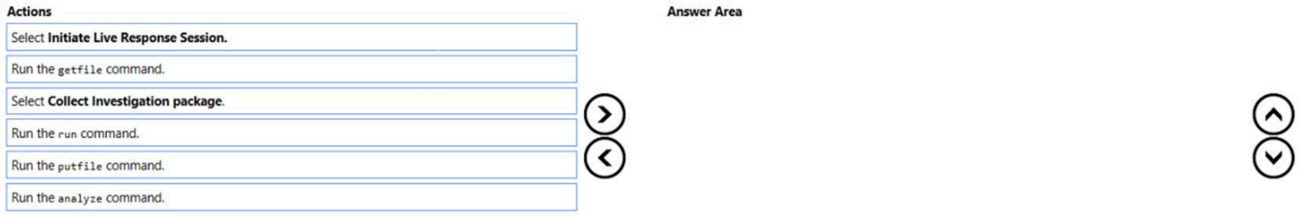
You have a PowerShell script named script1 that collects forensic data and saves the results as a file on the device from which the script is run.

You receive a Microsoft Defender for Endpoint alert for suspicious activities on Device1.

You need to run script1 on Device1 and retrieve the output file of the script.

Which four actions should you perform in sequence in Microsoft 365 Defender portal? 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:

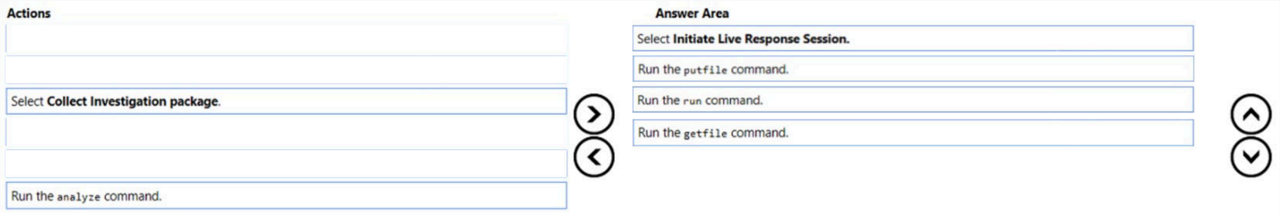


Actions

- Select **Initiate Live Response Session.**
- Run the `getfile` command.
- Select **Collect Investigation package**.
- Run the `run` command.
- Run the `putfile` command.
- Run the `analyze` command.

Answer Area

Suggested Answer:



Actions

- Select **Collect Investigation package**.
- Run the `analyze` command.

Answer Area

- Select **Initiate Live Response Session.**
- Run the `putfile` command.
- Run the `run` command.
- Run the `getfile` command.

Step 1: Select Initiate Live Response Session.

Initiate a live response session on a device

1. Sign in to Microsoft 365 Defender portal.
2. Navigate to Endpoints > Device inventory and select a device to investigate. The devices page opens.
3. Launch the live response session by selecting Initiate live response session. A command console is displayed. Wait while the session connects to the device.
4. Use the built-in commands to do investigative work.
5. After completing your investigation, select Disconnect session, then select Confirm.

Note: Initiate live response Session

Live response is a capability that gives you instantaneous access to a device by using a remote shell connection. This gives you the power to do in-depth investigative work and take immediate response actions to promptly contain identified threats in real time.

Live response is designed to enhance investigations by enabling you to collect forensic data, run scripts, send suspicious entities for analysis, remediate threats, and proactively hunt for emerging threats.

Step 2: Run the putfile command -

putfile - Puts a file from the library to the device. Files are saved in a working folder and are deleted when the device restarts by default.

Step 3: Run the run command -

run - Runs a PowerShell script from the library on the device.

Step 4: Run the getfile command -

getfile <file_path> - Downloads a file.

For scenarios when you'd like get a file from a device you're investigating, you can use the getfile command. This allows you to save the file from the device for further investigation.

Incorrect:

* Select Collect Investigation package.

Collect investigation package from devices

As part of the investigation or response process, you can collect an investigation package from a device. By collecting the investigation package, you can identify the current state of the device and further understand the tools and techniques used by the attacker.

* Run the analyze command

Analyze - Analyses the entity with various incrimination engines to reach a verdict.

