Question #1 *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 are deploying Microsoft Endpoint Manager.
You successfully enroll Windows 10 devices in Endpoint Manager.
When you try to enroll an iOS device in Endpoint Manager, you get an error.
You need to ensure that you can enroll the iOS device in Endpoint Manager.
Solution: You add your user account as a device enrollment manager.
Does this meet the goal?

A. Yes

B. No

Suggested Answer: *B*

Community vote distribution

B (100%)

Chris_Rock Highly Voted 3 years, 6 months ago
An Apple MDM Push certificate is required for Intune to manage iOS/iPadOS and macOS devices. After you add the certificate to Intune, your users can enroll their devices. So correct answer is B
upvoted 16 times

Roche4ever Most Recent 1 year, 3 months ago
This series of questions are still valid
Was in Exam Today, 25 Sept 23
Answer is correct (No)
upvoted 1 times

lin6257 1 year, 5 months ago
B False is the answer
upvoted 1 times

Ayham_J 1 year, 9 months ago
On exam 4/1/2023
upvoted 2 times

Contactfornitish 2 years, 4 months ago
On exam on 13 aug'22
upvoted 3 times

Kevinfm_81 2 years, 6 months ago
Apple MDM Push Certificate is needed. Though I thought in 2019 Apple launched User enrollment as a part of ABM. Either way, B is the answer
upvoted 1 times

KofiKofi 2 years, 7 months ago
Selected Answer: B
Apple MDM push certificate is neccessary
upvoted 3 times

Alien1981 2 years, 7 months ago
Selected Answer: B
B is the correct answer
upvoted 2 times

riahisami77 3 years ago

Apple MDM Push Certificate is a prerequisite
To Enroll Apple Devices then flow the 5 steps to upload the Push Cert

Accept the licence agreement
Download Intune CSR
Create your MDM Push Cert
Enter the Apple ID
upload the push Cert
upvoted 4 times

NikPat3125 3 years, 5 months ago
come in exam 27.07.2021
upvoted 2 times

adaniel89 3 years, 6 months ago
Device Enrollment Manager can enroll any devices yeah ? https://docs.microsoft.com/en-us/mem/intune/enrollment/device-enrollment-manager-enroll
upvoted 1 times

Jaxon_84 3 years, 6 months ago
Yea, but they just successfully enrolled a windows 10 device, so obviously, that isn't the issue it would appear.
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 are deploying Microsoft Endpoint Manager.
You successfully enroll Windows 10 devices in Endpoint Manager.
When you try to enroll an iOS device in Endpoint Manager, you get an error.
You need to ensure that you can enroll the iOS device in Endpoint Manager.
Solution: You configure the Apple MDM Push certificate.
Does this meet the goal?

A. Yes

B. No

Suggested Answer: *A*
References:
https://docs.microsoft.com/en-us/intune/apple-mdm-push-certificate-get

Community vote distribution
A (100%)

Tonysurge Highly Voted 3 years, 5 months ago
Correct
upvoted 7 times

Domza Highly Voted 3 years, 4 months ago
Correct
upvoted 5 times

Roche4ever Most Recent 1 year, 3 months ago
This series of questions are still valid
Was in Exam Today, 25 Sept 23
Answer is correct
upvoted 1 times

in_cloud 1 year, 5 months ago
On exam july/2023
upvoted 1 times

iAwwad 1 year, 9 months ago
How about other enrollment restrictions!?
upvoted 1 times

Gillactus 1 year, 10 months ago
On exam Feb 21/2023
upvoted 2 times

Contactfornitish 2 years, 4 months ago
On exam on 13 aug'22
upvoted 2 times

bejeyep89 2 years, 5 months ago
Selected Answer: A
Correct
upvoted 3 times

potterknot 2 years, 6 months ago
Selected Answer: A

A, you need push certificate

upvoted 4 times

jeff1988 2 years, 11 months ago

Selected Answer: A

A is the correct one

upvoted 3 times

ThinhTr 3 years, 1 month ago

Correct answer

upvoted 3 times

AM77 3 years, 1 month ago

Correct Answer

upvoted 3 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 are deploying Microsoft Endpoint Manager.
You successfully enroll Windows 10 devices in Endpoint Manager.
When you try to enroll an iOS device in Endpoint Manager, you get an error.
You need to ensure that you can enroll the iOS device in Endpoint Manager.
Solution: You create an Apple Configurator enrollment profile.
Does this meet the goal?

A. Yes

B. No

Suggested Answer: *B*

Community vote distribution

B (100%)

junior6995 Highly Voted 3 years, 1 month ago
Apple configurator it is just an enrollment method not a pre requisite for enrolling apple devices. Answer is correct.
upvoted 9 times

Domza Highly Voted 3 years, 4 months ago
Apple push cert
upvoted 5 times

Roche4ever Most Recent 1 year, 3 months ago
This series of questions are still valid
Was in Exam Today, 25 Sept 23
Answer is correct (No)
upvoted 1 times

Contactfornitish 2 years, 4 months ago
On exam on 13 aug'22
upvoted 1 times

TV56_ 2 years, 5 months ago
Selected Answer: B
https://docs.microsoft.com/en-us/mem/intune/enrollment/apple-configurator-enroll-ios
upvoted 3 times

LillyLiver 2 years, 10 months ago
02/13/2022
So, yes, you can use the Apple Configurator Enrollment to register an iOS device. That is according to the MS doc in the link below.

The thing of note is, for this to work, you need to import the Apple Push Cert BEFORE the Apple Configurator settings are enabled. As noted in my tenant with no Apple Push Certificate applied and all other settings are disabled.

https://docs.microsoft.com/en-us/mem/intune/enrollment/apple-configurator-enroll-ios#:~:text=%20Create%20an%20Apple%20Configurator%20profile%20for%20devices,Next%20to%20display%20the%20Settings%20page.%20More%20

So the given answer is correct. No.
upvoted 3 times

DiscGolfer 3 years, 2 months ago

I think the answer is Yes
https://docs.microsoft.com/en-us/mem/intune/enrollment/apple-configurator-enroll-ios#create-an-apple-configurator-profile-for-devices
upvoted 1 times

JT19760106 2 years, 11 months ago
The question seems to indicate that the iOS device was trying to enroll manually through the Company Portal and not a direct USB connection to a Mac:

"Intune supports the enrollment of iOS/iPadOS devices using Apple Configurator running on a Mac computer. Enrolling with Apple Configurator requires that you USB-connect each iOS/iPadOS device to a Mac computer to set up corporate enrollment."
upvoted 1 times

NikPat3125 3 years, 5 months ago
come in exam 27.07.2021
upvoted 4 times

Domza 3 years, 4 months ago
feedback. Thx
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.
Your network contains an Active Directory domain named contoso.com that is synced to Microsoft Azure Active Directory (Azure AD).
You manage Windows 10 devices by using Microsoft System Center Configuration Manager (Current Branch).
You configure pilot co-management.
You add a new device named Device1 to the domain. You install the Configuration Manager client on Device1.
You need to ensure that you can manage Device1 by using Microsoft Intune and Configuration Manager.
Solution: You create a device configuration profile from the Device Management admin center.
Does this meet the goal?

A. Yes

B. No

Suggested Answer: *B*

Jade Highly Voted 3 years, 9 months ago
It looks like the given answer is correct.
There is an on-premises Active Directory synced to Azure Active Directory (Azure AD)
So the co-management path1 - Auto-enroll existing clients
1. Hybrid Azure AD
2. Client agent setting for hybrid Azure AD-join
3. Configure auto-enrollment of devices to Intune
4. Enable co-management in Configuration Manager
https://docs.microsoft.com/en-us/mem/configmgr/comanage/tutorial-co-manage-client
upvoted 7 times

JT19760106 2 years, 11 months ago
The question states "You configure pilot co-management" so it's assumed you've gone through the steps of Hybrid AAD, auto-ennrollment to Intune, enabling in config manager, now you have to setup the pilot collection:

"When you enable co-management, you'll assign a collection as a Pilot group. This is a group that contains a small number of clients to test your co-management configurations. We recommend you create a suitable collection before you start the procedure. Then you can select that collection without exiting the procedure to do so. You may need multiple collections since you can assign a different Pilot group for each workload."

https://docs.microsoft.com/en-us/mem/configmgr/comanage/tutorial-co-manage-clients#enable-co-management-in-configuration-manager
upvoted 1 times

NikPat3125 Highly Voted 3 years, 5 months ago
come in exam 27.07.2021
upvoted 6 times

OneplusOne Most Recent 2 years, 12 months ago
The goal is to be able to manage the device from SCCM ánd Intune.
Creating a Device Configuration Profile in Intune is not a necessary action needed to accomplish the goal.
upvoted 5 times

kiketxu 3 years, 9 months ago
Right. Isn't enough.
https://docs.microsoft.com/en-us/mem/configmgr/comanage/tutorial-co-manage-clients
upvoted 1 times

lucidgreen 3 years, 8 months ago

With hybrid Azure AD set-up and Configuration Manager client configurations in place, you're ready to flip the switch and enable co-management of your Windows 10 devices. The phrase Pilot group is used throughout the co-management feature and configuration dialogs. A pilot group is a collection containing a subset of your Configuration Manager devices. Use a pilot group for your initial testing, adding devices as needed, until you're ready to move the workloads for all Configuration Manager devices. There isn't a time limit on how long a pilot group can be used for workloads. A pilot group can be used indefinitely if you don't wish to move the workload to all Configuration Manager devices.
upvoted 2 times

lucidgreen 3 years, 8 months ago
The irony of that phrasing is great, isn't it?
upvoted 2 times

Question #5 *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.
Your network contains an Active Directory domain named contoso.com that is synced to Microsoft Azure Active Directory (Azure AD).
You manage Windows 10 devices by using Microsoft System Center Configuration Manager (Current Branch).
You configure pilot co-management.
You add a new device named Device1 to the domain. You install the Configuration Manager client on Device1.
You need to ensure that you can manage Device1 by using Microsoft Intune and Configuration Manager.
Solution: You add Device1 to an Active Directory group.
Does this meet the goal?

A. Yes

B. No

Suggested Answer: *B*
Reference:
https://docs.microsoft.com/en-us/mem/configmgr/comanage/tutorial-co-manage-clients

Kelek Highly Voted 4 years, 10 months ago
Device1 has the Configuration Manager client installed so you can manage Device1 by using Configuration Manager.
To manage Device1 by using Microsoft Intune, the device has to be enrolled in Microsoft Intune. In the Co-management Pilot configuration, you configure a Configuration Manager Device Collection that determines which devices are auto-enrolled in Microsoft Intune. You need to add Device1 to the Device Collection, not an Active Directory Group. Therefore, this solution does not meet the requirements.
Reference:
https://docs.microsoft.com/en-us/configmgr/comanage/how-to-enable
upvoted 56 times

airairo 3 years, 7 months ago
The short answer is NO.
upvoted 11 times

moh15 4 years, 8 months ago
Agree must be in collection
upvoted 3 times

dailyup 3 years, 8 months ago
I'll go with Kelek cause I remember there is a question from MS-100 and the answer is add device to pilot collection.
upvoted 2 times

lucidgreen 3 years, 8 months ago
A pilot group is a collection containing a subset of your Configuration Manager devices.
In other words, it needs to be a device collection consisting of only Windows 10 devices.
upvoted 2 times

GregD133 Highly Voted 4 years, 10 months ago
This answer is wrong. you need to add the device to the collection comanagement pilot was turned on for.
upvoted 15 times

Meebler Most Recent 1 year, 10 months ago
B. No.

Adding Device1 to an Active Directory group alone does not enable the device to be managed by both Microsoft Intune and Configuration Manager.

To achieve this goal, you need to perform the following steps:

Enable Co-Management in Configuration Manager.
Configure the Co-Management workload in Configuration Manager.
Create a Configuration Manager device collection for pilot Co-Management.
Configure Azure AD automatic enrollment in Intune.
Assign Configuration Manager policies to the pilot device collection.
Verify that Device1 is enrolled in Intune and the Configuration Manager client is installed and registered.
By completing these steps, you can manage Device1 by using both Microsoft Intune and Configuration Manager.
upvoted 2 times

Kevinfm_81 2 years, 6 months ago
Answer B. If you wanted to use AD you'd need to set up a AD group policy for device management
upvoted 1 times

jontini 2 years, 10 months ago
Answer is NO
upvoted 3 times

Tonysurge 3 years, 5 months ago
"Add Device1 to the collection" is a correct answer for this question, therefore, the answer is NO here.
upvoted 4 times

Stasn 3 years, 7 months ago
Similar question from Official MS prep exam:

Your on-premises network is configured as a Windows AD domain. You setup Win 10 device management using SCCM.
Windows AD domain users are synced with Azure AD Premium and all network devices are Azure AD joined.
You need to prepare for a limited pilot test of co-management. What should you do?
A. Create a Windows AD group for pilot users
B. Unjoin the pilot devices from Windows AD
C. Create an Azure AD group for pilot users
D. Create a Windows AD group for pilot devices

That correct answer they give is "D" - Create a Windows AD group for pilot devices
upvoted 3 times

Dan_Turnbull 3 years, 8 months ago
I've been trying to find the right answer to this, it does look like it's possible to use an AD Group:

You can enable the synchronization of collection memberships to an Azure Active Directory (Azure AD) group. This synchronization allows you to use your existing on premises grouping rules in the cloud by creating Azure AD group memberships based on collection membership results. You can synchronize device or user collections. Only resources with an Azure AD record are reflected in the Azure AD group.

https://docs.microsoft.com/en-us/mem/configmgr/core/clients/manage/collections/create-collections

https://oxfordcomputergroup.com/resources/systems-center-configuration-manager-comanagement-intune/

Any thoughts welcome :)
upvoted 3 times

marckinez 3 years, 8 months ago
I think the answer is correct, AD is synchronized with AZAD and you can manage from Intune and it has the SCCM agent
upvoted 1 times

itmp 3 years, 11 months ago
Device1 needs to be in the pilot collection. Adding Device 1 to Active Directory group doesn't mean it is added to collection...just my 2cents.
upvoted 3 times

kiketxu 3 years, 9 months ago
Thanks!
upvoted 2 times

mkoprivnj 3 years, 11 months ago
No is correct!

upvoted 3 times

Mr01z0 4 years, 2 months ago

There is no evidence in the provided text that you have created a collection with a dynamic membership rule to include the AD security group, this answer should be: No

upvoted 3 times

Alvaroll 4 years, 2 months ago

Same as MS-100 Topic1-22 https://www.examtopics.com/exams/microsoft/ms-100/view/5/

upvoted 1 times

VTHAR 4 years, 3 months ago

Answer is "B.NO" Device1 needs to be added into Collection not Active Directory group. But it's possible to create collection based on AD group but there is no such set up mentioned in question. So, it's B.

upvoted 4 times

Benoit_HAMET 4 years, 3 months ago

co-management applies to device collection; adding the device to a group does not allow it
unless the group is a collection membership rule which is not stated

upvoted 1 times

ExamStudy68 4 years, 3 months ago

I wonder if its because you need to add your device to AD because Co-Management requires auto-enrollment for Intune? Unsure but that is the only thing I can come up with

upvoted 1 times

Nibhath 4 years, 3 months ago

Since device is already managed using configuration manager clients, it needs AD security group to connect to Azure AD through which we connect to Microsoft Intune. So anser is YES.

upvoted 1 times

Question #6 *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.
Your network contains an Active Directory domain named contoso.com that is synced to Microsoft Azure Active Directory (Azure AD).
You manage Windows 10 devices by using Microsoft System Center Configuration Manager (Current Branch).
You configure pilot co-management.
You add a new device named Device1 to the domain. You install the Configuration Manager client on Device1.
You need to ensure that you can manage Device1 by using Microsoft Intune and Configuration Manager.
Solution: You unjoin Device1 from the Active Directory domain.
Does this meet the goal?

A. Yes

B. No

Suggested Answer: *B*

Community vote distribution

B (100%)

Zaz11 Highly Voted 4 years, 5 months ago
Correct, answer is B (No).
upvoted 14 times

Jake1 Highly Voted 3 years, 9 months ago
The device needs to be added to a Device Collection in order to be able to manage it from Intune
upvoted 13 times

lucidgreen 3 years, 8 months ago
They may use the term "Pilot Group". A pilot group is a collection containing a subset of your Configuration Manager devices. Semantics.
upvoted 6 times

prabhjot 1 year, 8 months ago
Solution: Define a Configuration Manager device collection as the pilot collection. Add Device1 to the collection. (it is there as q23 in MS 100)
upvoted 1 times

aims123456 Most Recent 2 years, 6 months ago
Selected Answer: B
Answer is B.
upvoted 2 times

kiketxu 3 years, 9 months ago
Agreed
upvoted 5 times

Question #7 *Topic 1*

HOTSPOT -

Your network contains an Active Directory forest named contoso.com that is synced to Microsoft Azure Active Directory (Azure AD).

You use Microsoft Endpoint Configuration Manager for device management.

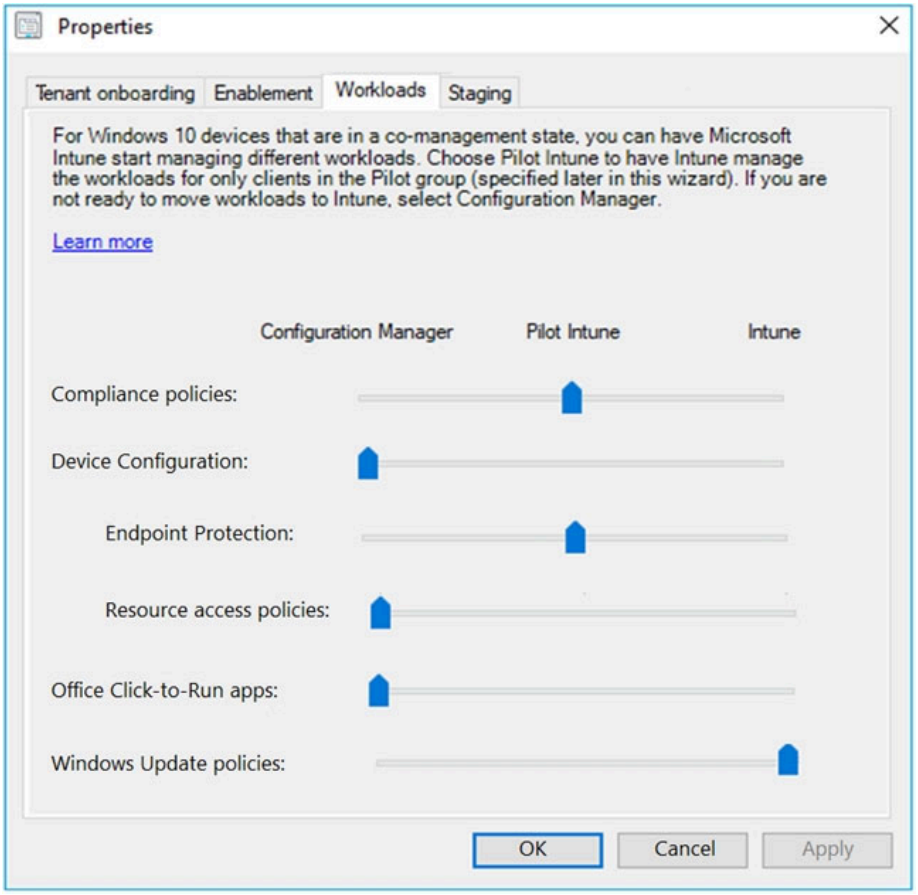
You have the Windows 10 devices shown in the following table.

Name	Collection
Device1	Collection1
Device2	Collection2

You configure Endpoint Configuration Manager co-management as follows:

- Automatic enrollment in Intune: Pilot
- Pilot collection for all workloads: Collection2

You configure co-management workloads as shown in the following exhibit.



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

NOTE: Each correct selection is worth one point.

Hot Area:

Answer Area

Statements	Yes	No
Microsoft Intune manages the compliance policies for Device1.	○	○
Configuration Manager manages the Windows Update policies for Device1.	○	○
Microsoft Intune manages Endpoint Protection for Device2.	○	○

Suggested Answer:

Answer Area

Statements	Yes	No
Microsoft Intune manages the compliance policies for Device1.	○	◉
Configuration Manager manages the Windows Update policies for Device1.	○	◉
Microsoft Intune manages Endpoint Protection for Device2.	◉	○

Prianishnikov Highly Voted 3 years, 9 months ago

NO-YES-YES

upvoted 60 times

lucidgreen 3 years, 8 months ago

The only devices enrolled in Co-management are those in the collection used as the Pilot Group.

upvoted 2 times

lucidgreen 3 years, 8 months ago

This means the only devices in Intune are those enrolled in co-management.

upvoted 1 times

LillyLiver 2 years, 10 months ago

Never mind. I re-read it and you are right. N,N,Y...

upvoted 2 times

LillyLiver 2 years, 10 months ago

I disagree. I think the given answers are correct.

You are assuming thing on the other end of the system that have nothing to do with the question. You have no proof of the SCCM setup, or whether Device1 is being managed by anything at all.

The question is asking, given the provided information, is Device1 being affected by the setting in the workload. The answer is no. The only device that is being affected is Device2.

Remember this is a Microsoft exam and they are looking for the answer to the question as asked. Don't read into the question or try to piece together the other end of it.

Answer is N, N, Y.

upvoted 7 times

Bulldozzer 2 years, 10 months ago

I disagree because, in the question statement, it is said that all devices are managed by Microsoft Endpoint Configuration Management. So the answer is N, Y, Y

upvoted 6 times

lucidgreen 3 years, 8 months ago

No. Device 1 is not in the "Pilot Group".

Yes. Device 1 can be assumed to be managed by Configuration Manager since it's not yet managed by Intune (hence the use of the term pilot).

Yes. Device 2 is part of the "Pilot Group" collection.

upvoted 24 times

lucidgreen 3 years, 5 months ago

One should also note that Device 1 is in Collection 1. The policy applies to Collection 2. So it has nothing to do with either the policy, co-management or Intune. Device 1 is most likely completely managed by Configuration Manager -- including updates. So the second answer is Yes. If it were Device 2, then the answer would be no.

upvoted 5 times

donathon Highly Voted 3 years, 8 months ago

N: Device1 is not in the pilot group

N: All devices regardless of in the pilot group or not are switched to update via InTune.

Y: Device2 is in the pilot group and anything in the pilot group should be managed by InTune.

Configuration Manager: Configuration Manager continues to manage this workload.

Pilot Intune: Switch this workload only for the devices in the pilot collection. You can change the Pilot collections on the Staging tab of the co-management properties page.

Intune: Switch this workload for all Windows 10 devices enrolled in co-management.

upvoted 23 times

donathon 3 years, 8 months ago

https://docs.microsoft.com/en-us/mem/configmgr/comanage/how-to-switch-workloads

upvoted 1 times

F_M 3 years, 3 months ago

"Intune: Switch this workload for all Windows 10 devices enrolled in co-management."

Nothing tells you that Device 1 has been enrolled in co-management...

upvoted 4 times

KSvh53 2 years, 9 months ago

"Intune: Switch this workload for all Windows 10 devices enrolled in co-management."
Nothing tells you that Device 1 has been enrolled in co-management...

This is incorrect. The question shows the co-management workloads tab of the co-management properties. In order to get to those settings, you would first have to enable co-management. Any devices in configuration manager would be enrolled in co-management once you activate it, and from there the workloads settings in the question are pretty straightforward on what happens next. Read this document, particularly the line where it says "You can switch workloads when you enable co-management, or later when you're ready. If you haven't already enabled co-management, do that first." The question states configuration manager is used to manage the devices, and those properties settings tell you configuration manager was enabled.
https://docs.microsoft.com/en-us/mem/configmgr/comanage/how-to-switch-workloads
upvoted 1 times

KSvh53 2 years, 9 months ago

typo, "and those properties settings tell you *co-management was enabled."
upvoted 1 times

Nunununu 3 years, 8 months ago

>N: All devices regardless of in the pilot group or not are switched to update via InTune.
why?
upvoted 1 times

kiketxu 3 years, 6 months ago

Look at the image. The switch is on the right of the bar for WU policies.
upvoted 1 times

mutleychunter 3 years, 6 months ago

There is nothing that tells you Device 1 is enrolled to Intune, so you can only assume all its workloads will be managed by Config Mgr. If it's not enrolled to intune then Co-management doesn't apply to it
upvoted 6 times

Chetithy 2 years, 5 months ago

"You use Microsoft Endpoint Configuration Manager for device management." this assumes that all of your devices are enrolled in Intune (otherwise you wouldn't be using it for device management)
upvoted 1 times

Chetithy 2 years, 5 months ago

Ignore me, I can't read.
upvoted 1 times

Amir1909 Most Recent 11 months ago

No
Yes
Yes
upvoted 1 times

EsamiTopici 1 year, 9 months ago

No,yes,yes?
upvoted 1 times

RiTh73 1 year, 10 months ago

The answer should be No, Yes, Yes.
1. Device1 doesn't enroll to co-management since it's not in the pilot collection. Thus everything's must be manage by CM. -> No
2. Since every setting or configuration of Devices1 must be manage by CM, thus the answer is -> Yes
3. This is obviously clear that device2 is in the pilot collection, so it's being manage by co-management -> Yes
upvoted 2 times

Fala_Fel 1 year, 11 months ago

No Yes Yes
Quest 2 is catching a lot of people out, it is asking about 'Config Manager' not Intune (unlike qu1), so as Device 1 isn't being managed by intune at all (not a member of pilot group) the answer is actually Yes.
upvoted 1 times

IT_Nerd31 2 years, 2 months ago

➩ Automatic enrollment in Intune: Pilot

➩ Pilot collection for all workloads: Collection2

Collection 1 (Device 1) is not being targeted, so answer has to be N-N-Y

upvoted 1 times

ServerBrain 2 years, 1 month ago

I agree with IT_Nerd31, and the shortest and simplest explanation.. this is the correct answer, N-N-Y,

upvoted 1 times

AVR31 2 years, 5 months ago

The answer is pretty clear, if you read the question carefully.
First one - NO. Device1 is not part of the Pilot collection (Collection2) so compliance is managed by CM.
Second one - NO. Same reason as above. Even if "Windows Update Policies" slider is set to "Intune", the question clearly states that "Automatic enrollment in Intune: Pilot" so only the devices from the Pilot collection (Collection2) are enrolled in Intune and thus have the update policies managed by Intune.
Third one is yes, for obvious reasons (Device2 is part of the Pilot Collection).

upvoted 2 times

AVR31 2 years, 5 months ago

Oh heck, I cannot edit my answer... The second one is YES. I missed the "Configuration Manager" from the beginning. The idea is that Device1 is not enrolled in Intune so everything related to it is managed by CM.

upvoted 4 times

Wojer 2 years, 6 months ago

its N,Y,Y.
The second question indeed does not mention the configuration of the ConfigMngr but by default settings for Clients Updates are enabled, so by default ConfigMngr is controlling updates.

upvoted 2 times

KSvh53 2 years, 9 months ago

There is a lot of confusion on this question, specifically number 2. Some people seem to think these settings don't tell us anything about co-management for device 1. That's incorrect. We know all devices are in configuration manager based on what the question said, and (this is where the confusion is at) we know co-management was enabled because we wouldn't be able to get to the properties of co-management before activating co-management, so co-management is enabled, and that means the answer for option 2 is NO. The policy created only determines which devices are in the pilot group. All other devices not in that group follow the co-management settings.

If you read this document, you will see what I am referring to. "You can switch workloads when you enable co-management, or later when you're ready. If you haven't already enabled co-management, do that first."
https://docs.microsoft.com/en-us/mem/configmgr/comanage/how-to-switch-workloads

Answers are N, N, Y.

upvoted 2 times

JAPo123 2 years, 9 months ago

+ You use Microsoft Endpoint Configuration Manager for device management.

+ Device1 -->Collection1

+ Pilot collection for all workloads : Collection2 --> ("co-management")

+ Answer 2: Yes

upvoted 1 times

jontini 2 years, 10 months ago

NO, Yes, Yes

upvoted 2 times

karank19 2 years, 11 months ago

No- YES- YES(refer lucidgreens explanation)
It makes Perfect Sense

upvoted 2 times

us3r 3 years ago

Obvious:
1: NO
3: YES

Now lets go to the 2nd question: I will go with the (NO)
Explanation
The device1 Windows updates are NOT managed by Intune, that is for sure.
All of you assume that device1 Win updates are managed by ConfigManager because they are not managed by Intune. Why? Do we have this information in the facts of the question?
No! The Win Updates could be not managed at all! Think out of the box!

NO
NO
YES

upvoted 5 times

ZuluHulu 3 years, 2 months ago

N-Y-Y
Auto enrollment in Intune excludes device 1 from being managed by Intune.
https://docs.microsoft.com/en-us/mem/configmgr/comanage/how-to-enable

upvoted 2 times

Patrick2401 3 years, 3 months ago

So what's the right answer?
--
Nothing tells me that Device1 is a part of a pilot collection group.

Microsft Intune manages the compliance policies for Device1: NO
ConfMgr manages the Windows Update policies for Device1: Yes
Intune manages Endpoint Protection for Device2: Yes

upvoted 2 times

mnak 3 years, 3 months ago

YYN
2 is Yes because Device 1 is NOT enrolled in Intune and therefore cannot use any Intune workload. It can only use CM.
Read:
Automatic enrollment into Intune - Pilot: Only the Configuration Manager clients that are members of the Intune Auto Enrollment collection are automatically enrolled to Intune.
https://docs.microsoft.com/en-us/mem/configmgr/comanage/tutorial-co-manage-clients.

upvoted 2 times

mnak 3 years, 3 months ago

Typo . I meant NYY as the answer not, YYN.

upvoted 2 times

Question #8 *Topic 1*

HOTSPOT -

You have three devices enrolled in Microsoft Intune as shown in the following table.

Name	Platform	Member of
Device1	Windows 10	Group1
Device2	Android	Group2, Group3
Device3	Windows 10	Group2, Group3

The device compliance policies in Intune are configured as shown in the following table.

Name	Platform	Assigned
Policy1	Windows 10 and later	Yes
Policy2	Android	No
Policy3	Windows 10 and later	Yes

The device compliance policies have the assignments shown in the following table.

Name	Include	Exclude
Policy1	Group3	*None*
Policy2	Group2	Group3

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 Device3.	○	○
Policy2 applies to Device2.	○	○

Suggested Answer:

Answer Area

Statements	Yes	No
Policy1 applies to Device3.	◯	○
Policy2 applies to Device2.	◯	○

ALPHA_DELTA Highly Voted 3 years, 9 months ago

Taken from a previous comment on this question:

Policy 1 applies to Device 3. YES.

Policy 2 applies to Device 2. NO

Policy 2 also doesn't apply to Device 2 because that device is in Group 3, which is excluded from the policy.

Exclusion takes precedence over inclusion in the following same group type scenarios:

upvoted 96 times

marckinez Highly Voted 3 years, 8 months ago

Policy1 applies to Device 3. YES

Policy2 applies to Device 2. NO

The second policy no applies to Device 2 because the policy is not assigned

upvoted 41 times

lucidgreen 3 years, 8 months ago

True. Plus, it excludes Group 3. Excludes override all includes.

upvoted 9 times

MiZi 3 years, 8 months ago

I agree. In addition have a question. How you can have a policy unassigned and still have assigned groups to the policy. Isn't it a contradiction? Or maybe I am missing something.

upvoted 7 times

Daanvanbeek 2 years, 7 months ago

They are seperate steps, it just doesn't apply untill everything is assigned correctly.

upvoted 1 times

EsamiTopici Most Recent 1 year, 9 months ago

No yes yes?

upvoted 1 times

EsamiTopici 1 year, 9 months ago

wrong comment, obv this is yes no.

upvoted 2 times

ServerBrain 2 years, 1 month ago

1. Yes - Policy 1 is assigned to Group 3
2. No - Group 3 is excluded, Group 2 is not assigned

upvoted 2 times

SaeedFarvardin 2 years, 4 months ago

100% YES/NO

upvoted 6 times

Kevinfm_81 2 years, 6 months ago

Doesn't appear Android Devices (device 2) have an Intune policy assigned...so answers would be Y and N

upvoted 4 times

L33D 2 years, 6 months ago

Still valid, on exam Jun 25, 2022

upvoted 3 times

KofiKofi 2 years, 7 months ago

1 Yes

2 No - Policy2 is not assigned and exclusion overrides inclusion

upvoted 4 times

KSvh53 2 years, 9 months ago

The assigned contradiction makes no sense, but knowing exclusions take priority over inclusions is key to being able to answer this correctly.
Correct answer: Y, N.

"Exclusion takes precedence over inclusion in the following same group type scenarios:
Including user groups and excluding user groups when assigning apps
Including device groups and excluding device group when assigning apps"
https://docs.microsoft.com/en-us/mem/intune/apps/apps-inc-exl-assignments

upvoted 2 times

JamesM9 2 years, 9 months ago

1. Policy applies to device 3 - Yes. Policy 1 is assigned to Group3, which takes priority. The assigned category in policy is set to yes, so the policy will be assigned to any Windows 10 devices.

2. Group3 takes priority for Device 2 but is excluded from Policy 2, which leaves Group2. Group2 is is not assigned, which means the answer is no. Remember that an exclude action overrides an include action.

Answers:

1. Yes
2. No

upvoted 2 times

JAPo123 2 years, 9 months ago

Either the groups are "assigned" or not.
The displayed settings of the device compliance policies are incorrect.

upvoted 1 times

gxsh 3 years ago

Policy 1 > Group 3 > Device 3 => YES, assigned, windows 10, so YES
Policy 2 > Group 2 > Device 2 => NO, not assigned

upvoted 8 times

riahisami77 3 years ago

so why the answer is YES YES?? since the most Voted YES, NO !!!

upvoted 3 times

auton 3 years, 2 months ago

I agree with "YES NO".

Policy 1 applies to Device3 because Policy1 is applied and assigned (Windows 10 policy, assigned to Group3).

Policy2 on the other hand is an Android policy, which is not even assigned yet. Group3 is also excluded from the policy, and it would not apply anyways. This makes it a "NO".

upvoted 4 times

Patrick2401 3 years, 4 months ago

Answer must be:

Yes

No - Excludes override includes

upvoted 3 times

Carlo5 3 years, 4 months ago

The keyword is 'apply'. Since the Device 2 is an Android device ...

upvoted 1 times

Domza 3 years, 5 months ago

Also, Policy 2 is NOT assigned. lol

upvoted 3 times

Question #9 *Topic 1*

You have Windows 10 Pro devices that are joined to an Active Directory domain.
You plan to create a Microsoft 365 tenant and to upgrade the devices to Windows 10 Enterprise.
You are evaluating whether to deploy Windows Hello for Business.
What are two prerequisites of the deployment? Each correct answer presents a complete solution.
NOTE: Each correct selection is worth one point.

A. Microsoft Endpoint Manager enrollment

B. Microsoft Azure Active Directory (Azure AD)

C. smartcards

D. TPM-enabled devices

Suggested Answer: *AB*
Reference:
https://docs.microsoft.com/en-us/windows/security/identity-protection/hello-for-business/hello-hybrid-aadj-sso-base

Community vote distribution
AB (89%) 11%

marckinez Highly Voted 3 years, 9 months ago
it's correct
upvoted 17 times

[Removed] Highly Voted 3 years, 3 months ago
The answer is A and B, there is the ref. https://docs.microsoft.com/en-us/windows/security/identity-protection/hello-for-business/hello-identity-verification
upvoted 9 times

OomensRob 3 years, 2 months ago
For all who claim TPM is pre-requisite for WH4B: TPM is ONLY used for biometric recognition in conjunction with WH4B. WH4B can be used with just a pin code as well and thus no TPM is required for WH4B
upvoted 11 times

RahulX Most Recent 1 year, 5 months ago
Correct answer is A & B
upvoted 1 times

PL1313 1 year, 9 months ago
Answer is A and D. TPM Enabled Devices are now a requirement for Windows Enterprise:

Since July 28, 2016, all new device models, lines, or series (or if you're updating the hardware configuration of an existing model, line, or series with a major update, such as CPU, graphic cards) must implement and enable by default TPM 2.0 (details in section 3.7 of the Minimum hardware requirements page). The requirement to enable TPM 2.0 only applies to the manufacturing of new devices. For TPM recommendations for specific Windows features, see TPM and Windows Features.
upvoted 1 times

ann0ysum0 1 year, 8 months ago
The scope of the question is evaluating WH4B deployment. For that, TPM isn't required. Though the devices will have to have it for Win10 Ent upgrade, they don't need it for WH4B. Given answer (A&B) is correct.
upvoted 2 times

TechMinerUK 2 years, 2 months ago
The question seems to be incorrectly worded as from my understanding none of the listed answers are requirements for WHFB. Whilst in a hybrid deployment you would need AzureAD (In order for it to be hybrid) you wouldn't ever "Require" TPM, Smartcards or Intune despite it being possible to use all of them in the deployment of WHFB.

"Required" would make me assume that it is mandatory regardless of the setup e.g. it is required you need a computer
upvoted 2 times

ARYMBS 2 years, 3 months ago

Selected Answer: AB

At first I also answered incorrectly. Problem lies with the question itself... IGNORE the sentence "You are evaluating whether to deploy Windows Hello for Business" because none of the four answers are the WHfB requirements.... Pay attention only to "You plan to create a Microsoft 365 tenant and to upgrade the devices to Windows 10 Enterprise.". If we apply this logic:
B - because you plan to create Microsoft 365 tenant.
A - because you plan to upgrade the devices to Windows 10 Enterprise (I think it is a modern way to upgrade Pro to Enterprise without sign out).

SO the answers are correct?
I'm really sad about this kind of questions from Microsoft :(

upvoted 7 times

AVR31 2 years, 5 months ago

Selected Answer: AB

From the answers provided, TPM and smart cards are definitely NOT required.
Intune isn't either, but it given as optional in the official documentation, so choosing that:
https://docs.microsoft.com/en-us/windows/security/identity-protection/hello-for-business/hello-identity-verification

upvoted 3 times

Krish1610 2 years, 5 months ago

Selected Answer: AB

Correct answer is A & B

upvoted 3 times

Contactfornitish 2 years, 6 months ago

Selected Answer: AB

Windows Hello for Business definitely possible without TPM or Smart card
https://docs.microsoft.com/en-us/windows/security/information-protection/tpm/tpm-recommendations

upvoted 3 times

Alv86 2 years, 6 months ago

Selected Answer: AD

I have set it up and we do not have intune, only ad connect and tpm for devices.

upvoted 2 times

Zardu 2 years, 9 months ago

Required:
Windows 10, version 1511 or later, or Windows 11
Microsoft Azure Account
Azure Active Directory
Azure AD Multifactor Authentication
Optinoal:
Modern Management (Intune or supported third-party MDM), optional
Azure AD Premium subscription - optional, needed for automatic MDM enrollment when the device joins Azure Active Directory
(from link provided by AniIT)

upvoted 3 times

PDR 3 years ago

TPM definitely not required - I use WHFB on my desktop that does not have TPM and I login with a fingerprint reader (or pin).
I think A and B is the correct answer because to enable Windows Hello for Business (N.B. not just Windows Hello which can be used on a standalone machine) you need to do this through intune. A user would have to have an account in an AAD tenant also

upvoted 4 times

gxsh 3 years ago

Answer is correct.

upvoted 3 times

UWSFish 3 years, 3 months ago

According to the literature neither TPM nor Intune is actually required. However I believe TPM is the better answer. However between the two TPM seems the better answer. The whole point is to use PIN/biometric as a mechanism to load the private key. While this key can be stored on the file system, the whole idea is for it to be stored on TPM. So I think AAD & TPM is correct.

upvoted 2 times

Patrick2401 3 years, 4 months ago

I think the right answer is AAD/TPM.

Microsoft state: Modern Management (Intune or supported third-party MDM), optional
It's optional not a requirement.

The device has to be AAD-joined.
Smart cards solution has nothing to do with this.
So the only option left is TPM.

upvoted 1 times

JhonyTrujillo 3 years, 4 months ago

A Trusted Platform Module (TPM) provides an additional layer of data security. If set to required, only devices with an accessible TPM can provision Windows Hello for Business. If set to preferred, devices attempt to use a TPM, but if not available will provision using software.

upvoted 1 times

afbnfz 3 years, 6 months ago

A and B.
TPM is NOT a prerequisite for Hello for Business.
https://docs.microsoft.com/en-us/windows/security/identity-protection/hello-for-business/hello-identity-verification

upvoted 5 times

Question #10 *Topic 1*

You have a Microsoft 365 tenant.
All users are assigned the Enterprise Mobility + Security license.
You need to ensure that when users join their device to Microsoft Azure Active Directory (Azure AD), the device is enrolled in Microsoft Endpoint Manager automatically.
What should you configure?

A. Enrollment restrictions from the Endpoint Manager admin center

B. device enrollment managers from the Endpoint Manager admin center

C. MAM User scope from the Azure Active Directory admin center

D. MDM User scope from the Azure Active Directory admin center

Suggested Answer: *D*
References:
https://docs.microsoft.com/en-us/mem/intune/enrollment/windows-enroll

Glorence Highly Voted 2 years, 11 months ago
still valid, came in the exam feb 5, 2022
upvoted 10 times

NikPat3125 Highly Voted 3 years, 5 months ago
come in exam 27.07.2021
upvoted 9 times

haazybanj 3 years, 1 month ago
Thanks
upvoted 1 times

RahulX Most Recent 1 year, 5 months ago
Correct Answer: D
upvoted 1 times

in_cloud 1 year, 5 months ago
On exam july/2023
upvoted 2 times

Rocky83 3 years, 1 month ago
That's correct.
upvoted 8 times

sammyjj 3 years, 5 months ago
D for sure
upvoted 5 times

Question #11 *Topic 1*

HOTSPOT -

You have several devices enrolled in Microsoft Endpoint Manager.

You have a Microsoft Azure Active Directory (Azure AD) tenant that includes the users shown in the following table.

Name	Member of
User1	Group1
User2	Group1, Group2
User3	**None**

The device type restrictions in Endpoint Manager are configured as shown in the following table.

Priority	Name	Allowed platform	Assigned to
1	Policy1	Android, iOS, Windows (MDM)	**None**
2	Policy2	Windows (MDM)	Group2
3	Policy3	Android, iOS	Group1
Default	All users	Android, Windows (MDM)	All users

You add User3 as a device enrollment manager in Endpoint Manager.

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

NOTE: Each correct selection is worth one point.

Hot Area:

Answer Area

Statements	Yes	No
User1 can enroll Windows devices in Endpoint Manager.	○	○
User2 can enroll Android devices in Endpoint Manager.	○	○
User3 can enroll iOS devices in Endpoint Manager.	○	○

Suggested Answer:

Answer Area

Statements	Yes	No
User1 can enroll Windows devices in Endpoint Manager.	○	○
User2 can enroll Android devices in Endpoint Manager.	○	○
User3 can enroll iOS devices in Endpoint Manager.	○	○

Box 1:

No. User1 is in Group1. The two device type policies that apply to Group1 are Policy3 and the Default (All Users) policy. However, Policy3 has a higher priority than the default policy so Policy3 is the only effective policy. Policy3 allows the enrolment of Android and iOS devices only, not Windows.

Box 2:

No. User2 is in Group1 and Group2. The device type policies that apply to Group1 and Group2 are Policy2, Policy3 and the Default (All Users) policy. However,

Policy2 has a higher priority than Policy 3 and the default policy so Policy2 is the only effective policy. Policy2 allows the enrolment of Windows devices only, not

Android.

Box 3:

Yes. User3 is a device enrollment manager. Device restrictions to not apply to a device enrollment manager.

Reference:

https://docs.microsoft.com/en-us/intune/enrollment/enrollment-restrictions-set

techtest848 Highly Voted 3 years ago

I believe it should be No, No, No

The device enrollment manager role only gives you the option to enroll up to 1000 devices. I think enrollment OS type restricions still apply

upvoted 23 times

Bulldozzer 2 years, 10 months ago

I agree. Device Type is more applicable for blocking OS platforms without taking into account of the user logged in.

upvoted 1 times

jodtzz 3 years ago

I think you're right. I can't find any documentation that says enrollment managers are not subject to platform restrictions, though the linked article explicitly states they aren't subject to device limit restrictions.

upvoted 5 times

Llex 3 years ago

This is so not correct.

upvoted 1 times

Llex 3 years ago

The closest answer is N N Y

upvoted 4 times

[Removed] 3 years ago

I would also vote for that. Can't find any other prove on https://docs.microsoft.com/en-us/mem/intune/enrollment/device-enrollment-manager-enroll and https://docs.microsoft.com/en-us/mem/intune/enrollment/enrollment-restrictions-set

upvoted 1 times

Storm Highly Voted 3 years ago

Answer is definitely correct...

NNY

Device limit restrictions don't apply for the following Windows enrollment types:

- Co-managed enrollments
- GPO enrollments
- Azure Active Directory joined enrollments
- Bulk Azure Active Directory joined enrollments
- Autopilot enrollments
- Device Enrollment Manager enrollments

Device limit restrictions are not enforced for these enrollment types because they're considered shared device scenarios. You can set hard limits for these enrollment types in Azure Active Directory.

https://docs.microsoft.com/en-us/mem/intune/enrollment/enrollment-restrictions-set

upvoted 7 times

Wojer 2 years, 6 months ago

Device limit restriction have nothing to do with device type restriction

upvoted 9 times

dyers Most Recent 2 years, 2 months ago

Didn't test this, but No, No, Yes.

If you google "device type restrictions in mem"

You get two results, the first is https://learn.microsoft.com/en-us/mem/intune/enrollment/enrollment-restrictions-set

the second is https://learn.microsoft.com/en-us/mem/intune/enrollment/create-device-platform-restrictions

These are actually in the same hierarchy, on the first link it says:

"Device limit restrictions can't be applied to devices in the following Windows enrollment scenarios, because these scenarios utilize shared device mode:

Co-managed enrollments

...

Device enrollment manager enrollments"

The second link which more explicitly says "device type restrictions" rather than "Limitations" but even the bullet point above the one I posted says, "Device enrollment limitations apply to users", then lists all the ways users enroll, not isn't in the list. DEM is using shared device mode, so

not subject to those limitations. I think the swapping between limitations and restrictions is getting everyone confused. If you look, it's covering the same topic. Do your research, test it out if you have the time and capability.

upvoted 4 times

veteran_tech 2 years, 4 months ago

The original answer is correct. User 3 is a device enrollment manager. There are certain limits on a DEM. One of the limits is that conditional access only applies if the device you are enrolling is Windows 10 1803 or Windows 11. You can enroll certain iOS and Android devices.

upvoted 1 times

aims123456 2 years, 6 months ago

NO, No, No..The first are simple to understand..the 3rd one is No as stated on MS site. (https://docs.microsoft.com/en-gb/mem/intune/enrollment/device-enrollment-manager-enroll)
Apple Automated Device Enrollment
DEM isn't compatible with Apple Automated Device Enrollment (ADE).

upvoted 1 times

Wojer 2 years, 6 months ago

You are right but type restriction still apply

upvoted 1 times

Fala_Fel 2 years, 2 months ago

DEM can enroll Apple Devices, it is just not compatible with ADE, but that is not the only method of enrolling iOS devices.
https://learn.microsoft.com/en-us/mem/intune/fundamentals/deployment-guide-enrollment-ios-ipados

upvoted 1 times

Mendel 2 years, 8 months ago

As stated by Techtest848 and OneplusOne this should be No, No, No. Unless of course NONE (which is in bold) is the name of a group.

DEM account does bypass the Device limit restriction, but not Device type.

upvoted 3 times

MichaelMu 2 years, 8 months ago

answers are correct

upvoted 2 times

LillyLiver 2 years, 10 months ago

I say it's N, N, N.

User1, in Group1, can't add a Windows machine because Group1 is applied to policy 3 allowing Android.

User2, In Group1/2, can't add an Android device because Group2 is a higher priority allowing Windows only.

User3 isn't a member of any group. The only policy that works for this is the Default policy allowing Android, and Windows Only. So User3 cannot add an iOS device.

upvoted 4 times

ericwiley 2 years, 11 months ago

No, No, Yes

upvoted 4 times

KornienkoBoris 2 years, 11 months ago

https://docs.microsoft.com/en-us/mem/intune/enrollment/enrollment-restrictions-set#create-a-device-limit-restriction
look at the Important block:
Device limit restrictions don't apply for the following Windows enrollment types: ... Device Enrollment Manager enrollments
NNY

upvoted 2 times

TimurKazan 3 years ago

N,N,Y https://docs.microsoft.com/en-us/mem/intune/enrollment/enrollment-restrictions-set
this does not apply to DEmanager as described in the link below

upvoted 4 times

Bulldozzer 2 years, 11 months ago

This is only applicable for Device Limit Restriction.

upvoted 2 times

venwaik 2 years, 8 months ago

Device limit and device type restrictions are two different stories for the DEM account. Answer should be NO in this particular case

upvoted 2 times

Goena 3 years ago

N, N, Y

User1: Group 1: Policy 3, Android and iOS only

User2: Group 2: Policy 2, Windows Only

User3: No group but DEM can enroll up to 1000 devices

upvoted 6 times

gxsh 3 years ago

Answers are correct.

upvoted 4 times

Question #12 *Topic 1*

HOTSPOT -

You create two device compliance policies for Android devices as shown in the following table.

Policy	Configuration	Action	Assigned to
Policy1	Require encryption of the data storage on the device.	Mark as noncompliant immediately.	Group1
Policy2	Require Google Play services.	Mark as noncompliant immediately.	Group2

You have the Android devices shown in the following table.

Name	User	Configuration
Android1	User1	Not encrypted
Android2	User2	Google Play services not configured
Android3	User3	Not encrypted Google Play services configured

The users belong to the groups shown in the following table.

User	Group
User1	Group1
User2	Group1, Group2
User3	Group2

The users enroll their device in Microsoft Endpoint Manager.

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

NOTE: Each correct selection is worth one point.

Hot Area:

Answer Area

Statements	Yes	No
The device of User1 is compliant.	○	○
The device of User2 is compliant.	○	○
The device of User3 is compliant.	○	○

Suggested Answer:

Answer Area

Statements	Yes	No
The device of User1 is compliant.	○	◉
The device of User2 is compliant.	○	◉
The device of User3 is compliant.	◉	○

References:

https://docs.microsoft.com/en-us/intune-user-help/enroll-your-device-in-intune-android

kiketxu Highly Voted 3 years, 8 months ago

NO

NO

YES

upvoted 41 times

lucidgreen 3 years, 8 months ago

No. User 1, Device 1, Group 1, Not encrypted. Marked Not Compliant by Policy 1

No. User 2, Device 2, Groups 1&2, Google Play Services not configured. Marked Not Compliant by Policy 2.

Yes. User 3, Device 3, Group 2, Not encrypted & Google Play Services configured. No policy can mark it "Not Compliant".

upvoted 16 times

Prianishnikov Highly Voted 3 years, 9 months ago

NO-NO-YES

upvoted 9 times

gkp_br Most Recent 3 years, 5 months ago

NO-NO-YES

Assign a resulting compliance policy status
If a device has multiple compliance policies, and the device has different compliance statuses for two or more of the assigned compliance policies, then a single resulting compliance status is assigned. This assignment is based on a conceptual severity level assigned to each compliance status. Each compliance status has the following severity level:

ASSIGN A RESULTING COMPLIANCE POLICY STATUS
Status Severity
Unknown 1
NotApplicable 2
Compliant 3
InGracePeriod 4
NonCompliant 5
Error 6
When a device has multiple compliance policies, then the highest severity level of all the policies is assigned to that device.

For example, a device has three compliance policies assigned to it: one Unknown status (severity = 1), one Compliant status (severity = 3), and one InGracePeriod status (severity = 4). The InGracePeriod status has the highest severity level. So, all three policies have the InGracePeriod compliance status.

https://docs.microsoft.com/en-us/mem/intune/protect/create-compliance-policy
upvoted 6 times

lucidgreen 3 years, 5 months ago
Remind me if there is some form of precedence here -- like if one policy marks it as compliant, can a second one mark it as non-compliant? If it can't, N,Y,Y. If it can N,N,Y.
upvoted 1 times

Yetijo 3 years, 5 months ago
If a device is assigned to one or more applicable policies, then its compliance is tied to all assigned policies. So, if the device is compliant by the terms of policy one, but is not compliant by the terms of policy 2, then the device is rendered not-compliant.
upvoted 4 times

PersonT 3 years, 9 months ago
question doesn't make sense, but
Mark devices with no compliance policy assigned as

This setting determines how Intune treats devices that haven't been assigned a device compliance policy. This setting has two values:

Compliant (default): This security feature is off. Devices that aren't sent a device compliance policy are considered compliant.
Not compliant: This security feature is on. Devices that haven't received a device compliance policy are considered noncompliant.
If you use Conditional Access with your device compliance policies, we recommended you change this setting to Not compliant to ensure that only devices that are confirmed as compliant can access your resources.
upvoted 2 times

Question #13 *Topic 1*

HOTSPOT -

Your network contains an Active Directory domain named contoso.com. All client devices run Windows 10 and are joined to the domain.

You update the Windows 10 devices by using Windows Update for Business.

What is the maximum amount of time you can defer Windows 10 updates? To answer, select the appropriate options in the answer area.

NOTE: Each correct selection is worth one point.

Hot Area:

Answer Area

Quality updates: [14 days / 30 days / 60 days / 120 days]

Feature updates: [60 days / 180 days / 365 days / 540 days]

Suggested Answer:

Answer Area

Quality updates: [14 days / **30 days** / 60 days / 120 days]

Feature updates: [60 days / 180 days / **365 days** / 540 days]

References:

https://docs.microsoft.com/en-us/windows/deployment/update/waas-manage-updates-wufb

kiketxu Highly Voted 3 years, 8 months ago

Both are correct.

https://docs.microsoft.com/en-us/windows/deployment/update/waas-manage-updates-wufb#defer-an-update

upvoted 19 times

NikPat3125 Highly Voted 3 years, 5 months ago

come in exam 27.07.2021

upvoted 8 times

Glorence Most Recent 2 years, 11 months ago

still valid, came in the exam feb 5, 2022

upvoted 5 times

Question #14 *Topic 1*

Your company uses Microsoft Endpoint Configuration Manager and Microsoft Endpoint Manager to co-manage devices.
Which two actions can be performed only from Endpoint Manager? Each correct answer presents a complete solution.
NOTE: Each correct selection is worth one point.

A. Deploy applications to Windows 10 devices.

B. Deploy VPN profiles to iOS devices.

C. Deploy VPN profiles to Windows 10 devices.

D. Publish applications to Android devices.

Suggested Answer: *BD*
References:
https://docs.microsoft.com/en-us/sccm/comanage/overview
https://docs.microsoft.com/en-us/sccm/mdm/deploy-use/create-vpn-profiles

Community vote distribution
BD (100%)

Chris_Rock Highly Voted 3 years, 6 months ago
B and D are correct answers. Because Co managment will be for windows 10 devices. And Android and iOS vpn is only from MEM
upvoted 29 times

RazielLycas Highly Voted 2 years, 6 months ago
damn Microsoft rebranding with similar names :D
upvoted 7 times

FumerLaMoquette Most Recent 2 years, 9 months ago
Damned trick question.
upvoted 2 times

KrokodilBLUEZZ 2 years, 11 months ago
Selected Answer: BD
MECM have no options to manage IOS or Android
upvoted 6 times

morito 2 years, 6 months ago
I believe you mean SCCM has no option to manage IOS or Android?
upvoted 5 times

wwwhogmxnet 1 year, 8 months ago
MECM is the new name for SCCM. MEM is the name for MS Endpoint Manger, which is the new name for Intune.
upvoted 2 times

us3r 3 years ago
once again Microsoft does not make a sense...
upvoted 3 times

amymay101 3 years, 1 month ago
Selected Answer: BD
these management functions are not available in SCCM
upvoted 3 times

70mach1 3 years, 2 months ago
Which two actions can be performed ONLY from Endpoint Manager? This is the question, the first part is misleading and irrelevant. ANS:B and D
upvoted 2 times

Patrick2401 3 years, 4 months ago
I have to go with B/D, WIndows 10 devices are co-management. When it comes to managing iOS and Android the only option is through Intune.
upvoted 4 times

Domza 3 years, 4 months ago

Little hint. Co-management is when you have Config Manager and Intune. In this question there is no "Config Mgr" > windows 10 only
upvoted 1 times

FarhaanKhanPathan 3 years, 5 months ago
Can someone tell me the correct answer
upvoted 1 times

adaniel89 3 years, 6 months ago
Co-management is only available with Windows 10 devices, therefore, answer should be AC
https://docs.microsoft.com/en-us/mem/configmgr/comanage/overview
upvoted 2 times

joyyyyyyyyyyyy 3 years, 6 months ago
then what is the correct ans?
upvoted 1 times

lucidgreen 3 years, 8 months ago
This question is misleading. All can be done from either MECM or MEM, but only Windows 10 devices can be co-managed.
upvoted 3 times

islamelmassry 3 years, 6 months ago
The answer A,C ?
upvoted 1 times

lucidgreen 3 years, 6 months ago
We know that MECM and MEM can manage almost everything under the sun with regards to Windows 10 devices. So what's left?
B,D
upvoted 3 times

AnoniMouse 3 years, 7 months ago
I agree, the question is misleading. You could stick any words and that doesn't change the answer. MECM cannot deploy VPN profiles to Android and iOS
upvoted 6 times

Nunununu 3 years, 8 months ago
I'd say the following link answers this question
https://docs.microsoft.com/en-us/mem/configmgr/core/plan-design/choose-a-device-management-solution#:~:text=Microsoft%20recommends%20using%20Intune%20to,and%20Windows%2010%20mobile%20devices.
upvoted 1 times

Question #15 *Topic 1*

HOTSPOT -

Your network contains an Active Directory domain named contoso.com that uses Microsoft System Center Configuration Manager (Current Branch).

You have Windows 10 and Windows 8.1 devices.

You need to ensure that you can analyze the upgrade readiness of all the Windows 8.1 devices and analyze the update compliance of all the Windows 10 devices.

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

First action to perform:

- Enroll the devices in Microsoft Intune.
- Configure device compliance in Microsoft Intune.
- Create a Microsoft Azure Log Analytics workspace.
- Add an alias (CNAME) record to the DNS zone of contoso.com.

Second action to perform:

- Configure all the devices to have a commercial ID.
- Configure software inventory in Configuration Manager.
- Configure all the devices to join the Windows Insider Program.
- Configure and restart the Windows Update service on all the devices.

Suggested Answer:

Answer Area

First action to perform:

- Enroll the devices in Microsoft Intune.
- Configure device compliance in Microsoft Intune.
- **Create a Microsoft Azure Log Analytics workspace.**
- Add an alias (CNAME) record to the DNS zone of contoso.com.

Second action to perform:

- **Configure all the devices to have a commercial ID.**
- Configure software inventory in Configuration Manager.
- Configure all the devices to join the Windows Insider Program.
- Configure and restart the Windows Update service on all the devices.

References:

https://docs.microsoft.com/en-us/windows/deployment/upgrade/upgrade-readiness-get-started https://docs.microsoft.com/en-us/windows/deployment/update/update-compliance-get-started

kiketxu Highly Voted 3 years, 8 months ago

First:

Create a Microsoft Azure Log Analytics workspace

Second:

Configure all the devices to have a commercial ID

https://www.examtopics.com/discussions/microsoft/view/4795-exam-ms-101-topic-1-question-15-discussion/

upvoted 19 times

makovec25 Highly Voted 3 years, 7 months ago

https://www.petervanderwoude.nl/post/deploy-the-commercial-id-via-windows-10-mdm/

upvoted 5 times

Rhoddy Most Recent 2 years, 4 months ago

"Desktop Analytics is deprecated and will be retired on November 30, 2022."

https://docs.microsoft.com/en-us/mem/configmgr/desktop-analytics/overview

upvoted 4 times

gills 1 year, 5 months ago

Desktop Analytics will be retired on November 30, 2022. Over the next year, the types of insights currently found in Desktop Analytics will be incorporated directly into the Microsoft Intune admin center.

upvoted 1 times

KrokodilBLUEZZ 2 years, 11 months ago

Given answer is correct

upvoted 3 times

JT19760106 3 years ago

I doubt this is still an exam question?

upvoted 4 times

junior6995 2 years, 11 months ago

Very Unlikely, safe to skip that one

upvoted 6 times

Question #16 *Topic 1*

You have a Microsoft Azure Active Directory (Azure AD) tenant named contoso.onmicrosoft.com.
You have a Microsoft 365 subscription.
You need to ensure that administrators can manage the configuration settings for all the Windows 10 devices in your organization.
What should you configure?

A. the Enrollment restrictions

B. the mobile device management (MDM) authority

C. the Exchange on-premises access settings

D. the Windows enrollment settings

Suggested Answer: *B*
References:
https://docs.microsoft.com/en-us/intune/mdm-authority-set

Community vote distribution
B (100%)

Prianishnikov Highly Voted 3 years, 9 months ago
B. the mobile device management (MDM) authority
upvoted 17 times

Storm Highly Voted 3 years ago
Answer B is only relevant for tenants using pre. 1911, but guess question is old and B is correct.

For tenants using the 1911 service release and later, the MDM authority is automatically set to Intune.

For pre-1911 service release tenants, if you haven't yet set the MDM authority, follow the steps below.

https://docs.microsoft.com/en-us/mem/intune/fundamentals/mdm-authority-set#set-mdm-authority-to-intune
upvoted 6 times

venwaik Most Recent 2 years, 8 months ago
Selected Answer: B
Provided answer is correct
upvoted 3 times

KrokodilBLUEZZ 2 years, 11 months ago
Selected Answer: B
B correct
upvoted 4 times

jeff1988 2 years, 11 months ago
Selected Answer: B
B is the correct awnser
upvoted 5 times

Storm 3 years ago
D. Devices - Windows - Windows Enrollment - Automatic Enrollment - MDM User scope -ALL
wonder why you would want to change the authority...
upvoted 1 times

Leontr 3 years, 1 month ago
B is correct answer, administrators can manage all enrolled in MEM W-10 devices in your organization.
upvoted 3 times

keefe 3 years, 7 months ago
B is the correct one
upvoted 3 times

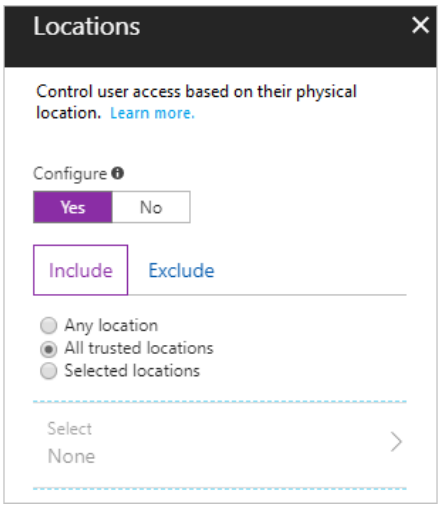
kiketxu 3 years, 8 months ago

B for sure!

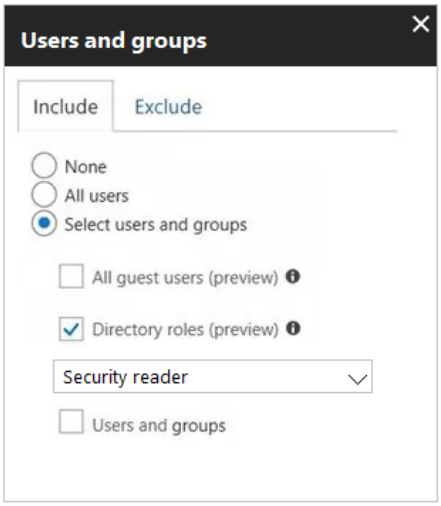
upvoted 4 times

Question #17 *Topic 1*

You configure a conditional access policy. The locations settings are configured as shown in the Locations exhibit. (Click the Locations tab.)



The users and groups settings are configured as shown in the Users and Groups exhibit. (Click Users and Groups tab.)



Members of the Security reader group report that they cannot sign in to Microsoft Active Directory (Azure AD) on their device while they are in the office.

You need to ensure that the members of the Security reader group can sign in in to Azure AD on their device while they are in the office. The solution must use the principle of least privilege.

What should you do?

A. From the conditional access policy, configure the device state.

B. From the Azure Active Directory admin center, create a custom control.

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

D. From the Azure Active Directory admin center, create a named location.

Suggested Answer: *D*

Reference:

https://docs.microsoft.com/en-us/azure/active-directory/conditional-access/location-condition

Community vote distribution

D (100%)

MCSA11 Highly Voted 4 years, 8 months ago

D. From the Azure Active Directory admin center, create a named location.

upvoted 38 times

stromnessian Highly Voted 3 years, 10 months ago

D for sure. One of the most straightforward questions possible. Add a named location IP range (in Azure AD portal -> Security -> Named locations) and mark it as trusted.

upvoted 12 times

KrokodilBLUEZZ Most Recent 2 years, 11 months ago

Selected Answer: D

D is correct.

upvoted 4 times

us3r 3 years ago

Selected Answer: D

D is always the answer ;-)

upvoted 4 times

Prianishnikov 3 years, 9 months ago

D. From the Azure Active Directory admin center, create a named location.

upvoted 9 times

Rstilekar 3 years, 11 months ago

Conditional access policy has to work with Compliance policy. So i think the right answer should be C.

upvoted 2 times

HvD 3 years, 8 months ago

Could you elaborate? CA CAN use compliancy (as a condition), but it's not required.

upvoted 2 times

Yetijo 3 years, 3 months ago

This is incorrect. The answer is D. You need to create a named location.

I can understand where you might think this is correct without experience, but it is not accurate.

upvoted 1 times

mkoprivnj 3 years, 11 months ago

D is correct!

upvoted 3 times

hosseny 4 years ago

D. From the Azure Active Directory admin center, create a named location.

upvoted 2 times

TonySuccess 4 years, 4 months ago

You have the policy, so now you need the named location. D.

upvoted 4 times

RascoPK 4 years, 9 months ago

Notmsure this is right.

Nothing on MS page that would explain this anwser

upvoted 1 times

piceknick 4 years, 9 months ago

Named locations are trusted for CA policies

upvoted 10 times

Storm 3 years ago

When you create a named location, you can choose trusted or not trusted

upvoted 1 times

Question #18 *Topic 1*

You have computers that run Windows 10 Enterprise and are joined to the domain.
You plan to delay the installation of new Windows builds so that the IT department can test application compatibility.
You need to prevent Windows from being updated for the next 30 days.
Which two Group Policy settings should you configure? Each correct answer presents part of the solution.
NOTE: Each correct selection is worth one point.

A. Select when Quality Updates are received

B. Select when Preview Builds and Feature Updates are received

C. Turn off auto-restart for updates during active hours

D. Manage preview builds

E. Automatic updates detection frequency

Suggested Answer: *BD*
References:
https://insider.windows.com/en-us/for-business-organization-admin/

Community vote distribution
AB (50%) BD (50%)

TonySuccess Highly Voted 4 years, 4 months ago
I actually ended up raising this with Microsoft's Devices and Deployment team because it was annoying me not knowing:

After essentially replicating the exam question, the final email I got from Microsoft themselves was:

Yes Tony, these below 2 GPO's needs to be configured in order to delay in the feature update installation.

- Manage Preview Builds
- Select when Preview Builds and Feature Updates are received

Select when Quality Updates are received- You can use this when you want to disable cumulative updates (Would not make sense in this scenario).

I hope this helps everyone!
upvoted 90 times

VTHAR 4 years, 3 months ago
This is troubling and I've to reluctantly agree to it because the question contains "delay + Build". But in the real world scenarios for testing application compatibility and you still won't allow quality updates to go through. Really wish this question is more fine tuned.
upvoted 3 times

VTHAR 4 years, 2 months ago
Forget it! I'll just go with A&B. "Manage Preview Builds" is for those clients opt-in to Windows Insider program and there is no such mentioned here in the question. https://getadmx.com/?Category=Windows_10_2016&Policy=Microsoft.Policies.WindowsUpdate::ManagePreviewBuilds
upvoted 2 times

lucidgreen 3 years, 8 months ago
I think the point is that IT is using these machines for testing of new features. I'm going with B&D.
upvoted 2 times

lucidgreen 3 years, 6 months ago
Never mind. A&B.
There are two types of updates. Feature Updates and Quality updates.

A. Select when Quality Updates are received

This is the setting used to defer monthly updates.

B. Select when Preview Builds and Feature Updates are received
This is the setting used to defer Feature Updates or Preview Builds.

C. Turn off auto-restart for updates during active hours
This just means that the computer won't restart automatically after updating. If a user or another accidental or automated process restarts the computer... Well, you get the idea.

D. Manage preview builds
This setting has everthing to do with allowing users to opt-in to Preview Buids. This should probably be set to Disabled, unless you have computer specifically designated to test these, which most people don't have the time to do, let alone deal with users doing this.

E. Automatic updates detection frequency
This is the number of hour-long intervals the computer will wait to check for updates.
upvoted 9 times

lucidgreen 3 years, 5 months ago
And I'm back to B and D. Preview builds are new builds. Set this to disabled.
B is for Preview and Feature Updates. This also refers to upgrading the build.
A will not upgrade the build, just security updates, cumulative updates and other regular updates.
upvoted 5 times

show Highly Voted 5 years, 3 months ago
Bit of a vague question. But I think Microsoft is asking about preventing/deferring a "new" Windows (build) release.

New build (new feature) come in as a new Preview Build and/or Feature updates.
Quality updates are not introducing "new" Windows features but improving existing features (bug fixes / security patches)

https://www.windowscentral.com/whats-difference-between-quality-updates-and-feature-updates-windows-10

Hence I stick to BD as the correct answer
upvoted 48 times

CharlieBash 3 years, 4 months ago
This is not correct. New feature is the version of Windows, Updates makes new builds. See https://support.microsoft.com/en-us/topic/windows-10-and-windows-server-2019-update-history-725fc2e1-4443-6831-a5ca-51ff5cbcb059 So to stop new builds you would als have to stop the monthly quality updates. So answer A + B
upvoted 2 times

OomensRob Most Recent 1 year, 4 months ago
Selected Answer: BD
All agree on B so let's skip that one.
Why D and not A? The question relates only to new builds. A build in Windows does NOT change when a quality update is installed; that only fixes bugs and deliveres security patches (hence the term "quality" update). Both the insider preview and normal releases can deliver new builds, which is the question.
upvoted 1 times

ThomasMcThomasface 1 year, 5 months ago
Selected Answer: BD
When I read the comment from TonySuccess, I read the question again. B+D are about the builds, as stated in the question. I guess I can see why this answer is given.
upvoted 3 times

jaycenornin 1 year, 8 months ago
"You plan to delay the installation of new Windows **builds**..."
Windows version numbers follow the format:
<major version>.<minor version>.<build number>.<revision>
Only feature updates (and feature preview updates) change the build number. Quality updates change the revision number only and do not affect

"builds".
B & D.
upvoted 2 times

ahmedkmicha 1 year, 9 months ago
the correct answers are A and C:
A-policy setting allows you to defer quality updates for up to 30 days. By selecting this option, you can delay the installation of new Windows builds for up to 30 days, giving your IT department time to test application compatibility.
C- This policy setting prevents Windows from automatically restarting to install updates during active hours. This will prevent any unexpected interruptions during the testing process.
Option B is incorrect as it is related to preview builds and feature updates which are not applicable in this scenario. Option D is also incorrect as it is about managing preview builds which are not needed in this scenario. Option E is not relevant as it is about the frequency of automatic updates detection, and not the delay of updates.
upvoted 2 times

Meebler 1 year, 10 months ago
A,B
Configuring the "Select when Preview Builds and Feature Updates are received" policy is correct to defer the installation of feature updates for up to 30 days, but configuring the "Manage preview builds" policy is not necessary to prevent Windows from being updated for the next 30 days.

The "Manage preview builds" policy is used to control whether preview builds of Windows are received by the device. Preview builds are pre-release versions of Windows that are intended for testing and are not recommended for production use. This policy can be used to defer the installation of preview builds or to disable them altogether.

However, to prevent Windows from being updated for the next 30 days, the correct policies to configure are:

A. Select when Quality Updates are received: This policy defers quality updates, which include security updates and critical bug fixes, for up to 30 days.

B. Select when Preview Builds and Feature Updates are received: This policy defers feature updates, which include major releases of Windows, for up to 30 days.

Therefore, the correct answer is A and B.
upvoted 3 times

DenisRossi 1 year, 11 months ago
Selected Answer: AB
"To pause feature updates, use the Select when Preview Builds and feature updates are Received policy and to pause quality updates use the Select when Quality Updates are Received policy. For more information, see Pause feature updates and Pause quality updates."

https://learn.microsoft.com/en-us/windows/deployment/update/waas-manage-updates-wufb
upvoted 1 times

theaaronmello 1 year, 11 months ago
Selected Answer: BD
Quality updates are security patches, not new builds and do not apply to this question.
upvoted 2 times

bac0n 2 years ago
This one's BD. Check here https://insider.windows.com/en-us/articles/easier-way-manage-insider-preview-builds-organization
upvoted 1 times

manis73 2 years, 5 months ago
why is this M365?
upvoted 1 times

takei 2 years, 7 months ago
This answer is A & B
upvoted 2 times

DARKK 2 years, 8 months ago
Selected Answer: BD
BD As per TonySuccess

upvoted 2 times

JamesM9 2 years, 9 months ago

This question is outdated now - the answers are found in the link below (that was updated on March 16, 2022).

https://docs.microsoft.com/en-us/windows/deployment/update/waas-manage-updates-wufb

"To pause feature updates, use the Select when Preview Builds and feature updates are Received policy and to pause quality updates use the Select when Quality Updates are Received policy".

Therefore, the answers are A & B.

upvoted 7 times

rainbowforest 2 years, 9 months ago

https://docs.microsoft.com/en-us/windows/deployment/update/waas-configure-wufb#pause-quality-updates would go with A and B

upvoted 1 times

rainbowforest 2 years, 9 months ago

I would suggest A+B on this one "To pause feature updates, use the Select when Preview Builds and feature updates are Received policy and to pause quality updates use the Select when Quality Updates are Received policy. For more information, see Pause feature updates and Pause quality updates."

https://docs.microsoft.com/en-us/windows/deployment/update/waas-manage-updates-wufb

upvoted 1 times

LillyLiver 2 years, 10 months ago

Selected Answer: AB

Under the "Pause an Update" heading...

https://docs.microsoft.com/en-us/windows/deployment/update/waas-manage-updates-wufb

upvoted 2 times

Question #19 *Topic 1*

HOTSPOT -

You have three devices enrolled in Microsoft Endpoint Manager as shown in the following table.

Name	Platform	BitLocker Drive Encryption (BitLocker)	Member of
Device1	Windows 10	Disabled	Group1, Group2
Device2	Windows 10	Disabled	Group2, Group3
Device3	Windows 10	Disabled	Group3

The device compliance policies in Endpoint Manager are configured as shown in the following table.

Name	Require BitLocker	Mark noncompliant after (days)	Assigned
Policy1	Require	5	No
Policy2	Require	10	Yes
Policy3	Non configured	15	Yes

The device compliance policies have the assignments shown in the following table.

Name	Assigned to
Policy2	Group2
Policy3	Group3

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 marked as noncompliant after 10 days.	○	○
Device2 is marked as noncompliant after 10 days.	○	○
Device3 is marked as noncompliant after 15 days.	○	○

Suggested Answer:

Answer Area

Statements	Yes	No
Device1 is marked as noncompliant after 10 days.	◯	○
Device2 is marked as noncompliant after 10 days.	◯	○
Device3 is marked as noncompliant after 15 days.	○	◯

ALPHA_DELTA Highly Voted 3 years, 9 months ago

Taken from previous comment:

Device1 is marked as noncompliant after 10 Days: Yes, because Device 1 is member of group 1 and 2, only group 2 is assigned to a policy (policy 2), policy 2 requires Bitlocker, device does not have it so the device will be marked as non compliant after 10 days.

Device2 is marked as noncompliant after 10 Days: Yes, because Device 2 is member of group 2 and 3, only policy 2 requires Bitlocker, therefore Device is marked as non compliant after 10 days.

Device3 is marked as noncompliant after 10 Days: No, because Device 3 is only a member of group 3, group 3 is assigned to Policy 3, policy 3 does not require Bitlocker, so the device will not be marked as non compliant at all, also if it was required it will be after 15 days, not 10 days.

upvoted 47 times

mir000 3 years, 6 months ago

Maybe the question got changed but Device 3 is asked to be noncompliant after 15 days so YES

upvoted 3 times

Nilzuka 2 years, 11 months ago

No it has not been changed. Policy 3 does not require bitlocker.

upvoted 7 times

kiketxu 3 years, 8 months ago

Agreed!

upvoted 3 times

keefe Highly Voted 3 years, 7 months ago
Agreed! YYN
upvoted 11 times

donb21 Most Recent 2 years, 2 months ago
YYN I will go with
upvoted 2 times

Contactfornitish 2 years, 4 months ago
On exam on 13 aug'22
upvoted 5 times

rrrr5r 2 years, 3 months ago
16 Sep 22
upvoted 4 times

L33D 2 years, 6 months ago
Still valid, on exam Jun 25, 2022
upvoted 3 times

takei 2 years, 7 months ago
This answer is yes,yes,no
upvoted 1 times

LillyLiver 2 years, 10 months ago
This one confused me quite a bit. I answered N,N,Y because I didn't know that the days to mark as non-compliant will still ALLOW your device to enroll. Giving you a grace-period to get your device in line with the policy before marking you as non-compliant.

I see in my tenant that it is in fact allowing the enrollment for up to N days.

So, I agree, the answer is Y,Y,N.
upvoted 1 times

us3r 3 years, 2 months ago
Y(es)
Y(es)
N(o)
upvoted 6 times

NightMonkey 3 years, 1 month ago
Answer is Y,Y,Y not Y,Y,N....
upvoted 2 times

Chetithy 2 years, 5 months ago
Policy 3 is not configured, so there is no criteria for it to test and thus mark devices as non-compliant against. (the alternative would be that, given there's no criteria specified, all devices assigned to that policy would be marked non-compliant, which is bogus).
upvoted 3 times

Pleebb 3 years, 4 months ago
Y, Y, Y
upvoted 3 times

Pleebb 3 years, 4 months ago
actually, YYN
upvoted 4 times

otday 3 years, 6 months ago
Looks like the wording of this question has been updated in the last 2 months.
Now the answer should be: Y, Y, Y.
Device3 is marked as non compliant after 15 days.
upvoted 5 times

sdabrai 3 years, 6 months ago
Bitlocker is not-configured in the compliance policy, i.e. it is not a requirement for the device to be compliant. Why would it be marked as non-compliant?

upvoted 14 times

JT19760106 3 years ago

It is possible to configure a compliance policy to not require bitlocker or any other settings and still mark the device as non-compliant.

upvoted 3 times

OneplusOne 2 years, 12 months ago

Just tested and you are correct, creating a compliance policy without any requirements but with 'mark non compliant after 15 days' is possible and can be assigned.

Y Y Y

upvoted 5 times

Chetithy 2 years, 5 months ago

Require bitlocker is not configured for policy 3, so there is no criteria for it to mark devices as noncompliant as.

upvoted 1 times

Question #20 *Topic 1*

You have a Microsoft Azure Active Directory (Azure AD) tenant named contoso.com.
You need to provide a user with the ability to sign up for Microsoft Store for Business for contoso.com. The solution must use the principle of least privilege.
Which role should you assign to the user?

A. Cloud application administrator

B. Application administrator

C. Global administrator

D. Service administrator

Suggested Answer: *C*
References:
https://docs.microsoft.com/en-us/microsoft-store/roles-and-permissions-microsoft-store-for-business

Community vote distribution
C (100%)

[Removed] Highly Voted 5 years, 1 month ago
https://docs.microsoft.com/en-us/microsoft-store/roles-and-permissions-microsoft-store-for-business
upvoted 20 times

MCSA11 Highly Voted 4 years, 8 months ago
C. Global administrator
upvoted 18 times

yawb Most Recent 1 year, 8 months ago
Selected Answer: C
Question is probably no longer valid. MS4B has been retired.
upvoted 3 times

venwaik 2 years, 8 months ago
Selected Answer: C
I think the key word(s) here are " Sign Up". When you read fast, you can misread it as " Sign In" very fast. Only Global Administrators can sign up their tenant to configure and use the Microsoft Store Business.
See:
https://docs.microsoft.com/en-us/microsoft-store/sign-up-microsoft-store-for-business
upvoted 6 times

petersonal 1 year, 10 months ago
That is the point, I like it. Also: "Microsoft Store for Business and Microsoft Store for Education will be retired in the first quarter of 2023." so maybe this will be not seen in exam any more. Reference it the link above.
upvoted 1 times

us3r 3 years ago
Selected Answer: C
Globale admin
upvoted 4 times

NikPat3125 3 years, 5 months ago
come in exam 27.07.2021
upvoted 6 times

AnoniMouse 3 years, 7 months ago
Although I am not going to discuss the question per se, rather than laughing at this sentence: "The solution must use the principle of least privilege", and the least privilege is a GLOBAL ADMINISTRATOR! Ha ha ha ha ha ha ha ha.
upvoted 14 times

joyyyyyyyyyyyy 3 years, 6 months ago

same here..!
hahahaha
upvoted 2 times

keefe 3 years, 7 months ago
that's right.hahahaha
upvoted 2 times

Turak64 3 years, 2 months ago
Typical MS trick question to fill you with doubt. Though it is nuts that only a GA can do this.
upvoted 1 times

kiketxu 3 years, 8 months ago
C for sure!
upvoted 1 times

Prianishnikov 3 years, 9 months ago
C. Global administrator
upvoted 2 times

gijsw 3 years, 11 months ago
C is correct, only a Global Admin can perform the first sign up for MSfb
upvoted 2 times

Question #21 *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 are deploying Microsoft Endpoint Manager.
You successfully enroll Windows 10 devices in Endpoint Manager.
When you try to enroll an iOS device in Endpoint Manager, you get an error.
You need to ensure that you can enroll the iOS device in Endpoint Manager.
Solution: You create the Mobility (MDM and MAM) settings.
Does this meet the goal?

A. Yes

B. No

Suggested Answer: *B*

Patrick2401 Highly Voted 3 years, 4 months ago
No, you need a Apple Push Cert. to manages iOS devices in Endpoint
upvoted 11 times

Contactfornitish Most Recent 2 years, 4 months ago
On exam on 13 aug'22
upvoted 3 times

ercluff 2 years, 9 months ago
B. NO. Similar questions are listed in Topic 1 questions 1,2,3,35,& 57. Mirroring Chris_rock's reply to question 1: "An Apple MDM Push certificate is required for Intune to manage iOS/iPadOS and macOS devices. After you add the certificate to Intune, your users can enroll their devices. So correct answer is B) (See comments by riahisami77:) “Apple MDM Push Certificate is a prerequisite. To Enroll Apple Devices then show the 5 steps to upload the Push Certificate: (1) Accept the licence agreement
(2) Download Intune CSR
(3) Create your MDM Push Cert
(4) Enter the Apple ID
(5) upload the push Cert”
upvoted 3 times

Question #22 *Topic 1*

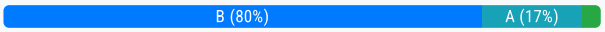
Note: This question is part of a series of questions that present the same scenario. Each question in the series contains a unique solution that might meet the stated goals. Some question sets might have more than one correct solution, while others might not have a correct solution.
After you answer 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.
Your network contains an Active Directory domain named contoso.com that is synced to Microsoft Azure Active Directory (Azure AD).
You manage Windows 10 devices by using Microsoft System Center Configuration Manager (Current Branch).
You configure pilot co-management.
You add a new device named Device1 to the domain. You install the Configuration Manager client on Device1.
You need to ensure that you can manage Device1 by using Microsoft Intune and Configuration Manager.
Solution: You add Device1 to a Configuration Manager device collection.
Does this meet the goal?