Reference:

https://docs.microsoft.com/en-us/microsoft-365/security/defender-endpoint/live-response https://docs.microsoft.com/en-us/microsoft-365/security/defender-endpoint/respond-machine-alerts

subhuman 1 year, 6 months ago

Answer is correct.

upvoted 1 times

EM1234 1 year, 10 months ago

For those of you making labs for these, this may help:

https://learn.microsoft.com/en-us/microsoft-365/security/defender-endpoint/live-response?view=o365-worldwide

This doc needs an update. It says to get to it you:
"Initiate a live response session on a device

Sign in to Microsoft 365 Defender portal.

Navigate to Endpoints > Device inventory and select a device to investigate. The devices page opens."

Really though, I had to go to:

M365 defender portal > Devices (under assets) > click the device > go to the "..." on the top right > then Initiate live response

Note: I had to go to settings > endpoints > advanced and turn on live session for it to work.

upvoted 2 times

ChachaChatra 1 year, 11 months ago

Valid on28/01/23

upvoted 2 times

Question #62 *Topic 2*

You have a Microsoft 365 E5 subscription and a Microsoft Sentinel workspace named Sentinel1.

You need to launch the Guided Investigation – Process Alerts notebook in Sentinel1.

What should you create first?

A. an Azure logic app

B. a Log Analytics workspace

C. an Azure Machine Learning workspace

D. a Kusto query

Suggested Answer: *C*

Community vote distribution

D (50%) C (33%) A (17%)

KarimaMaf 1 year, 6 months ago

o use Jupyter notebooks in Microsoft Sentinel, you must first have the right permissions, depending on your user role.

While you can run Microsoft Sentinel notebooks in JupyterLab or Jupyter classic, in Microsoft Sentinel, notebooks are run on an Azure Machine Learning (Azure ML) platform. To run notebooks in Microsoft Sentinel, you must have appropriate access to both Microsoft Sentinel workspace and an Azure ML workspace.

upvoted 1 times

KarimaMaf 1 year, 6 months ago

C IS CORRECT

upvoted 1 times

KarimaMaf 1 year, 6 months ago

CASE THE LOG ANALYTICS WORKSPACE IS ALREADY DEPLOYED

upvoted 1 times

Maxx4 1 year, 6 months ago

Selected Answer: C

The answer is C. an Azure Machine Learning workspace.

Microsoft Sentinel notebooks are run on an Azure Machine Learning (Azure ML) platform. To run notebooks in Microsoft Sentinel, you must have appropriate access to both Microsoft Sentinel workspace and an Azure ML workspace.

So, the first thing you need to do is create an Azure ML workspace. Once you have created an Azure ML workspace, you can then launch the Guided Investigation – Process Alerts notebook in Sentinel1.

The other options are incorrect.

Option A, an Azure logic app, is incorrect because Azure logic apps are used to automate workflows, not to run notebooks.
Option B, a Log Analytics workspace, is incorrect because Log Analytics workspaces are used to store and analyze data, not to run notebooks.
Option D, a Kusto query, is incorrect because Kusto queries are used to query data in Log Analytics workspaces, not to run notebooks.
Therefore, the correct answer is C.
https://learn.microsoft.com/en-us/azure/sentinel/notebooks

upvoted 1 times

Brigg5 1 year, 7 months ago

C is correct. "Microsoft Sentinel, notebooks are run on an Azure Machine Learning (Azure ML) platform. To run notebooks in Microsoft Sentinel, you must have appropriate access to both Microsoft Sentinel workspace and an Azure ML workspace." https://learn.microsoft.com/en-us/azure/sentinel/notebooks#manage-access-to-microsoft-sentinel-notebooks

upvoted 1 times

TavoGC 1 year, 7 months ago

Answer seems to be correct according to this link https://learn.microsoft.com/en-us/azure/sentinel/notebooks

While you can run Microsoft Sentinel notebooks in JupyterLab or Jupyter classic, in Microsoft Sentinel, notebooks are run on an Azure Machine Learning (Azure ML) platform. To run notebooks in Microsoft Sentinel, you must have appropriate access to both Microsoft Sentinel workspace and an Azure ML workspace.