A. Yes

B. No

Suggested Answer: *A*
Reference:
https://docs.microsoft.com/en-us/mem/configmgr/comanage/tutorial-co-manage-clients

Community vote distribution



d3an Highly Voted 4 years, 11 months ago
This should be yes - to Pilot Co-Management, you must provide a Pilot Device Collection, so it can be assumed that by adding the device to a Collection, you are granting it the ability to participate in the Pilot.
upvoted 38 times

Lopsios 3 years, 8 months ago
Specify the pilot collection for each of the workloads that are set to Pilot Intune
upvoted 1 times

lucidgreen 3 years, 8 months ago
Agreed. A pilot group is nothing more than a device collection used for co-management purposes. It's not necessary, if you know what you're doing or if you have already enabled this on another collection. Either way, you need to add it to a collection where co-management is enabled.
upvoted 4 times

Mr01z0 4 years, 2 months ago
There is no proof in the provided text that you add device1 to the correct collection. So the answer should be No.
upvoted 8 times

lucidgreen 3 years, 6 months ago
This is true. Simply assigning a device to a collection doesn't guarantee that collection is configured for co-management. Although, a pilot group is simply a collection.
upvoted 9 times

lucidgreen 3 years, 5 months ago
I just read a little word in there that might make a difference. They called it Pilot Co-Management. Not sure this is a typo but if they are inferring this is a Pilot scenario, this has to be a Pilot Group (which is pretty much a preconfigured collection for piloting co-management). Say Pilot 5 times and you might get the idea.
Pilot!
upvoted 4 times

Jakub2023 1 year, 7 months ago
Well, there's no proof that it's the wrong device collection either. So on what grounds do you answer No? ;-)

I would go for Yes on the basis of the information provided.

upvoted 3 times

blaatlama 4 years, 10 months ago

Still no because the solution doesn't mention to which device collection you add Device1, so basically this could mean any collection ;-)

upvoted 22 times

Lynxy Highly Voted 4 years, 6 months ago

Pilot collection or pilot group is usually co-management on a subset of clients to initially test co-management, and rollout co-management using a phased approach.

The question is ambiguous as to what the goal is. If it is for testing /phased approach, than it is YES.

upvoted 9 times

diego17 Most Recent 1 year, 5 months ago

Se você adicionar a qualquer coleção vai funcionar? Não, então como ele não especifica coleção piloto a resposta é B.

upvoted 1 times

djharris27 1 year, 5 months ago

Selected Answer: B

"A collection" doesn't mean specifically the Intune pilot device collection, it could be added to any old collection you made in MECM therefore the answer is "No"

upvoted 2 times

jadye527 1 year, 7 months ago

Selected Answer: B

Doesn't specify that device is added to configured pilot intune device collection. Question needs to be refined.

upvoted 2 times

hufflepuff 1 year, 10 months ago

Selected Answer: B

See Question 34 for the correct answer.

Given that one is correct, makes me free this answer must be No.

upvoted 3 times

ServerBrain 2 years, 1 month ago

Correct answer is B,

See the same question and answer in Question 34 here, which says "Define a Configuration Manager device collection as the pilot collection. Add Device1 to the collection."

Unless we are assuming the Device Collection here is the Pilot Device Collection, then the Answer is A.

upvoted 1 times

donb21 2 years, 2 months ago

I would say no as it does not indicate configuration manger group was one of the auto pilot collection

upvoted 1 times

RazielLycas 2 years, 5 months ago

Selected Answer: B

Later there is the same question and answer but is specified that it the pilot device collection so here it's "NO"

upvoted 5 times

RazielLycas 2 years, 6 months ago

Selected Answer: B

Question #34 of this list reports the same scenario with answer "Solution: Define a Configuration Manager device collection as the pilot collection. Add Device1 to the collection" so this one is no

upvoted 6 times

morito 2 years, 6 months ago

Selected Answer: B

This question is a bit confusing. The action is correct, but only if the mentioned collection has been configured as the pilot collection in SCCM, given the fact that we should take these questions as literal as possible, I'd answer B.

upvoted 1 times

cdatexwintel 2 years, 8 months ago

Pilot collection or pilot group is usually co-management on a subset of clients to initially test co-management, and rollout co-management using a phased approach.

The question is ambiguous as to what the goal is. If it is for testing /phased approach, than it is YES.

upvoted 1 times

cdatexwintel 2 years, 8 months ago

Selected Answer: A

Yes, Co-Management

upvoted 2 times

Notorious19 2 years, 9 months ago

Selected Answer: A

a correct

upvoted 1 times

KrokodilBLUEZZ 2 years, 10 months ago

Selected Answer: A

Pilot device collection is one of the prereqs to configure co-management. You can see it in config wizard when setting up co-management

upvoted 3 times

VirtualJP 3 years ago

Selected Answer: B

I'm going to say No to this question, due to there being the question that actually mentions the solution as "Define a Configuration Manager device collection as the pilot collection. Add Device1 to the collection." - Question #34

upvoted 6 times

[Removed] 3 years ago

Good point, im going with you

upvoted 1 times

Buzupower 3 years ago

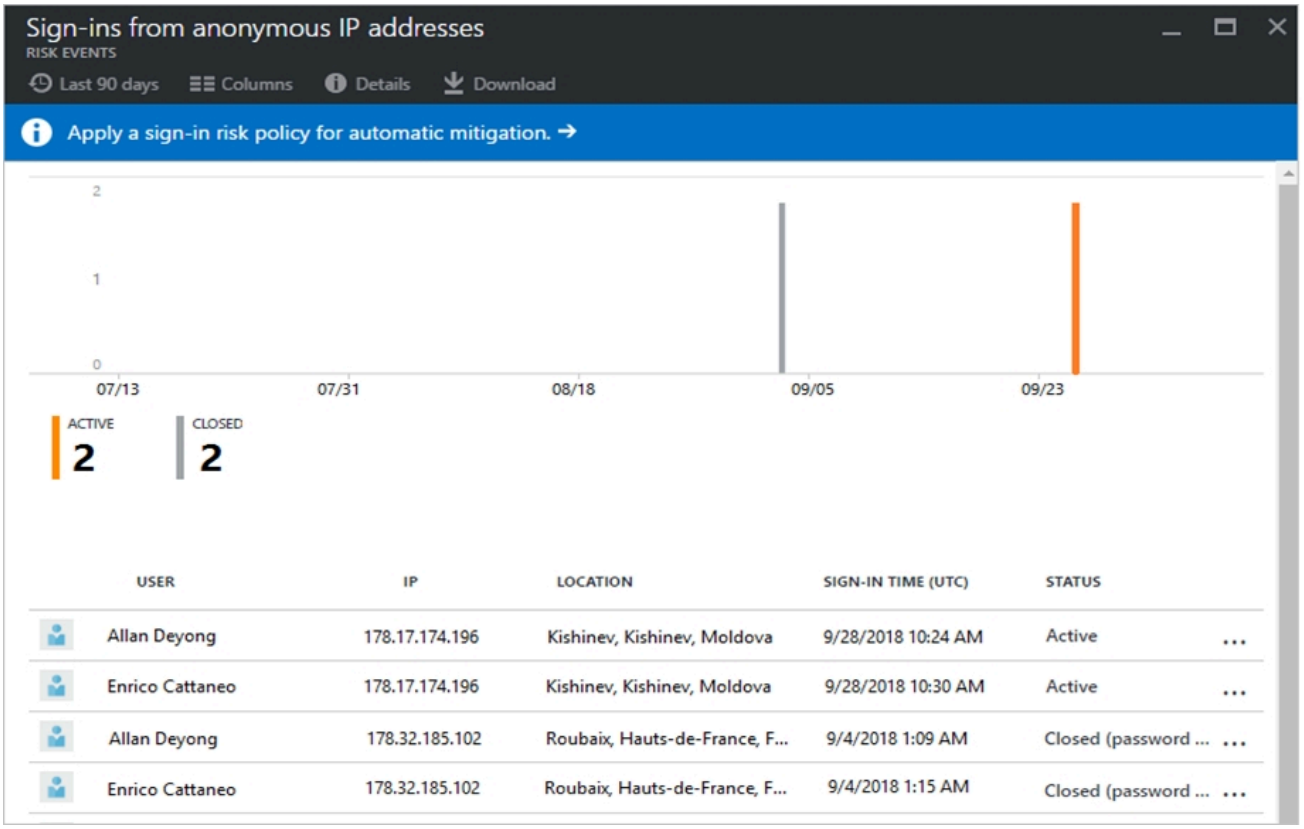
Selected Answer: B

Device collection needs to be defined as a pilot device collection for co-management. Hence answer should be NO.

upvoted 3 times

Question #23 *Topic 1*

From the Microsoft Azure Active Directory (Azure AD) Identity Protection dashboard, you view the risk events shown in the exhibit. (Click the Exhibit tab.)



You need to reduce the likelihood that the sign-ins are identified as risky.

What should you do?

A. From the Security & Compliance admin center, create a classification label.

B. From the Security & Compliance admin center, add the users to the Security Readers role group.

C. From the Azure Active Directory admin center, configure the trusted IPs for multi-factor authentication.

D. From the Conditional access blade in the Azure Active Directory admin center, create named locations.

Suggested Answer: *D*

References:

https://docs.microsoft.com/en-us/azure/active-directory/conditional-access/location-condition

Community vote distribution

D (100%)

Alvaroll Highly Voted 4 years, 2 months ago

Same as MS-100 Topic1-34 https://www.examtopics.com/exams/microsoft/ms-100/view/7/

upvoted 13 times

kiketxu Highly Voted 3 years, 8 months ago

D for sure!

upvoted 9 times

Mendel Most Recent 2 years, 8 months ago

Selected Answer: D

D is correct

upvoted 4 times

Prianishnikov 3 years, 9 months ago

D. From the Conditional access blade in the Azure Active Directory admin center, create named locations.

upvoted 5 times

Takloy 3 years, 10 months ago

Answer D

upvoted 7 times

Question #24 *Topic 1*

Your company has a Microsoft 365 E5 subscription.
Users in the research department work with sensitive data.
You need to prevent the research department users from accessing potentially unsafe websites by using hyperlinks embedded in email messages and documents. Users in other departments must not be restricted.
What should you do?

A. Create a data loss prevention (DLP) policy that has a Content is shared condition.

B. Modify the safe links policy Global settings.

C. Create a data loss prevention (DLP) policy that has a Content contains condition.

D. Create a new safe links policy.

Suggested Answer: *D*
References:
https://docs.microsoft.com/en-us/office365/securitycompliance/set-up-atp-safe-links-policies#policies-that-apply-to-specific-email-recipients

Community vote distribution
D (100%)

in_cloud 1 year, 5 months ago
On exam july/2023
upvoted 1 times

Crixsus 2 years, 2 months ago
On exam today 10/23/22. D is correct.
upvoted 4 times

ajiejeng 2 years, 3 months ago
Selected Answer: D
D is correct
upvoted 4 times

ARYMBS 2 years, 3 months ago
Selected Answer: D
If I remember correctly you cannot specify group of Users in Default policy.
So if you want to include/exclude any group of members from default (Global) policy - you must create a new one.
upvoted 3 times

Question #25 *Topic 1*

You have a Microsoft 365 tenant.
You have a line-of-business application named App1 that users access by using the My Apps portal.
After some recent security breaches, you implement a conditional access policy for App1 that uses Conditional Access App Control.
You need to be alerted by email if impossible travel is detected for a user of App1. The solution must ensure that alerts are generated for App1 only.
What should you do?

A. From Microsoft Cloud App Security, create a Cloud Discovery anomaly detection policy.

B. From Microsoft Defender for Cloud Apps, modify the impossible travel alert policy.

C. From Microsoft Defender for Cloud Apps, create an app discovery policy.

D. From the Azure Active Directory admin center, modify the conditional access policy.

Suggested Answer: *A*
References:
https://docs.microsoft.com/en-us/cloud-app-security/cloud-discovery-anomaly-detection-policy

Community vote distribution
B (54%) A (46%)

XW_64 Highly Voted 2 years, 2 months ago
Selected Answer: B
The policy exist, it just needs to be modified and It's now called Microsoft Defender for Cloud Apps

https://www.rebeladmin.com/2018/09/step-step-guide-manage-impossible-travel-activity-alert-using-azure-cloud-app-security/
upvoted 5 times

andrigof 2 years, 1 month ago
But, if it is Microsoft Defender for Cloud Apps, how B is not the answer?
upvoted 1 times

microsoftexamshredder Most Recent 1 year, 6 months ago
The answer is A. You need to create a new policy specifically for the app.
B mentions MODIFYING a policy which means impossible travel already applies to other apps
upvoted 2 times

Debadatta 1 year, 6 months ago
B is the correct answer
The impossible travel detection identifies unusual and impossible user activity between two locations. The activity should be unusual enough to be considered an indicator of compromise and worthy of an alert.
https://learn.microsoft.com/en-us/defender-cloud-apps/anomaly-detection-policy
upvoted 1 times

Webleyboy 1 year, 7 months ago
Selected Answer: A
I`m going for A, as this question is the same as in MS-100 including the same error.
Microsoft hates to change built-in policies. Always go for a new policy.
upvoted 2 times

boxojunk 1 year, 8 months ago
Selected Answer: B
https://docs.microsoft.com/en-us/defender-cloud-apps/anomaly-detection-policy
upvoted 3 times

Feyenoord 1 year, 8 months ago
Selected Answer: A
I'm going for A, although there is an existing Impossible traffic policy which you can edit, you cannot filter on a specific App there. Only way to do that is to create a new anomaly detection policy with a filter.

upvoted 2 times

aaa535 1 year, 8 months ago

https://learn.microsoft.com/en-us/defender-cloud-apps/anomaly-detection-policy

Impossible travel

upvoted 1 times

JackeD 1 year, 8 months ago

Selected Answer: B

b esta bien

upvoted 2 times

Pepeti 1 year, 8 months ago

o Microsoft Defender for Cloud Apps, modifique a política de alerta de viagem impossível.

Para atender aos requisitos, é necessário configurar a política de alerta de viagem impossível no Microsoft Defender for Cloud Apps. Isso garantirá que o alerta seja gerado apenas para o aplicativo App1. O Controle de Aplicativo de Acesso Condicional deve ser configurado para fornecer informações ao Microsoft Defender for Cloud Apps, que por sua vez gera alertas de acordo com a política definida.

upvoted 1 times

ahmedkmicha 1 year, 9 months ago

To be alerted by email if impossible travel is detected for a user of App1, you should modify the impossible travel alert policy in Microsoft Defender for Cloud Apps.

A is incorrect because creating a Cloud Discovery anomaly detection policy in Microsoft Cloud App Security will not help to generate alerts for impossible travel. Cloud Discovery anomaly detection policy is used to detect anomalous activity in cloud apps.

upvoted 1 times

Fala_Fel 1 year, 11 months ago

Selected Answer: B

B would work, you can modify the existing impossible travel alert policy in Defender for Cloud apps, to send an email alert and only alert for app1. That will achieve the question objective. So I'm answering B

A is wrong for 2 reasons. Email alerts are set up in Defender for Cloud Apps NOT 'Cloud App Security and 'impossible travel' is an 'anomaly detection policy' NOT a 'Cloud Discovery anomaly detection policy' So answer is B

I wouldn't actually do that though as it's editing the in built impossible travel policy and now the only alerts are for app1. But that's what the question wants you to do I suppose. I would set up a new impossible travel policy to just apply to app1 and set up email alert for that, but cannot currently see how that is done.

upvoted 3 times

RenegadeOrange 2 years, 3 months ago

Agree, the policy is an available option, it includes impossible travel and can be filtered to an app.

upvoted 3 times

MaptaN 2 years, 3 months ago

Selected Answer: A

Should be A. Even when renaming, the text of the documentation says that impossible travel is an anomaly *detection* policy, not *alert policy*

upvoted 4 times

MaptaN 2 years, 3 months ago

Updated Doc: https://docs.microsoft.com/en-us/defender-cloud-apps/anomaly-detection-policy

upvoted 1 times

andrigof 2 years, 1 month ago

And the A says to enable an Anomaly Detection policy, not an alert policy. So how is this corrent and not B?

upvoted 1 times

owenMS 1 year, 11 months ago

B says to modify the impossible travel policy, the question is about just app1 so we would create its own policy.

upvoted 2 times

ARYMBS 2 years, 3 months ago

Selected Answer: A

I agree with A...
But It's now called Microsoft Defender for Cloud Apps (?).
upvoted 3 times

Question #26 *Topic 1*

A user receives the following message when attempting to sign in to https://myapps.microsoft.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.`
Which configuration prevents the users from signing in?

A. Microsoft Azure Active Directory (Azure AD) Identity Protection policies

B. Microsoft Azure Active Directory (Azure AD) conditional access policies

C. Endpoint Manager compliance policies

D. Security & Compliance data loss prevention (DLP) policies

Suggested Answer: *B*
References:
https://docs.microsoft.com/en-us/azure/active-directory/conditional-access/overview https://docs.microsoft.com/en-us/mem/intune/protect/device-compliance-get-started

Community vote distribution
A (100%)

BGM_YKA Highly Voted 3 years, 7 months ago
A. as the texts match the user message for Risky Sign-in

https://docs.microsoft.com/en-us/azure/active-directory/identity-protection/concept-identity-protection-user-experience
upvoted 45 times

DAL114 2 years, 6 months ago
You are correct
upvoted 3 times

jjong 3 years, 4 months ago
the message listed in the link is 'This Sign-in was blocked'. Note 'This'. The question is 'Your Sign-in'. Note 'Your', and not 'This'. I believe that'll be a differentiation between the 2x kinds of errors.
upvoted 3 times

mic88 3 years, 4 months ago
I think you are right and A is the right answer. In case of a conditional access policy would apply, the message would be something like "your sign-in was successful but does not meet the criteria to access this resource..."
upvoted 8 times

Edward2086 Most Recent 1 year, 10 months ago
yes its A https://learn.microsoft.com/en-us/answers/questions/772956/we-have-detected-something-unusual-about-this-sign
upvoted 1 times

petersonal 1 year, 10 months ago
Selected Answer: A
We've detected something unusual about this sign-in. --> This is the key. Conditional access does not telling you this. Conditional access works as you requested. However, Identity protection listens for signs. In this case something changed, new location, device, app etc. (also in the question) triggering more caution and require another verifications.
upvoted 2 times

Learner2022 1 year, 11 months ago
This is a terrible question as both A and B are correct. Risky Sign in can be configured from both policies. https://learn.microsoft.com/en-us/azure/active-directory/conditional-access/howto-conditional-access-policy-risk
upvoted 1 times

ServerBrain 2 years, 1 month ago
Selected Answer: A
A - this is substantiated by link provided by BGM-YKA
upvoted 1 times

DCT 2 years, 1 month ago

A Ia, sohai

upvoted 1 times

simoen 2 years, 3 months ago

Selected Answer: A

https://docs.microsoft.com/en-us/azure/active-directory/identity-protection/concept-identity-protection-user-experience

upvoted 3 times

sliix 2 years, 3 months ago

Selected Answer: A

See BGM_YKA

upvoted 2 times

gmKK 2 years, 3 months ago

https://docs.microsoft.com/en-us/azure/active-directory/conditional-access/overview

Common signals that Conditional Access can take in to account when making a policy decision include the following signals:

...

Real-time and calculated risk detection

Signals integration with Azure AD Identity Protection allows Conditional Access policies to identify risky sign-in behavior. Policies can then force users to change their password, do multi-factor authentication to reduce their risk level, or block access until an administrator takes manual action.

upvoted 2 times

soydlm 2 years, 5 months ago

(A) all the way. Admins please for fix this. Thank you

upvoted 2 times

DAL114 2 years, 6 months ago

Selected Answer: A

https://docs.microsoft.com/en-us/azure/active-directory/identity-protection/concept-identity-protection-user-experience#risky-sign-in-remediation

upvoted 2 times

morito 2 years, 6 months ago

Selected Answer: A

This is A for sure. Azure Identity Protection detects a risky sign-in.

upvoted 3 times

MichaelMu 2 years, 8 months ago

Selected Answer: A

sign in risk policy

upvoted 4 times

dumpmaster 2 years, 8 months ago

Selected Answer: A

https://techcommunity.microsoft.com/t5/itops-talk-blog/what-s-the-difference-between-azure-active-directory-identity/ba-p/1320887

upvoted 2 times

KSvh53 2 years, 9 months ago

Selected Answer: A

Answer is A. Look at the screenshot here for identity protection. It has the exact wording. This is not conditional access.

https://docs.microsoft.com/en-us/azure/active-directory/identity-protection/concept-identity-protection-user-experience#risky-sign-in-self-remediation

upvoted 4 times

Panku 2 years, 11 months ago

Tasted the right answer is B

upvoted 1 times

John 2 years, 11 months ago

Selected Answer: A

https://evertoncollins.com/azure-identity-protection-enterprise-mobility-security/

upvoted 2 times

HOTSPOT -

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

Name	Member of
User1	Group1
User2	Group2

Your company uses Microsoft Intune.

Several devices are enrolled in Intune as shown in the following table.

Name	Platform	BitLocker Drive Encryption (BitLocker)	Member of
Device1	Windows 10	Disabled	Group3
Device2	Windows 10	Disabled	Group4

The device compliance policies in Intune are configured as shown in the following table.

Name	Require BitLocker	Assigned to
Policy1	Not configured	Group3
Policy2	Require	Group4

You create a conditional access policy that has the following settings:

➩ The Assignments settings are configured as follows:

1. Users and groups: Group1
2. Cloud apps: Microsoft Office 365 Exchange Online
3. Conditions: Include All device state, exclude Device marked as compliant

➩ Access controls is set to Block access.

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 access Microsoft Exchange Online from Device1.	○	○
User1 can access Microsoft Exchange Online from Device2.	○	○
User2 can access Microsoft Exchange Online from Device2.	○	○

Suggested Answer:

Answer Area

Statements	Yes	No
User1 can access Microsoft Exchange Online from Device1.	○	○
User1 can access Microsoft Exchange Online from Device2.	○	○
User2 can access Microsoft Exchange Online from Device2.	○	○

Box 1: Yes.

User1 is in Group1. The Conditional Access Policy applies to Group1. The Conditional Access Policy blocks access unless the device is marked as compliant.

BitLocker is disabled for Device1. Device1 is in Group3 which is assigned device Policy1. The BitLocker policy in Policy1 is not configured so BitLocker is not required.

Therefore, Device1 is compliant so User1 can access Exchange online from Device1.

Box 2: No.

User1 is in Group1. The Conditional Access Policy applies to Group1. The Conditional Access Policy blocks access unless the device is marked as compliant.

BitLocker is disabled for Device2. Device2 is in Group4 which is assigned device Policy2. The BitLocker policy in Policy2 is Required so BitLocker is required.

Therefore, Device2 is not compliant so User1 cannot access Exchange online from Device2.

Box3: Yes.

User2 is in Group2. The Conditional Access Policy applies to Group1. The Conditional Access Policy does not apply to Group2. So even though Device2 is non- compliant, User2 can access Exchange Online using Device2 because there is no Conditional Access Policy preventing him/her from doing so.
Reference:
https://docs.microsoft.com/en-us/azure/active-directory/conditional-access/conditions

Goena Highly Voted 3 years, 9 months ago
Yes: user 1 is member of group 1
No: user 1 is member of group 1 but device 2 is not compliant
Yes: user 2 is not member of group 1
upvoted 39 times

Prianishnikov Highly Voted 3 years, 9 months ago
YES-NO-YES
upvoted 15 times

OomensRob Most Recent 1 year, 4 months ago
just to clarify:

Conditional Access policies are triggered by a condition which enforces a rule (access granted/not granted/MFA required etc.)

Compliance Policies apply a state to a device (Compliant/Non-Compliant). Like a sticker on the device. It doesn't DO anything to the device other than applying the sticker (I appreciate that this is not 100% accurate but in the given context of the question it is).

You can apply Conditional Access Policies BECAUSE a device has the sticker, but it's not mandatory. You can have non-compliant devices without any problems signing in to anything. User 2 may be non-compliant, but there is no policy preventing anything for user 2. Y-N-Y
upvoted 1 times

Kevinfm_81 2 years, 6 months ago
My thought is Y,N,N. Wouldn't User 2 default to the Intune Device Policy?
upvoted 4 times

J_IOIT 2 years, 7 months ago
'Device state' has been depreciated, replaced with filter for devices now. https://docs.microsoft.com/en-us/azure/active-directory/conditional-access/concept-conditional-access-conditions#device-state-deprecated
upvoted 1 times

venwaik 2 years, 8 months ago
Y,N,N.
box3: User2 does not have the conditional access policy affecting him, but he does have the compliance policy (policy 2) affecting him.
This policy states that device2 is required to have bitlocker enabled. This device hasn't and User2 cannot access MS Exchange Online because of that.
Third answer should be NO.
upvoted 2 times

venwaik 2 years, 8 months ago
Keep in mind that you can mark devices with no compliance policy assigned. If the question would've state that, the answer on box3 was YES. The question doesn't and policy4 is affecting device2 on bitlocker level, so the answer on box3 is NO.
upvoted 2 times

Chipper 3 years, 1 month ago
Why is user 1 yes? The access control is specified to block access. Am I missing something?
upvoted 1 times

Chipper 3 years, 1 month ago
Nevermind, I see why now....
upvoted 4 times

[Removed] 3 years, 1 month ago
If "➪ Access controls is set to Block access.", doesn't this mean that All Users in Group 1 cannot access Exchange Online in the first place? So NNN should be the answer?
upvoted 3 times

chewitt 1 year, 10 months ago

So User 1 will be able to access exchange online IF the device is compliant.

Groups 3 & 4 are groups for what makes the device compliant.

upvoted 1 times

us3r 3 years, 2 months ago

Y.
N.
Y.

upvoted 2 times

scottims 3 years, 7 months ago

Yes-No-No
while the policy is assigned to user Group 1, device 2 is not compliant as Policy 4 requires BL to be enabled.

upvoted 1 times

bellorg 3 years, 7 months ago

CA policy works in the name of user, so if user is not in group CA policy don't apply.

upvoted 2 times

LillyLiver 2 years, 10 months ago

True, but the compliance police is requiring BitLocker, which is disabled on device2. So Device2 is marked as non-compliant and not allowed.

Answer is Y,N,N.

upvoted 2 times

dyers 2 years, 2 months ago

Just because the device is non-compliant, it still will not match the CA, so those rules don't even apply. CA kind of builds from the top down, who matches the policy? Group 1 (User 1), then you apply conditionals, all device states except compliant. But you see how user 3 instantly fails to match the user or group category so no CA is applied and with no CA a licensed user can log in to exchange. So YNY

upvoted 3 times

keefe 3 years, 7 months ago

same, YNN, because Policy2 is required and assigned to G4 where Dev2 is member of

upvoted 1 times

AnoniMouse 3 years, 7 months ago

I think the answer should be YES, NO, YES, here is why:

User1 is a member of Group1 (where the policy is assigned). Device1 belongs to Group3 which has Policy1 that doesn't enforce BL so if BL is disabled it doesn't matter thus this device according to Policy1 is compliant.

User1 is a member of Group1 (where the policy is assigned), but Device2 is a member of Group4 which has a policy that requires BL to be ON but it is off, so it is NOT compliant. So even if the user is compliant, the device is NOT, hence User1 from Device2 cannot access

User2 is a member of Group2 and there is no conditional access for this group, so there is nothing to evaluate, hence Users2 should be able to access the application from both devices actually

upvoted 9 times

ALPHA_DELTA 3 years, 9 months ago

User1 can access Microsoft Exchange Online from Device1: Yes, because Device 1 is member of group 3. Policy 1 is assigned to group 3, policy 1 does not require Bitlocker encryption thus Device is 1 compliant. The conditional access policy conditions exclude Devices marked as compliant, thus access is allowed.

User1 can access Microsoft Exchange Online from Device2: No, because Device 2 is a member of Group 4. Policy 2 is assigned to group 4, policy 2 requires Bitlocker encryption, Device 2 does not have bitlocker encryption thus is Device 2 marked as non compliant. Conditional access policy Access controls is set to Block access, so Device 2 is not allowed.

User2 can access Microsoft Exchange Online from Device2: No, because Device 2 is non compliant (see answer above why) and also User 2 is not in group 1 and thereby is also not allowed access.

upvoted 5 times

Prianishnikov 3 years, 9 months ago

No, YES-NO-YES

upvoted 3 times

PersonT 3 years, 9 months ago

last one: depends how the tenant has configured " Mark devices with no compliance policy assigned". According to below devices with no compliance policy assigned are marked as Compliant (default). Checked in my lab and its true, so Yes..
https://docs.microsoft.com/en-us/mem/intune/protect/device-compliance-get-started

upvoted 1 times

PersonT 3 years, 9 months ago

misread. its no.

upvoted 1 times

ALPHA_DELTA 3 years, 8 months ago

I was wrong, its Y-N-Y

upvoted 3 times

PP39 3 years, 9 months ago

the answer is incorrect, should Yes NO Yes

upvoted 2 times

bkrich 3 years, 9 months ago

I also think its YES-NO-YES

User1 / Device1 = Yes, because the conditional access policy is scoped for Group1 and User1 is a member. Using Device1 which is apart of Group3, Group3 bitlocker is Not Configured so it should be compliant and pass the Conditional Access

User1 / Device2 = No, because Device2 is apart of Group4 which requires bitlocker so it wouldn't be compliant even though User1 is apart of Group1

User2 / Device1 = Yes, because User2 is not scoped in the Conditional Access Policy being that it is apart of Group2, so I would think the conditional address wouldn't apply to users in Group2 and it will be able to access EXO regardless of the conditional access policy

upvoted 4 times

kiketxu 3 years, 8 months ago

Agreed. YES/NO/YES.

upvoted 2 times

AnoniMouse 3 years, 7 months ago

I think you are confusing here. The third answer should be NO. You wrote "User2 / Device1" but the question states "User2 / Device2" not device 1

upvoted 1 times

prabhjot 1 year, 8 months ago

It is User 2 / Device 2 (not device 1)

upvoted 1 times

Question #28 *Topic 1*

HOTSPOT -

You have several devices enrolled in Microsoft Endpoint Manager.

You have a Microsoft Azure Active Directory (Azure AD) tenant that includes the users shown in the following table.

Name	Role	Member of
User1	Cloud device administrator	GroupA
User2	Intune administrator	GroupB
User3	**None**	**None**

The device limit restrictions in Endpoint Manager are configured as shown in the following table.

Priority	Name	Device limit	Assigned to
1	Policy1	15	GroupB
2	Policy2	10	GroupA
Default	All users	5	All Users

You add User3 as a device enrollment manager in Endpoint Manager.

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

NOTE: Each correct selection is worth one point.

Hot Area:

Answer Area

Statements	Yes	No
User1 can enroll a maximum of 10 devices in Endpoint Manager.	○	○
User2 can enroll a maximum of 10 devices in Endpoint Manager.	○	○
User3 can enroll an unlimited number of devices in Endpoint Manager.	○	○

Suggested Answer:

Answer Area

Statements	Yes	No
User1 can enroll a maximum of 10 devices in Endpoint Manager.	○	○
User2 can enroll a maximum of 10 devices in Endpoint Manager.	○	○
User3 can enroll an unlimited number of devices in Endpoint Manager.	○	○

Reference:

https://docs.microsoft.com/en-us/intune/device-enrollment-manager-enroll

Ronger Highly Voted 3 years ago

DEM is an Intune permission that can be applied to an Azure AD user account and lets the user enroll up to 1,000 devices. (not unlimited)

https://docs.microsoft.com/en-us/mem/intune/enrollment/device-enrollment-manager-enroll

Y-N-N is correct

upvoted 21 times

JT19760106 Highly Voted 2 years, 11 months ago

Yes - User 1 is a Cloud Device Admin, and this role has no bearing on device enrollment. User 1 is a member of GroupA, which has a device limit of 10. So YES, user 1 can enroll a maximum of 10 devices in Endpoint Manager.

No - User 2 is a member of GroupB who can enroll up to 15 devices, so they can enroll more than 10 devices.

No - User 3 is a device enrollment manager and may enroll up to 1000 devices, so not unlimited.

upvoted 18 times

m43s 2 years, 4 months ago

Thank you man!

upvoted 1 times

RenegadeOrange 2 years, 3 months ago

Y

N - Assume as an Intune Administrator has no limitation as well...

N

upvoted 3 times

Fala_Fel 1 year, 11 months ago

Agree with JT197..

Yes: you only need an intune license to enroll up to 15 devices. This user is limited by policy to 10

No: User 2 is member of Group 2 which is limited to 15 (not 10)

No: DEM not limitless

upvoted 1 times

potterknot Most Recent 2 years, 5 months ago

it is still valid 08/07/2022

upvoted 1 times

rrrr5r 2 years, 3 months ago

16 Sep 22

upvoted 5 times

VirtualJP 3 years ago

I think the key thing to bear in mind with this question is that it's assessing knowledge on device limits as opposed to user enrolment scopes...

upvoted 2 times

edzio 3 years ago

You are right

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

Create devices (enroll in Azure AD)

https://docs.microsoft.com/en-us/azure/active-directory/roles/permissions-reference#cloud-device-administrator

upvoted 1 times

Goena 3 years ago

No: Cloud device administrator cannot enroll devices.

Yes: Intune administrator can enroll. Max 10 devices because member of group B

No: DEM can enroll up to 1000 devices, but not unlimited

upvoted 8 times

allesglar 3 years ago

I agree on that, Cloud Device Admin does not have the right to enroll.

upvoted 2 times

allesglar 3 years ago

Answer is N,N,N

The Intune Admin because of the policy assigned to group B cannot enroll up to 15 devices.

upvoted 5 times

Fala_Fel 1 year, 11 months ago

But Group B device limit IS 15 so answer Yes

upvoted 1 times

edzio 3 years ago

You are right

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

Create devices (enroll in Azure AD)

https://docs.microsoft.com/en-us/azure/active-directory/roles/permissions-reference#cloud-device-administrator

upvoted 1 times

PDR 3 years ago

but you do not need a specific role to enroll into intune, if the user has an intune licence they can enroll a device if there is not a restriction in place that prevents them from doing so

upvoted 3 times

JT19760106 3 years ago

Let's think about this for a minute. If this is true, then nobody other than a Device Enrollment Manager could register a device. Simply isn't the case, the answer, as it stands, is correct. https://docs.microsoft.com/en-us/mem/intune/enrollment/enrollment-restrictions-set

upvoted 2 times

Fala_Fel 1 year, 11 months ago

Yes: you only need an intune license to enroll up to 15 devices. This user is limited by policy to 10

No: User 2 is member of Group 2 which is limited to 15 (not 10)

No: DEM not limitless

upvoted 1 times

VirtualJP 3 years ago

I'd say this is correct.

Originally thought No to User3 but remembered that there is a limit of 1000 for DEM accounts

upvoted 1 times

Question #29 *Topic 1*

HOTSPOT -

Your company has a Microsoft 365 tenant.

You plan to allow users that are members of a group named Engineering to enroll their mobile device in mobile device management (MDM).

The device type restrictions are configured as shown in the following table.

Priority	Name	Allowed platform	Assigned to
1	iOS	iOS	Marketing
2	Android	Android	Engineering
Default	All users	All platforms	All users

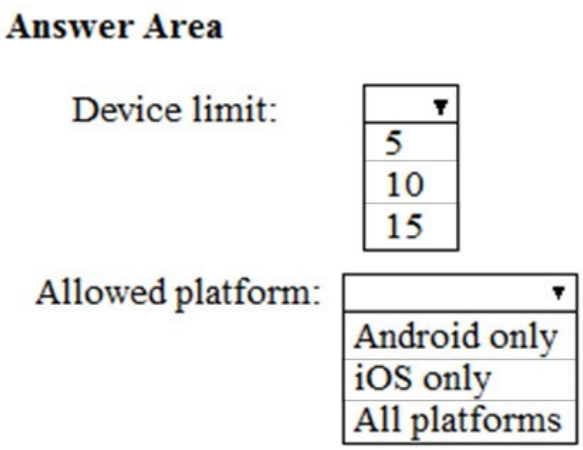
The device limit restrictions are configured as shown in the following table.

Priority	Name	Device limit	Assigned to
1	Engineering	15	Engineering
2	West Region	5	Engineering
Default	All users	10	All users

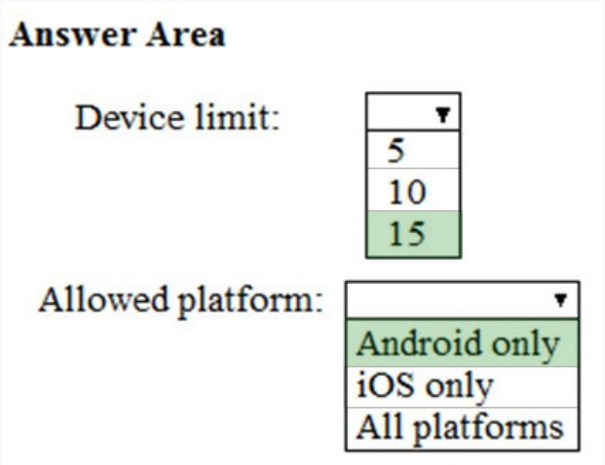
What is the effective configuration for the members of the Engineering group? To answer, select the appropriate options in the answer area.

NOTE: Each correct selection is worth one point.

Hot Area:



Suggested Answer:



Goena Highly Voted 3 years ago

Answer is correct.

upvoted 13 times

rrrr5r Most Recent 2 years, 3 months ago

Valid in 16 Sep 22

upvoted 4 times

reastman66 2 years, 4 months ago

https://docs.microsoft.com/en-us/mem/intune/enrollment/enrollment-restrictions-set

Answer is correct.

Change restriction priority

When a group is assigned multiple restrictions, the priority level determines which policy gets applied. The restriction with highest priority (1 being the highest priority position) is applied and the other restrictions are disregarded.

upvoted 3 times

wiouxev 2 years, 10 months ago

This is a confusing use of "effective" .. I initially understood this as "What should you set for each to allow Engineering group to enroll their mobile device? Which would be "all platforms" as they currently only allow Android, which doesn't "allow enrollment for mobile devices" as it doesn't include iOS...while the question is really asking you to label what you see already configured... "what is 'in effect' based on what you see"

upvoted 2 times

Adi_0001 2 years, 6 months ago

How to ascertain this, as per the most restrictive policy, it should be 5 devices?

upvoted 1 times

[Removed] 2 years ago

Highest priority (lowest number) applies, not the most restrictive.

upvoted 2 times

Question #30 *Topic 1*

Your network contains an Active Directory domain named contoso.com. The domain contains 100 Windows 8.1 devices.
You plan to deploy a custom Windows 10 Enterprise image to the Windows 8.1 devices.
You need to recommend a Windows 10 deployment method.
What should you recommend?

A. a provisioning package

B. an in-place upgrade

C. wipe and load refresh

D. Windows Autopilot

Suggested Answer: *B*
References:
https://docs.microsoft.com/en-us/microsoft-365/enterprise/windows10-infrastructure

Community vote distribution
C (100%)

Marz Highly Voted 5 years, 1 month ago
i reconsider: It sasy you plan to install a custom image. This only leaves wipe and load refresh. IN place upgrade keeps all settings and apps. So wrong. Prov. package is installing on top of existing Win 10 OS. So wrong.
upvoted 67 times

JT19760106 2 years, 11 months ago
C. Wipe and then dump load
upvoted 5 times

MCPsince1999 4 years, 11 months ago
True. Because existing applications are preserved through the process, the upgrade process uses the standard Windows installation media image (Install.wim); custom images are not needed and cannot be used because the upgrade process is unable to deal with conflicts between apps in the old and new operating system.
upvoted 12 times

ZakS 4 years, 11 months ago
Correct ans should be C - wipe and load refresh
The question specifies a custom image.
In place upgrade cannot do custom images.
Also, for provisioning packages Win 10 is a pre-requisite. Hence, that cannot be the correct answer.
upvoted 46 times

mgmjtech Highly Voted 4 years, 8 months ago
Answer is C. Here is why

A. a provisioning package method is self-contained package that contains all of the configuration, settings, and apps that need to be applied to a machine. this method is mainly for new machines.

B. an in-place upgrade - For existing computers running Windows 7, Windows 8, or Windows 8.1, the recommended path for organizations deploying Windows 10 leverages the Windows installation program (Setup.exe) to perform an in-place upgrade, which automatically preserves all data, settings, applications, and drivers from the existing operating system version. HOWEVER - Custom images are not needed and cannot be used because the upgrade process is unable to deal with conflicts between apps in the old and new operating system.