upvoted 1 times

esabkov 1 year, 9 months ago

Selected Answer: C

Seems like C is correct - https://www.youtube.com/watch?v=OWjXee8o04M, please ignore other comments.

upvoted 1 times

esabkov 1 year, 9 months ago

Selected Answer: A

Seems like A is correct - https://www.youtube.com/watch?v=OWjXee8o04M

upvoted 1 times

esabkov 1 year, 9 months ago

Seems like A is correct - https://www.youtube.com/watch?v=OWjXee8o04M

upvoted 1 times

Unicorn02 1 year, 10 months ago

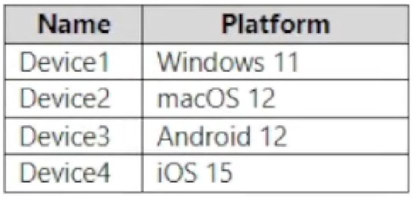
Selected Answer: D

No real idea here.Other Dumps mention Kusto Query as correct. Could not find any real proof from Microsoft Sources that relate to this question.

upvoted 3 times

Question #63 *Topic 2*

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



Name	Platform
Device1	Windows 11
Device2	macOS 12
Device3	Android 12
Device4	iOS 15

The devices are enrolled in Microsoft Endpoint Manager.

Which devices will be included in the encryption report?

A. Device1, Device3, and Device4 only

B. Device1 only

C. Device1 and Device2 only

D. Device2 and Device4 only

E. Device1, Device2, Device3, and Device4

Suggested Answer: *C*

Community vote distribution

C (100%)

Maxx4 1 year, 6 months ago

Selected Answer: C

Only Mac OS and Windows devices

upvoted 1 times

Porter5000 1 year, 8 months ago

Selected Answer: C

only MacOS and Windows, other two are phone operating systems

upvoted 1 times

formazionehs 1 year, 10 months ago

Correct answer: C

The encryption report supports reporting on devices that run the following operating system versions:

macOS 10.13 or later

Windows version 1607 or later

reference: https://learn.microsoft.com/en-us/mem/intune/protect/encryption-monitor

upvoted 3 times

Question #64 Topic 2

You have a Microsoft 365 E5 subscription named contoso.com.

You create a user named User1.

You need to ensure that User1 can change the status of Microsoft Defender for Identity health alerts. The solution must use principle of the least principle.

What should you do?

A. From the Microsoft 365 Defender portal, assign User1 the Security Operator role.

B. From the Microsoft 365 admin center, add User1 to the Azure ATP contoso.com Administrators group.

C. From the Microsoft 365 admin center, add User1 to the Azure ATP contoso.com Users group.

D. From the Microsoft 365 admin center, assign User1 the Hybrid Identity Administrator role.

Suggested Answer: *A*

Community vote distribution

A (100%)

Maxx4 1 year, 6 months ago

Selected Answer: A

The answer is A. From the Microsoft 365 Defender portal, assign User1 the Security Operator role.

The Security Operator role in Microsoft Defender for Identity allows users to change the status of health alerts. This role is a member of the Microsoft 365 Defender Security Users group, which is the least privileged group that can change the status of health alerts.

The other options are incorrect.

Option B, From the Microsoft 365 admin center, add User1 to the Azure ATP contoso.com Administrators group, is incorrect because this group has too many permissions.
Option C, From the Microsoft 365 admin center, add User1 to the Azure ATP contoso.com Users group, is incorrect because this group does not have the permissions to change the status of health alerts.
Option D, From the Microsoft 365 admin center, assign User1 the Hybrid Identity Administrator role, is incorrect because this role has too many permissions.
Therefore, the correct answer is A.

upvoted 1 times

Dhamus 1 year, 8 months ago

It's correct.

upvoted 2 times

Question #65 *Topic 2*

You have a Microsoft 365 E5 subscription.

You need to investigate threats to the subscription by using the Campaigns view in Microsoft Defender for Office 365.

Which types of threats will appear?

A. phishing only

B. phishing and malware only

C. phishing and password attacks only

D. malware only

E. malware and password attacks only

Suggested Answer: *B*

Community vote distribution

B (100%)

Maxx4 1 year, 6 months ago

Selected Answer: B

The answer is B. phishing and malware only.