C. wipe and load refresh - this method is usually for custom images

D. Windows Autopilot- completely wrong. Windows Autopilot enables IT professionals to customize the Out of Box Experience (OOBE) for Windows 10 PCs and provide end users with a fully configured new Windows 10 device after just a few clicks. There are no images to deploy, no drivers to inject, and no infrastructure to manage.
upvoted 58 times

Rtstrider 2 years, 4 months ago

Thank you for this! This is a really good break down!

upvoted 2 times

Mary_Yvette 4 years, 6 months ago

agree should be C. Wipe and Load Refresh

upvoted 5 times

BigDazza_111 Most Recent 1 year, 4 months ago

Selected Answer: C

Yep c. Provisioning packages let you configure up to a few hundred device OS's without the need of a new image, not an upgrade tool. Not In place upgrade becuase Custom image no no no. Not Apilot as that is for OOBE. So C it is. https://learn.microsoft.com/en-us/windows/configuration/provisioning-packages/provisioning-packages

upvoted 1 times

Pepeti 1 year, 8 months ago

Estudei essa na MS-10O, e lá é limpar e carregar atualização

upvoted 1 times

StudyBM 1 year, 9 months ago

Selected Answer: C

for Custom Image best option is 'Wipe and Load'...

upvoted 1 times

Kuriatk0 1 year, 10 months ago

it was in my exam 17.feb.2023

upvoted 2 times

DCT 2 years, 1 month ago

niama, answer C la

upvoted 1 times

EliasMartinelli 2 years, 1 month ago

Selected Answer: C

100% C

upvoted 1 times

francescoc 2 years, 6 months ago

In the MS-100 there was the same question, and answer was C. C is correct.

upvoted 1 times

Dolhave2 2 years, 6 months ago

Selected Answer: C

The "Custom Image" says it all

upvoted 1 times

takei 2 years, 7 months ago

This answer is A

upvoted 1 times

venwaik 2 years, 8 months ago

Selected Answer: C

With an in-place upgrade you cannot use custom images.
https://docs.microsoft.com/en-us/windows/deployment/windows-10-deployment-scenarios

Answer: C

upvoted 2 times

MichaelMu 2 years, 8 months ago

Selected Answer: C

Windows 8.1 need wipe and load

upvoted 1 times

martinsch 2 years, 10 months ago

Selected Answer: C

Answer c is correct, its also a question from ms 100

upvoted 2 times

m43s 2 years, 2 months ago

+1 I had this question on the ms-100 exam.

upvoted 1 times

Panku 2 years, 11 months ago

Selected Answer: C

upvoted 1 times

superboy1981 2 years, 11 months ago

https://docs.microsoft.com/en-us/windows-hardware/manufacture/desktop/deploy-a-custom-image?view=windows-10
Setup supports the following:
Upgrading an existing Windows installation.

is it means in-place upgrade ?

upvoted 1 times

haazybanj 2 years, 11 months ago

Because existing applications are preserved through the process, the upgrade process uses the standard Windows installation media image (Install.wim); custom images are not needed and cannot be used because the upgrade process is unable to deal with conflicts between apps in the old and new operating system. (For example, Contoso Timecard 1.0 in Windows 7 and Contoso Timecard 3.0 in the Windows 10 image.)

https://docs.microsoft.com/en-us/windows/deployment/windows-10-deployment-scenarios#computer-refresh

upvoted 1 times

Question #31 *Topic 1*

You use Microsoft System Center Configuration Manager (Current Branch) to manage devices.
Your company uses the following types of devices:
- Windows 10
- Windows 8.1
- Android
- iOS

Which devices can be managed by using co-management?

A. Windows 10 and Windows 8.1 only

B. Windows 10, Android, and iOS only

C. Windows 10 only

D. Windows 10, Windows 8.1, Android, and iOS

Suggested Answer: *C*
You can manage only Windows 10 devices by using co-management.
When you concurrently manage Windows 10 devices with both Configuration Manager and Microsoft Intune, this configuration is called co-management. When you manage devices with Configuration Manager and enroll to a third-party MDM service, this configuration is called coexistence.
Reference:
https://docs.microsoft.com/en-us/configmgr/comanage/overview

Community vote distribution
C (100%)

Gowdhaman Highly Voted 5 years, 1 month ago
Correct answer C
upvoted 68 times

shanem 5 years, 1 month ago
It says to use co-management, so D is correct.
upvoted 4 times

SJ31 5 years ago
C is the correct answer, see: https://docs.microsoft.com/en-us/configmgr/comanage/overview#prerequisites

Prerequisites say Windows 10.
upvoted 33 times

Sushant0622 3 years, 10 months ago
Important

Windows 10 mobile devices don't support co-management., So how can we expect android and iOS. Answer is C
upvoted 3 times

dailyup 3 years, 8 months ago
Also shows in MS-100 and ans is C
upvoted 8 times

Examtopicisawesome 4 years, 9 months ago
Co-management is only possible for Windows 10. Answer is C
upvoted 13 times

Marz Highly Voted 5 years ago
only win10 supported REF: https://docs.microsoft.com/en-us/configmgr/core/plan-design/choose-a-device-management-solution#bkmk_comanage
upvoted 10 times

Pepeti Most Recent 1 year, 8 months ago

Somente Windows 10 pergunta da MS-100
upvoted 1 times

Kaloy 1 year, 9 months ago

Selected Answer: C

Agreed! Ans:C
upvoted 1 times

k9_bern_001 2 years, 4 months ago

The answer is C, Co management aspect is brought by Intune even if its not mentioned in the question.
upvoted 1 times

Prates_BR 3 years, 4 months ago

Correct: C
Prerequisites
Co-management has these prerequisites in the following areas:

Licensing
Configuration Manager
Azure Active Directory (Azure AD)
Microsoft Intune
Windows 10
Permissions and roles
upvoted 2 times

Domza 3 years, 5 months ago

Ok, ok i found it. Please read second paragraph:
https://docs.microsoft.com/en-us/mem/configmgr/comanage/overview

Windows 10 devices! cheers!
upvoted 1 times

keefe 3 years, 7 months ago

only Win10 devices can be managed by co-management
upvoted 1 times

scottims 3 years, 7 months ago

C
Windows 10 is a pre-req.
https://docs.microsoft.com/en-us/mem/configmgr/comanage/overview#windows-10
upvoted 2 times

Prianishnikov 3 years, 9 months ago

C. Windows 10 only
upvoted 2 times

kiketxu 3 years, 8 months ago

C for sure!
upvoted 1 times

SimoneV 3 years, 9 months ago

Co-management is out of the skills measured per Feb 24 2021:
https://query.prod.cms.rt.microsoft.com/cms/api/am/binary/RE3VEHZ Page 4 under old: plan for devices and apps. New: Plan for apps.
upvoted 1 times

kiketxu 3 years, 8 months ago

Thanks for the tip.
upvoted 1 times

Takloy 3 years, 10 months ago

This should be Windows 10 Only.
upvoted 1 times

mkoprivnj 3 years, 11 months ago

C is correct!

upvoted 2 times

beeejlil 4 years, 1 month ago

Make that 5 incorrect questions....

upvoted 3 times

Leimo 4 years, 2 months ago

Correct answer C

Co-management is for Windows 10 devices only. Windows 10 devices must be connected to Azure AD.

upvoted 1 times

Alvaroll 4 years, 2 months ago

Same as MS-100 Topic1-45 https://www.examtopics.com/exams/microsoft/ms-100/view/9/

upvoted 3 times

EddyHeddy 4 years, 3 months ago

The answer is correct:

https://docs.microsoft.com/en-us/mem/configmgr/comanage/overview

upvoted 1 times

VTHAR 4 years, 3 months ago

The answer is incorrect because of your link. https://docs.microsoft.com/en-us/mem/configmgr/comanage/overview

"Note : When you concurrently manage Windows 10 devices with both Configuration Manager and Microsoft Intune, this configuration is called co-management. When you manage devices with Configuration Manager and enroll to a third-party MDM service, this configuration is called coexistence."

Therefore, the correct answer is "C. Windows 10 ONLY" for co-management (that specific capabilities). But in real world scenario if you have enabled Intune + SCCM, you can manage all those devices with the different portal for managing iOS/Android from Intune ONLY and Windows 10 from both (SCCM+Intune).

upvoted 1 times

Question #32 *Topic 1*

HOTSPOT -

You have three devices enrolled in Microsoft Endpoint Manager as shown in the following table.

Name	Platform	BitLocker Drive Encryption (BitLocker)	Member of
Device1	Windows 10	Disabled	Group3
Device2	Windows 10	Disabled	Group2, Group3
Device3	Windows 10	Disabled	Group2

The device compliance policies in Endpoint Manager are configured as shown in the following table.

Name	Platform	Require BitLocker	Assigned
Policy1	Windows 10 and later	Require	Yes
Policy2	Windows 10 and later	Not configured	Yes
Policy3	Windows 10 and later	Require	No

The device compliance policies have the assignments shown in the following table.

Name	Assigned to
Policy1	Group3
Policy2	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
Device1 is compliant.	○	○
Device2 is compliant.	○	○
Device3 is compliant.	○	○

Suggested Answer:

Answer Area

Statements	Yes	No
Device1 is compliant.	○	●
Device2 is compliant.	○	●
Device3 is compliant.	●	○

ALPHA_DELTA Highly Voted 3 years, 9 months ago

Device1 is compliant: No, because Device 1 is member of group 3 so policy 1 is assigned. Policy 1 requires Bitlocker encryption which device 1 does not have thus is Device 1 marked as non compliant

Device2 is compliant: No, because Device 2 is member of group 2 and 3, Device 2 is marked as non compliant by the same reason as Device 1.

Device3 is compliant: Yes, Device 3 is member of group 2, Policy 2 applies to Group 2, the policy does not require Bitlocker encryption, thus the device is compliant

upvoted 35 times

us3r Highly Voted 3 years, 2 months ago

NO (policy1)

NO (policy1 applied by priority - higher)

YES (policy2)

upvoted 8 times

junior6995 2 years, 11 months ago

Most restrictive polices overrides less restrictive policies

upvoted 3 times

edzio 2 years, 11 months ago

Does assignment or no policy matter?? Policy 3 is not assigned - device 2 is still not complaint.

upvoted 2 times

mir000 2 years, 11 months ago

policy 3 is not assigned and not even used here, it should be completly ignored in this question

upvoted 4 times

Futfuyfyjfj 2 years ago

Compliance policies do not have priorities.

upvoted 3 times

rrrr5r Most Recent 2 years, 3 months ago

Valid in 16 Sep 22

upvoted 5 times

Domza 3 years, 5 months ago

There we go: https://docs.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

When two or more policies are assigned to the same user or device, then the setting that's applied happens at the individual setting level:
• Compliance policy settings always have precedence over configuration profile settings.
• If a compliance policy evaluates against the same setting in another compliance policy, then the most restrictive compliance policy setting applies.
• If a configuration policy setting conflicts with a setting in another configuration policy, this conflict is shown in Intune. Manually resolve these conflicts.

Thanks for the link " kiketxu "

upvoted 4 times

adaniel89 3 years, 6 months ago

So only the most secure policy is chosen ? referring to Device 2

upvoted 1 times

GiJoe1987 3 years, 6 months ago

Policy 3 is not assigned so why is device 2 not complaint.

upvoted 1 times

Prianishnikov 3 years, 9 months ago

NO-NO-YES or YES-YES-YES ?

upvoted 1 times

Lopsios 3 years, 8 months ago

Why YYY?

upvoted 1 times

lucidgreen 3 years, 8 months ago

If the device is marked as non-compliant by one policy, it cannot be marked as compliant by another policy. If one policy marks it as non-compliant it is non-compliant until the discrepancy is resolved.
N, N, Y.

upvoted 6 times

MSGrady 3 years, 9 months ago

How is device 2 not compliant if it is in group 2 that is "Assigned" but not requiring bitlocker?

upvoted 2 times

barleyhutcher 3 years, 9 months ago

because its also in group 3 which does require bitlocker. When there is more than 1 CA policy assigned, the more secure one takes precedence.

upvoted 6 times

kiketxu 3 years, 8 months ago

Agreed.
https://docs.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

Question #33 *Topic 1*

Your company has a Microsoft 365 E3 subscription.
All devices run Windows 10 Pro and are joined to Microsoft Azure Active Directory (Azure AD).
You need to change the edition of Windows 10 to Enterprise the next time users sign in to their computer. The solution must minimize downtime for the users.
What should you use?

A. Windows Autopilot

B. Windows Update

C. Subscription Activation

D. an in-place upgrade

Suggested Answer: *C*
Reference:
https://docs.microsoft.com/en-us/windows/deployment/windows-10-subscription-activation

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

Fronkler Highly Voted 5 years, 5 months ago
I think it's C. It would only require assigning the license and then having the user sign in. Autopilot is used for new/reset devices that are at the OOBE screen.
upvoted 83 times

show 5 years, 3 months ago
Also I think it should be C.
Question information is hinting about that the company has a Microsoft E3 subscription.

https://docs.microsoft.com/en-us/windows/deployment/windows-10-subscription-activation
upvoted 21 times

lucidgreen 3 years, 8 months ago
Subscription activation only requires the user to log off and log back on. So yes, least disruptive.
upvoted 11 times

momakill1 Highly Voted 5 years, 1 month ago
C is the correct answer. Please edit.
upvoted 21 times

Debadatta Most Recent 1 year, 6 months ago
Selected Answer: C
C is correct answer.
Windows Enterprise E3 and E5 are available as online services via subscription. You can deploy Windows Enterprise in your organization without keys and reboots.
Devices with a current Windows Pro edition license can be seamlessly upgraded to Windows Enterprise.
https://learn.microsoft.com/en-us/windows/deployment/windows-10-subscription-activation
upvoted 1 times

Pepeti 1 year, 8 months ago
é a letra C ativação de assinatura a resposta correta, pergunta da MS-100
upvoted 1 times

ahmedkmicha 1 year, 9 months ago
Selected Answer: A
Windows Autopilot is a cloud-based deployment service that allows you to configure and pre-provision new devices for your organization, and can also be used to upgrade the edition of Windows 10 on existing devices.

Subscription Activation allows you to activate Windows 10 Enterprise edition using your existing Microsoft 365 subscription, but does not provide a mechanism for upgrading the edition on existing devices.
upvoted 1 times

Kuriatk0 1 year, 10 months ago
On exam today 02/17/2023, but answers are are more extesive
upvoted 2 times

sapt 1 year, 10 months ago
are you remember the cuestion??
upvoted 1 times

rrrr5r 2 years, 3 months ago
Valid in 16 Sep 22
upvoted 6 times

ARYMBS 2 years, 3 months ago
Selected Answer: C
Subscription Activation + E3/E5 License
upvoted 1 times

Rsham 2 years, 4 months ago
C is the answer
upvoted 1 times

k9_bern_001 2 years, 4 months ago
The correct answer is C
upvoted 1 times

Dolhave2 2 years, 6 months ago
Selected Answer: C
Tested and confirmed
upvoted 2 times

Velda 3 years, 1 month ago
C is correct.
Same question as in MS-100 (Question #41 Topic 1) which i already labored.
upvoted 1 times

us3r 3 years, 2 months ago
As Autopilot is destined for NEW endpoints configuration, the correct answer is
C - sub activation
upvoted 1 times

Kanta 3 years, 4 months ago
A and C both can achieve this but less disruptive is C - Subs Activation (no reboot needed but just logoff).

Windows 10 Subscription Activation
Windows 10 Subscription Activation is a modern deployment method that enables you to change the SKU from Pro to Enterprise with no keys and no reboots. For more information about Subscription Activation

Ref:
https://docs.microsoft.com/en-us/windows/deployment/windows-10-deployment-scenarios
upvoted 1 times

Domza 3 years, 5 months ago
C is correct.

Thanks for links below: https://docs.microsoft.com/en-us/windows/deployment/windows-10-subscription-activation#subscription-activation-for-windows-10-enterprise
upvoted 1 times

pmendez 3 years, 6 months ago
C

https://docs.microsoft.com/en-us/windows/deployment/windows-10-subscription-activation

upvoted 2 times

keefe 3 years, 7 months ago

Subscription activation where users will be assigned a license

upvoted 1 times

Question #34 *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.
Your network contains an Active Directory domain named contoso.com that is synced to Microsoft Azure Active Directory (Azure AD).
You manage Windows 10 devices by using Microsoft System Center Configuration Manager (Current Branch).
You configure pilot co-management.
You add a new device named Device1 to the domain. You install the Configuration Manager client on Device1.
You need to ensure that you can manage Device1 by using Microsoft Intune and Configuration Manager.
Solution: Define a Configuration Manager device collection as the pilot collection. Add Device1 to the collection.
Does this meet the goal?

A. Yes

B. No

Suggested Answer: *A*
Reference:
https://docs.microsoft.com/en-us/mem/configmgr/comanage/tutorial-co-manage-clients

Community vote distribution
A (100%)

TFou0076 Highly Voted 4 years, 11 months ago
Yes is the right answer, check it on :
https://docs.microsoft.com/en-us/configmgr/comanage/how-to-enable
upvoted 55 times

Dylan 4 years, 11 months ago
I'd agree with this - once setup it's just a matter of adding a client to a collection
upvoted 9 times

VTHAR 4 years, 3 months ago
Agreed.
upvoted 3 times

kiketxu 3 years, 8 months ago
Agree here
upvoted 3 times

dailyup 3 years, 8 months ago
So, I think that Q22 Topic1 is No.
upvoted 11 times

blaatlama Highly Voted 4 years, 10 months ago
Answer is No as de Pilot Collection is automatically created. The device only has to be added to the Pilot device collection!
upvoted 5 times

diggity801 4 years, 9 months ago
"When you enable co-management, you'll assign a collection as a Pilot group. This is a group that contains a small number of clients to test your co-management configurations. We recommend you create a suitable collection before you start the procedure. Then you can select that collection without exiting the procedure to do so." So this would lead me to believe that answer A is correct.
upvoted 18 times

mgmjtech 4 years, 8 months ago
Agreed.
upvoted 3 times

VirtualJP Most Recent 3 years ago

Selected Answer: A

Question/answer is not vague, like some of the other questions around this same point.

upvoted 4 times

AnoniMouse 3 years, 7 months ago

There is another similar question to this in the exam. This question explicitly mentioned creating a collection for co-management, thus devices in this collection will be co-managed. So the answer is definitely YES. Where as in the other question, it vaguely says: "Add the device to a device collection" which is too generic! Almost all devices are part of built-in collections, and even if you add the device into a custom collection that doesn't mean that it is the co-management collection, hence for that type of question the answer is NO.

upvoted 4 times

init2winit 3 years, 8 months ago

Yes is the correct answer

upvoted 3 times

lucidgreen 3 years, 8 months ago

If you designate a Pilot Group, yes. Remember that a Pilot Group is nothing more than a Pilot device collection for testing purposes. Often this group is left in production. Either way a Pilot Group or otherwise configure device collection will work.

upvoted 1 times

Dooa 3 years, 9 months ago

Yes....100%

upvoted 1 times

mkoprivnj 3 years, 11 months ago

Yes is correct!

upvoted 2 times

PattiD 4 years ago

"...This action enables automatic client enrollment in Intune for existing Configuration Manager clients. When you choose Pilot, only the Configuration Manager clients that are members of the pilot collection are automatically enrolled to Intune. This option allows you to enable co-management on a subset of clients to initially test co-management, and rollout co-management using a phased approach."

upvoted 1 times

Leimo 4 years, 2 months ago

Answer: A

Explanation

Device1 has the Configuration Manager client installed so you can manage Device1 by using
Configuration Manager. To manage Device1 by using Microsoft Intune, the device has to be enrolled in Microsoft Intune. In the Co-management Pilot configuration, you configure a Configuration Manager Device Collection that determines which devices are auto-enrolled in Microsoft Intune. You need to add Device1 to the Device Collection so that it auto-enrols in Microsoft Intune. You will then be able to manage Device1 using Microsoft Intune.

https://docs.microsoft.com/en-us/configmgr/comanage/how-to-enable

upvoted 3 times

Alvaroll 4 years, 2 months ago

Same as MS-100 Topic1-23 https://www.examtopics.com/exams/microsoft/ms-100/view/5/

upvoted 4 times

Benoit_HAMET 4 years, 3 months ago

co-management applies ONLY to device collection
hence the answer is A

upvoted 2 times

Question #35 *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 are deploying Microsoft Endpoint Manager.
You successfully enroll Windows 10 devices in Endpoint Manager.
When you try to enroll an iOS device in Endpoint Manager, you get an error.
You need to ensure that you can enroll the iOS device in Endpoint Manager.
Solution: You configure the Mobility (MDM and MAM) settings.
Does this meet the goal?

A. Yes

B. No

Suggested Answer: *B*

bdedecker Highly Voted 3 years, 6 months ago
You need to make sure your Apple MDM push certificate is added in Endpoint Manager
upvoted 12 times

Contactfornitish Most Recent 2 years, 4 months ago
On exam on 13 aug'22
upvoted 2 times

jjong 3 years, 4 months ago
this is repeated question in the list of questions. We answered this earlier between qns 20-30
upvoted 3 times

Question #36 *Topic 1*

Your company has 10 offices.
The network contains an Active Directory domain named contoso.com. The domain contains 500 client computers. Each office is configured as a separate subnet.
You discover that one of the offices has the following:
✑ Computers that have several preinstalled applications
✑ Computers that use nonstandard computer names
✑ Computers that have Windows 10 preinstalled
✑ Computers that are in a workgroup
You must configure all computers in the office to meet the following corporate requirements:
All computers in the office must be joined to the domain.
▪
✑ All computers in the office must have computer names that use a prefix of CONTOSO.
✑ All computers in the office must only have approved corporate applications installed.
You need to recommend a solution to redeploy the computers. The solution must minimize the deployment time.
Which deployment method should you recommend?

A. a provisioning package

B. wipe and load refresh

C. Windows Autopilot

D. an in-place upgrade

Suggested Answer: *A*
By using a Provisioning, IT administrators can create a self-contained package that contains all of the configuration, settings, and apps that need to be applied to a device.
Incorrect Answers:
C: With Windows Autopilot the user can set up pre-configure devices without the need consult their IT administrator.
D: Use the In-Place Upgrade option when you want to keep all (or at least most) existing applications.
References:
https://docs.microsoft.com/en-us/windows/deployment/windows-10-deployment-scenarios https://docs.microsoft.com/en-us/windows/deployment/windows-autopilot/windows-autopilot

Community vote distribution
A (100%)

Richmawdsley Highly Voted 2 years, 10 months ago
Selected Answer: A
Literally no one would use a Provisioning Package for this in real life, you'd wipe and load them. But here, in MS land, sure, A it is.
upvoted 18 times

Glorence Highly Voted 2 years, 11 months ago
still valid, it was in my exam last feb 5, 2022
upvoted 8 times

One111 Most Recent 1 year, 3 months ago
(1) Computers have preinstalled Windows, might be home, pro or enterprise. (2) You can't add home to domain or (3) use provisioning package to upgrade from home to pro or enterprise.
upvoted 1 times

Kuriatk0 1 year, 10 months ago
it was in my exam 17.feb.2023
upvoted 2 times

Contactfornitish 2 years, 4 months ago
On exam on 13 aug'22
upvoted 3 times

manis73 2 years, 5 months ago

What's this got to do with Microsoft 365? Other than the Microsoft 365 solution is the wrong answer

upvoted 1 times

L33D 2 years, 6 months ago

Still valid, on exam Jun 25, 2022

upvoted 1 times

Goena 3 years ago

A. a provisioning package

upvoted 3 times

VirtualJP 3 years ago

Selected Answer: A

I'd say this answer could be either A or C but as the solution calls for minimizing the deployment time, that leaves a provisioning package as the most suitable option.

upvoted 5 times

ARYMBS 2 years, 3 months ago

Agree with A.

I can also add that nowhere it states that we have O365 subscription.

upvoted 1 times

Question #37 *Topic 1*

Your company has a Microsoft 365 subscription. The subscription contains 500 devices that run Windows 10 and 100 devices that run iOS.
You need to create Microsoft Endpoint Manager device configuration profiles to meet the following requirements:
✑ Configure Wi-Fi connectivity to a secured network named ContosoNet.
✑ Require passwords of at least six characters to lock the devices.
What is the minimum number of device configuration profiles that you should create?

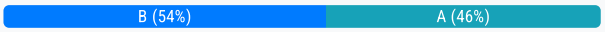
A. 4

B. 2

C. 1

Suggested Answer: *B*

Community vote distribution



d3an Highly Voted 4 years, 10 months ago
Correct answer is 4. Configuration Profiles are not cross-platform, and W-Fi settings are contained within their own Profile.
upvoted 62 times

D3t0 4 years, 10 months ago
That's correct.
upvoted 6 times

melki_zedek 4 years, 2 months ago
Except that WiFi falls under configuration profile but password falls under compliance policy.
upvoted 8 times

MiZi 3 years, 8 months ago
You can find the "Require password to access device" settings under MEM -> Devices -> Configuration Profiles -> Templates "Device restrictions" at "Password" section. Doesn't it cover the requirement in the question?
upvoted 8 times

Flojo2 3 years, 7 months ago
MiZi, I just checked this in MEM, and you are absolutely correct. You can create a Configuration Profile under the path you mentioned that determines how long a password must be. Which means the correct answer is 4. All of these other comments are from quite some time ago, so maybe this has changed since these people posted here that password must be configured in Compliance policy. If you are here reading these comments for yourself, I urge you to look at configuration policies in your MEM and verify the correct answer yourself.
upvoted 4 times

Requi3m 3 years, 5 months ago
I think it's 2.

Just checked in MEM. You can set password length in a configuration profile as well as in a compliance policy. However, the password settings in the Compliance policy specifies "Require password to unlock mobile devices", where the Configuration profile seems to be amore general password policy.

The question is a bit vague, but I think it should be 2. They're asking for the minimum amount of configuration policies and the requirements state "Require passwords of at least six characters to lock the devices", so you could configure this as a Compliance policy.
upvoted 5 times

Requi3m 3 years, 4 months ago
After reviewing this question again I changed my mind: I think it's 4.

I think myself and others have gotten lost in what's technically possible. Even though password policies can be set in configuration policies and compliance policies (discussions on best practices asside), the question clearly states:

"You need to create Microsoft Intune device configuration profiles to meet the following requirements"

suggesting the password policy should be configured in a configuration policy in the context of this question.
upvoted 4 times

ACTOSA 2 years, 2 months ago
that is incorrect. Settings catalogue allows you to mix and match policies from the templates.
upvoted 3 times

TechMinerUK 2 years, 2 months ago
This is incorrect, whilst you can configure PIN/passcode requirements for iOS and Windows devices in settings catalogs (seperate policies for each OS) you cannot deploy WiFi networks via settings catalogs, this is a seperate policy meaning you would still need 4
upvoted 4 times

piotrxj 4 years, 4 months ago
2 configuration policies is correct answer - B.
This is because lock password policy is configured under Compliance policies: MEM -> Devices- > Compliance Policies. The question is "minimal no. of configuration policies".
Verified it on my tenant Dev environment.
upvoted 16 times

ntcct 4 years, 2 months ago
I think 4 is correct. The target is to CONFIGURE the devices.
upvoted 3 times

Tyranius 3 years, 5 months ago
Not exactly, the wording in what is required specifies only that you are "Configuring" the WiFi, but just "requiring" the password. This one is difficult though and I understand arguments both ways here. Not a well worded question.
upvoted 1 times

TonySuccess Highly Voted 4 years, 5 months ago
I have tested this by going to: endpoint.microsoft.com - Devices - Configuration Profiles.

From here I can confirm that you can not make a password profile and a wi-fi profile within the same configuration. Therefore as suggested previously I can conclude that you would need:

1 x ios wifi profile
1 x ios password profile
1 x Windows wifi profile
1 x Windows passowrd profile

Add them up and that = 4

Answer is A.
upvoted 30 times

mgmjtech 4 years, 5 months ago
Agreed. total of 4. Tested. In case you can't find a password profile. It's under device restriction.
upvoted 3 times

melki_zedek 4 years, 2 months ago
Except that WiFi falls under configuration profile but password falls under compliance policy. So 2 config profile, 2 compliance policies
upvoted 4 times

Futfuyfyjfj 1 year, 8 months ago
You enforce passwords in a device configuration profile. You check on passwords with a compliance policy. The question is only on device configuration profiles. So answer is 4
upvoted 1 times

piotrxj 4 years, 4 months ago
2 configuration policies is correct answer - B.
This is because lock password policy is configured under Compliance policies: MEM -> Devices- > Compliance Policies. The question is "minimal no. of configuration policies".
Verified it on my tenant Dev environment.

Two kind off setting land under different policies nodes:
- configuration policies: Wi-Fi policy
- compliance policies: Lock Password policy
upvoted 7 times

Futfuyfyjfj 1 year, 8 months ago
You enforce passwords in a device configuration profile. You check on passwords with a compliance policy. The question is only on device configuration profiles. So answer is 4
upvoted 2 times

Hazul Most Recent 1 year, 6 months ago
B is correct according to bing. You need to create Microsoft Endpoint Manager device configuration profiles to configure Wi-Fi connectivity to a secured network named ContosoNet and require passwords of at least six characters to lock the devices. The minimum number of device configuration profiles that you should create is 2. One profile for the Windows 10 devices and one profile for the iOS devices.
upvoted 1 times

Webleyboy 1 year, 6 months ago
Selected Answer: A
Answer should be 4. If I test this at this moment I can click on Create Profile.
Then I need to choose a platform and then a profile type. After this I need to create another profile for the other platform. So yes, a profile can be setup for Windows or iOS, but not within one profile.
upvoted 2 times

BobDobolina 1 year, 8 months ago
Selected Answer: B
You can create two Microsoft Endpoint Manager device configuration profiles to meet the requirements:

Wi-Fi connectivity: You can create a device configuration profile to configure Wi-Fi connectivity to the ContosoNet network. This profile can be applied to both Windows 10 and iOS devices.

Password policy: You can create a separate device configuration profile to require passwords of at least six characters to lock the devices. This profile can also be applied to both Windows 10 and iOS devices.

By creating two device configuration profiles, one for Wi-Fi connectivity and one for the password policy, you can meet both of the requirements with a minimum number of profiles.

Therefore, the minimum number of device configuration profiles that you should create is 2.
upvoted 3 times

fofo1960 2 years ago
Test and seems to be 4, you cannot add the Wifi settings and the Device restriction settings together
upvoted 1 times

smkartha 2 years ago
Selected Answer: B
Go with B - re-read the question again it asking minimum configuration profile that is 2 One is for iOS and second one is for Windows(Wi-Fi Profile) rest 2 Profile will be compliance Policy (Password Policy) which is not in question.
upvoted 4 times

ServerBrain 2 years, 1 month ago
Selected Answer: B
Correct answer B, as you have two device types, and the question states "What is the minimum number of device configuration profiles" Key word here is minimum, so 2 profiles at minimum will suffice..
upvoted 3 times

Futfuyfyjfj 2 years ago
You need 1 for WiFi Android
You need 1 for passcode Android
You need at leest 1 for Windows (probably 2)
So at least 3 separate configs, given 3 is not an optie witling the answers I would-be assumptie it is 4
upvoted 1 times

dyn36 1 year, 9 months ago

Password Policy is configured in Compliance Profile, not Configuration profile. So correct is B-2
upvoted 3 times

ACTOSA 2 years, 2 months ago
2 is the correct answer - Device Lock and Wifi settings in Settings catalogue if you want to double check
upvoted 2 times

SaeedFarvardin 2 years, 4 months ago
You can define only 2 Customs Policy(Android and IOS) and in them define WIFI, pw etc.) so the answer can be "2"!
;O)

like it if useful! ;O)
upvoted 2 times

Contactfornitish 2 years, 4 months ago
On exam on 13 aug'22
upvoted 1 times

Kevinfm_81 2 years, 6 months ago
Not sure where this was a while back but believe it's 4. there's a 'template' config policy for Wi-Fi (along with things like certificates, VPN, etc) then there's a 'settings' preview option that allows you set passcode length as an option under the security node (at least for iOS/iPadOS..assuming it's available within Win10 devices). Tested in demo tenant.
upvoted 1 times

L33D 2 years, 6 months ago
Still valid, on exam Jun 25, 2022
upvoted 1 times

Durden871 2 years, 5 months ago
Great. A vague question in the test. Awesome. I'm going with 2 here because 2 config , 2 compliance
upvoted 2 times

K4NIUS 2 years, 6 months ago
Selected Answer: A
Answer is A, you need to create 4 different configuration profiles to achieve those requirements.
upvoted 2 times

Alien1981 2 years, 7 months ago
Selected Answer: A
The correct answer is 4
upvoted 2 times

Musa007 2 years, 7 months ago
Selected Answer: A
4 is correct
upvoted 3 times

KSvh53 2 years, 9 months ago
Selected Answer: B
Just tested this out and the way I see it, config profiles and compliance policies are two completely separate items. You can create a compliance policy for passwords for each OS, so you don't need to create a config profile for passwords. You do need to create config profiles for wifi though, so you will need one for each OS. So answer is 2.
I don't see any reason for treating compliance policies the same as config profiles when they have separate blades, and a profile is not the same as a policy conceptually. The question asks for minimum amount of config profiles needed, so even if you could create config profiles for the passwords, you don't need to when you can create compliance policies instead. It's possible to do it with 4 but you don't need to. You need a minimum of 2. That's how I read it and make sense of it, not sure if Microsoft sees it the same way or not. That's the real question. How will Microsoft see it?
upvoted 4 times

Question #38 *Topic 1*

Your company has a Microsoft Azure Active Directory (Azure AD) tenant named contoso.com and a Microsoft 365 subscription.
The company recently hired four new users who have the devices shown in the following table.

Name	Operating system
User1	Windows 8
User2	Windows 10
User3	Android 8.0
User4	iOS 11

You configure the Microsoft 365 subscription to ensure that the new devices enroll in Microsoft Endpoint Manager automatically.
Which users have a device that can enroll in Microsoft Endpoint Manager automatically?

A. User1, User2, User3, and User4

B. User2 only

C. User1 and User2 only

D. User1, User2, and User3 only

Suggested Answer: *B*

Community vote distribution

B (100%)

Sprinqfield Highly Voted 3 years, 6 months ago
Yes, it's true.

https://docs.microsoft.com/en-us/mem/intune/enrollment/quickstart-setup-auto-enrollment

For win 8 or other clients need to use user enrollment
https://docs.microsoft.com/en-us/mem/intune/enrollment/windows-enroll
upvoted 14 times

jeff1988 Most Recent 2 years, 11 months ago
Selected Answer: B
B for dure
upvoted 3 times

us3r 3 years, 2 months ago
w10 only
upvoted 4 times

Question #39 *Topic 1*

Your company has a Microsoft 365 subscription that contains the domains shown in the following table.

Name	Can enroll devices to Microsoft Endpoint Manager by using auto-discovery
Contoso.com	Yes
Contoso.onmicrosoft.com	Yes

The company plans to add a custom domain named fabrikam.com to the subscription, and then to enable enrollment of devices to Endpoint Manager by using auto-discovery for fabrikam.com.

You need to add a DNS record to the fabrikam.com domain to enable device enrollment by using auto-discovery.

Which record type should you use for the new record?

A. PTR

B. SRV

C. CNAME

D. TXT

Suggested Answer: *C*

Reference:

https://docs.microsoft.com/en-us/mem/intune/enrollment/windows-enroll#simplify-windows-enrollment-without-azure-ad-premium

Community vote distribution

C (100%)

Jake1 Highly Voted 3 years, 9 months ago

C is correct.To simplify enrollment, create a domain name server (DNS) alias (CNAME record type) that redirects enrollment requests to Intune servers. Otherwise, users trying to connect to Intune must enter the Intune server name during enrollment.

upvoted 19 times

Prianishnikov Highly Voted 3 years, 9 months ago

C. CNAME

upvoted 8 times

Ayham_J Most Recent 1 year, 9 months ago

On exam 4/1/2023

upvoted 1 times

Goshler 2 years, 2 months ago

Selected Answer: C

C for sure.

upvoted 1 times

L33D 2 years, 6 months ago

Still valid, on exam Jun 25, 2022

upvoted 4 times

gxsh 3 years ago

For auto-discover are used CNAMs.

upvoted 2 times

us3r 3 years, 2 months ago

(C)NAME

upvoted 5 times

Mujja 1 year, 6 months ago

Nice, just like your us3rname :)

upvoted 1 times

airairo 3 years, 7 months ago

The answer is C. CNAME

https://docs.microsoft.com/en-us/mem/intune/enrollment/windows-enroll

upvoted 6 times

kiketxu 3 years, 8 months ago

This is correct

upvoted 5 times

Question #40 *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.
Your network contains an on-premises Active Directory domain. The domain contains 2,000 computers that run Windows 8.1 and have applications installed as shown in the following table.

Name	Application count	Used by
App1	20	Finance department, sales department
App2	100	Marketing department

You enroll all the computers in Upgrade Readiness.
You need to ensure that App1 and App2 have an UpgradeDecision status of Ready to upgrade.
Solution: You set the ReadyForWindows status of App2 to Highly adopted.
Does this meet the goal?

A. Yes

B. No

Suggested Answer: *A*
App1 has a ı€low install countı€ (2% or less) so will be Ready to upgrade. We just need to change the setting for App2.
References:
https://docs.microsoft.com/en-us/windows/deployment/upgrade/upgrade-readiness-identify-apps

Community vote distribution
B (100%)

slaoui Highly Voted 3 years, 8 months ago
the answer is B
You cannot change the adoption status of an application.

https://docs.microsoft.com/en-us/mem/configmgr/desktop-analytics/compat-assessment

"The Adoption Status is based on information from commercial devices that share data with Microsoft"
upvoted 11 times

Jake1 Highly Voted 3 years, 9 months ago
Answer is NO. App 2 needs to set to "Low Install Count" since it's use is 5%, higher than the standard threshold of 2% to be considered low enough to be ready for upgrade. See Page 10 for correct answer and explanation. https://docs.microsoft.com/en-us/mem/configmgr/desktop-analytics/create-deployment-plans
upvoted 10 times

lucidgreen 3 years, 6 months ago
https://docs.microsoft.com/en-us/mem/configmgr/desktop-analytics/create-deployment-plans#readiness-rules
upvoted 2 times

Srle 3 years, 9 months ago
Can you please elaborate? This option can be set between 0 and 10% and it is within this range (120), this is all "standard threshold" how come is no longer ready for upgrade?
upvoted 1 times

wwwhogmxnet 1 year, 8 months ago
The Adoption Status is based on information from commercial devices that share data with Microsoft. The status is integrated with support statements from software vendors.

Desktop Analytics provides the adoption status for each version of an asset found in commercial devices. This status doesn't include data from consumer devices or devices that don't share data. The status may not be representative of the adoption rate across all Windows 10

devices.
https://learn.microsoft.com/en-us/mem/configmgr/desktop-analytics/compat-assessment#ready-for-windows
upvoted 1 times

NitishKarmakar Most Recent 1 year, 6 months ago
Desktop Analytics is deprecated so I believe this question is no longer valid.
"Desktop Analytics is deprecated and will be retired on November 30, 2022. For more information, see What's new."
https://learn.microsoft.com/en-us/mem/configmgr/desktop-analytics/overview
upvoted 3 times

Feyenoord 1 year, 8 months ago
Desktop analytics is deprecated in November 2022
upvoted 2 times

DCT 2 years, 1 month ago
jialat, answer is B man~
upvoted 1 times

KrokodilBLUEZZ 2 years, 10 months ago
Selected Answer: B
You can't set highly adopted manually. You can instead raise installations count bar to 10%(max) to skip both apps checks.
upvoted 6 times

jeff1988 2 years, 11 months ago
Selected Answer: B
NO is here the answer you should set it on Low instance count. See page 10 wit the correct answer!
upvoted 3 times

OneplusOne 2 years, 12 months ago
Answer is NO:
Highly Adopted is is not a value you can apply yourself.

'Highly adopted: At least 100,000 commercial Windows 10 devices have installed this app.'
upvoted 2 times

Storm 3 years ago
I do not think you can change the adoption status: I would go for NO

The Adoption Status is based on information from commercial devices that share data with Microsoft. The status is integrated with support statements from software vendors.

Desktop Analytics provides the adoption status for each version of an asset found in commercial devices. This status doesn't include data from consumer devices or devices that don't share data. The status may not be representative of the adoption rate across all Windows 10 devices.
https://docs.microsoft.com/en-us/mem/configmgr/desktop-analytics/compat-assessment
upvoted 1 times

riahisami77 3 years ago
Aswer is YES: i was confused at first, i looked at MS doc and the comment here but after reading this artcle every thing become clear for me now about readiness status
https://thewindowsupdate.com/2018/04/30/introducing-a-more-efficient-way-to-review-low-risk-applications-and-drivers/
upvoted 2 times

PersonT 3 years, 9 months ago
Is that possible?
Believe you filter apps ReadyForWindows status of "Highly adopted": From here, you can bulk select the results, select "Ready to upgrade", and click save. This will mark all apps meeting this criterion "Ready to upgrade" and no further validation is required.
upvoted 1 times

Rens19991 3 years, 9 months ago
NO is here the answer you should set it on Low instance count. See page 10 wit the correct answer!
upvoted 2 times

GeraldB 3 years, 9 months ago
You are correct! answer here is NO
upvoted 2 times

Question #41 *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.
Your network contains an on-premises Active Directory domain. The domain contains 2,000 computers that run Windows 8.1 and have applications installed as shown in the following table.

Name	Application count	Used by
App1	20	Finance department, sales department
App2	100	Marketing department

You enroll all the computers in Upgrade Readiness.
You need to ensure that App1 and App2 have an UpgradeDecision status of Ready to upgrade.
Solution: You set the Importance status of App1 to Business critical.
Does this meet the goal?

A. Yes

B. No

Suggested Answer: *B*
Business Critical will prevent the app having a status of Ready to upgrade.
References:
https://docs.microsoft.com/en-us/windows/deployment/upgrade/upgrade-readiness-identify-apps

Community vote distribution
B (100%)

MiZi Highly Voted 3 years, 7 months ago
If you mark an app as not important, Desktop Analytics automatically sets it to Ready to upgrade
https://docs.microsoft.com/en-us/mem/configmgr/desktop-analytics/about-deployment-plans#importance
upvoted 7 times

NitishKarmakar Most Recent 1 year, 6 months ago
Desktop analytics has been deprecated hence this question may not be valid for the exam anymore.
"Desktop Analytics is deprecated and will be retired on November 30, 2022. For more information, see What's new."
https://learn.microsoft.com/en-us/mem/configmgr/desktop-analytics/overview
upvoted 1 times

petersonal 1 year, 10 months ago
Selected Answer: B
The answer is B, but the given explanation is senseless. Just need to read the references what is liked to these type of questions.
The "solution" is saying you set the importance of App1 to business critical.

"If you mark one as critical or important, Desktop Analytics includes in the pilot deployment some devices with that app. The service includes in the pilot more instances of a critical app."
Nothing more.