The Campaigns view in Microsoft Defender for Office 365 shows all the phishing and malware campaigns that have targeted your organization. It does not show password attacks.

The other options are incorrect.

Option A, phishing only, is incorrect because the Campaigns view also shows malware campaigns.
Option C, phishing and password attacks only, is incorrect because the Campaigns view does not show password attacks.
Option D, malware only, is incorrect because the Campaigns view also shows phishing campaigns.
Option E, malware and password attacks only, is incorrect because the Campaigns view does not show password attacks.
Therefore, the correct answer is B.

upvoted 1 times

RomanV 1 year, 8 months ago

Campaigns in the Microsoft 365 Defender portal identifies and categorizes coordinated email attacks, including phishing and malware.

Source: https://learn.microsoft.com/en-us/microsoft-365/security/office-365-security/campaigns?view=o365-worldwide

upvoted 4 times

Question #66 *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 Defender for Office 365 reports from the Threat management dashboard.

Which role provides User1 with the required role permissions?

A. Security reader

B. Information Protection administrator

C. Reports reader

D. Exchange administrator

Suggested Answer: *A*

RomanV 1 year, 8 months ago

Answer A is correct.

Organization Management
Security Administrator
Security Reader <-----
Global Reader

Source: https://learn.microsoft.com/en-us/microsoft-365/security/office-365-security/reports-defender-for-office-365?view=o365-worldwide

upvoted 3 times

Question #67 *Topic 2*

You have a Microsoft 365 subscription that contains 50 devices. The devices are enrolled in Microsoft Endpoint Manager and have Microsoft Defender for Endpoint enabled.

You need to identify devices that have a pending offline scan.

What should you do?

A. From the Microsoft 365 Defender portal, review the Threat analytics dashboard.

B. From the Microsoft Endpoint Manager admin center, review the Antivirus agent status report.

C. From the Microsoft Endpoint Manager admin center, review the Detected malware report.

D. From the Microsoft 365 Defender portal, review the Threat & Vulnerability Management dashboard.

Suggested Answer: *D*

Community vote distribution

B (83%) C (17%)

Maxx4 1 year, 6 months ago

Selected Answer: B

The answer is B. From the Microsoft Endpoint Manager admin center, review the Antivirus agent status report.

The Antivirus agent status report in Microsoft Endpoint Manager shows the status of the antivirus agent on each device. This includes the status of the latest scan, whether the device is pending an offline scan, and any other relevant information.

The other options are incorrect.

Option A, From the Microsoft 365 Defender portal, review the Threat analytics dashboard, is incorrect because this dashboard does not show the status of offline scans.
Option C, From the Microsoft Endpoint Manager admin center, review the Detected malware report, is incorrect because this report shows the devices that have detected malware, not the devices that have a pending offline scan.
Option D, From the Microsoft 365 Defender portal, review the Threat & Vulnerability Management dashboard, is incorrect because this dashboard does not show the status of offline scans.
Therefore, the correct answer is B.

upvoted 1 times

mares79 1 year, 6 months ago

Selected Answer: B

B, https://howtomanagedevices.com/intune/5371/antivirus-agent-status-intune-report-endpoint-manager/

upvoted 1 times

raffykian 1 year, 6 months ago

Selected Answer: C

Microsoft 365 admin center

/ Endpoint Manager/

Antivirus - view pending

Microsoft 365 admin center

/ Endpoint Manager/

Antivirus - view pending

upvoted 1 times

Flacky_Penguin32 1 year, 7 months ago

Selected Answer: B

Confirmed, B.

upvoted 3 times

⊟ **dadmundur** 1 year, 8 months ago

The answer is wrong, there is no list of devices on the threat and vulnerability dashboard, which is now called "vulnerability management".

I believe the correct answer to be option B but the name of the report today is "Microsoft Defender Antivirus". It will show you pending scans.