Also App1 is installed only 1% (2000/20) on the PC-s.
"If an app is installed on less than 2% of the targeted devices, it's marked Low install count. (...) Desktop Analytics automatically marks these apps as Ready to upgrade."

Reference: https://learn.microsoft.com/en-us/mem/configmgr/desktop-analytics/about-deployment-plans#importance

So App1 is fine, and the given solution achieves nothing.
upvoted 2 times

otday 3 years, 6 months ago

App1 is already set to Ready to upgrade as it already meets the low install count due to sitting at 1%.
Answer No is correct
upvoted 4 times

Jake1 3 years, 9 months ago
No is the correct answer. It needs to be set to low install count.https://docs.microsoft.com/en-us/mem/configmgr/desktop-analytics/create-deployment-plans
upvoted 4 times

Prianishnikov 3 years, 9 months ago
I think - B. No
upvoted 3 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.

Your network contains an on-premises Active Directory domain. The domain contains 2,000 computers that run Windows 8.1 and have applications installed as shown in the following table.

Name	Application count	Used by
App1	20	Finance department, sales department
App2	100	Marketing department

You enroll all the computers in Upgrade Readiness.

You need to ensure that App1 and App2 have an UpgradeDecision status of Ready to upgrade.

Solution: You set the ReadyForWindows status of App1 to Highly adopted.

Does this meet the goal?

A. Yes

B. No

Suggested Answer: *B*

App1 has a ı€low install countı€ (2% or less) so will be Ready to upgrade. We need to change the setting for App2.

References:

https://docs.microsoft.com/en-us/windows/deployment/upgrade/upgrade-readiness-identify-apps

Community vote distribution

B (100%)

Prianishnikov Highly Voted 3 years, 9 months ago

I think - B. No

upvoted 10 times

MiZi Highly Voted 3 years, 7 months ago

https://docs.microsoft.com/en-us/mem/configmgr/desktop-analytics/about-deployment-plans#importance

If an app is installed on less than 2% of the targeted devices, it's marked Low install count. Two percent is the default value. You can adjust the threshold in the readiness settings from 0% to 10%. Desktop Analytics automatically marks these apps as Ready to upgrade.

upvoted 5 times

Dolhave2 Most Recent 2 years, 6 months ago

Selected Answer: B

You can not change the adoption readyness for an application.

upvoted 5 times

Sprinqfield 3 years, 4 months ago

the answer is B

You cannot change the adoption status of an application.

https://docs.microsoft.com/en-us/mem/configmgr/desktop-analytics/compat-assessment

"The Adoption Status is based on information from commercial devices that share data with Microsoft"

upvoted 4 times

Question #43 *Topic 1*

HOTSPOT -

You have 100 computers that run Windows 8.1 and are enrolled in Upgrade Readiness.

Two of the computers are configured as shown in the following table.

Name	Architecture	Memory	Applications installed
Computer1	64-bit	1 GB	App1
Computer2	32-bit	2 GB	App2

From Upgrade Readiness, you view the applications shown in the following table.

Name	UpgradeDecision
App1	Ready to upgrade
App2	Review in progress

You enroll a computer named Computer3 in Upgrade Readiness. Computer3 has the following configurations:

- 8 GB of memory
- 64-bit architecture
- An application named App3 installed

App3 is installed on Computer3 only.

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
Computer1 has an UpgradeDecision status of Ready to upgrade.	○	○
Computer2 has an UpgradeDecision status of Ready to upgrade.	○	○
Computer3 has an UpgradeDecision status of Ready to upgrade.	○	○

Suggested Answer:

Answer Area

Statements	Yes	No
Computer1 has an UpgradeDecision status of Ready to upgrade.	○	○
Computer2 has an UpgradeDecision status of Ready to upgrade.	○	○
Computer3 has an UpgradeDecision status of Ready to upgrade.	○	○

Ceuse Highly Voted 3 years, 8 months ago

No No Yes is Correct - App 3 is only installed on one Computer, therefor its marked low install count (1% is less then the default threshold of 2%)

upvoted 27 times

otday 3 years, 6 months ago

Correct

upvoted 3 times

Jake1 Highly Voted 3 years, 9 months ago

Computer 1 - No - Does not have enough RAM

Computer 2 - No - App2 not ready

Computer 3 - No - The inventory data for that device is incomplete and Desktop Analytics can't do a full compatibility assessment, therefor it will cause a Blocked Windows upgrade decision. https://docs.microsoft.com/en-us/mem/configmgr/desktop-analytics/about-deployment-plans.

upvoted 11 times

otday 3 years, 6 months ago

WDYM? the inventory data for computer 3 is complete?

This meets Read to Upgrade standards.

upvoted 1 times

Requi3m 3 years, 5 months ago

"The inventory data for that device is incomplete and Desktop Analytics can't do a full compatibility assessment" causes a "Blocked" status, but this is after a scan on the computer has been done and couldn't collect all necessary data. So Computer 3 should be a Yes.

upvoted 6 times

donathon 3 years, 8 months ago

RAM: 1 gigabyte (GB) for 32-bit or 2 GB for 64-bit. https://support.microsoft.com/en-us/windows/windows-10-system-requirements-6d4e9a79-66bf-7950-467c-795cf0386715

upvoted 6 times

ServerBrain Most Recent 2 years, 1 month ago

The answer is correct.

Here, do not be misled by the Apps status, it's the Computer resources that count of which Computer 3 is the only one ready..

upvoted 2 times

TimurKazan 3 years ago

No No Yes

upvoted 1 times

Fcnet 3 years, 5 months ago

should be No No No as ready status for app3 is not yet known

device 1 is not compliante / not ready

device is compliante/ready but app2 not yet

and device 3 is ready but app3 is not yet known

upvoted 1 times

Prianishnikov 3 years, 9 months ago

This answer is correct?

upvoted 2 times

Question #44 *Topic 1*

Your network contains an on-premises Active Directory domain that syncs to Azure Active Directory (Azure AD).
The domain contains two servers named Server1 and Server2 that run Windows Server 2016. Server1 has the File Server Resource Manager role service installed.
You need to configure Server1 to use the Azure Rights Management (Azure RMS) connector.
You install the Microsoft Management connector on Server1.
What should you do next on Server1?

A. Run the GenConnectorConfig.ps1 script.

B. Configure the URL of the AIPMigrated group.

C. Enable BitLocker Drive Encryption (BitLocker).

D. Install a certification authority (CA).

Suggested Answer: *A*
If you want to use the server configuration tool for the RMS connector, to automate the configuration of registry settings on your on-premises servers, download and run the GenConnectorConfig.ps1 script.
References:
https://docs.microsoft.com/en-us/azure/information-protection/install-configure-rms-connector#installing-the-rms-connector

Community vote distribution
A (100%)

Eltooth Highly Voted 3 years, 7 months ago
RMS is no longer in use as of April 1st 2021. AIP now default.
upvoted 9 times

Jake1 Highly Voted 3 years, 9 months ago
Correct answer is A but not sure this is still in use. https://docs.microsoft.com/en-us/azure/information-protection/deploy-rms-connector
upvoted 8 times

psp65 Most Recent 2 years ago
Correct answer is A (https://learn.microsoft.com/en-us/azure/information-protection/install-configure-rms-connector#installing-the-rms-connector)
upvoted 1 times

us3r 3 years ago
Selected Answer: A
A but... AIP now rules
upvoted 5 times

TimurKazan 3 years, 1 month ago
https://docs.microsoft.com/en-us/azure/information-protection/install-configure-rms-connector
upvoted 1 times

otday 3 years, 6 months ago
I don't think that this is relevant to MS-101 exam
upvoted 4 times

Prianishnikov 3 years, 9 months ago
A. Run the GenConnectorConfig.ps1 script.
upvoted 2 times

kazaki 3 years, 11 months ago
RMS Is deprecated and AIP is also deprecated
upvoted 3 times

allesglar 3 years, 1 month ago
Nothing is true from what you say. Do some research first!
upvoted 1 times

kiketxu 3 years, 8 months ago

Please that's not true. Deprecated is the AIP classic client and label creation/editing from the AIP Azure portal. Everything related RMS (connector included) and AIP Unified client and portal are the base for sensitivity and protection labels.

upvoted 5 times

Question #45 *Topic 1*

Your company has a Microsoft Azure Active Directory (Azure AD) tenant named contoso.com.
You sign up for Microsoft Store for Business.
The tenant contains the users shown in the following table.

Name	Microsoft Store for Business role	Azure AD role
User1	Purchaser	*None*
User2	Basic Purchaser	*None*
User3	*None*	Application administrator
User4	*None*	Cloud application administrator

Microsoft Store for Business has the following Shopping behavior settings:
✑ Make everyone a Basic Purchaser is set to Off.
✑ Allow app requests is set to On.
You need to identify which users can add apps to the Microsoft Store for Business private store.
Which users should you identify?

A. User1 and User2 only

B. User3 only

C. User1 only

D. User3 and User4 only

Suggested Answer: *A*

Community vote distribution

C (77%) A (23%)

Goseu Highly Voted 3 years, 7 months ago
The answer is Correct A . Both User1 and User2
Basic Purchaser is available in both MS Store for Education and Business
upvoted 23 times

lucidgreen 3 years, 5 months ago
Also, see the following NOTE:
https://docs.microsoft.com/en-us/microsoft-store/microsoft-store-for-business-overview#set-up
upvoted 1 times

FreddyLao 3 years ago
yes. I can find Basic Purchaser role to be available in my company MS Store for Business.
Answer is A.
upvoted 1 times

KSvh53 2 years, 9 months ago
lucidgreen that link you provided is great, but don't miss the note. "Currently, the Basic purchaser role is only available for schools using Microsoft Store for Education. For more information, see Microsoft Store for Education permissions." So correct answer is C.
upvoted 4 times

prabhjot 1 year, 8 months ago
Currently, the Basic purchaser role is only available for schools using Microsoft Store for Education. For more information, see Microsoft Store for Education permissions. (so ans is User1) - https://learn.microsoft.com/en-us/microsoft-store/microsoft-store-for-business-overview#set-up
upvoted 5 times

amymay101 Highly Voted 3 years ago
Selected Answer: C
Basic purchaser cannot add apps to the private store. Confirmed in my test tenant
upvoted 10 times

JT19760106 2 years, 11 months ago
Same results here. Basic purchaser can request an app and that's about it.

upvoted 1 times

edzio 2 years, 9 months ago

What about Purchaser role, it can add to app to apps to the private store?

upvoted 1 times

Debadatta Most Recent 1 year, 6 months ago

Selected Answer: C

Correct answer is C

Currently, the Basic purchaser role is only available for schools using Microsoft Store for Education.

https://learn.microsoft.com/en-us/microsoft-store/microsoft-store-for-business-overview#set-up

upvoted 1 times

Meebler 1 year, 10 months ago

No, a basic purchaser in the Microsoft Store for Business cannot add apps to the store. Only users with the "Admin" or "Product Purchaser" roles can add apps to the store.

The basic purchaser role in the Microsoft Store for Business allows the user to purchase apps for the organization, but they do not have permission to manage or publish apps in the store. They can only install apps that have already been added to the store by an admin or product purchaser.

upvoted 2 times

kimble3k 1 year, 11 months ago

Selected Answer: C

A because this https://learn.microsoft.com/en-us/microsoft-store/microsoft-store-for-business-overview#set-up states in the note that "Basic purchaser role is only available for schools using Microsoft Store for Education"

upvoted 3 times

kimble3k 1 year, 11 months ago

C is the correct answer

upvoted 1 times

ServerBrain 2 years, 1 month ago

Selected Answer: C

Please note the difference between these two settings:

Allow app requests is set to On.

Allow users to shop is set to On.

Explanation:

Make everyone a Basic Purchaser is set to Off.

Allow users to shop controls the shopping experience in Microsoft Store for Education. When this setting is on, Purchasers and Basic Purchasers can purchase products and services from Microsoft Store for Education.

In this question it's only the setting: Allow app requests is set to On.

upvoted 3 times

TechMinerUK 2 years, 2 months ago

Selected Answer: A

I know there are alot of people here stating that Basic Purchaser is only available on Education tenants and I know that numerous pieces of Microsoft documentation also backs up those comments however I have just checked my tenant and we have both "Purchaser" and "Basic Purchaser" available to assign to users, both roles of which have the ability to purchase apps from the Microsoft Store.

As such I believe A is the answer since both roles can acquire new apps

upvoted 1 times

TechMinerUK 2 years, 1 month ago

I will revise my answer as after further investigation whilst you can "Request" an app with the Basic Purchaser role assigned on a Business tenant you are unable to actually purchase and assign an app without the standard "Purchaser" role

This means Answer C is correct, it may differ on educational tenants

upvoted 1 times

k9_bern_001 2 years, 4 months ago

The questions is asking MS store for Business not MS Store for education, MS store for business does not have basic purchaser role. So the correct answer is C, purchaser only https://docs.microsoft.com/en-us/microsoft-store/microsoft-store-for-business-overview

upvoted 4 times

L33D 2 years, 6 months ago

Still valid, on exam Jun 25, 2022

upvoted 1 times

Dolhave2 2 years, 6 months ago

Selected Answer: A

I don't care what the article says. It is outdated.

I have Basic Purchaser active in my MS Store for Business.

upvoted 2 times

Dolhave2 2 years, 6 months ago

Selected Answer: A

I can add Basic Purchaser in my ms store for business.

upvoted 1 times

Rickert 2 years, 8 months ago

Selected Answer: A

A is correct

upvoted 1 times

KSvh53 2 years, 9 months ago

Selected Answer: A

I don't know how recent this was changed, but currently, as of 4/5/2022, both purchaser and basic purchaser can acquire apps for business or for education. So anyone saying C is now wrong. Answer is A. It tells you that exactly in this link here:

https://docs.microsoft.com/en-us/microsoft-store/microsoft-store-for-business-overview#set-up

upvoted 1 times

KSvh53 2 years, 9 months ago

And I stand corrected. That link also says "Currently, the Basic purchaser role is only available for schools using Microsoft Store for Education. For more information, see Microsoft Store for Education permissions." So correct answer is C after all.

upvoted 4 times

JamesM9 2 years, 9 months ago

Currently, the Basic purchaser role is only available for schools using Microsoft Store for Education. Since this question is in relation to the Store for Business private store, the answer is C - User 1 only.

https://docs.microsoft.com/en-us/microsoft-store/microsoft-store-for-business-overview

upvoted 1 times

Jeff8989 2 years, 11 months ago

Currently, the Basic purchaser role is only available for schools using Microsoft Store for Education.

https://docs.microsoft.com/en-us/microsoft-store/microsoft-store-for-business-overview#set-up

upvoted 1 times

ubt 2 years, 11 months ago

Selected Answer: A

Purchaser can assign access to all purchased apps.

Basic Purchaser is only able to assign access to apps they have purchased.

So both can assign apps

upvoted 1 times

us3r 3 years ago

Selected Answer: C

siuuuuuu

upvoted 3 times

Question #46 *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.

Your network contains an on-premises Active Directory domain. The domain contains 2,000 computers that run Windows 8.1 and have applications installed as shown in the following table.

Name	Application count	Used by
App1	20	Finance department, sales department
App2	100	Marketing department

You enroll all the computers in Upgrade Readiness.

You need to ensure that App1 and App2 have an UpgradeDecision status of Ready to upgrade.

Solution: You set the importance status of App2 to Low install count.

Does this meet the goal?

A. Yes

B. No

Suggested Answer: *A*

If an app is installed on less than 2% of the targeted devices, it's marked Low install count. Two percent is the default value. You can adjust the threshold in the readiness settings from 0% to 10%. Desktop Analytics automatically marks these apps as Ready to upgrade.

Reference:

https://docs.microsoft.com/en-us/configmgr/desktop-analytics/about-deployment-plans

Community vote distribution

Jake1 Highly Voted 3 years, 9 months ago

I think YES too. App 1 already meets the 2% threshold so you have to manually change it for App 2 since its currently at 5%.

The apps that Desktop Analytics show as noteworthy are based on the low install count threshold. Set this threshold in the readiness rules for the deployment plan. By default, this threshold is 2.0%. You can change the value from 0.0 to 10.0. https://docs.microsoft.com/en-us/mem/configmgr/desktop-analytics/create-deployment-plans.

upvoted 10 times

LoremanReturns Highly Voted 3 years, 5 months ago

I think NO.

"Low install count" is not available as "Importance Status"

Importance can be set as:

Critical

Important

Ignore

Not reviewed

Not important

https://docs.microsoft.com/en-us/mem/configmgr/desktop-analytics/about-assets#apps

upvoted 7 times

gkp_br 3 years, 5 months ago

I agree. Or they are using the wrong expression in this simulate. We need to pay attention in the exam.

upvoted 1 times

ChizzyO Most Recent 1 year, 6 months ago

This is tricky but I think we should just look at the part of the question where it says the apps need to have the UpgradeDecisionStatus of ReadyToUpgrade.

From Microsoft Learn https://learn.microsoft.com/en-us/mem/configmgr/desktop-analytics/about-deployment-plans

If an app is installed on less than 2% of the targeted devices, it's marked Low install count. Two percent is the default value. You can adjust the threshold in the readiness settings from 0% to 10%. Desktop Analytics automatically marks these apps as Ready to upgrade.

For apps, choose an importance of Critical, Important, or Not important. If you mark one as critical or important, Desktop Analytics includes in the pilot deployment some devices with that app. The service includes in the pilot more instances of a critical app. If you mark an app as not important, Desktop Analytics automatically sets it to Ready to upgrade.

upvoted 1 times

us3r 3 years ago

Selected Answer: A

tough one

upvoted 6 times

Requi3m 3 years, 5 months ago

The solution is weirdly formulated. It's a YES if they mean the solution is to set the Low Install Count thresshold to a higher percentage. This would result in a change of the importance status of App2. This is a nasty question...

upvoted 6 times

lucidgreen 3 years, 8 months ago

Interesting that the explanation of the answer says that this isn't a complete solution, though it is on the right track. I'm not sure what to think of this. It seems half the solution because you still need to raise the threshold to at least 5%.

upvoted 2 times

Prianishnikov 3 years, 9 months ago

I think YES

upvoted 1 times

Question #47 *Topic 1*

You have two conditional access policies named Policy1 and Policy2.
Policy1 has the following settings:
✑ Assignments:
- Users and groups: User1
- Cloud apps or actions: Office 365 Exchange Online
- Conditions: 0 conditions selected
✑ Access controls:
- Grant: Grant access
- Session: 0 controls selected
✑ Enable policy: On
Policy2 has the following settings:
✑ Assignments:
- Users and groups: User1
- Cloud apps or actions: Office 365 Exchange Online
- Conditions: 0 conditions selected
✑ Access controls:
- Grant: Block access
- Session: 0 controls selected
✑ Enable policy: On
You need to ensure that User1 can access Microsoft Exchange Online only from devices that are marked as compliant.
What should you do?

A. Modify the Grant settings of Policy2.

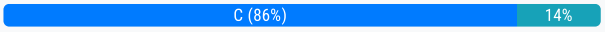
B. Disable Policy2.

C. Modify the Conditions settings of Policy2.

D. Modify the Grant settings of Policy1.

Suggested Answer: *C*

Community vote distribution



techtest848 Highly Voted 3 years, 1 month ago
When two CA policies apply to an object, Block rule takes priority over Grant rule. In order to achieve the desired outcome, Policy 2 conditions will have to be edited. Block All but Exclude Devices Marked as Compliant. The give answer (C) is correct.
upvoted 21 times

prabhjot 1 year, 8 months ago
https://danielchronlund.com/2018/11/23/how-multiple-conditional-access-policies-are-applied/ (when both are present teh Block CA wins over Grant CA policy) so Ans is to modify the Polict 2
upvoted 1 times

owenMS Most Recent 1 year, 11 months ago
Selected Answer: C
C. Exclude/block takes priority over allow/grant rules.
upvoted 1 times

ovd 1 year, 11 months ago
D - Grant and "Require device to be market as compliant"
so
pol 1 - Grant for compliant only, after them
pol 2 - Block for all
upvoted 1 times

KrisDeb 2 years, 1 month ago
Selected Answer: C

C - only GRANT has 'Require device to be marked as compliant'
upvoted 2 times

TechMinerUK 2 years, 2 months ago

Selected Answer: A

Whilst C is correct as you could change the "Grant" requirement to be something such as require MFA the question seems unclear as Policy1 would allow the user to access if Policy2 wasn't present. Having said that Policy1 is missing a grant access requirement entirely which isn't possible in AzureAD Conditional Access as Grant requires at least one requirement to be present in the policy
upvoted 1 times

KrisDeb 2 years, 1 month ago

You are right - Policy 1 wouldn't exist.
'You must configure either the "Grant" or "Session" section' error.
upvoted 2 times

k9_bern_001 2 years, 4 months ago

C is correct
upvoted 2 times

L33D 2 years, 6 months ago

Still valid, on exam Jun 25, 2022
upvoted 3 times

JT19760106 2 years, 11 months ago

Policy 2 would take precedence because of the conflict with Policy 1 and having the block condition.
Requiring a compliant device can be done with either:
Condition -> Device State -> Exclude Device Marked as Compliant
Or
Grant -> Require device to be marked as compliant

Since the question states Grant is Block, then that would make C the logical answer
upvoted 4 times

Bulldozzer 2 years, 10 months ago

This condition is being depreciated. Now you should use "Filter for devices" condition.
upvoted 1 times

ubt 2 years, 11 months ago

Selected Answer: C

Block always wins, so need to change Policy 2 to exclude "Devices as compliant"
upvoted 3 times

[Removed] 3 years ago

Ambiguous question... You can't even create a policy with "Grant access" without selecting a grant or session control so Policy1 makes no sense! If you try it in a tenant, you can not save the policy. The easiest way would seem to add "Require device to be compliant" to the grant controls in Policy1. Since Policy2 blocks, it will take precedence so you would need to disable that policy as well. Following that logic, the answer would be to choose B and D. However, you could also modify the grant controls on Policy2 from "Block access" to "Grant access" with "Require device to be masked as compliant". That would mean Answer A, but you still have Policy1 that makes no sense!
upvoted 3 times

Goena 3 years ago

C. Modify the Conditions settings of Policy2: Exclude "Devices as compliant"
upvoted 3 times

Flacky_Penguin32 3 years, 3 months ago

https://docs.microsoft.com/en-us/azure/active-directory/conditional-access/require-managed-devices#require-hybrid-azure-ad-joined-devices
upvoted 3 times

DiscGolfer 3 years, 2 months ago

I think the answer is A(link above that Flacky posted explains)
upvoted 2 times

Flacky_Penguin32 3 years, 3 months ago

Specifically, take note of the exclude section under Device State
upvoted 1 times

Flacky_Penguin32 3 years, 3 months ago

This is enforced via the Device State in the Assignments > Conditions, but is set as a control in the Access Controls > Grant via "Require device to be marked as compliant". Should note, this needs to have a device compliance policy in Intune setup.

upvoted 1 times

F_M 3 years, 4 months ago

By the way, a policy like the first one can't be created in Azure! It forces you to select a session control or a condition for granting the access. The last one can be set both under grant access (for example, grant access but require device marked as compliant) and in the condition panel.

upvoted 3 times

Question #48 *Topic 1*

You have a Microsoft 365 E5 subscription that uses an Azure Active Directory (Azure AD) tenant named contoso.com.
You need to ensure that users can enroll devices in Microsoft Endpoint Manager without manually entering the address of Microsoft Endpoint Manager.
Which two DNS records should you create? Each correct answer presents part of the solution.
NOTE: Each correct selection is worth one point.

A. a CNAME record for AutoDiscover.contoso.com

B. a CNAME record for EnterpriseEnrollment.contoso.com

C. a TXT record for EnterpriseRegistration.contoso.com

D. an SRV record for _SIP._TLS.contoso.com

E. an SRV record for _SIPfederationTLS.contoso.com

F. a CNAME record for EnterpriseRegistration.contoso.com

G. a TXT record for EnterpriseEnrollment.contoso.com

Suggested Answer: *BF*
Reference:
https://docs.microsoft.com/en-us/mem/intune/enrollment/windows-enroll#simplify-windows-enrollment-without-azure-ad-premium

Community vote distribution
BF (100%)

Jake1 Highly Voted 3 years, 9 months ago
Given answers are Correct. Need CNAME records for EnterpriseEnrollment and EnterpriseRegistration.
upvoted 23 times

NikPat3125 Highly Voted 3 years, 5 months ago
came in exam 27.07.2021
upvoted 9 times

agnesmandriva Most Recent 1 year, 9 months ago
Selected Answer: BF
Correct
upvoted 2 times

Madskillz13 2 years, 4 months ago
Still a valid question. Featured in my exam August 2022
upvoted 7 times

Glorence 2 years, 11 months ago
still valid, it was in my exam last feb 5, 2022
upvoted 4 times

Flacky_Penguin32 3 years, 3 months ago
B & F are correct.
upvoted 4 times

Eltooth 3 years, 8 months ago
Agreed B &F
upvoted 4 times

Hani_Ajaj 3 years, 9 months ago
Provided answer is correct.
upvoted 3 times

Prianishnikov 3 years, 9 months ago
Yes, I also agree
upvoted 3 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.
Your network contains an on-premises Active Directory domain. The domain contains domain controllers that run Windows Server 2019. The functional level of the forest and the domain is Windows Server 2012 R2.
The domain contains 100 computers that run Windows 10 and a member server named Server1 that runs Windows Server 2012 R2.
You plan to use Server1 to manage the domain and to configure Windows 10 Group Policy settings.
You install the Group Policy Management Console (GPMC) on Server1.
You need to configure the Windows Update for Business Group Policy settings on Server1.
Solution: You raise the forest functional level to Windows Server 2016. You copy the Group Policy Administrative Templates from a Windows 10 computer to the
Netlogon share on all the domain controllers.
Does this meet the goal?

A. Yes

B. No

Suggested Answer: *B*

JMG73 Highly Voted 4 years, 2 months ago
I stick with the answer.

B. No

In order to configure the Windows Update for Business Group Policy settings on Server1, we can...

...copy the templates files to the C:\Windows\PolicyDefinitions folder on Server1.
...implement a central store and provision the template files in the central store.
...upgrade Server1 to Windows Server 2019.
upvoted 10 times

dexter56 Highly Voted 4 years, 4 months ago
No, it should be copied to the PolicyDefinitions folder, which should be located in the SYSVOL-share:
https://support.microsoft.com/en-us/help/3087759/how-to-create-and-manage-the-central-store-for-group-policy-administra
upvoted 7 times

bleroblero Most Recent 1 year, 8 months ago
Was in exam on 2 May 2023
upvoted 2 times

veteran_tech 2 years, 4 months ago
Group Policy templates manually copied to a DC's SYSVOL share -- man! talk about taking us back in time...
upvoted 2 times

OneplusOne 2 years, 12 months ago
No.

Functional level 2016 requires that all DC's are at least WinSrV2016.
https://docs.microsoft.com/en-us/windows-server/identity/ad-ds/active-directory-functional-levels
upvoted 1 times

OneplusOne 2 years, 12 months ago
Whoops Dc's are 2019 according to the question. Still No.
upvoted 1 times

Flacky_Penguin32 3 years, 3 months ago

admx = \\contoso.com\SYSVOL\contoso.com\policies\PolicyDefinitions

adml = \\contoso.com\SYSVOL\contoso.com\policies\PolicyDefinitions\en-us

upvoted 2 times

lucidgreen 3 years, 5 months ago

There are no forest functional level requirements for this feature.

The Windows policy templates must copied to the domain SYSVOL.

The policies in GPMC are magically available as they are brought down from the SYSVOL, so long as the policies exist in the SYSVOL.

Policies have been available since Windows 10 1607.

I can apply these policies from a domain running 2012 R2 domain controllers only, I believe. I may have had on 2016 domain controller by the time I noticed this policy. So the only requirement is to have the appropriate Windows 10 policy templates in the domain policy share (usually SYSVOL).

upvoted 3 times

lucidgreen 3 years, 5 months ago

I've also been able to manage this policy from GPMC from Server 2012 R2.

upvoted 2 times

donathon 3 years, 8 months ago

https://support.microsoft.com/en-us/topic/an-update-is-available-to-enable-the-use-of-local-admx-files-for-group-policy-editor-24ea6900-fa03-d53f-c666-199e5ac02be9

upvoted 1 times

Jake1 3 years, 9 months ago

\\contoso.com\SYSVOL\contoso.com\policies\PolicyDefinitions. A PolicyDefinitions directory needs to be created in SYSVOL and the templates needs to be placed in there.

upvoted 2 times

PattiD 4 years ago

SYSVOL SHARE

upvoted 2 times

PattiD 4 years ago

SYSVOL SHARE

upvoted 2 times

PattiD 4 years ago

Copy the templates files to the C:\Windows\PolicyDefinitions folder on Server1.

Upgrade Server1 to Windows Server 2019.

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.
Your network contains an on-premises Active Directory domain. The domain contains domain controllers that run Windows Server 2019. The functional level of the forest and the domain is Windows Server 2012 R2.
The domain contains 100 computers that run Windows 10 and a member server named Server1 that runs Windows Server 2012 R2.
You plan to use Server1 to manage the domain and to configure Windows 10 Group Policy settings.
You install the Group Policy Management Console (GPMC) on Server1.
You need to configure the Windows Update for Business Group Policy settings on Server1.
Solution: You copy the Group Policy Administrative Templates from a Windows 10 computer to Server1.
Does this meet the goal?

A. Yes

B. No

Suggested Answer: *A*

Community vote distribution

A (50%) B (50%)

us3r Highly Voted 3 years ago

Selected Answer: B

NO
the answer WOULD BE 'yes' if the Server1 was a Doco...
upvoted 15 times

us3r Highly Voted 3 years, 2 months ago

Answer: NO
Server is not a Domain Controller.
upvoted 11 times

Kevinfm_81 2 years, 6 months ago

Wondering if this is implied in the question though? Member server can obv be promoted to DC using the AD DS promo wizard. Funny thing is that from what I've heard DCPROMO stops working at a concerning rate when NetBIOS/TCP IP is disabled on 12R2
upvoted 2 times

vanr2000 Most Recent 1 year, 8 months ago

Selected Answer: B

Server1 is not a Domain Controller, is a member server.

To create a Central Store for .admx and .adml files, create a new folder named PolicyDefinitions in the following location (for example) on the domain controller:

\\contoso.com\SYSVOL\contoso.com\policies\PolicyDefinitions

When you already have such a folder that has a previously built Central Store, use a new folder describing the current version such as:

\\contoso.com\SYSVOL\contoso.com\policies\PolicyDefinitions-1803

Copy all files from the PolicyDefinitions folder on a source computer to the new PolicyDefinitions folder on the domain controller
---
https://learn.microsoft.com/en-US/troubleshoot/windows-client/group-policy/create-and-manage-central-store
upvoted 3 times

ahmedkmicha 1 year, 9 months ago

Selected Answer: A

The Administrative Templates contain the Group Policy settings that can be configured for Windows 10 devices, including the Windows Update for Business settings. By copying the latest version of the Administrative Templates for Windows 10 to Server1, you can configure and manage the Windows Update for Business Group Policy settings from Server1 using the Group Policy Management Console.

upvoted 3 times

mfaisal786 1 year, 9 months ago

Selected Answer: A

You need to upgrade your group policy templates and you then need to manage GPO's from a Windows 10 desktop or 2016 server

upvoted 2 times

Acbrownit 2 years, 2 months ago

Selected Answer: A

This server is being used to *manage* group policy, not *deploy* group policy. For this server to be able to edit the policies required it needs to have a copy of the Windows 10 Admin templates and GPMC. The scope of this question is limited to server 1. For the policies to deploy properly, those admx templates need to be copied to the policy store as well, but that ism't necessary for server 1 to see the applicable policies in gpmc. DCs are out of scope. So answer is A

upvoted 8 times

TechMinerUK 2 years, 2 months ago

Selected Answer: B

So after testing on my home lab I believe the answer is B.

The reason behind this is as follows:
- When you install RSAT on a client to adminster a DC it references the policies on the DC it is connected to or the central store (if present)
- This means that although the user has coppied the ADMX templates to their local PolicyDefinitions folder it will not show in gpmc.msc

Whilst it would not be "mandatory" (Although it would be sensible) for them to create a "Central Store" as this is only required if you are administering policies across multiple DCs it would make life easier as then regardless of which DC there system is connected to it will have the required policies to edit the WUFB policy.

All of this means the answer should be B as the bare minimum would be to install RSAT tools on their client, connect it to a DC and at a minimum copy the ADMX files to the C:\Windows\PolicyDefinitions folder on that DC or better yet make a Central Store by copying files to SYSVOL\domain.tld\Policy

upvoted 5 times

rrrr5r 2 years, 3 months ago

Very vague description but this one showed up in the exam in Sep 16 2022.

I chosed A. Very general speaking update GPO template from a win10 computer is the right way for a win2012 r2 server to be able to manage the said policies.

upvoted 3 times

Silverfire 2 years, 2 months ago

Ok, but in the description we can read that there is already Server 2019, promoted as Domain Controller, so this server will have newer admx settings.

upvoted 1 times

Silverfire 2 years, 2 months ago

Forget about it, you still have to upload the admx files. My bad.

upvoted 1 times

FumerLaMoquette 2 years, 8 months ago

Selected Answer: A

Yeah just copy the admx to the windows/policy definition folder. No need for this server to be a domain controller to managed GPOs.

upvoted 4 times

Chetithy 2 years, 5 months ago

the Server certainly does need to be a Domain Controller to be editing and pushing GPOs.

upvoted 1 times

FumerLaMoquette 2 years, 3 months ago

Nonsense. You can use a domain-joined server to modify domain GPOs. How you do it is by installing RSAT tools on your domain-joined server.
upvoted 4 times

stealthster 2 years, 9 months ago
It's A, it states that you plan to use Server1 to manage the domain. Even though it is only a member server, you can install admin tools and edit group policies from it. Copying the templates from a Windows 10 computer will meet the goal.
upvoted 4 times

tagada 2 years, 10 months ago
Selected Answer: A
no need to be a DC if he just share ADMX/ADML files
upvoted 6 times

mojito2323_ 2 years, 11 months ago
Selected Answer: A
This is A.
upvoted 4 times

JT19760106 2 years, 11 months ago
Selected Answer: B
SYSVOL replication is the requirement.
upvoted 4 times

Somnio 3 years ago
"You plan to use Server1 to manage the domain and to configure Windows 10 Group Policy settings."
Is that not a DC?
upvoted 3 times

Bonesurfer 2 years, 7 months ago
You can manage the domain from any Windows OS (10/11/2012R2/2016/etc.) with RSAT or even with MMC by adding the corresponding snap-ins
upvoted 3 times

zul_n 3 years, 1 month ago
Please correct me if I'm wrong..

But I'd say the answer is A. Yes.

the domain controller is Server 2019, which should already have the required ADMX and ADML.

Copying them from Windows 10 to NETLOGON won't make any difference, as the DC already have the needed files.

Thoughts?
upvoted 2 times

Chipper 3 years, 1 month ago
Where are you getting Netlogon from in the question? As others have said, you can copy them to a central store to manage but the question does not indicate where it is being copied to.
upvoted 1 times

Flacky_Penguin32 3 years, 3 months ago
yes, this is correct; gotta copy admx and adml.
upvoted 2 times

roubchi 3 years, 4 months ago
Answer is YES: I am 120% sure docs.microsoft.com clearly documents Registry key to prefer LOCAL store OVER the Sysvol one. Means yes, local copy of ADMX. Did it without any AD at all, by the way. EDIT GPO has nothing to do with actually Applying it, by the way. GPO edit can be 100% all local standalone and applied for test also locally.
upvoted 5 times

Question #51 *Topic 1*

Note: This question is part of a series of questions that present the same scenario. Each question in the series contains a unique solution that might meet the stated goals. Some question sets might have more than one correct solution, while others might not have a correct solution.
After you answer a question in this section, you will NOT be able to return to it. As a result, these questions will not appear in the review screen.
Your network contains an on-premises Active Directory domain. The domain contains domain controllers that run Windows Server 2019. The functional level of the forest and the domain is Windows Server 2012 R2.
The domain contains 100 computers that run Windows 10 and a member server named Server1 that runs Windows Server 2012 R2.
You plan to use Server1 to manage the domain and to configure Windows 10 Group Policy settings.
You install the Group Policy Management Console (GPMC) on Server1.
You need to configure the Windows Update for Business Group Policy settings on Server1.
Solution: You upgrade Server1 to Windows Server 2019.
Does this meet the goal?

A. Yes

B. No

Suggested Answer: *A*

Community vote distribution

B (64%) A (36%)

Noppawat Highly Voted 4 years ago

B. No

To create a Central Store for .admx and .adml files, create a new folder named PolicyDefinitions in the following location (for example) on the domain controller:

\\contoso.com\SYSVOL\contoso.com\policies\PolicyDefinitions

When you already have such a folder that has a previously built Central Store, use a new folder describing the current version such as:

\\contoso.com\SYSVOL\contoso.com\policies\PolicyDefinitions-1803

Copy all files from the PolicyDefinitions folder on a source computer to the new PolicyDefinitions folder on the domain controller. The source location can be either of the following ones:

The C:\Windows\PolicyDefinitions folder on a Windows 8.1-based or Windows 10-based client computer
The C:\Program Files (x86)\Microsoft Group Policy\<version-specific>\PolicyDefinitions folder, if you have downloaded any of the Administrative Templates separately from the links above.
The PolicyDefinitions folder on the Windows domain controller stores all .admx files and .adml files for all languages that are enabled on the client computer.
upvoted 17 times

Chetithy 2 years, 5 months ago

Agreed. This forum also contains' people's experiences with the admin templates: https://social.technet.microsoft.com/Forums/en-US/be7526ff-31d1-4932-900d-abbb64c58be5/admx-templates-windows-server-2019?forum=ws2019

(the solution in that thread is to install them from a win 10 device)
upvoted 1 times

NitishKarmakar 1 year, 3 months ago

Permission and access to SYSVOL are needed to manage GPMC from a member server.
upvoted 1 times

Bakje Highly Voted 3 years, 3 months ago

A lot of confusion for something pretty simple.
Once the group policy management console (gpmc) is installed you can edit GPO's on any system.
As for the policy templates there are two options:
1) (Default) When editing the policy the templates on the system itself are used.
2) (Best Practice) A central template store is implemented with all needed templates copied to SYSVOL. In this case the GPMC always uses the central template store (no exceptions).
For answering the question:
A) It is clearly given the gpmc is istalled on the member server
B) The default for policy templates is used because there is no mention of any other setting.
All that remains now is whether the required templates are present on the server after upgrading to 2019 (They for sure won't be on a 2012 server). For this I will trust Donaton's remark that the templates are included in 2019.
--> Answer: Yes you can edit the policy setting.
upvoted 8 times

ahmedkmicha Most Recent 1 year, 9 months ago

Selected Answer: A

Upgrading Server1 to Windows Server 2019 would allow you to install the latest version of the Administrative Templates for Windows 10 and configure the Windows Update for Business Group Policy settings using the Group Policy Management Console.
upvoted 3 times

PrepTool 1 year, 9 months ago

Selected Answer: B

Defenatly NO.
It says in the Question "You plan to use Server1 to manage the domain and to configure Windows 10 Group Policy settings". You plan to use the server to MANAGE and to configure W10 GPO's. Cant manage a domain with only GPMC installed!
upvoted 3 times

Meebler 1 year, 10 months ago

Yes,

upgrading Server1 to Win Server 2019 would meet the goal of configuring the Windows Update for Business GP settings on Server1. Win Server 2019 includes updated GP settings and admin templates for Win 10, allowing you to properly configure the Windows Update for Business GP settings for the Win 10 computers in the domain using the Group Policy Management Console (GPMC) on Srv1.

copying the GP Administrative Templates from a Windows 10 computer to Server1 is also valid, but it may not be as comprehensive as upgrading Srv1 to Windows Server 2019. Copying the Admin Templates would provide access to the latest settings, but upgrading the OS would ensure that all updates and features related to win 10 Group Policy settings are available.

raising the forest functional level to Win Server 2016. You copy the GP Admin Templates from a Win 10 computer to the Netlogon share on all the domain controllers is not necessary to configure the Windows Update for Business GP settings on Server1. While it is possible to copy the Admin Templates to the Netlogon share, it may not be the most efficient or effective solution
upvoted 1 times

hufflepuff 1 year, 10 months ago

Selected Answer: A

Answer is yes as stated by some others - Upgrading the server to 2019 will add the policies since it already has GPMC.
There are two correct answers available for this scenario: copy admx templates from win 10 *or* upgrade to 2019.
upvoted 1 times

Acbrownit 2 years, 2 months ago

Selected Answer: A

Like the question before this, the scope is limited to server 1. Upgrading the server to 2019 will allow the applicable policies to show in gpmc on server 1, which is all we care about. There are two correct answers available for this scenario: copy admx templates from win 10 *or* upgrade to 2019. That will allow the policies to show in gpmc.
upvoted 1 times

TechMinerUK 2 years, 2 months ago

Selected Answer: B

Similar reasoning here to the previous question on page 5, editing the local PolicyDefinitions folder is not necessary since RSAT gpmc.msc will reference the policies on the DC it is connected to or the Central Store if there is one
upvoted 2 times

rrrr5r 2 years, 3 months ago

In the exam in Sep 16 2022.

upvoted 4 times

H3adcap 2 years, 4 months ago

Was in exam today 20 Aug 2022

upvoted 4 times

m2L 2 years, 5 months ago

Yes.Because the administrative templates of Windows Server 2019 are the same as the administrative templates of Windows 10.

upvoted 1 times

LillyLiver 2 years, 10 months ago

Selected Answer: B

I say the answer is No.

Windows Update for Business was released with Windows 10 1511 in November, 2015. Server 2012 R2 was released in October, 2013.

The Server OS does not carry the group policy templates. You need to get those from the Win 10 OS, or download them separately. Once you have the templates, you need to add them to the Central Store on a DC.