Link to report: https://endpoint.microsoft.com/?ref=AdminCenter#view/Microsoft_Intune_Enrollment/ReportingMenu/~/defender

upvoted 4 times

⊟ **Tanasi** 1 year, 7 months ago

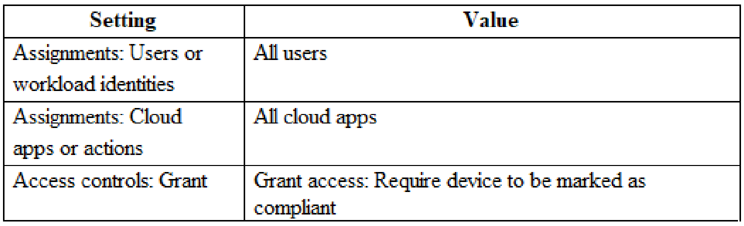
You are correct

upvoted 1 times

Question #68 Topic 2

You have a Microsoft 365 E5 subscription that contains 500 Windows 10 devices. The subscription uses Microsoft Defender for Endpoint and is integrated with Microsoft Endpoint Manager. All the devices have Defender for Endpoint deployed.

You create a Conditional Access policy as shown in the following table.



Setting	Value
Assignments: Users or workload identities	All users
Assignments: Cloud apps or actions	All cloud apps
Access controls: Grant	Grant access: Require device to be marked as compliant

You need to ensure that devices that have a machine risk score of high are blocked.

What should you do in Microsoft Endpoint Manager?

A. Apply a security baseline to all the devices.

B. Apply an endpoint detection and response policy to the subscription.

C. Apply a compliance policy to all the devices.

D. Configure the Compliance policy settings.

Suggested Answer: *A*

Community vote distribution

C (100%)

dadmundur Highly Voted 1 year, 8 months ago

Given answer is incorrect, C is the correct one.
To ensure that devices with a high machine risk score are blocked, you should apply a compliance policy to all the devices.

By applying a compliance policy to all the devices, you can configure the settings to evaluate the machine risk score and thus classify high risk devices as noncompliant and have them blocked by the conditional access policy.

upvoted 6 times

Maxx4 Most Recent 1 year, 6 months ago

Selected Answer: C

The answer is C. Apply a compliance policy to all the devices.

A compliance policy in Microsoft Endpoint Manager allows you to define the security requirements for your devices. You can use a compliance policy to block devices that have a high machine risk score.

The other options are incorrect.

Option A, Apply a security baseline to all the devices, is incorrect because a security baseline is a set of recommended security settings for your devices. It does not allow you to block devices that have a high machine risk score.
Option B, Apply an endpoint detection and response policy to the subscription, is incorrect because an endpoint detection and response policy is used to detect and respond to threats on your devices. It does not allow you to block devices that have a high machine risk score.
Option D, Configure the Compliance policy settings, is incorrect because this option is not available in Microsoft Endpoint Manager.

upvoted 2 times

andreane 1 year, 7 months ago

I believe C is correct:
https://learn.microsoft.com/en-us/mem/intune/protect/advanced-threat-protection-configure

upvoted 2 times

⊟ 👤 **Brigg5** 1 year, 7 months ago

C should be the answer. If you want a machine to be marked non-compliant and blocked by a conditional access policy, you need a compliance policy.

upvoted 3 times

Question #69 *Topic 2*

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

You need to protect users from malicious emails that attempt to capture their credentials. The solution must ensure that suspicious emails contain tips alerting the users to potential threats.

What should you create?

A. a Safe Links policy

B. an anti-phishing policy

C. an alert policy for delivered phishing email

D. an alert policy for suspicious email

Suggested Answer: *B*

Community vote distribution

B (100%)

Maxx4 1 year, 6 months ago

Selected Answer: B

The answer is B. an anti-phishing policy.

An anti-phishing policy in Microsoft Defender for Office 365 allows you to define the settings for detecting and blocking phishing emails. You can also configure the policy to include tips alerting users to potential threats.

The other options are incorrect.

Option A, a Safe Links policy, is incorrect because Safe Links policies are used to protect users from malicious links in emails. They do not include tips alerting users to potential threats.
Option C, an alert policy for delivered phishing email, is incorrect because this type of policy only alerts you when a phishing email is delivered. It does not include tips alerting users to potential threats.
Option D, an alert policy for suspicious email, is incorrect because this type of policy only alerts you when a suspicious email is detected. It does not include tips alerting users to potential threats.
Therefore, the correct answer is B.

upvoted 2 times

Question #70 *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 Microsoft Defender for Identity 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. Modify the Domain synchronizer candidate settings on the Microsoft Defender for Identity sensors.