You can install RSAT and manage the policies from any system, it doesn't have to be a server. But upgrading Server1 to 2019 won't add those policy templates (ADMX and ADML files) to the domain. That's a manual add. If the DC's don't already have the templates applied, you can upgrade Server1 all day long and it's not going to help because the target of the templates has to be on a DC.

Now, with all MS exams you have to be careful to answer the question as it's written, not trying to extrapolate the missing information on the other end. The question is asking if the upgraded Server1 will allow you to configure the WUfB policies. The answer is no.

upvoted 4 times

FreddyLao 3 years ago

Answer should be YES.
here is why: "You need to configure the Windows Update for Business Group Policy settings on Server1."

1 very tricky part is the word "configure" the GPO setting. configure only. not applying.
I can configure the GPO as long as I have the GPMC. if I need to make the GPO apply to win 10 clients. i can export the GPO setting and then import it back to the DC to apply later on.

the point is. as long as the GPO setting is presented. you can configure.
so upgrade to WIndows 2019 makes the required settings available to configure. so answer is YES.
while the DC is already 2019. the Win 10 GPO setting is already there ready to apply in the whole domain

upvoted 4 times

smudo1965 3 years ago

Exactly as Noppowat and others are relying on: https://docs.microsoft.com/en-us/troubleshoot/windows-client/group-policy/create-and-manage-central-store
As there is nowhere stated that the central store has been created I would also vote for NO

upvoted 1 times

lucidgreen 3 years, 5 months ago

Again, NO!
I have a 2012 R2 Server with GPMC on it and I can manage this policy from there. It grabs the templates for managing this policy from SYSVOL. It reads everything from SYSVOL.
Unless you're trying to change where the PolicyDefinitions share is located to try your hand at security through obfuscation, this is pointless. And security through obfuscation isn't very effective.

upvoted 2 times

potpal 3 years, 7 months ago

No!
Server 1 is a Member Server upgrading it to 2019 does not make it a DC

upvoted 4 times

roubchi 3 years, 4 months ago

Has nothing to do with any DC in the World: you can have GMPC installed locally, you can have ADMX copied locally, you have officially documented Registry key to PREFER Local Store OVER the Central Store, and it is all your totally alone to edit GPO locally. Only it will NOT work at all outside your PC, however this is NOT asked :) You can later copy GPO back to the domain when connected to AD.
upvoted 1 times

AnoniMouse 3 years, 7 months ago
You don't have to use a DC to be able to manage GPO. I always install GPMC on my on-premise SCCM to manage GP. All you need is GPMC feature installed AND the correct templates, so in this case if you upgrade the serer to 2019 you'd have all the templates in place so the answer is YES
upvoted 8 times

potpal 3 years, 6 months ago
Agree very good explanation
upvoted 1 times

adaniel89 3 years, 5 months ago
Merely upgrading Server 1 to Windows Server 2019 does nothing. You still need to add GPMC, and create a Central Store
https://docs.microsoft.com/en-us/troubleshoot/windows-client/group-policy/create-and-manage-central-store
upvoted 1 times

bk_apex 3 years, 4 months ago
Your central store point is taken, but the question does state "You install the Group Policy Management Console (GPMC) on Server1" before asking the question.
upvoted 2 times

lucidgreen 3 years, 8 months ago
The schema is already raised to 2019 by having a single 2019 DC. I don't think upgrading the management server is necessary. All you need is to have the templates in an accessible repository. The group policy management console will operate based on that availability. Upgrading the management server achieves nothing.
upvoted 2 times

Bouncy 2 years, 8 months ago
Uhm, what? No, the schema will totally not be raised by installing a single 2019 DC. Just imagine the implications of such an idea, crazy...
upvoted 2 times

Question #52 *Topic 1*

You have a hybrid Azure Active Directory (Azure AD) tenant and a Microsoft Endpoint Configuration Manager deployment.
You have the devices shown in the following table.

Name	Platform	Configuration
Device1	Windows 10	Hybrid joined to on-premises Active Directory and Azure AD only
Device2	Windows 10	Joined to Azure AD and enrolled in Configuration Manager only
Device3	Windows 10	Enrolled in Microsoft Endpoint Manager and has the Configuration Manager agent installed only

You plan to enable co-management.
You need to identify which devices support co-management without requiring the installation of additional software.
Which devices should you identify?

A. Device1 only

B. Device2 only

C. Device3 only

D. Device2 and Device3 only

E. Device1, Device2, and Device3

Suggested Answer: *D*

Community vote distribution

C (95%) 5%

donathon Highly Voted 3 years, 8 months ago

C
Device1: Not enrolled into InTune or SCCM.
Device2: No SCCM client
upvoted 19 times

BGM_YKA 3 years, 7 months ago

C is correct but both device 1 and 2 are missing the SCCM client and this question is only asking about software installation requirements not configuration requirements.
upvoted 5 times

lucidgreen 3 years, 8 months ago

I agree. It seems that if an weren't required, the answer would be E, but since it is required, C is the only viable answer.
upvoted 3 times

Chetithy 2 years, 5 months ago

Agreed. You could enroll device 2 in intune without requiring additional software, but you would still need to install SCCM, so it's a no-go.
Device 3 already has SCCM installed and is Intune Enrolled, so it's good to go.
upvoted 1 times

LillyLiver Highly Voted 2 years, 10 months ago

Selected Answer: C
From the "MS-101T00-A Microsoft Mobility and Security" class e-book:

Scenarios to enable co-management
Co-management implies that:

- Windows 10 devices are joined to AD DS.
- On-premises AD DS is synced to Azure AD.
- Those devices are managed by Configuration Manager and Intune at the same time.

Since the clients have to have the SCCM client AND be enrolled in Intune, Device 3 is the only one that can be co-managed.
upvoted 14 times

aDpAsh Most Recent 1 year, 3 months ago

Device 2 (Azure Joined so InTune registered too + Enrolled in configuration manager which suggest an agent is already there)

& 3 (Agent Installed + Registered in InTune)

Well thats how i see it!

upvoted 1 times

Debadatta 1 year, 6 months ago

Selected Answer: D

Correct answer D

Co-management enables you to concurrently manage Windows 10 or later devices by using both Configuration Manager and Microsoft Intune.

There are two main paths to reach to co-management:

>> Existing Configuration Manager clients: You have Windows 10 or later devices that are already Configuration Manager clients. You set up hybrid Azure AD, and enroll them into Intune.

>>New internet-based devices: You have new Windows 10 or later devices that join Azure AD and automatically enroll to Intune. You install the Configuration Manager client to reach a co-management state.

https://learn.microsoft.com/en-us/mem/configmgr/comanage/overview#paths-to-co-management

upvoted 1 times

qhuy199 11 months, 2 weeks ago

It say "only", mean no additional task to Install Configure Manager Client via Intune.

upvoted 1 times

k9_bern_001 2 years, 4 months ago

C is the correct

upvoted 2 times

KSvh53 2 years, 9 months ago

Wouldn't the enrollment in Configuration Manager automatically trigger the SCCM local agent install during the enrollment process? Or no?

upvoted 4 times

JT19760106 2 years, 11 months ago

Selected Answer: C

Going with C since Device 3 is the only one with the Configuration Manager client installed.

upvoted 3 times

PDR 3 years ago

annoying question really as seems quite confusing and not enough info , plus from experience having the config manager agent installed without co-management in place makes it impossible to enroll into intune as a non co-management enrollment so not even sure device 3 is possible

upvoted 2 times

amymay101 3 years ago

Selected Answer: C

when a device is enrolled SCCM does not install an agent

https://docs.microsoft.com/en-us/mem/configmgr/mdm/understand/manage-mobile-devices-with-on-premises-infrastructure

upvoted 3 times

jkklim 3 years, 1 month ago

C is the answer. Co-management requires a SCCM agent aka CM agent.

When u see the word ENROLLED, it is usually refer to endpoint manger (not sccm)

upvoted 2 times

BluMoon 3 years, 4 months ago

This is a tricky one but I believe D is the correct answer because we use MEM to run the CCM Setup command to configure/reconfigure the installed client since the CM agent is already installed on device 3.

upvoted 2 times

AlexBa 3 years ago

without requiring the installation of additional software...

upvoted 1 times

applejoe6 3 years, 4 months ago

This one has me all mixed up. The answer says it's "D" Device 2 and 3. But why not Device 1?

From what I see there are two paths to co-management.
1. Existing Configuration Manager clients: You have Windows 10 devices that are already Configuration Manager clients. You set up hybrid Azure AD, and enroll them into Intune.
2. New internet-based devices: You have new Windows 10 devices that join Azure AD and automatically enroll to Intune. You install the Configuration Manager client to reach a co-management state.

The keyword here is "Configuration Manager". Device 1 does not have Configuration Manager listed.
Source: https://docs.microsoft.com/en-us/mem/configmgr/comanage/overview#paths-to-co-management
upvoted 2 times

gkp_br 3 years, 5 months ago
Is it possible enroll Configuration Manager without client agent?
upvoted 3 times

Requi3m 3 years, 5 months ago
Yes, although it's probably a little used method. You can create an enrollment package in Configuration Manager, export it and manually install it on a device without a Configuration Manager client.

So answer D is technically possible.

https://docs.microsoft.com/en-us/mem/configmgr/mdm/deploy-use/bulk-enroll-devices-on-premises-mdm
upvoted 1 times

Requi3m 3 years, 5 months ago
Scrath that, should be C. Although enrollment in Configuration Manager without a client is possible, co-managing a device is not. So for device for device 2 to be managed, the client must be installed which is additional software.

https://docs.microsoft.com/en-us/mem/configmgr/comanage/overview
upvoted 6 times

alex_p 2 years ago
No, of course!
upvoted 1 times

encxorblood 3 years, 6 months ago
Only Device 3. Without a agent you can not manage the client in configuration manager and then he is not co-managed.
upvoted 4 times

AnoniMouse 3 years, 7 months ago
This is a tricky question. It states: [You need to identify which devices support co-management WITHOUT requiring the installation of additional software]. Device 1 does NOT have SCCM agent installed so it CANNOT be co-managed
Device 2 and 3 have the SCCM agent installed, so you can co-manage them
upvoted 6 times

lucidgreen 3 years, 6 months ago
Device 2 is only enrolled. No agent installed.
upvoted 5 times

MiZi 3 years, 7 months ago
Do devices enrolled in Configuration Manager have the agent installed automatically?
Does the Config Manager agent installation automatically enroll the device?
If the answer for both questions is yes, then I guess the answer is correct.
upvoted 4 times

JAPo123 2 years, 10 months ago
https://docs.microsoft.com/en-us/mem/configmgr/core/clients/deploy/plan/client-installation-methods
upvoted 1 times

jonker 3 years, 7 months ago
Device 2 and 3 only, bcoz already installed with SCCM agent

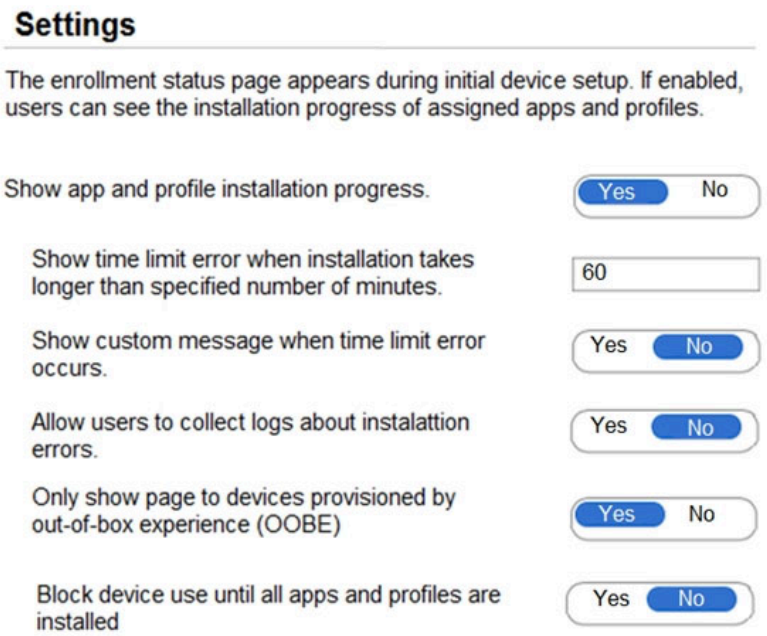
upvoted 3 times

HOTSPOT -

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

Name	Member of	Azure Active Directory (Azure AD) role
User1	Group1	Global administrator
User2	Group2	Cloud device administrator

You configure an Enrollment Status Page profile as shown in the following exhibit.



You assign the policy to Group1.

You purchase the devices shown in the following table.

Name	Platform
Device1	Windows 10
Device2	Android

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

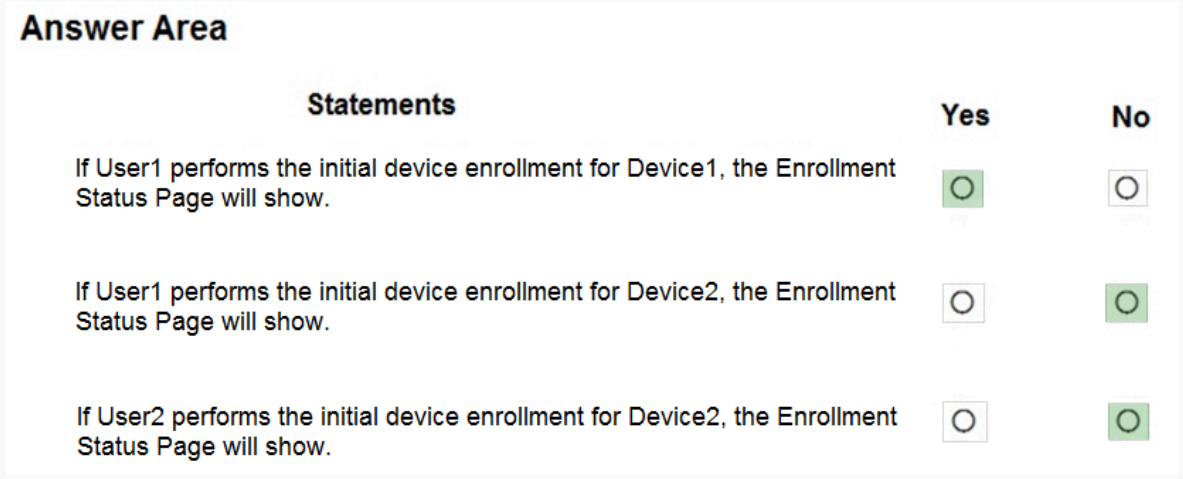
NOTE: Each correct selection is worth one point.

Hot Area:

Answer Area

Statements	Yes	No
If User1 performs the initial device enrollment for Device1, the Enrollment Status Page will show.	○	○
If User1 performs the initial device enrollment for Device2, the Enrollment Status Page will show.	○	○
If User2 performs the initial device enrollment for Device2, the Enrollment Status Page will show.	○	○

Suggested Answer:



Reference:
https://docs.microsoft.com/en-us/mem/intune/enrollment/windows-enrollment-status

JFRigot Highly Voted 3 years, 9 months ago
Device 2 is Android, it never gets any ESP. Yes / No /No
upvoted 33 times

NikPat3125 Highly Voted 3 years, 5 months ago
came in exam 27.07.2021
upvoted 15 times

rrrr5r Most Recent 2 years, 3 months ago
In the exam in Sep 16 2022.
upvoted 8 times

Madskillz13 2 years, 4 months ago
Still a valid question. Featured on my exam August 2022
upvoted 4 times

Chetithy 2 years, 5 months ago
Answer is correct. This won't appear on Android, and User 2 hasn't been assigned to the correct group.
upvoted 4 times

Jake1 3 years, 9 months ago
Answers seem to be correct. There is no ESP for non Windows 10 machines.The ESP can be used as part of any Windows Autopilot provisioning scenario, and can also be used separately from Windows Autopilot as part of the default out-of-box experience (OOBE) for Azure AD Join, as well as for any new users signing into the device for the first time.
upvoted 6 times

Prianishnikov 3 years, 9 months ago
answers are correct
upvoted 3 times

Goena 3 years, 9 months ago
The give answers are correct.
upvoted 3 times

mojefa 3 years, 9 months ago
If User 3 is a member of both Group 1 and Group 2, and Group 1 is configured for "Some - Select the Groups that can automatically enroll their Windows 10 devices" in the MDM User Scope, then Device 1 would, in fact, be automatically enrolled in Intune. So, the answers should be Yes, No, Yes.
upvoted 1 times

Turak64 3 years, 2 months ago
How would an Andriod device get the Windows enrollment page?
upvoted 3 times

ServerBrain 2 years, 1 month ago
The policy is assigned to Group 1

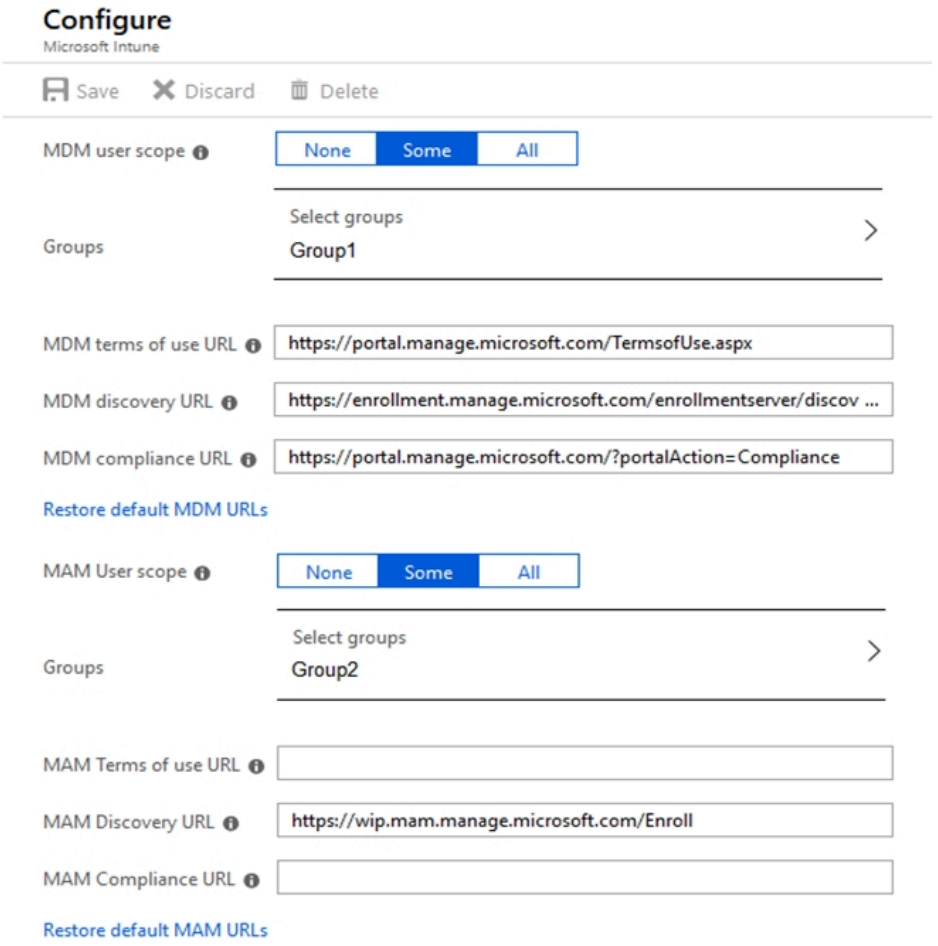
upvoted 1 times

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
User3	Group1, Group2

You integrate Microsoft Intune and contoso.com as shown in the following exhibit.



You purchase a Windows 10 device named Device1.

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

NOTE: Each correct selection is worth one point.

Hot Area:

Answer Area

Statements	Yes	No
If User1 joins Device1 to contoso.com, Device1 is enrolled in Intune automatically.	○	○
If User2 joins Device1 to contoso.com, Device1 is enrolled in Intune automatically.	○	○
If User3 registers Device1 in contoso.com, Device1 is enrolled in Intune automatically.	○	○

Suggested Answer:

Answer Area

Statements	Yes	No
If User1 joins Device1 to contoso.com, Device1 is enrolled in Intune automatically.	○	○
If User2 joins Device1 to contoso.com, Device1 is enrolled in Intune automatically.	○	○
If User3 registers Device1 in contoso.com, Device1 is enrolled in Intune automatically.	○	○

Reference:
https://docs.microsoft.com/en-us/mem/intune/enrollment/windows-enroll

AnoniMouse Highly Voted 3 years, 7 months ago
I think the answer should be YES, NO, NO
If Device3 was a corporate device, then the answer would be Y,N,Y as per:

As per https://docs.microsoft.com/en-us/mem/intune/enrollment/windows-enroll,

[For corporate devices, the MDM user scope takes precedence if both MDM and MAM user scopes are enabled. The device will get automatically enrolled in the configured MDM]

But Device3 is in fact a BYOD because it is REGISTERED and not ENROLLED
upvoted 35 times

derksperte 3 years, 5 months ago
There is no Device 3. Only 1 Device and 3 Users.
upvoted 8 times

Domza 3 years, 5 months ago
lol someone is paying attention))
upvoted 4 times

us3r 3 years ago
he is talking about device 4!! Sorry for the confusion.
upvoted 2 times

mojefa Highly Voted 3 years, 9 months ago
If User 3 is a member of both Group 1 and Group 2, and Group 1 is configured for "Some - Select the Groups that can automatically enroll their Windows 10 devices" in the MDM User Scope, then Device 1 would, in fact, be automatically enrolled in Intune. So, the answers should be Yes, No, Yes.
upvoted 32 times

bellorg 3 years, 7 months ago
Question is User 3 "Register" device 1 so is configured as AD Registered so Enrollment won't proceed
upvoted 26 times

Durden871 2 years, 5 months ago
What an annoying trick question. You read all of these long winded questions and they sneak a change of verbiage in the question. Frustrating.
upvoted 11 times

in_cloud Most Recent 1 year, 5 months ago
On exam july/2023
upvoted 3 times

ChizzyO 1 year, 5 months ago
Yes No, No since the question on device 3 is about registering it.
upvoted 1 times

vanr2000 1 year, 8 months ago

The answer is Y, N, Y

With user3, device1 will enroll in Intune just for MAM, not MDM.

Simplify Windows enrollment for you and device users by enabling automatic enrollment in Microsoft Intune. This enrollment method enables devices to enroll automatically when they join or register in your Azure Active Directory.

Important:
For Windows BYOD devices, the MAM user scope takes precedence if both the MAM user scope and the MDM user scope (automatic MDM enrollment) are enabled for all users (or the same groups of users). The device will not be MDM enrolled, and Windows Information Protection (WIP) Policies will be applied if you have configured them.

If your intent is to enable automatic enrollment for Windows BYOD devices to an MDM: configure the MDM user scope to All (or Some, and specify a group) and configure the MAM user scope to None (or Some, and specify a group – ensuring that users are not members of a group targeted by both MDM and MAM user scopes).

https://learn.microsoft.com/en-us/mem/intune/enrollment/windows-enroll
upvoted 2 times

riahisami77 2 years ago
corrrect Answer Y, N, N
User 3 registers Device1, INCONTOSO.COM , here Device1 is REGISTERED in AAD and not ENROLLED
MS sources: Intune marks devices that are Azure AD-registered as personally-owned devices.
then we know that the Device1 is marked as Personal Device, this can bring us to the second explanation :
MS sources: For Windows BYOD devices, the MAM user scope takes precedence if both the MAM user scope and the MDM user scope (automatic MDM enrollment) are enabled for all users (or the same groups of users). The device will not be MDM enrolled, and Windows Information Protection (WIP) Policies will be applied if you have configured them.
upvoted 1 times

Crixsus 2 years, 2 months ago
On exam today 10/23/22
upvoted 2 times

Crixsus 2 years, 2 months ago
I answered NYN. I passed.
upvoted 3 times

Crixsus 2 years, 2 months ago
Oops, I meant YNY.
upvoted 6 times

TechMinerUK 2 years, 2 months ago
The answer is correct as the key is in the details.

User 1 is in Group 1 so when they JOIN a device to AzureAD it is enrolled in Intune (MDM)
User 2 is not in Group 1 so when the JOIN a device to AzureAD it is not enrolled in Intune (MDM) (They would however be able to enrol the system in MAM if they REGISTERED it)
User 3 a member of Group 1 and Group 2 however they are REGISTERING a system meaning it would be enrolled in MAM. If they JOINED the system it would be enrolled in Intune (MDM)

The key point for user 3 is they are REGISTERING instead of JOINING AzureAD
upvoted 9 times

petersonal 1 year, 10 months ago
I like your reasoning.
upvoted 1 times

Chetithy 2 years, 5 months ago
Correct.
User 1 is in the correct group + joins the device (Y)

User 2 is not in the correct group- doesn't matter whether they join the device or not (N)
User 3 only registers (BYOD), so there is no auto enrolment (N)
upvoted 3 times

us3r 3 years ago
YNN
Keyword;
user3 REGISTERS (!!!) the device
upvoted 5 times

TimurKazan 3 years, 1 month ago
I don't like the answers you have provided there guys. I am lil saddened by you. Please read link below and you will know the truth
upvoted 1 times

us3r 3 years ago
why don't you provide your answer and explanation? I think that this is a technical discussion, not a political.
friendly,
us3r
upvoted 3 times

Arlecchino 2 years, 3 months ago
He is trying to be a smartass.
upvoted 3 times

jkklim 3 years, 1 month ago
YNN is correct.

Device 1 is PURCHASED means not company device, BYOD. When you BYOD, u do not want the device to enrolled automatically. You applied MAM to manage the application within the BYOD only. Therefore user3 is a NO
upvoted 2 times

Domza 3 years, 5 months ago
ok, i found it lol - from a reference link provided: Its all about having both MAM and MDM groups. Please read carefully. :)

`Important`

For Windows BYOD devices, the MAM user scope takes precedence if both the MAM user scope and the MDM user scope (automatic MDM enrollment) are enabled for all users (or the same groups of users). The device will not be MDM enrolled, and Windows Information Protection (WIP) Policies will be applied if you have configured them.

If your intent is to enable automatic enrollment for Windows BYOD devices to an MDM: configure the MDM user scope to All (or Some, and specify a group) and configure the MAM user scope to None (or Some, and specify a group – ensuring that users are not members of a group targeted by both MDM and MAM user scopes).

For corporate devices, the MDM user scope takes precedence if both MDM and MAM user scopes are enabled. The device will get automatically enrolled in the configured MDM.
upvoted 9 times

Domza 3 years, 5 months ago
Key: "You purchase a Windows 10 device named Device1" NOT a company's device.
upvoted 2 times

JT19760106 2 years, 11 months ago
They also say "you have an Azure Active Directory..." and "you integrate Microsoft Intune and contoso.com..." so in this context "you" is an AAD/MEM admin and I can't assume it's a BYOD device.
upvoted 3 times

Jake1 3 years, 9 months ago
Given answers are correct. PersonT is correct for the reason. If a user is part of both MDM and MAM scope, the MAM scope takes precedence therefore, no auto enrollment.https://docs.microsoft.com/en-us/mem/intune/enrollment/windows-enroll.
upvoted 2 times

yvette0013 3 years, 8 months ago
this is only true in case of Windows BYOD devices. For Corporate devices, MDM will take precedence

upvoted 2 times

Domza 3 years, 5 months ago

MAM is for Application only - Mobile Apps Management. You dont have to use MAM.
MDM - Mobile device management - Since User 3 in both - He/she gets Apps and well as device. It says"register" there we need to scratch out head a bit lol

upvoted 1 times

Prianishnikov 3 years, 9 months ago

Y-N-N or Y-N-Y?

upvoted 1 times

[Removed] 3 years, 1 month ago

yes yes yes

upvoted 1 times

us3r 3 years ago

Maybe Maybe Maybe
or

or
DUNNO DUNNO DUNNO

upvoted 3 times

Goena 3 years, 9 months ago

It is indeed as JFRigot mentioned. Also, If your intent is to enable automatic enrollment for Windows BYOD devices to an MDM: configure the MDM user scope to All (or Some, and specify a group) and configure the MAM user scope to None (or Some, and specify a group – ensuring that users are not members of a group targeted by both MDM and MAM user scopes)
Yes, No, No

upvoted 3 times

JFRigot 3 years, 9 months ago

Yes, no, no. Sorry

upvoted 2 times

PersonT 3 years, 9 months ago

Correct. Registered device means For Windows BYOD devices, the MAM user scope takes precedence if both the MAM user scope and the MDM user scope (automatic MDM enrollment) are enabled

upvoted 5 times

Question #55 *Topic 1*

HOTSPOT -

You have an Azure subscription and an on-premises Active Directory domain. The domain contains 50 computers that run Windows 10.

You need to centrally monitor System log events from the computers.

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

In Azure:

- Add and configure the Diagnostics settings for the Azure Activity Log.
- Add and configure an Azure Log Analytics workspace.
- Add an Azure Storage account and Azure Cognitive Search
- Add an Azure Storage account and a file share.

On the computers:

- Create an event subscription.
- Modify the membership of the Event Log Readers group.
- Enroll in Microsoft Endpoint Manager.
- Install the Microsoft Monitoring Agent.

Suggested Answer:

Answer Area

In Azure:

- Add and configure the Diagnostics settings for the Azure Activity Log.
- **Add and configure an Azure Log Analytics workspace.**
- Add an Azure Storage account and Azure Cognitive Search
- Add an Azure Storage account and a file share.

On the computers:

- Create an event subscription.
- Modify the membership of the Event Log Readers group.
- Enroll in Microsoft Endpoint Manager.
- **Install the Microsoft Monitoring Agent.**

Reference:

https://docs.microsoft.com/en-us/azure/azure-monitor/learn/quick-collect-windows-computer

lucidgreen Highly Voted 3 years, 6 months ago

Saw this on the test.

upvoted 25 times

DiscGolfer 3 years, 2 months ago

https://docs.microsoft.com/en-us/services-hub/health/mma-setup#download-and-install-the-microsoft-monitoring-agent-mma-setup-file-from-azure-log-analytics

upvoted 3 times

Jake1 Highly Voted 3 years, 9 months ago

Given answers are correct.https://docs.microsoft.com/en-us/azure/azure-monitor/vm/quick-collect-windows-computer

upvoted 13 times

Question #56 *Topic 1*

HOTSPOT -

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

Name	Member of
User1	Group1
User2	Group1, Group2
User3	Group3

In Microsoft Endpoint Manager, you create two device type restrictions that have the settings shown in the following table.

Priority	Name	Allowed platform	Assigned to
1	TypeRest1	Android, Windows (MDM)	Group1
2	TypeRest2	iOS	Group2

In Microsoft Endpoint Manager, you create three device limit restrictions that have the settings shown in the following table.

Priority	Name	Device limit	Assigned to
1	LimitRest1	7	Group2
2	LimitRest2	10	Group1
3	LimitRest3	5	Group3

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 enroll up to 10 Windows 10 devices in Microsoft Endpoint Manager.	○	○
User2 can enroll up to 10 iOS devices in Microsoft Endpoint Manager.	○	○
User3 can enroll up to five Android devices in Microsoft Endpoint Manager.	○	○

Suggested Answer:

Answer Area

Statements	Yes	No
User1 can enroll up to 10 Windows 10 devices in Microsoft Endpoint Manager.	◉	○
User2 can enroll up to 10 iOS devices in Microsoft Endpoint Manager.	○	◉
User3 can enroll up to five Android devices in Microsoft Endpoint Manager.	○	◉

Rens19991 Highly Voted 3 years, 9 months ago

Question 3 is Yes, because he does not have OS restricstions set

upvoted 41 times

veteran_tech 2 years, 4 months ago

Correct - Y, N, Y. I just took a look at the Endpoint Manager admin center console:

Devices | Enrollment device limit restrictions - Default All Users 5 Yes

Devices | Enrollment device platform restrictions - Default All Users Yes

upvoted 4 times

Feyenoord 1 year, 7 months ago

You need to have at least one restriction, else the enrollment won't work.

upvoted 1 times

lucidgreen 3 years, 6 months ago

This would only be true if white-glove enrollment was being used, meaning all users can join devices. This is not the default, we can only assume the default, which means only users specifically allowed to enroll devices can do so.

Y, N, N.

upvoted 15 times

lucidgreen 3 years, 6 months ago

Also, priority does take precedence.

upvoted 2 times

sdabrai 3 years, 6 months ago

User 3 could register the devices if the account was a Device Enrollment Manager or if the default policy had not been modified. Question does not specify.

upvoted 2 times

veteran_tech 2 years, 4 months ago

White glove is the default as of August 8, 2022

upvoted 2 times

MSGrady Highly Voted 3 years, 9 months ago

There is no "group assigned" for Group 3 so question 3 should be no

upvoted 14 times

otday 3 years, 6 months ago

There is no device restrictions for User 3 so should be Y-N-Y

upvoted 17 times

TechMinerUK Most Recent 2 years, 2 months ago

Based on the information provided the answer should be Y, N, Y.

Y and N (1 & 2) are right as the users have the correct enrollment restrictions stated.

User 3 in Group 3 is the one I believe is incorrect as when a tenant is configured the default enrollment policy (Which would be applied to User 3 as no other policies are being applied) would allow them to enrol any OS device.

If the question had mentioned that the default policy had been changed then this would impact user 3 however based on the lack of information provided it would be logical to assume the default policies being present meaning user 3 can enroll 5 devices of any platform to Intune

upvoted 6 times

Durden871 2 years, 5 months ago

I feel like whomever wrote this question didn't consider default policy. I'm willing to bet on the test it is indeed YNN, despite the fact that it's clearly YNY because we're left to assume the default policy is unchanged. I feel like the tester wrote this without thinking of a default policy and just assumed that not being applied to a policy meant, "no".

So, it's YNY, but who the heck knows what MS wants. Every dump is pointing to YNN, but I get the feeling they all just copy and paste from each other and change one or two questions to make them look different.

upvoted 8 times

L33D 2 years, 6 months ago

Still valid, on exam Jun 25, 2022

upvoted 3 times

Durden871 2 years, 5 months ago

Great. Love knowing that an unclear question is going to be on the exam. After reading the comments I'm guessing it is NYY. My first reaction was NYN, but there's no device restrictions listed, so am I suppose to assume there is one? Complete garbage.

upvoted 2 times

Durden871 2 years, 5 months ago

*I meant for the default policy.

upvoted 1 times

Arlecchino 2 years, 3 months ago

Yeah, F us.

upvoted 1 times

rrrr5r 2 years, 3 months ago

In the exam in Sep 16 2022.

upvoted 3 times

venwaik 2 years, 8 months ago

User3 does have a device limit but not a device TYPE limit. User3 can therefore enroll all device types. 3rd answer is Y

upvoted 4 times

venwaik 2 years, 8 months ago

Correction: User3 does have a device LIMIT restriction but not a device TYPE restriction. User3 can therefore enroll all device types. 3rd answer is Y

upvoted 3 times

OneplusOne 2 years, 12 months ago

"In Intune, by default, there is a limit for the maximum number of enrolled devices per user, which means one user account only can enroll 5 devices. "

upvoted 2 times

EG_Jack 2 years, 12 months ago

I don't know why I payed for the contributor access. I'll be glad to support Examtopics, but I've found to many wrong answers. This is one. Correct answer is surely Y - N - Y

Who else has payed? :-)

upvoted 4 times

JT19760106 2 years, 11 months ago

Thinking the same thing. Would be happy to support them, but they have the exact same questions and answers as ITEXAMS.COM. Not sure if they are affiliated, but over 60 wrong answers on this exam. They need to do better to continue getting my $$.

upvoted 6 times

Patrick2401 3 years, 4 months ago

Y-N-Y

User3 has the default settings of 5 devices (no OS restrictions)

upvoted 9 times

larnyx 3 years, 4 months ago

Should be Y, N, Y.

By default you're not restricted in what type of device to enroll, and since User3 only has a deviceLIMIT and not deviceTYPE, he could in theory enroll 5 users of whatever platform he chooses.

upvoted 6 times

FarhaanKhanPathan 3 years, 5 months ago

Why B is no?

upvoted 1 times

gkp_br 3 years, 5 months ago

Group2 = Divice limit 7.

upvoted 2 times

Khazetul1 3 years, 7 months ago

There is no displayed rule that allows enrollment. You are referring to a policy that states that everyone can enroll, but that isn't displayed. Based on the rules as displayed, the anwer is Y-N-N

upvoted 4 times

bibabongo 3 years, 7 months ago

Wouldn't that mean N - N - N with this logic, as the other users also are not displayed to be allowed?

upvoted 1 times

OG_Diablo 3 years, 1 month ago

The other users are listed as group members, and the policies shown are assigned to the groups.

upvoted 2 times

originalwitness 3 years, 8 months ago

Yes-No-Yes?

Hard to determine, we don't know if the default policy has been modified at all..

upvoted 10 times

lucidgreen 3 years, 6 months ago

Assume it has not.

upvoted 1 times

Prianishnikov 3 years, 9 months ago

YES-NO-YES????

upvoted 7 times

Goena 3 years, 9 months ago

Yes, No, Yes

upvoted 5 times

Question #57 *Topic 1*

DRAG DROP -

You have a Microsoft 365 E5 subscription.

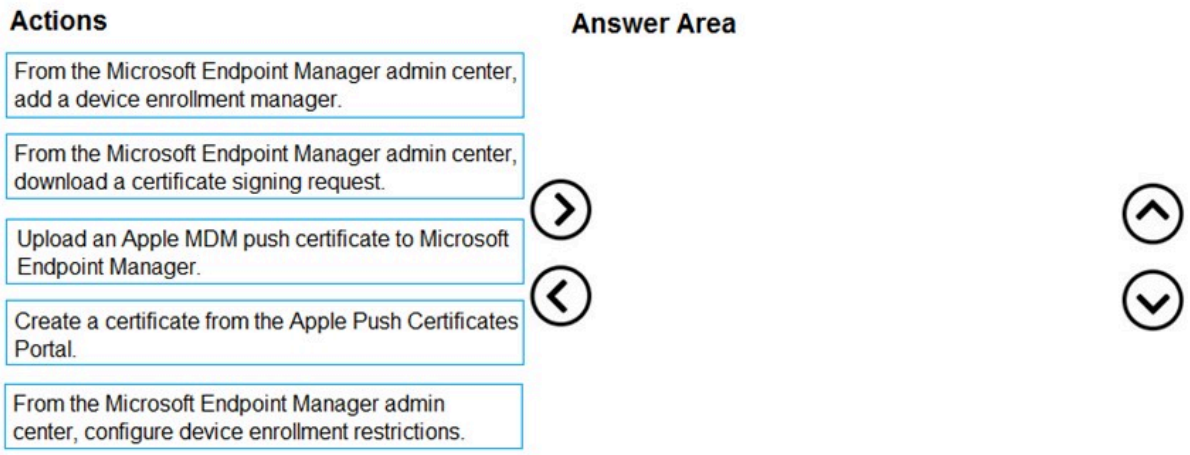
Several users have iOS devices.

You plan to enroll the iOS devices in Microsoft Endpoint Manager.

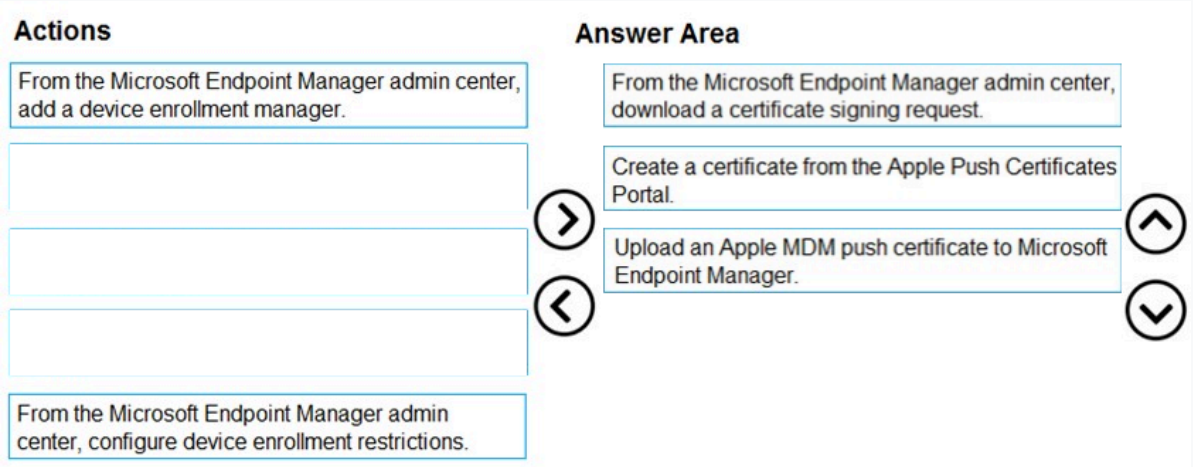
You need to ensure that you can create an iOS/iPadOS enrollment profile in Microsoft Endpoint Manager.

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:



Suggested Answer:



Reference:

https://docs.microsoft.com/en-us/mem/intune/enrollment/apple-mdm-push-certificate-get

Jake1 Highly Voted 3 years, 9 months ago

Answers are correct.https://docs.microsoft.com/en-us/mem/intune/enrollment/apple-mdm-push-certificate-get

upvoted 9 times

lucidgreen Highly Voted 3 years, 6 months ago

Create request, submit request, install push certificate. This is not unlike any other 3rd-party certificate management scenario.

Also, saw this one on the test.

upvoted 8 times

bac0n Most Recent 2 years ago

Correct. Do this in MaaS360 all the time, it's the same.

upvoted 1 times

Contactfornitish 2 years, 4 months ago

On exam on 13 aug'22

upvoted 4 times

L33D 2 years, 6 months ago

Still valid, on exam Jun 25, 2022

upvoted 2 times

gxsh 3 years ago

Answer is correct.

upvoted 3 times

BLLDM 3 years, 2 months ago

Answer is correct!

upvoted 3 times

Prianishnikov 3 years, 9 months ago

Answer is correct

upvoted 5 times

Question #58 *Topic 1*

HOTSPOT -

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

Name	Member of
User1	UserGroup1
User2	UserGroup2
User3	UserGroup3

The tenant contains the devices shown in the following table.

Name	Owner	Installed apps	Platform	Microsoft Intune
Device1	User1	*None*	Windows 10	Enrolled
Device2	User2	App2	Android	Not enrolled
Device3	User3	*None*	iOS	Not enrolled

You have the apps shown in the following table.

Name	Type
App1	iOS store app
App2	Android store app
App3	Microsoft store app

You plan to use Microsoft Endpoint Manager to manage the apps for the users.

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
App1 can be assigned as a required install for User3.	○	○
App2 can be uninstalled from Device2 by using Microsoft Endpoint Manager.	○	○
App3 can be installed automatically for UserGroup1.	○	○

Suggested Answer:

Answer Area

Statements	Yes	No
App1 can be assigned as a required install for User3.	○	○
App2 can be uninstalled from Device2 by using Microsoft Endpoint Manager.	○	○
App3 can be installed automatically for UserGroup1.	○	○

Reference:

https://docs.microsoft.com/en-us/mem/intune/apps/apps-deploy

https://docs.microsoft.com/en-us/mem/intune/apps/apps-windows-10-app-deploy

jkklim Highly Voted 3 years, 1 month ago

NNY - is correct

upvoted 24 times

Durden871 2 years, 5 months ago

YNY:
1 - apps can be assigned even if not enrolled (just can't be installed or removed)
2 - Same answer as above, it's not enrolled.
3 - User1 = Group 1. Group 1 is enrolled.

Assign apps to groups with Microsoft Intune
Assign to users - YES
Assign to devices - NO
Uninstall apps - NO
https://docs.microsoft.com/en-us/mem/intune/apps/apps-deploy
upvoted 2 times

gmKK 2 years, 3 months ago
NNY - Apps can be assigned even if not enrolled - but to a Group not an individual user! Wording.. :)
upvoted 8 times

Futfuyfyjfj 1 year, 8 months ago
NNN, besides the enrollment state of the device as mentioned in the question, technically you CANNOT assign Microsoft Store apps as required aka automatically installed. Only Microsoft Store for Business apps can be assigned as required.
upvoted 1 times

donathon Highly Voted 3 years, 6 months ago
To deploy and remove apps, the device needs to be enrolled in InTune.
upvoted 10 times

ARYMBS 2 years, 3 months ago
MAM-WE
upvoted 1 times

m2L Most Recent 1 year ago
Hello, you have to keep in mind that User1 and Device2 are groups but single objects
upvoted 1 times

in_cloud 1 year, 5 months ago
On exam july/2023
upvoted 1 times

EsamiTopici 1 year, 9 months ago
Anyone explain this please?
upvoted 1 times

aims123456 1 year, 11 months ago
After a lot of research and reading on Microsoft Learn my answer is YNY
Yes: You can assign app to devices that aren't enrolled in iOS (but can't receive updates)
No: Required and Uninstall app targeting are not supported for non-enrolled devices in Android
Yes: As UserGroup1 members would be targeted as User1's device (Device1) is enrolled, apps would be automatically (by setting assignment as "Required")
upvoted 1 times

aims123456 1 year, 10 months ago
Changing my answer to N, N, Y
as 1 = No because it supports app assigned to users to keyword is "required install" and it doesn't support that.
upvoted 1 times

Futfuyfyjfj 1 year, 8 months ago
NNN, besides the enrollment state of the device as mentioned in the question, technically you CANNOT assign Microsoft Store apps as required aka automatically installed. Only Microsoft Store for Business apps can be assigned as required.
upvoted 1 times

fofo1960 1 year, 12 months ago
Can anyone explain to me why 3rd question is Y?
UserGroup1 is not mentioned anywhere in the question. The user is a member of a group that is actually not assigned anywhere
can someone explain this
upvoted 2 times

TechMinerUK 2 years, 2 months ago

I would say this is NNN due to the following:
1 - App1 can be assigned as a required install to a group but not an individual user (Regardless of enrolled devices it can be required for a user group or device group)
2 - The device is not enrolled to allow the software to be uninstalled
3 - Microsoft Store apps can only be made "Available" you can't make them required, to be required it must be a Microsoft Store for Business app (Devil in the detail)

upvoted 2 times

certacc 2 years, 3 months ago

The answer is actually NNN. .

You can't automatically install "Microsoft Store Apps", you can only make them available for installation. This would mean the user having to install from the Company Portal which is not automatic as specified in the question.

You can only require installation of store apps if the are "Microsoft Store for Business" apps. This would automatically install the app on enrolled devices, but a business store app isn't specified.

upvoted 3 times

Chetithy 2 years, 5 months ago

NNY - User 3 has the correct groups, and is enrolled in Intune. Other devices are not and so cannot have auto installations regardless of user config.

upvoted 2 times

TimNov 2 years, 6 months ago

NNN

Agree with BGM_YKA's logic.

upvoted 4 times

AZalan 2 years, 8 months ago

Apps can be assigned to users whether Device Enrolled or not. So, Y | N | Y
https://docs.microsoft.com/en-us/mem/intune/apps/apps-deploy

upvoted 8 times

lucidgreen 3 years, 6 months ago

The only question I have is whether an app can be assigned as a required install even though it can't be installed on the device. I mean, it shouldn't matter. It just won't happen. However, what if User 3 decides to sign in to a Windows 10 device? If you require it, it would install.
Device 2 is not enrolled in Intune, so no.
Device 3 is a Windows 10 device, so yes.

upvoted 3 times

F_M 3 years, 4 months ago

You're right but assignment are managed on group basis. You can't assign an app as required to a user but you can to a use group. So, in this case:
Can you assign appX as required to userX? N
Can you assign appX as required to groupX? Y

upvoted 2 times

BGM_YKA 3 years, 7 months ago

N - N - N
because first two are not configured in intune and the last is to the "group" group1 not user1 and there is no information on group assignments.

upvoted 6 times

lucidgreen 3 years, 5 months ago

The devices are assigned by owner.

upvoted 1 times

us3r 3 years ago

Owner of the device?
How is this linked with the user and group relationship?

upvoted 1 times

techtest848 3 years ago

Agreed with BGM_YKA
Only user1's assignment is given
upvoted 2 times

asdasdadssdsas 3 years, 6 months ago
Its assigned to UserGroup1, which contains User1, so the answer is N-N-Y
upvoted 5 times

NikPat3125 3 years, 5 months ago
But UserGroup1 is not enrolled, it is user1 who is enrolled.
upvoted 2 times

MomoLomo 3 years, 4 months ago
Available assignments are only valid for user groups, not device groups.

so it's legitimate
upvoted 2 times

us3r 3 years ago
you do not have a point.
upvoted 2 times

Durden871 2 years, 5 months ago
YNY:
1 - apps can be assigned even if not enrolled (just can't be installed or removed)
2 - Same answer as above, it's not enrolled.
3 - User1 = Group 1. Group 1 is enrolled.

Assign apps to groups with Microsoft Intune
Assign to users - YES
Assign to devices - NO
Uninstall apps - NO
https://docs.microsoft.com/en-us/mem/intune/apps/apps-deploy
upvoted 2 times

us3r 3 years ago
Agree
N
N
N
upvoted 3 times

Durden871 2 years, 5 months ago
YNY:
1 - apps can be assigned even if not enrolled (just can't be installed or removed)
2 - Same answer as above, it's not enrolled.
3 - User1 = Group 1. Group 1 is enrolled.

Assign apps to groups with Microsoft Intune
Assign to users - YES
Assign to devices - NO
Uninstall apps - NO
https://docs.microsoft.com/en-us/mem/intune/apps/apps-deploy

You can assign to the user, but not the device. The question asks for user, not device.
upvoted 1 times

Question #59 *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.
Your network contains an on-premises Active Directory domain. The domain contains domain controllers that run Windows Server 2019. The functional level of the forest and the domain is Windows Server 2012 R2.
The domain contains 100 computers that run Windows 10 and a member server named Server1 that runs Windows Server 2012 R2.
You plan to use Server1 to manage the domain and to configure Windows 10 Group Policy settings.
You install the Group Policy Management Console (GPMC) on Server1.
You need to configure the Windows Update for Business Group Policy settings on Server1.
Solution: You raise the domain functional level to Windows Server 2019. You copy the Group Policy Administrative Templates from a Windows 10 computer to the
Netlogon share on all the domain controllers.
Does this meet the goal?

A. Yes

B. No

Suggested Answer: *B*

lucidgreen Highly Voted 3 years, 6 months ago
Sysvol, not Netlogon..
Functional level doesn't matter for this feature.
https://docs.microsoft.com/en-us/windows/deployment/update/waas-wufb-group-policy
upvoted 15 times

Sledgehammer Highly Voted 2 years, 10 months ago
The answer is correct: B. No
upvoted 5 times

bleroblero Most Recent 1 year, 8 months ago
Seen in exam on 2 May 2023
upvoted 3 times

Meebler 1 year, 10 months ago
This solution would enable the use of Windows Server 2019 Group Policy settings, but it does not specifically address configuring the Windows Update for Business Group Policy settings on Server1.
So the answer is B. No.
upvoted 2 times

Csed 2 years, 11 months ago
NetLogon is for scripts, so it should be SYSVOL. Using Zakyntos's link. So NO.
upvoted 4 times

JakeH 3 years, 1 month ago
What's the correct answer here?
upvoted 1 times

zakyntos 3 years, 5 months ago
should be YES,
https://social.technet.microsoft.com/wiki/contents/articles/8548.active-directory-sysvol-and-netlogon.aspx
upvoted 2 times

Chipper 3 years, 1 month ago
Question says NETLOGON not SYSVOL so the answer is no.
upvoted 5 times

otday 3 years, 6 months ago

Is this correct?

upvoted 1 times

Question #60 *Topic 1*

You have a Microsoft 365 E5 subscription.
You plan to deploy 100 new Windows 10 devices.
You need to identify the appropriate version of Windows 10 for the new devices. The version must meet the following requirements:
✑ Be serviced for a minimum of 24 months.
Support Microsoft Application Virtualization (App-V).
▪
Which version should you identify?

A. Windows 10 Pro, version 1909

B. Windows 10 Pro, version 2004

C. Windows 10 Enterprise, version 1909

D. Windows 10 Enterprise, version 2004

Suggested Answer: *D*
Reference:
https://docs.microsoft.com/en-us/windows/release-health/release-information https://docs.microsoft.com/en-us/windows/application-management/app-v/appv-supported-configurations

Community vote distribution
C (100%)

mutleychunter Highly Voted 3 years, 5 months ago
Answer is C. H1/04 releases are only supported for 18 months. H2/09 release for 30 months
upvoted 29 times

sh_gu 3 years, 5 months ago
Agree too
upvoted 3 times

arunjana 3 years, 5 months ago
https://docs.microsoft.com/en-us/lifecycle/faq/windows
upvoted 3 times

LoremanReturns Highly Voted 3 years, 5 months ago
I believe the answer is to test the knowledge of features and lifecycle for Windows 10 versions. Based on the question:
- APPv requires the enterprise edition
- 24 minimum of support requires a H2 version
In my opinion answer is C
upvoted 7 times

Kevinfm_81 Most Recent 2 years, 6 months ago
Link to service lifecycle for enterprise versions in question
https://docs.microsoft.com/en-us/lifecycle/products/windows-10-enterprise-and-education
upvoted 4 times

L33D 2 years, 6 months ago
Still valid, on exam Jun 25, 2022
upvoted 6 times

Stevie_B 2 years, 11 months ago
Selected Answer: C
Only Enterprise 09/H2 have 30 Month Support... all others 18 month
upvoted 4 times

ubt 2 years, 11 months ago
Selected Answer: C
https://docs.microsoft.com/en-us/lifecycle/faq/windows
upvoted 5 times

OneplusOne 2 years, 12 months ago

https://docs.microsoft.com/en-us/lifecycle/announcements/windows-10-servicing-support-updates

upvoted 3 times

edzio 3 years ago

Selected Answer: C

C - Enterprise September 9 version

upvoted 5 times

jkklim 3 years, 1 month ago

all Sept versions of Windows can last more than 2 years

all April versions of windows last only 1.5 years

So we can pick the 9 versions at the end, and the enterprise versions supports App-V

upvoted 2 times

lucidgreen 3 years, 5 months ago

30 months for Fall versions.

18 months for Spring versions.

No Spring version is going be serviced for 24 months. So xxH2 or xx09.

upvoted 6 times

Tonysurge 3 years, 5 months ago

https://docs.microsoft.com/en-us/lifecycle/products/windows-10-enterprise-and-education

Answer: C

upvoted 5 times

zakyntos 3 years, 5 months ago

C

https://docs.microsoft.com/en-us/windows/release-health/release-information

upvoted 5 times

Question #61 *Topic 1*

HOTSPOT -

You have a Microsoft 365 E5 tenant that contains two users named User1 and User2 and the groups shown in the following table.

Name	Members
Group1	User1
Group2	User2, Group1

You have a Microsoft Intune enrollment policy that has the following settings:

➪ MDM user scope: Some

- Groups: Group1

➪ MAM user scope: Some

- Groups: Group2

You purchase the devices shown in the following table.

Name	Platform
Device1	Windows 10
Device2	Android

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 enroll Device1 in Intune by using automatic enrollment	○	○
User1 can enroll Device2 in Intune by using automatic enrollment	○	○
User2 can enroll Device2 in Intune by using automatic enrollment	○	○

Suggested Answer:

Answer Area

Statements	Yes	No
User1 can enroll Device1 in Intune by using automatic enrollment	○	○
User1 can enroll Device2 in Intune by using automatic enrollment	○	○
User2 can enroll Device2 in Intune by using automatic enrollment	○	○

Reference:

https://docs.microsoft.com/en-us/mem/intune/enrollment/windows-enroll https://docs.microsoft.com/en-us/mem/intune/enrollment/android-enroll-device-administrator

donathon Highly Voted 3 years, 6 months ago

YNN. Automatic enrollment is only for Windows 10 devices.

upvoted 78 times

Bulldozzer 2 years, 10 months ago

I agree

upvoted 6 times

encxorblood Highly Voted 3 years, 4 months ago

Y,N,N - Auto Enrollment is not for Android, only Windows 10 or higher

upvoted 26 times

aims123456 Most Recent 1 year, 11 months ago

Y, Y, N

Yes: User1 is part of Group1 configured to use MDM enrolment for Windows device (Device1)

Yes: User1 is part of Group1 configured to use MDM enrolment for Android Device (Device2) (https://learn.microsoft.com/en-us/mem/intune/fundamentals/deployment-guide-enrollment-android#byod-android-enterprise-personally-owned-devices-with-a-work-profile)

No: User 2 being in group 2 therefore takes precedence for MAM enrolment, hence automatic enrolment being no. (Also Group Nesting not supported here)

upvoted 1 times

Futfuyfyjfj 1 year, 8 months ago

The link you provide says enough, you have no idea what you are talking about. MAM and MDM user scope is only applicable for Windows. Correct answer is YNN.

upvoted 3 times

JamesM9 2 years, 9 months ago

Auto-Enrollment only applies to Windows devices in Intune.

https://docs.microsoft.com/en-us/mem/intune/enrollment/windows-enroll

Therefore, the answer here is YNN.

upvoted 7 times

karank19 2 years, 11 months ago

If we consider, the Devices to be BYOD, then the answer would be NO NO NO.

Else, Yes NO NO.

upvoted 2 times

girikedar 2 years, 12 months ago

Answer should be Yes,NO,NO

upvoted 5 times

girikedar 2 years, 12 months ago

User 1 can Enroll Device 2 automatically only if the Mange google play is configured prior

upvoted 1 times

Futfuyfyjfj 1 year, 8 months ago

No still not possible in that case, MDM and MAM user scope is only applicable to Windows

upvoted 1 times

riahisami77 3 years ago

i really don't understad how "examtopics" choose wich answer is correct, i believe that some answers are wrong !!!!

upvoted 9 times

FreddyLao 3 years ago

all the answers should be NO.

1. Intune auto enrollment is only for Windows 10.

https://docs.microsoft.com/en-us/mem/intune/enrollment/quickstart-setup-auto-enrollment

2. the devices are BYOD type. both users belong to the 2 groups (direct and nested)

For Windows BYOD devices, the MAM user scope takes precedence if both the MAM user scope and the MDM user scope (automatic MDM enrollment) are enabled for all users (or the same groups of users). The device will not be MDM enrolled, and Windows Information Protection (WIP) Policies will be applied if you have configured them.

https://docs.microsoft.com/en-us/mem/intune/enrollment/windows-enroll

upvoted 2 times

edzio 2 years, 9 months ago

There is no info about device1 is registered or joined.

upvoted 1 times

dyers 2 years, 2 months ago

it says "Enrolled" so company owned not BYOD

upvoted 1 times

TimurKazan 3 years, 1 month ago

N,N,N

"you purchase device" I guess this means BYOD

upvoted 3 times

JT19760106 3 years ago

Why are you assuming that "you purchase" is BYOD? You are managing an M365 E5 tenant, so would stand to reason that you are purchasing devices for the organization.

upvoted 4 times

Turak64 3 years, 2 months ago

It's only possible to automatically enroll Samsung Knox devices, so we have to once again presume that MS are not referring to this type of device? - https://docs.microsoft.com/en-us/mem/intune/enrollment/android-samsung-knox-mobile-enroll

upvoted 3 times

Dave12 3 years, 4 months ago

Yes

Yes, because its a user enrollment

No

upvoted 3 times

Chetithy 2 years, 5 months ago

"Enroll in Intune by using Automatic Enrolment" means user enrolment?

upvoted 1 times

DCT 2 years, 1 month ago

bro~wake up..

upvoted 3 times

Domza 3 years, 4 months ago

Hint: this is about MAM and MDM scopes. If GRP1 is in both scopes what takes precedence? lol

upvoted 1 times

ferrit 3 years, 5 months ago

YNN - Auto enrolment only for Windows 10

upvoted 3 times

zakyntos 3 years, 5 months ago

auto enroll is for win10

so YNN

https://docs.microsoft.com/en-us/mem/intune/enrollment/windows-enroll#enable-windows-10-automatic-enrollment

upvoted 5 times

[Removed] 3 years, 6 months ago

I believe question 3 is no because MAM user scope takes precedence over MDM user scope.

User 2 being in group 2 therefore takes precedence for MAM enrollment, hence automatic enrollment being no.

upvoted 1 times

agayam 3 years, 4 months ago

For Windows BYOD devices, the MAM user scope takes precedence if both the MAM user scope and the MDM user scope (automatic MDM enrollment) are enabled for all users (or the same groups of users). The device will not be MDM enrolled, and Windows Information Protection (WIP) Policies will be applied if you have configured them.

If your intent is to enable automatic enrollment for Windows BYOD devices to an MDM: configure the MDM user scope to All (or Some, and specify a group) and configure the MAM user scope to None (or Some, and specify a group – ensuring that users are not members of a group targeted by both MDM and MAM user scopes).

For corporate devices, the MDM user scope takes precedence if both MDM and MAM user scopes are enabled. The device will get automatically enrolled in the configured MDM

upvoted 2 times

Question #62 *Topic 1*

HOTSPOT -

You have a Microsoft 365 tenant that contains devices enrolled in Microsoft Intune. The devices are configured as shown in the following table.

Name	Platform
Device1	Windows 10
Device2	Android
Device3	iOS

You plan to perform the following device management tasks in Microsoft Endpoint Manager:

Deploy a VPN connection by using a VPN device configuration profile.

▪

➩ Configure security settings by using an Endpoint Protection device configuration profile.

You need to identify which devices will support the management tasks.

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

NOTE: Each correct selection is worth one point.

Hot Area:

Answer Area

VPN device configuration profile:

- Device1 only
- Device1 and Device2 only
- Device1 and Device3 only
- Device1, Device2 and Device3

Endpoint Protection device configuration profile:

- Device1 only
- Device1 and Device2 only
- Device1 and Device3 only
- Device1, Device2 and Device3

Suggested Answer:

Answer Area

VPN device configuration profile:

- Device1 only
- Device1 and Device2 only
- Device1 and Device3 only
- **Device1, Device2 and Device3**

Endpoint Protection device configuration profile:

- **Device1 only**
- Device1 and Device2 only
- Device1 and Device3 only
- Device1, Device2 and Device3

Reference:

https://docs.microsoft.com/en-us/mem/intune/configuration/vpn-settings-configure https://docs.microsoft.com/en-us/mem/intune/protect/endpoint-protection-macos

DiegoCr Highly Voted 3 years, 6 months ago

Can be Added to macOS and Windows 10 and later, So the question is correct.

upvoted 14 times

SaeedFarvardin Highly Voted 2 years, 4 months ago

The right answer 100% is: (A- all 3 / B- win10 only)!!!
bcz:

First Q. is VPN, so every part need 1 VPN config settings profile(Win10, Android & IOS)

2nd Q.: we have only 3 (Win10, Android & IOS), so, if you create in MDM " 'Endpoint Protection' device configuration profile" you have only 2 Options (Win10 and MacOS) but MacOS is not in our question forget it, so second answer will be only WIN10.

So, Answer will be all3 & win10 only

like it if usefull! ;O)
upvoted 13 times

SaeedFarvardin 2 years, 4 months ago
so the given answer is correct, all/win10!
upvoted 1 times

NitishKarmakar Most Recent 1 year, 6 months ago
Endpoint protection can be added for Mac os and WIn 10 and later.
upvoted 1 times

Y2 1 year, 11 months ago
A - All 3 B - none
The endpoint protection template in configuration profiles doesn't have a VPN setting?
has it been removed or?
upvoted 1 times

kimble3k 1 year, 11 months ago
about B, the question doesn't state you're supposed configure VPN via protection template. You can configure protection template only for win10.
upvoted 2 times

rrrr5r 2 years, 3 months ago
In the exam in Sep 16 2022.
upvoted 5 times

reastman66 2 years, 4 months ago
Looking at this just now this is what I can find by trying it.
Device1 (Windows 10) and Device2 (Android) have settings for VPN. Device3 (iOS) settings allow it to be created so that would be NO. Correct answer Device1 and Device2.

Device1 is the only correct answer for Endpoint Protection
upvoted 1 times

veteran_tech 2 years, 4 months ago
If you go to https://docs.microsoft.com/en-us/mem/intune/configuration/ and browse the left pane, you'll see that endpoint protection is only available for Windows 10/later and macOS
upvoted 3 times

AJCG 2 years, 6 months ago
Should be Device 1 and Device 3, so C and A, doesnt support Android
upvoted 2 times

Sledgehammer 2 years, 10 months ago
The given answers are correct
upvoted 2 times

TimurKazan 3 years, 1 month ago
correct
upvoted 1 times

MomoLomo 3 years, 4 months ago
the answers are correct
upvoted 6 times

Kanta 3 years, 4 months ago

Win 10 + Later and macOS supports Endpoint protection (Configuration policy).

upvoted 4 times

CharlieBash 3 years, 6 months ago

Endpoint protection can be configured for Windows and iOS:
https://docs.microsoft.com/en-us/mem/intune/protect/endpoint-protection-configure

So answer: D + C

upvoted 2 times

Domza 3 years, 4 months ago

It says:
"Configure security settings by using an Endpoint Protection device configuration profile".
link provided is wrong

upvoted 1 times

Domza 3 years, 4 months ago

I take that back. Link is good.

Answers are correct. D+A(Win10+macOS only)

upvoted 5 times

agayam 3 years, 4 months ago

The answer is D+A. The article you provided mentions MacOS which is not the same as iOS.

upvoted 5 times

otday 3 years, 6 months ago

It can be configured for macOS not iOS

upvoted 5 times

DiscGolfer 3 years, 2 months ago

Agree, D + A(Platform choices are Windows and macOS(not iOS))
https://docs.microsoft.com/en-us/mem/intune/protect/endpoint-protection-configure#create-a-device-profile-containing-endpoint-protection-settings

upvoted 1 times

SaeedFarvardin 2 years, 4 months ago

not correct!!! can not config for IOS, but can config MacOS!, MacOs is not in Question, so only Win10 is right answer for 2nd part of question and 1st part of Q will be ALL as answer ;O)

upvoted 2 times

Question #63 *Topic 1*

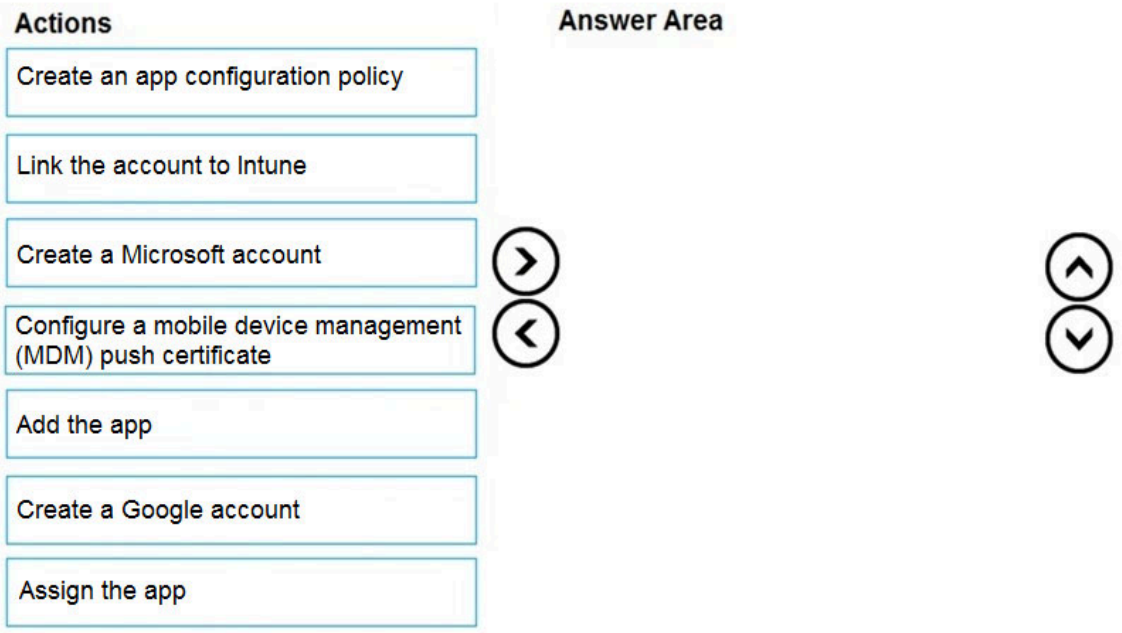
DRAG DROP -

You have a Microsoft 365 E5 tenant that contains 500 Android devices enrolled in Microsoft Intune.

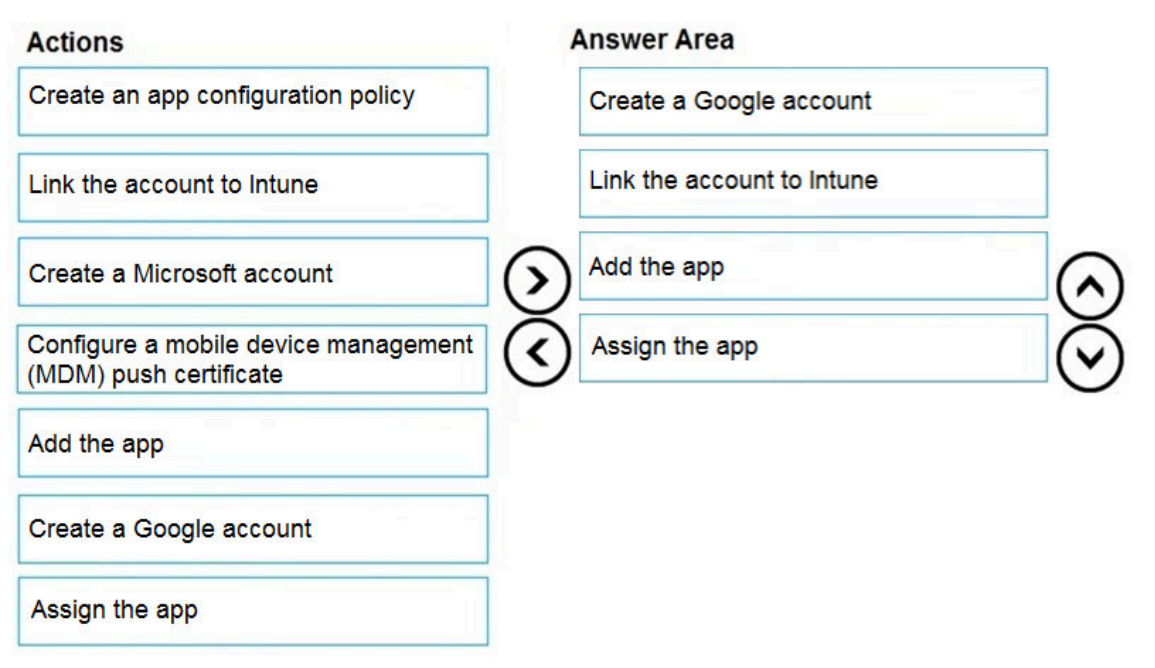
You need to use Microsoft Endpoint Manager to deploy a managed Google Play app to the devices.

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

Select and Place:



Suggested Answer:



Reference:

https://docs.microsoft.com/en-us/mem/intune/apps/apps-add-android-for-work#assign-a-managed-google-play-app-to-android-enterprise-fully-managed-devices

F_M Highly Voted 3 years, 4 months ago

Provided answer is right :)

upvoted 16 times

H3adcap Highly Voted 2 years, 4 months ago

Was in exam today 20 Aug 2022

upvoted 7 times

in_cloud Most Recent 1 year, 5 months ago

On exam july/2023

upvoted 1 times

bleroblero 1 year, 8 months ago

Seen in exam on 2 May 2023

upvoted 2 times

gxsh 3 years ago

Yes, answer is correct.

upvoted 3 times

arg_007 3 years, 3 months ago

https://docs.microsoft.com/en-us/mem/intune/apps/apps-add-android-for-work

upvoted 4 times

Question #64 *Topic 1*

You have a Microsoft 365 E5 tenant that contains four devices enrolled in Microsoft Intune as shown in the following table.

Name	Platform
Device1	Windows 10
Device2	Android
Device3	macOS
Device4	iOS

You plan to deploy Microsoft 365 Apps for enterprise by using Microsoft Endpoint Manager.
To which devices can you deploy Microsoft 365 Apps for enterprise?

A. Device1 only

B. Device1 and Device3 only

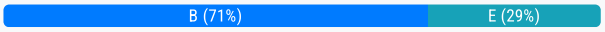
C. Device2 and Device4 only

D. Device1, Device2, and Device3 only

E. Device1, Device2, Device3, and Device4

Suggested Answer: *B*
Reference:
https://docs.microsoft.com/en-us/mem/intune/apps/apps-add

Community vote distribution



itstudy369 Highly Voted 3 years, 4 months ago
Guys, I think the keyword here is "deployed". You can deploy MS apps to Win and MacOS. You can make MS apps available to install on Android and iOS. Let me know your thoughts on this. thanks!
upvoted 23 times

JT19760106 3 years ago
I think the keyword here is M365 Apps for enterprise. You can force install apps for iOS and Android, but in MEM, M365 Apps is only available for Windows 10/11 and macOS.
upvoted 13 times

OneplusOne 2 years, 12 months ago
Correct
https://www.microsoft.com/en-us/microsoft-365/enterprise/microsoft-365-apps-for-enterprise-product
upvoted 7 times

veteran_tech 2 years, 4 months ago
Correct - M365 Apps for enterprise - Compatible with Windows 11, Windows 10, Windows 8.1, Windows Server 2019, Windows Server 2016, and the three most recent versions of macOS. All languages included.
upvoted 5 times

NikPat3125 Highly Voted 3 years, 5 months ago
came in exam 27.07.2021
upvoted 10 times

m2L Most Recent 1 year ago
Hello guys I want to give my opinion on this question.
For me the answer B is correct.
Because the question says by using "Microsoft Endpoint Management".
I verified that by using Microsft Endpoint", in the "Applications" tab when you click on the button "+" the type of applications are grouped by category;
In the category of "Microsoft 365 Apps", there are only two types of devices: Windows 10 and MacOS.
Best regards
upvoted 1 times

Jimboski 1 year, 8 months ago

I think its E after reviwing Apps for Enterprise on Microsoft website

Microsoft 365 Apps for enterprise

• Get always up-to-date Office apps: Word, Excel, PowerPoint, Outlook, and more.

• Try the Microsoft Teams Exploratory experience.1

• Install apps on up to five PCs, five tablets, and five mobile devices.

• Store and share files with 1 TB of OneDrive cloud storage.

• Have peace of mind knowing you're secure and compliant.

• Access FastTrack assistance.

• Get help anytime with around-the-clock support from Microsoft.

Compatible with Windows 11, Windows 10, Windows 8.1, Windows Server 2019, Windows Server 2016, and the three most recent versions of macOS. All languages included.

Talk with a sales expert

To speak with a sales expert, call 1 855-270-0615. Monday-Friday 6:00AM to 6:00PM Pacific Time.

upvoted 1 times

Jimboski 1 year, 8 months ago

NVM, I see how I was mislead here

upvoted 1 times

Fala_Fel 1 year, 11 months ago

Selected Answer: E

Microsoft 365 Apps for Enterprise is available for ALL devices here. And in Endpoint when assigning them they are all called by different names, even Windows version isn't called '...apps for enterprise' it is 'Microsoft 36 Apps for Windows'

You can also use Endpoint to push out 365 to all devices. So Ans is E

https://www.microsoft.com/en-gb/microsoft-365/enterprise/microsoft-365-apps-for-enterprise-product?activetab=pivot:techspecstab

See Operating System Section. Also lists Android & iOS

upvoted 1 times

RazielLycas 2 years, 5 months ago

Selected Answer: B

M365 Apps for enterprise is for Win 10/11 and macOS, on Android it's office for android and on iOS is Office for iOS

upvoted 7 times

Sategi 2 years, 5 months ago

Selected Answer: E

M365 apps includes mobile apps https://www.microsoft.com/en-au/microsoft-365/compare-microsoft-365-enterprise-plans

upvoted 1 times

slaoui 2 years, 7 months ago

B is correct

Microsoft 365 Apps for enterprise

"Compatible with Windows 11, Windows 10, Windows 8.1, Windows Server 2019, Windows Server 2016, and the three most recent versions of macOS. All languages included."

https://www.microsoft.com/en-au/microsoft-365/enterprise/microsoft-365-apps-for-enterprise-product?activetab=pivot%3aoverviewtab

upvoted 4 times

JamesM9 2 years, 9 months ago

The answer is E, all 4 devices - https://www.microsoft.com/en-gb/microsoft-365/enterprise/microsoft-365-apps-for-enterprise.

upvoted 1 times

JamesM9 2 years, 9 months ago

The answer is E, all 4 devices - https://www.microsoft.com/en-gb/microsoft-365/enterprise/microsoft-365-apps-for-enterprise

upvoted 2 times

Notorious19 2 years, 10 months ago

Selected Answer: B

B correct

upvoted 1 times

georgestile 2 years, 11 months ago

Selected Answer: B

only Windows & Mac OS are supported platforms

upvoted 2 times

bytea 3 years ago

Selected Answer: E

M365 apps includes mobile apps https://www.microsoft.com/en-au/microsoft-365/compare-microsoft-365-enterprise-plans

upvoted 2 times

gxsh 3 years ago

Device 1 and Device 3, link: https://docs.microsoft.com/en-us/mem/intune/apps/apps-add

upvoted 1 times

JhonyTrujillo 3 years, 4 months ago

https://www.microsoft.com/en-us/microsoft-365/enterprise/microsoft-365-apps-for-enterprise-product?activetab=pivot%3aoverviewtab

upvoted 1 times

Domza 3 years, 4 months ago

Boys and girls, the question is "to which devices can you deploy Microsoft 365 Apps"

There are 4 platforms in Intune/Endpoint Manger.

WIn

iOS/Pad

macOS

Android

upvoted 1 times

junior6995 3 years, 1 month ago

When you see "Apps for ENTERPRISE" read Windows and Mac Office Apps.

upvoted 2 times

Domza 3 years, 4 months ago

Oh boy, very sorry. Got confused there for a moment.

M365 Apps - WIn 10 + macOS.

Love to all lol

upvoted 11 times

us3r 3 years ago

love is in the air

upvoted 2 times

gkp_br 3 years, 5 months ago

Why not? "E. Device1, Device2, Device3, and Device4".

We can add Office 365 Apps for Android an IOS using Intune from Store Apps.

https://docs.microsoft.com/en-us/mem/intune/apps/store-apps-android

upvoted 2 times

HappyMudd 3 years, 3 months ago

Apps for ENTERPRISE, Win/Mac only.

upvoted 6 times

DiscGolfer 3 years, 2 months ago

"M365 Apps for Enterprise is Compatible with *Windows 11*, *Windows 10*, Windows 8.1, Windows Server 2019, Windows Server 2016, and the *three most recent versions of macOS*. All languages included."

https://www.microsoft.com/en-us/microsoft-365/enterprise/microsoft-365-apps-for-enterprise-product?activetab=pivot:techspecstab

upvoted 1 times

Question #65 *Topic 1*

You have a Microsoft 365 E5 tenant that contains the devices shown in the following table.

Name	Platform	Azure Active Directory (Azure AD)
Device1	Windows 10	Joined
Device2	Windows 10	Registered
Device3	Windows 10	Not joined or registered
Device4	Android	Registered

You plan to review device startup performance issues by using Endpoint analytics.
Which devices can you monitor by using Endpoint analytics?

A. Device1 only

B. Device1 and Device2 only

C. Device1, Device2, and Device3 only

D. Device1, Device2, and Device4 only

E. Device1, Device2, Device3, and Device4

Suggested Answer: *A*
Reference:
https://docs.microsoft.com/en-us/mem/analytics/overview

Community vote distribution
A (100%)

junior6995 Highly Voted 2 years, 11 months ago
Best explanation for the difference between Joined vs. Registered devices

Azure AD Joined is for
Corporate owned and managed devices
Authenticated using a corporate id that exists on Azure AD
Authentication is only through AAD.

Azure AD Registed Device is for
Personally owned corporate enabled
Authentication to the device is with a local id or personal cloud id
Authentication to corporate resources using a user id on AAD.
upvoted 15 times

Alien1981 Highly Voted 3 years, 6 months ago
Agreed
Endpoint analytics prerequisites: Windows 10 devices must be Azure AD joined or hybrid Azure AD joined. (Workplace joined or Azure AD registered devices aren't supported.)
https://docs.microsoft.com/en-us/mem/analytics/overview
upvoted 12 times

reastman66 Most Recent 2 years, 5 months ago
Selected Answer: A
Windows devices must be Azure AD joined or hybrid Azure AD joined. Workplace joined or Azure AD registered devices aren't supported.
upvoted 4 times

adaniel89 3 years, 6 months ago
The answer appears to be correct : https://docs.microsoft.com/en-us/mem/analytics/startup-performance
upvoted 5 times

Question #66 *Topic 1*

You have a Microsoft 365 E5 tenant that contains 100 Windows 10 devices.
You plan to deploy a Windows 10 Security Baseline profile that will protect secrets stored in memory.
What should you configure in the profile?

A. Microsoft Defender Credential Guard

B. BitLocker Drive Encryption (BitLocker)

C. Microsoft Defender

D. Microsoft Defender Exploit Guard

Suggested Answer: *A*

Alien1981 Highly Voted 3 years, 6 months ago
Agreed
Introduced in Windows 10 Enterprise and Windows Server 2016, Windows Defender Credential Guard uses virtualization-based security to isolate secrets so that only privileged system software can access them. Unauthorized access to these secrets can lead to credential theft attacks, such as Pass-the-Hash or Pass-The-Ticket. Windows Defender Credential Guard prevents these attacks by protecting NTLM password hashes, Kerberos Ticket Granting Tickets, and credentials stored by applications as domain credentials.

https://docs.microsoft.com/en-us/windows/security/identity-protection/credential-guard/credential-guard
upvoted 16 times

NikPat3125 Highly Voted 3 years, 5 months ago
came in exam 27.07.2021
upvoted 10 times

Glorence Most Recent 2 years, 11 months ago
still valid, it was in my exam last feb 5, 2022 but the choices are reshuffled
upvoted 6 times

gxsh 3 years, 1 month ago
A. Microsoft Defender Credential Guard, Correct.
upvoted 2 times

Dave12 3 years, 3 months ago
Came in exam 22.09.2021
upvoted 4 times

haazybanj 3 years ago
As usual, Thanks for the heads up!
upvoted 2 times

Fundiso 3 years, 5 months ago
Agreed, A is the correct answer.
upvoted 6 times

Question #67 *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 computer that runs Windows 10.
You need to verify which version of Windows 10 is installed.
Solution: From Device Manager, you view the computer properties.
Does this meet the goal?

A. Yes

B. No

Suggested Answer: *B*
Reference:
https://support.microsoft.com/en-us/windows/which-version-of-windows-operating-system-am-i-running-628bec99-476a-2c13-5296-9dd081cdd808

Community vote distribution

B (100%)

TechMinerUK 2 years, 2 months ago

Selected Answer: B

I've just tried this, there is no "Computer Properties" in Device Manager. As others have stated you can go to "Help, About Device Manager" however this is not explicitly stated in the question

upvoted 2 times

mackypatio 2 years, 3 months ago

Open devmgmt.msc > help > about MMC

upvoted 2 times

mackypatio 2 years, 3 months ago

not computer properties

upvoted 2 times

L33D 2 years, 6 months ago

Still valid, on exam Jun 25, 2022

upvoted 3 times

rrrr5r 2 years, 3 months ago

In the exam in Sep 16 2022.

upvoted 1 times

xavier11 2 years, 10 months ago

its a poweshell question

upvoted 1 times

[Removed] 3 years ago

Just to make sure the question is a bit ambiguous, if you open Device Manager, About, About MMC, you can see the OS version just fine. But hey, I guess that's not what they meant exactly... :)

upvoted 2 times

gxsh 3 years ago

NO, that (Device Manager) shows hardware components etc.

upvoted 1 times

Fundiso 3 years, 5 months ago

Agreed, you can confirm this for yourself in seconds by going to Device Manager then Computer then Properties. B is undoubtedly correct.

upvoted 3 times

Sansup89 3 years, 4 months ago

Its no because you can see version under Hardware section and not the properties section

upvoted 1 times

Velda 3 years, 1 month ago

Just to specify this - It's under "Properties" but under properties of "My Computer" not Device Manager.. So if you'll open file explorer window-> right click on "My computer" and "Properties", you can see there Win version. Device Manager has nothing to do with OS version and you cannot select there "Computer" or its "Properties".