C. Turn on Delayed updates for the Microsoft Defender for Identity sensors.

D. Enable the Audit account management Group Policy setting for the servers.

Suggested Answer: *A*

Community vote distribution

A (100%)

Maxx4 1 year, 6 months ago

Selected Answer: A

The answer is A. Configure Event Forwarding on the domain controllers.

Microsoft Defender for Identity uses Event Forwarding to collect security logs from domain controllers. By configuring Event Forwarding, you can ensure that Microsoft Defender for Identity can detect when sensitive groups are modified and when malicious services are created.

upvoted 1 times

Maxx4 1 year, 6 months ago

The other options are incorrect.

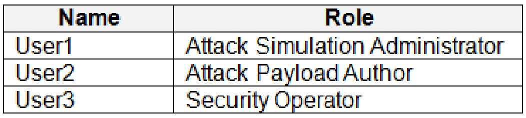
Option B, Modify the Domain synchronizer candidate settings on the Microsoft Defender for Identity sensors, is incorrect because this setting is used to determine which domain controllers are used to synchronize the Microsoft Defender for Identity database. It does not affect the detection of sensitive groups or malicious services.
Option C, Turn on Delayed updates for the Microsoft Defender for Identity sensors, is incorrect because this setting is used to delay the synchronization of the Microsoft Defender for Identity database. It does not affect the detection of sensitive groups or malicious services.
Option D, Enable the Audit account management Group Policy setting for the servers, is incorrect because this setting is used to audit account management events on the servers. It does not affect the detection of sensitive groups or malicious services.
Therefore, the correct answer is A.

upvoted 1 times

HOTSPOT

-

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



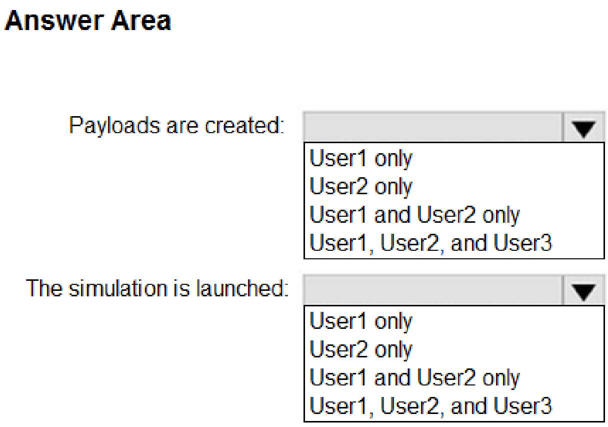
Name	Role
User1	Attack Simulation Administrator
User2	Attack Payload Author
User3	Security Operator

You need to run Attack simulation training. The solution must ensure that the following tasks are performed:

- Payloads are created.
- The simulation is launched.

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

NOTE: Each correct selection is worth one point.

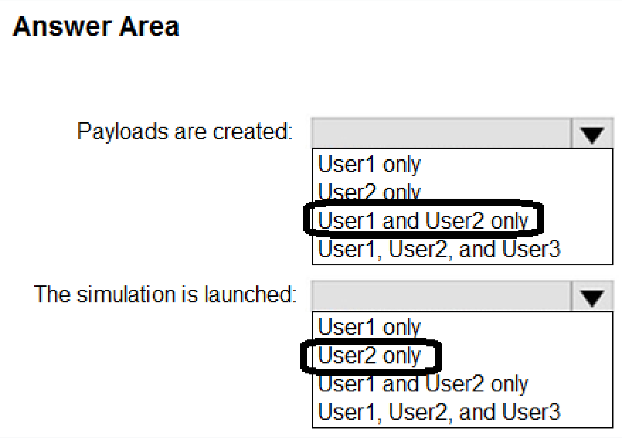


Answer Area

Payloads are created:
- User1 only
- User2 only
- User1 and User2 only
- User1, User2, and User3

The simulation is launched:
- User1 only
- User2 only
- User1 and User2 only
- User1, User2, and User3

Suggested Answer:



Answer Area

Payloads are created:
- User1 only
- User2 only
- [✓ User1 and User2 only]
- User1, User2, and User3

The simulation is launched:
- User1 only
- [✓ User2 only]
- User1 and User2 only
- User1, User2, and User3

McMac 1 year, 6 months ago

Attack Simulation Admin is the only one who can launch the Simulation, "Attack Payload Author*: Create attack payloads that an admin can initiate later." So the 2nd Answer shown is wrong.

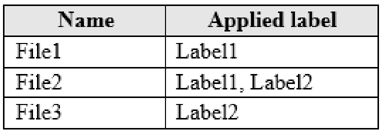
upvoted 2 times

Question #1 *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 that's shared with people outside my organization

✑ Actions: Restrict access to the content for external users

✑ User notifications: Notify the user who last modified the content

✑ User overrides: On

✑ Priority: 0

Rule2:

✑ Conditions: Label1 or Label2

✑ Actions: Restrict access to the content

✑ Priority: 1

Rule3:

✑ Conditions: Label2, Detect content that's shared with people outside my organization

✑ Actions: Restrict access to the content for external users

✑ User notifications: Notify the user who last modified the content

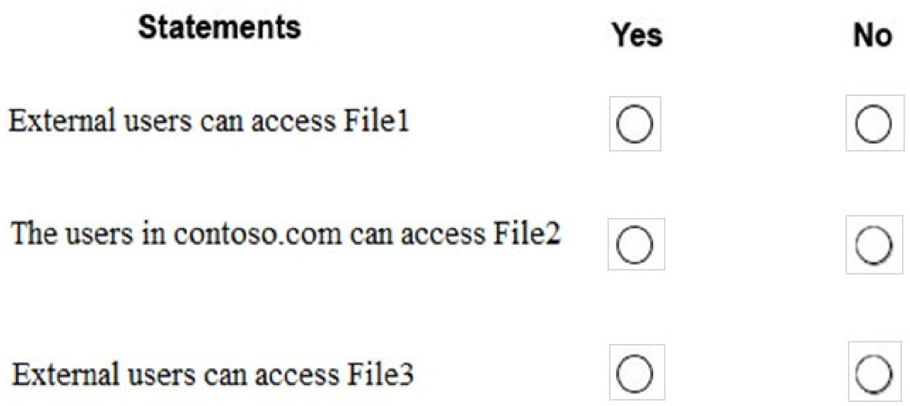
✑ User overrides: On

✑ Priority: 2

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

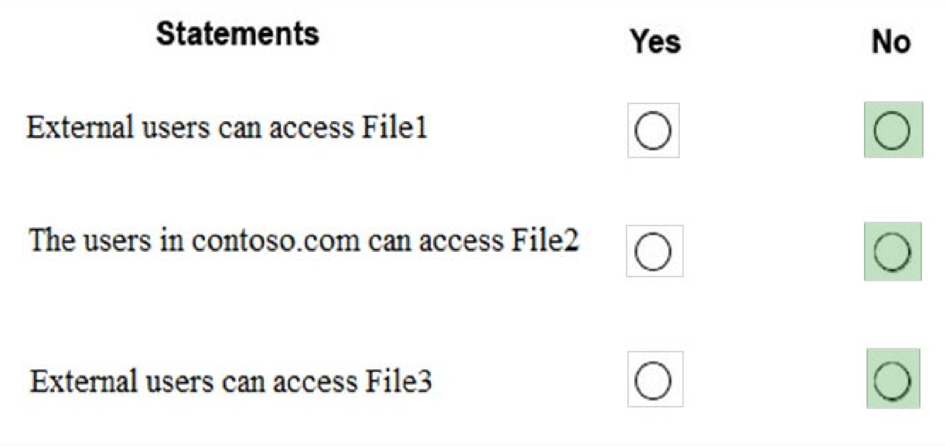
NOTE: Each correct selection is worth one point.

Hot Area:



Statements	Yes	No
External users can access File1	○	○
The users in contoso.com can access File2	○	○
External users can access File3	○	○

Suggested Answer:



Statements	Yes	No
External users can access File1	○	[✓ ○]
The users in contoso.com can access File2	○	[✓ ○]
External users can access File3	○	[✓ ○]

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. In this scenario rule 2 is the most restrictive.