All in all, provided answer is correct - answer is NO.

upvoted 4 times

Question #68 *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 computer that runs Windows 10.
You need to verify which version of Windows 10 is installed.
Solution: At a command prompt, you run the winver.exe command.
Does this meet the goal?

A. Yes

B. No

Suggested Answer: *A*
Reference:
https://support.microsoft.com/en-us/windows/which-version-of-windows-operating-system-am-i-running-628bec99-476a-2c13-5296-9dd081cdd808

Community vote distribution
A (100%)

otday Highly Voted 3 years, 6 months ago
Run the command, it works.
upvoted 10 times

Fundiso 3 years, 5 months ago
Agreed, the answer is correct.
upvoted 4 times

agnesmandriva Most Recent 1 year, 10 months ago
Selected Answer: A
Just test it
upvoted 1 times

dumpmaster 2 years, 4 months ago
Classic command!
upvoted 2 times

H3adcap 2 years, 4 months ago
Was in exam today 20 Aug 2022
upvoted 2 times

L33D 2 years, 6 months ago
Still valid, on exam Jun 25, 2022
upvoted 2 times

AM77 3 years, 2 months ago
This is the correct answer
upvoted 3 times

JhonyTrujillo 3 years, 4 months ago
winver, msinfo32, systeminfo.
upvoted 4 times

balajim212 3 years, 5 months ago
Correct answer
upvoted 3 times

Question #69 *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 computer that runs Windows 10.
You need to verify which version of Windows 10 is installed.
Solution: From the Settings app, you select Update & Security to view the update history.
Does this meet the goal?

A. Yes

B. No

Suggested Answer: *B*
Reference:
https://support.microsoft.com/en-us/windows/which-version-of-windows-operating-system-am-i-running-628bec99-476a-2c13-5296-9dd081cdd808

Community vote distribution

B (100%)

Dislexsick 1 year, 9 months ago
I totally understand winver is the most correct answer, but given "Some question sets might have more than one correct solution" I saw this questiong and internally laughed, going with "Yes, but it's probably officially a no" -- Because the updates screen will often have updates installed that tell you the version of Windows installed...
upvoted 1 times

rrrr5r 2 years, 3 months ago
Easy question but it's in the exam in Sep 16 2022.
upvoted 2 times

gxsh 3 years ago
winver.exe shows Microsoft Windows version, Update history shows Feature update to Windows 10, so Yes or No ???
upvoted 3 times

Jimboski 1 year, 8 months ago
Would say now since you would need to still look at the KB's and check the build number manually. Sys info would be the other way to get this info besides winver
upvoted 1 times

us3r 3 years ago
Selected Answer: B
Easy NO.

If you have not applied any updates, no version will be displayed.
If you have cleared the update history, no ver will be displayed.
and so on...
upvoted 4 times

MartiFC 3 years, 1 month ago
It seems to me that this option is not the best, winver and system properties we can see the version. But we can also see the version here. If I need to know the version, this option will be the last of all. I say that NO
upvoted 1 times

AM77 3 years, 2 months ago
winver.exe is the correct answer.
upvoted 3 times

Yetijo 3 years, 3 months ago

B. No

winver.exe is the correct answer

upvoted 2 times

Tonysurge 3 years, 5 months ago

I will stick with NO as this is not mentioned in MS Docs:

https://support.microsoft.com/en-us/windows/which-version-of-windows-operating-system-am-i-running-628bec99-476a-2c13-5296-9dd081cdd808

upvoted 4 times

[Removed] 3 years ago

Agree. Your solution also shows the build nr - same with winver. In Windows Updates you only see the update history… I go def with B - no.

upvoted 1 times

zakyntos 3 years, 5 months ago

should be YES (easy to verify :))

upvoted 3 times

otday 3 years, 6 months ago

Tested this, it also showed me the correct version

upvoted 2 times

adaniel89 3 years, 6 months ago

Yes and No, if you happen to clear the Software Distribution folder, all update history is gone.

Proper answer would be "winver.exe" Or under Settings > System > About > Windows specifications.

upvoted 3 times

[Removed] 3 years, 6 months ago

I think this answer should be yes.

For example, in update history it will show (in my case) cumulative update for Windows 10 20H2.

upvoted 2 times

Requi3m 3 years, 4 months ago

Does it also show on which computers the update is currently installed? If not, the answer should be no. The question asks to verify the Windows version on a specific computer.

upvoted 1 times

Question #70 *Topic 1*

You have a Microsoft 365 tenant that uses Microsoft Endpoint Manager for device management.
You need to add the phone number of the help desk to the Company Portal app.
What should you do?

A. From the Microsoft 365 admin center, modify Organization information.

B. From the Microsoft Endpoint Manager admin center, create an app configuration policy.

C. From Customization in the Microsoft Endpoint Manager admin center, modify the support information for the tenant.

D. From the Microsoft 365 admin center, modify Help desk information.

Suggested Answer: *C*
Reference:
https://systemcenterdudes.com/intune-company-portal-customization/

Community vote distribution
C (100%)

marckinez Highly Voted 3 years, 2 months ago
it´s correct, in Tenant admin--Customization you can add this information
upvoted 11 times

Dolhave2 Highly Voted 2 years, 6 months ago
Selected Answer: C
Correct checked in my Test tenant
upvoted 5 times

LillyLiver Most Recent 2 years, 10 months ago
Selected Answer: C
Agree. Just checked it in my tenant.
upvoted 4 times

ericwiley 2 years, 11 months ago
Correct,
upvoted 2 times

gxsh 3 years ago
Correct.
upvoted 3 times

Question #71 *Topic 1*

You have a Microsoft 365 E5 tenant.
You plan to deploy 1,000 new iOS devices to users. The devices will be shipped directly from the supplier to the users.
You need to recommend a Microsoft Intune enrollment option that meets the following requirements:
✑ Minimizes user interaction
✑ Minimizes administrative effort
✑ Automatically installs corporate apps
What should you recommend?

A. Apple Configurator enrollment

B. Automated Device Enrollment (ADE)

C. bring your own device (BYOD) user and device enrollment.

Suggested Answer: *B*
Reference:
https://docs.microsoft.com/en-us/mem/intune/enrollment/ios-enroll

marckinez Highly Voted 3 years, 2 months ago
Correct, I think this is the link: https://docs.microsoft.com/en-us/mem/intune/enrollment/device-enrollment-program-enroll-ios
upvoted 7 times

RiTh73 Most Recent 1 year, 10 months ago
Corporate-owned devices purchased through Apple Business Manager or Apple School Manager can be enrolled in Intune via automated device enrollment. This enrollment option applies your organization's settings from Apple Business Manager and Apple School Manager and enrolls devices without you needing to touch them. iPhones and iPads can be shipped directly to employees and students. When they turn on their devices, Apple Setup Assistant guides them through setup and enrollment.
upvoted 3 times

gdunlop 2 years, 3 months ago
A could be correct also?
For organizations that buy devices for their users, Intune supports the following iOS/iPadOS company-owned device enrollment methods:

Apple's Automated Device Enrollment (ADE)
Apple School Manager
Apple Configurator Setup Assistant enrollment
Apple Configurator direct enrollment
upvoted 2 times

Meeteetsee 2 years, 2 months ago
The question states that its shipping from a supplier to the users so that is why its B.
upvoted 3 times

gxsh 3 years ago
Correct.
upvoted 4 times

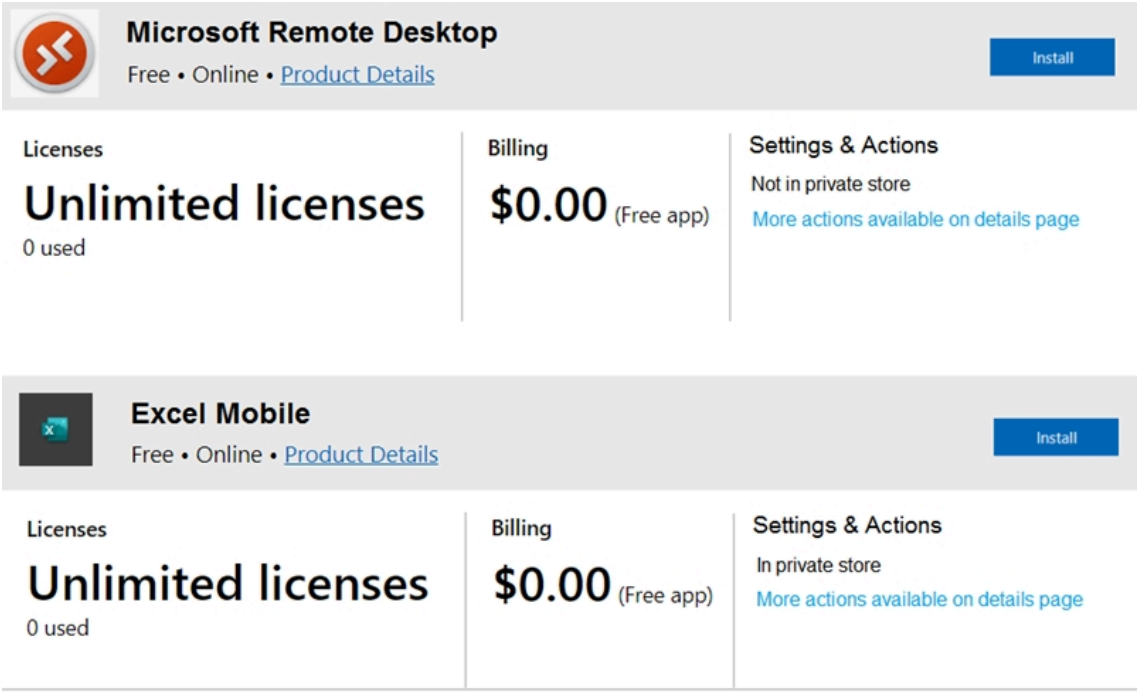
HOTSPOT -

You have a Microsoft 365 tenant that is signed up for Microsoft Store for Business and contains the users shown in the following table.

Name	Microsoft Store for Business role	Azure Active Directory (Azure AD) role
User1	Purchaser	Billing administrator
User2	Admin	Global administrator
User3	Basic Purchaser	None
User4	Basic Purchaser, Device Guard signer	Global reader

All users have Windows 10 Enterprise devices.

The Products & services settings in Microsoft Store for Business are shown in the following exhibit.



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

NOTE: Each correct selection is worth one point.

Hot Area:

Answer Area

Statements	Yes	No
User2 can install the Microsoft Remote Desktop app from the private store.	○	○
User1 can install the Microsoft Remote Desktop app from Microsoft Store for Business.	○	○
User4 can manage the Microsoft Remote Desktop app from the private store.	○	○

Suggested Answer:

Answer Area

Statements	Yes	No
User2 can install the Microsoft Remote Desktop app from the private store.	○	○
User1 can install the Microsoft Remote Desktop app from Microsoft Store for Business.	○	○
User4 can manage the Microsoft Remote Desktop app from the private store.	○	○

Reference:
https://docs.microsoft.com/en-us/microsoft-store/roles-and-permissions-microsoft-store-for-business

gxsh Highly Voted 3 years, 1 month ago
Microsoft Remote Desktop is not on private store, question 1 and 3.
upvoted 12 times

Durden871 Highly Voted 2 years, 5 months ago
NYN is correct. Eroc1990 said in another thread,
<App from the private store>
Remote Desktop is not in the Private store. It says it in the picture to the right under settings and actions.
upvoted 7 times

Bulldozzer Most Recent 2 years, 10 months ago
For me, the correct answer is Y, Y, N. Indeed, even if it is not specified in the question statement, the application can be added to the private store by user 2 since he has the administrator role.
upvoted 3 times

Durden871 2 years, 5 months ago
It's NYN, Remote Desktop isn't in the private store. It's a trick question.
upvoted 7 times

marckinez 3 years, 2 months ago
Global Administrator and Billing Administrator - IT Pros with these accounts have full access to Microsoft Store. They can do everything allowed in the Microsoft Store Admin role, plus they can sign up for Microsoft Store.
upvoted 2 times

eroc1990 3 years, 1 month ago
The catch here is that User2, the global admin, can't install Remote Desktop from the private store because the app is not in the private store. See some of the other replies in FabioC's thread.
upvoted 9 times

MartiFC 3 years, 2 months ago
We can install apps form private store:
https://docs.microsoft.com/en-us/microsoft-store/manage-private-store-settings
But I haven't clear if apply in this question.
Any suggestion?
upvoted 1 times

FabioC 3 years, 2 months ago
I don't understand. User 1 can't buy the app because it's a billing admin ?
upvoted 1 times

us3r 3 years ago
hi there!
upvoted 1 times

FabioC 3 years, 2 months ago
user 2 not user 1 sorry. :)
upvoted 1 times

Turak64 3 years, 2 months ago
Look under "Settings & Actions". The is not in the private store.
upvoted 9 times

Question #73 *Topic 1*

Your company has offices in five cities.
The company has a Microsoft 365 tenant.
Each office is managed by a local administrator.
You plan to deploy Microsoft Intune.
You need to recommend a solution to manage resources in Intune that meets the following requirements:
✑ Local administrators must be able to manage only the resources in their respective office.
✑ Local administrators must be prevented from managing resources in other offices.
✑ Administrative effort must be minimized.
What should you include in the recommendation?

A. scope tags

B. device categories

C. configuration profiles

D. conditional access policies

Suggested Answer: *A*
Reference:
https://docs.microsoft.com/en-us/mem/intune/fundamentals/scope-tags

Community vote distribution
A (100%)

marckinez Highly Voted 3 years, 2 months ago
Correct
upvoted 9 times

H3adcap Highly Voted 2 years, 4 months ago
Was in exam today 20 Aug 2022
upvoted 6 times

in_cloud Most Recent 1 year, 5 months ago
On exam july/2023
upvoted 1 times

agnesmandriva 1 year, 10 months ago
Now it colud be administrative units :) https://learn.microsoft.com/en-us/azure/active-directory/roles/administrative-units
upvoted 1 times

RazielLycas 2 years, 5 months ago
Selected Answer: A
scope tag is correct
upvoted 2 times

reastman66 2 years, 5 months ago
Agree with A. Scope tags determine which objects admins can see.
upvoted 2 times

HOTSPOT -

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

Name	Microsoft 365 role
User1	Cloud application administrator
User2	Application administrator
User3	Application developer
User4	**None**

Users are assigned Microsoft Store for Business roles as shown in the following table.

User	Role
User1	**None**
User2	Basic Purchaser
User3	Purchaser
User4	Device Guard signer

Which users can add apps to the private store in Microsoft Store for Business, and which users can install apps from the private store? To answer, select the appropriate options in the answer area.

NOTE: Each correct selection is worth one point.

Hot Area:

Answer Area

Add apps to the private store:
- User3 only
- User2 and User3 only
- User1 and User3 only
- User1, User2 and User3 only
- User1, User2, User3, and User4

Install apps from the private store:
- User3 only
- User2 and User3 only
- User1 and User3 only
- User2, User3 and User4 only
- User1, User2, User3, and User4

Suggested Answer:

Answer Area

Add apps to the private store:
- User3 only
- **User2 and User3 only**
- User1 and User3 only
- User1, User2 and User3 only
- User1, User2, User3, and User4

Install apps from the private store:
- User3 only
- User2 and User3 only
- User1 and User3 only
- User2, User3 and User4 only
- **User1, User2, User3, and User4**

Reference:

https://docs.microsoft.com/en-us/microsoft-store/acquire-apps-microsoft-store-for-business https://docs.microsoft.com/en-us/microsoft-store/distribute-apps-from-your-private-store

JT19760106 Highly Voted 2 years, 11 months ago

Answer1: User 3
Answer2: All
I've tried this in my test Microsoft Business Store environment and there are 4 roles:
-Admin
-Purchaser
-Basic Purchaser
-Device Guard signer
The first 3 had the permission to "Procure from the Microsoft Store", however when testing this by assigning someone the Basic Purchaser role, all they could do is request the app for themselves and an admin would have to approve it.
upvoted 16 times

ServerBrain 2 years, 1 month ago

The setting: Allow users to shop is set to On/Off.

Allow users to shop controls the shopping experience in Microsoft Store for Education. When this setting is on, Purchasers and Basic Purchasers can purchase products and services from Store.
In this case we are not told if this setting is ON, so answers are User 3 and All
upvoted 1 times

LK4723 2 years, 3 months ago

I would agree with this and get the same thing when trying to obtain apps from Microsoft Store for Business with basic purchaser assigned. A little confused on how others are stating basic purchaser does not exist as there are clearly four permissions in my tenant for Business Store. I sure hope Microsoft is considering the fact that is approved the app gets added as that it what happens but only after it is requested and approved by someone with permissions.
upvoted 2 times

MartiFC Highly Voted 3 years, 2 months ago

Basic Purchaser is for Store for Education, not for Bussiness. I thing that User2 isn't add an app to Store for Bussiness.

And for the future, the new information is that Microsoft Store for Business and Microsoft Store for Education will be retired in the first quarter of 2023. You can continue to use the current capabilities of free apps until that time
Starting on April 14th, 2021, only free apps will be available in Microsoft Store for Business and Education
upvoted 7 times

B1G_B3N 3 years ago

agreed
upvoted 2 times

owenMS Most Recent 1 year, 11 months ago

I have checked this with my test tenant and I have Basic Purchaser as an available permission in MSfB
upvoted 2 times

TechMinerUK 2 years, 2 months ago

This seems to be confusing and I don't have a definite answer however I would say that the presented answer is correct only if they are using the Microsoft Store for Education based on the following links: https://learn.microsoft.com/en-us/education/windows/education-scenarios-store-for-business#basic-purchaser-role and https://github.com/MicrosoftDocs/windows-itpro-docs/pull/6816

The first page states: "Basic Purchaser role can only manage (assign and reclaim licenses) for apps that they have purchased"

However the second page states "The basic purchaser role in Microsoft Store for business doesn't have the ability to acquire apps"

This means that both the purchaser and basic purchaser can assign apps to the Private Store if it is an Educational tenant however if it is a standard Business tenant the functionality wouldn't be present for the Basic Purchaser role
upvoted 1 times

Koryzed 2 years, 5 months ago

anser:correct, Admins, Purchasers, and Basic Purchasers can assign online-licensed apps to employees or students in their organization.
https://docs.microsoft.com/zh-tw/microsoft-store/assign-apps-to-employees
upvoted 2 times

Durden871 2 years, 5 months ago
Looks right:
Admins, Purchasers, and Basic Purchasers can assign online-licensed apps to employees or students in their organization.
upvoted 1 times

Koetjeboe 2 years, 7 months ago
Both Basic Basic Purchaser and Purchaser roles are available in the SfB. These 2 roles (and the SfB role Admin) can Procure from Microsoft Store.

To go to your own Sfb Roles: https://businessstore.microsoft.com/en-us/manage/permissions/users
upvoted 2 times

reastman66 2 years, 5 months ago
I agree and have tested in my SfB for Basic Purchaser.
upvoted 2 times

JamesM9 2 years, 9 months ago
The Basic Purchaser role cannot add apps and currently the Basic purchaser role is only available for schools using Microsoft Store for Education. So therefore the answer here is

1.User 3
2. Users 1, 2, 3, 4

https://docs.microsoft.com/en-us/microsoft-store/microsoft-store-for-business-overview
upvoted 5 times

us3r 3 years ago
Ans1 User2,User3
Ans2 User1,User2,User3,User4
upvoted 1 times

us3r 3 years ago
update:

Ans1 User3 ONLY

https://docs.microsoft.com/en-us/microsoft-store/microsoft-store-for-business-overview

Currently, the Basic purchaser role is only available for schools using Microsoft Store for Education. For more information, see Microsoft Store for Education permissions.
upvoted 4 times

B1G_B3N 3 years ago
https://docs.microsoft.com/en-us/microsoft-store/roles-and-permissions-microsoft-store-for-business
(If basic purchaser education store = purchaser business store) then answer correct. If not id say purchaser only. Again not well defined question

install apps is definitely all users
upvoted 1 times

JAPo123 3 years ago
https://docs.microsoft.com/en-us/microsoft-store/microsoft-store-for-business-overview#set-up
upvoted 1 times

TimurKazan 3 years ago
correct
upvoted 3 times

TimurKazan 3 years ago
sorry, 1 - user 3 only
2 - all users

upvoted 2 times

jkklim 3 years, 1 month ago

Microsoft Store for Business - USER3 can add apps

Install APPS - ALL users

upvoted 2 times

jkklim 3 years, 1 month ago

what is the answer then ?

upvoted 1 times

Question #75 *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 computer that runs Windows 10.
You need to verify which version of Windows 10 is installed.
Solution: From the Settings app, you select System, and then you select About to view information about the system.
Does this meet the goal?

A. Yes

B. No

Suggested Answer: *A*
Reference:
https://support.microsoft.com/en-us/windows/which-version-of-windows-operating-system-am-i-running-628bec99-476a-2c13-5296-9dd081cdd808

VirtualJP Highly Voted 3 years, 1 month ago
Correct
upvoted 6 times

GotDamnImIn Most Recent 1 year, 8 months ago
A definite yes!
upvoted 2 times

L33D 2 years, 6 months ago
Still valid, on exam Jun 25, 2022
upvoted 4 times

Johnnien 3 years, 1 month ago
Select the Start button > Settings > System > About .

Open About settings

Under Device specifications > System type, see if you're running a 32-bit or 64-bit version of Windows.

Under Windows specifications, check which edition and version of Windows your device is running.
upvoted 3 times

Question #76 *Topic 1*

You have a Microsoft 365 tenant that contains 1,000 iOS devices enrolled in Microsoft Intune.
You plan to purchase volume-purchased apps and deploy the apps to the devices.
You need to track used licenses and manage the apps by using Intune.
What should you use to purchase the apps?

A. Microsoft Store for Business

B. Apple Configurator

C. Apple Business Manager

D. Apple iTunes Store

Suggested Answer: *C*
Reference:
https://docs.microsoft.com/en-us/mem/intune/apps/vpp-apps-ios

Community vote distribution
C (100%)

gxsh Highly Voted 3 years ago
Correct.
upvoted 8 times

Jimboski Most Recent 1 year, 8 months ago
Correct, just set this up for one of my clients
upvoted 1 times

ServerBrain 2 years, 1 month ago
Selected Answer: C
Correct - Apple Business Manager
upvoted 1 times

DFFECT 2 years, 4 months ago
100% correct
upvoted 3 times

Question #77 *Topic 1*

You have a Microsoft 365 E5 tenant that contains the devices shown in the following table.

Name	Windows 10 edition	Azure Active Directory (Azure AD)	Mobile device management (MDM) enrollment
Device1	Windows 10 Pro	Registered	Microsoft Intune
Device2	Windows 10 Enterprise	Joined	Microsoft Intune
Device3	Windows 10 Pro	Joined	Not enrolled
Device4	Windows 10 Enterprise	Registered	Microsoft Intune
Device5	Windows 10 Enterprise	Joined	Not enrolled

You add custom apps to the private store in Microsoft Store Business.

You plan to create a policy to show only the private store in Microsoft Store for Business.

To which devices can the policy be applied?

A. Device2 only

B. Device1 and Device3 only

C. Device2 and Device4 only

D. Device2, Device3, and Device5 only

E. Device1, Device2, Device3, Device4, and Device5

Suggested Answer: *C*

Reference:

https://docs.microsoft.com/en-us/microsoft-store/manage-access-to-private-store#show-private-store-only-using-mdm-policy

B1G_B3N Highly Voted 3 years ago

answer correct - show only private store 2 ways, via group policy or via MDM - both ways require win10 enterprise

https://docs.microsoft.com/en-us/microsoft-store/manage-access-to-private-store

upvoted 9 times

Glorence Highly Voted 2 years, 11 months ago

still valid, it was in my exam last feb 5, 2022

upvoted 9 times

Contactfornitish Most Recent 2 years, 4 months ago

On exam on 13 aug'22

upvoted 8 times

haazybanj 2 years, 11 months ago

What if Windows 10 enterprise is not enrolled to intune and you use a group policy? What are your thoughts about this guys?

upvoted 2 times

EnricoVignali 3 years ago

At the beginning the statement is "Microsoft 365 E5 tenant"

The device #1 have to switch automatically from Win10 Pro to Win10 Enterprise with E5 license...

upvoted 1 times

EnricoVignali 3 years ago

sorry, my fault: the device is "registered", not "joined"

upvoted 2 times

goape 3 years ago

Answer seems correct. Link references that it's only applicable to Enterprise edition. So long as a device is enrolled within Intune, should take policy enforcements

upvoted 5 times

Question #78 *Topic 1*

HOTSPOT -

You have a Microsoft 365 E5 subscription that uses Microsoft Intune.

You have devices enrolled in Intune as shown in the following table.

Name	Platform	Member of	Scope (Tags)
Device1	Windows 10	Group1, Group3	Tag1
Device2	Android	Group2	Tag2

You create the device configuration profiles shown in the following table.

Name	Platform	Assignments: Included groups	Assignments: Excluded groups	Scope tags
Profile1	Windows 10 and later	Group1	Group3	Tag1, Tag2
Profile2	Android Enterprise	All devices	Group2	Tag1, Tag2
Profile3	Android Enterprise	Group2, Group3	Group3	Tag1
Profile4	Windows 10 and later	Group3	**None**	Default

Which profiles will be applied to each device? To answer, select the appropriate options in the answer area.

NOTE: Each correct selection is worth one point.

Hot Area:

Answer Area

Device1:
- No profiles
- Profile1 only
- Profile4 only
- Profile1 and Profile4 only
- Profile1, Profile1, and Profile4 only

Device2:
- No profiles
- Profile1 only
- Profile2 only
- Profile3 only
- Profile1 and Profile2 only
- Profile2 and Profile3 only

Suggested Answer:

Answer Area

Device1:
- No profiles
- Profile1 only
- Profile4 only
- **Profile1 and Profile4 only**
- Profile1, Profile1, and Profile4 only

Device2:
- No profiles
- Profile1 only
- Profile2 only
- **Profile3 only**
- Profile1 and Profile2 only
- Profile2 and Profile3 only

goape Highly Voted 3 years ago

Device 1 will only take Profile 4. It is a member of Group 3 which is excluded from profile 1. Answer is:
Device 1: Profile 4
Device 2: Profile 3
upvoted 70 times

Sledgehammer 2 years, 10 months ago

Agreed with Goape. Exclusion takes precedence over inclusion. Scopre tags are not relevant
upvoted 5 times

TimurKazan 3 years ago

correct. Scope tags only determine which objects admins can see.
upvoted 9 times

jodtzz 3 years ago

This is as close to a correct answer as I see possible with the configuration of this question. How can you include a group and also exclude the same group? Makes no sense.
upvoted 5 times

sonnen_x 2 years, 11 months ago

Device 2: No Profile I think because Tag does not match
upvoted 5 times

KennethYY 2 years, 6 months ago

tag for management only
upvoted 3 times

veteran_tech 2 years, 4 months ago

Correct. Tags don't impact what device a profile applies to. Tags limit what a local admin can see.
upvoted 7 times

ubt Highly Voted 3 years ago

I thought it would be
Device 1: Profile 4
Device 2: No Profile (as Tag doesn't match Profile 3)
upvoted 5 times

Durden871 2 years, 5 months ago

Tags are for management.
upvoted 2 times

TimNov Most Recent 2 years, 6 months ago

Agree 100% with goape. Exclusions take precedence and scope tags are irrelevant.
upvoted 3 times

Zardu 2 years, 8 months ago

Just went through this one and agree with goape -- for Dev 1 the Exclusion prevents Profile 1, so it gets Profile 4 only.
Dev 2 gets Policy 3
can ignore the Scope tags in this situation
upvoted 3 times

Sledgehammer 2 years, 10 months ago

Agreed with Goape. Exclusion takes precedence over inclusion. Scopre tags are not relevant
upvoted 1 times

stealthster 2 years, 11 months ago

I think it should be:
Device 1: No Profiles
Device 2: No Profiles

For Device 1: https://docs.microsoft.com/en-us/mem/intune/apps/apps-inc-exl-assignments : Exclusion takes precedence over inclusion in the following same group type scenarios so that makes Profile 1 not apply.
For Device 1 & 2: https://tech.nicolonsky.ch/intune-scope-tags-rbac-explained/- A scope tag assigns an Intune configuration (e.g. device

configuration, compliance policy, mobile app or managed device) to one or more specific management scope(s).

Default tag:
By default, all Intune entities which are created from a user without an Intune role (which means it was either an Intune Administrator or Global Admin) get automatically assigned this built-in scope tag. Every object in Intune needs to have at least one scope tag assigned.

This seems to make profile 4 for device 1 not apply and profile 3 for device 2 not apply so I believe it No Profiles for both.
upvoted 4 times

stealthster 2 years, 9 months ago
After reviewing again, I believe it is Device 1 - Profile 4 Only and Device 2 - Profile 3 only.
upvoted 5 times

AlexBa 3 years ago
I think, No profil for device 1 and 2 because the tag scope is not correct.
upvoted 1 times

AlexBa 3 years ago
https://tech.nicolonsky.ch/intune-scope-tags-rbac-explained/
upvoted 3 times

Futfuyfyjfj 1 year, 8 months ago
Apparently you don't know what scope tags are, they are not relevant in profile/configuration deployment.
upvoted 1 times

Goena 3 years ago
Answer seems correct:
Device 1: Profile 1 and 4 only - member of Group 1 and excluded of Group 3, but still member of Group 1.
Device 2: Profile 3 only.
upvoted 2 times

Durden871 2 years, 5 months ago
Even though Group 3 has been excluded from profile 1?
upvoted 1 times

MallonoX_111 2 years, 11 months ago
exclusion takes precedence over inclusion
upvoted 6 times

ZuluHulu 3 years ago
Correction: Are scope tags in the policy Profile relevant when applying to the device? Profile 3 has a scope tag1 but the device has tag2
upvoted 1 times

ZuluHulu 3 years ago
Are scope tags in the policy Profile relevant when applying to the device? Profile 3 has a scope tag2 but the device has tag1.
upvoted 1 times

chepeerick 2 years, 10 months ago
the device profile assign that tag to the system, it not used as criteria
upvoted 4 times

Question #79 *Topic 1*

You have a Microsoft 365 E5 tenant that uses Microsoft Intune.
You need to ensure that users can select a department when they enroll their device in Intune.
What should you create?

A. scope tags

B. device configuration profiles

C. device categories

D. device compliance policies

Suggested Answer: *C*
Reference:
https://docs.microsoft.com/en-us/mem/intune/enrollment/device-group-mapping

Goena Highly Voted 3 years ago
Answer is indeed C:
- create a dynamic group
- create a device group with an advanced rule, by using the deviceCategory
- configure Device category in Endpoint Manager
The user in the group will be prompted to assign Device Category.
upvoted 13 times

goape Highly Voted 3 years ago
Answer is C. When enrolling, company portal will prompt the user to assign the device a category.
upvoted 8 times

Question #80 *Topic 1*

HOTSPOT -

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

Name	Azure Active Directory (Azure AD) role	Microsoft Store for Business role	Member of
User1	Application administrator	Basic Purchaser	Group1
User2	**None**	Purchaser	Group2
User3	**None**	Basic Purchaser	Group3

You perform the following actions:

- Provision the private store in Microsoft Store for Business.
- Add an app named App1 to the private store.
- Set Private store availability for App1 to Specific groups, and then select Group3.

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 install App1 from the private store.	○	○
User2 can install App1 from the private store.	○	○
User3 can install App1 from the private store.	○	○

Suggested Answer:

Answer Area

Statements	Yes	No
User1 can install App1 from the private store.	○	○
User2 can install App1 from the private store.	○	○
User3 can install App1 from the private store.	○	○

Reference:

https://docs.microsoft.com/en-us/microsoft-store/app-inventory-management-microsoft-store-for-business#private-store-availability

B1G_B3N Highly Voted 3 years ago

answer correct - sets availability to group 3 only which is what can install the apps

upvoted 14 times

Glorence Highly Voted 2 years, 11 months ago

still valid, it was in my exam last Feb 5, 2022

upvoted 9 times

GotDamnImIn Most Recent 1 year, 8 months ago

Surprised how straightforward this was. Only User 3 can install because he's member of Group 3

upvoted 2 times

L33D 2 years, 6 months ago

Still valid, on exam Jun 25, 2022

upvoted 8 times

TimurKazan 3 years ago

So isn't Basic Purchaser role availvable only in Store for Education?

upvoted 3 times

FreddyLao 3 years ago

it has nothing to do with the role but the group assigned. so only group 3 users can install the app

upvoted 10 times

TimurKazan 3 years ago

thx, I got your point

upvoted 2 times

Goena 3 years ago

Answer correct.

upvoted 4 times

Question #81 *Topic 1*

You have a Microsoft 365 tenant that is signed up for Microsoft Store for Business and contains a user named User1.
You need to ensure that User1 can perform the following tasks in Microsoft Store for Business:
✑ Assign licenses to users.
✑ Procure apps from Microsoft Store.
✑ Manage private store availability for all items.
The solution must use the principle of least privilege.
Which Microsoft Store for Business role should you assign to User1?

A. Admin

B. Device Guard signer

C. Basic Purchaser

D. Purchaser

Suggested Answer: *A*
Reference:
https://docs.microsoft.com/en-us/microsoft-store/microsoft-store-for-business-overview

Community vote distribution
A (100%)

edzio Highly Voted 2 years, 11 months ago
"Manage private store availability for all items." - only for admin
upvoted 9 times

B1G_B3N Highly Voted 3 years ago
Selected Answer: A
By admin i'm assuming it means the MS Store for Business Admin role? In which case yes. It = global admin role which is what first person who signed up for the store must be also.
upvoted 6 times

Lelek Most Recent 1 year, 10 months ago
Selected Answer: A
Admin= Assign roles, Manage Microsoft Store for Business and Education settings, Acquire apps, Distribute apps, Sign policies and catalogs and Sign Device Guard changes

Purchaser = Acquire apps and Distribute apps

Device Guard signer = Sign Device Guard changes

https://learn.microsoft.com/en-us/microsoft-store/roles-and-permissions-microsoft-store-for-business
upvoted 2 times

Goena 3 years ago
Answer A is correct:
Once you are signed up with the Business store and have purchased apps, Admins can manage Store for Business settings and inventory.
upvoted 4 times

Question #82 *Topic 1*

Your company has multiple offices.
You have a Microsoft 365 E5 tenant that uses Microsoft Intune for device management. Each office has a local administrator.
You need to ensure that the local administrators can manage only the devices in their respective office.
What should you use?

A. scope tags

B. configuration profiles

C. device categories

D. conditional access policies

Suggested Answer: *A*
Reference:
https://docs.microsoft.com/en-us/mem/intune/fundamentals/scope-tags

Goena Highly Voted 3 years ago
Answer A is correct:
You can use role-based access control and scope tags to make sure that the right admins have the right access and visibility to the right Intune objects. Roles determine what access admins have to which objects. Scope tags determine which objects admins can see.
upvoted 9 times

TimNov Most Recent 2 years, 6 months ago
Couldn't you technically use conditional access too though ?
upvoted 1 times

xyz213 2 years, 3 months ago
I guess but it askes "What should you use?" not "What can you use?".
Classic MS BS.
upvoted 2 times

Question #83 *Topic 1*

HOTSPOT -

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

Name	Member of
User1	Group1
User2	Group2

You purchase the devices shown in the following table.

Name	Platform
Device1	Windows 10
Device2	Android

In Microsoft Endpoint Manager, you create an enrollment status page profile that has the following settings:

- ✑ Show app and profile configuration progress: Yes
- ✑ Allow users to collect logs about installation errors: Yes
- ✑ Only show page to devices provisioned by out-of-box experience (OOBE): No
- ✑ Assignments: 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
If User1 enrolls Device1 in Microsoft Endpoint Manager, the enrollment status page will appear.	○	○
If User2 enrolls Device1 in Microsoft Endpoint Manager, the enrollment status page will appear.	○	○
If User2 enrolls Device2 in Microsoft Endpoint Manager, the enrollment status page will appear.	○	○

Suggested Answer:

Answer Area

Statements	Yes	No
If User1 enrolls Device1 in Microsoft Endpoint Manager, the enrollment status page will appear.	○	○
If User2 enrolls Device1 in Microsoft Endpoint Manager, the enrollment status page will appear.	○	○
If User2 enrolls Device2 in Microsoft Endpoint Manager, the enrollment status page will appear.	○	○

Reference:

https://docs.microsoft.com/en-us/mem/intune/enrollment/windows-enrollment-status

Goena Highly Voted 3 years ago

Answers are correct:

- User 1 is not member of Group 2: NO
- User 2 is member of Group 2 which is shown the Status page: YES. The enrollment status page is shown to devices that go through the out-of-box experience (OOBE) and the first logged on user, but not to subsequent users who logon to the device.
- Device 2 is Android: NO

upvoted 18 times

Glorence Highly Voted 2 years, 11 months ago

still valid, it was in my exam last Feb 5, 2022

upvoted 9 times

TechMinerUK Most Recent 2 years, 2 months ago

As AlgeriaBoy has mentioned I think this question requires some additional detail as based on the standard Intune setup it would be Y, N, Y.

The reasoning is as follows:

1. Y - The default ESP configuration which would be applied to User 1 as they are not a member of Group 2 shows the ESP to all users on all Windows 10 or higher devices that are enrolled regardless of them being enrolled at the OOBE. The question also doesn't state that the stage where the device is enrolled (E.g. at OOBE or after OOBE is completed)
2. Y - User 2 will see the ESP as they have a custom policy assigned which shows the ESP to all enrolled devices regardless of enrollment at or after OOBE
3. - N - Android devices do not see ESP as it is not part of the OS

I can understand 1. being N if the question mentioned the default ESP with the lowest priority being configured to not show however this is never mentioned therefore it must be in the default configuration.

The question requires more detail to have a confident answer given
upvoted 1 times

TechMinerUK 2 years, 2 months ago
To clarify, I meant YYN not YNY
upvoted 2 times

TechMinerUK 2 years, 2 months ago
Actually, disregard both my above posts, the provided answer is indeed correct as I have just tested the above with a brand new tenant with no prior Intune configuration and it would by NYN as the tenant in question had the following setting configured on the default ESP policy

"Show app and profile configuration progress - No"

This would mean only User 2 would see the ESP as they have a policy configured to show the ESP, User 1 would have the default policy applied which does not show the ESP
upvoted 1 times

AlgeriaBoy 2 years, 11 months ago
YES,YES, NO
1. User1 is a member of Group1. Neither User1 nor Device1 has an Enrollment Status Page (ESP) assigned. The default ESP is used, which has "Only show page to devices provisioned by out-of-box experience (OOBE)" set to No.
This is the default enrollment status screen configuration applied with the lowest priority to all users and all devices regardless of group membership.
2. User2 is a member of Group2. User2 has the custom Enrollment Status Page (ESP) assigned. The custom ESP has "Only show page to devices provisioned by out-of-box experience (OOBE)" set to No.
3. The enrollment status page is shown on Windows devices only. Device2 is an Android device.
upvoted 7 times

edzio 2 years, 9 months ago
Only show page to devices provisioned by out-of-box experience (OOBE): Your options:

- No: The enrollment status page is shown on all Intune-managed and co-managed devices that go through the out-of-box experience (OOBE), and to the first user that signs in to each device. So subsequent users who sign in don't see the ESP.
- Yes: The enrollment status page is only shown on devices that go through the out-of-box experience (OOBE).

https://docs.microsoft.com/en-us/mem/intune/enrollment/windows-enrollment-status
upvoted 2 times

AVR31 2 years, 5 months ago
Yes, there is a default ESP but it has a single setting that says: "Show app and profile configuration progress" and it is set to NO. So first question is still a NO.
upvoted 1 times

gxsh 3 years ago
no, yes, no
upvoted 2 times

Question #84 *Topic 1*

DRAG DROP -

You have a Microsoft 365 E5 tenant.

You need to implement compliance solutions that meet the following requirements:

✑ Use a file plan to manage retention labels.

✑ Identify, monitor, and automatically protect sensitive information.

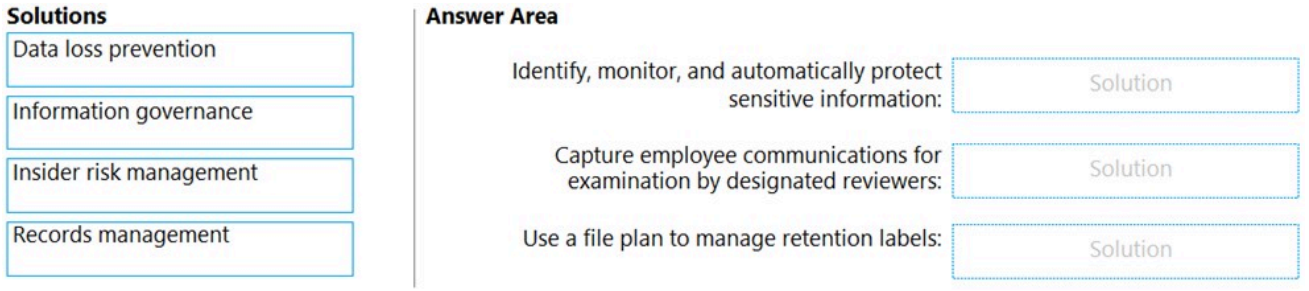
Capture employee communications for examination by designated reviewers.

▪

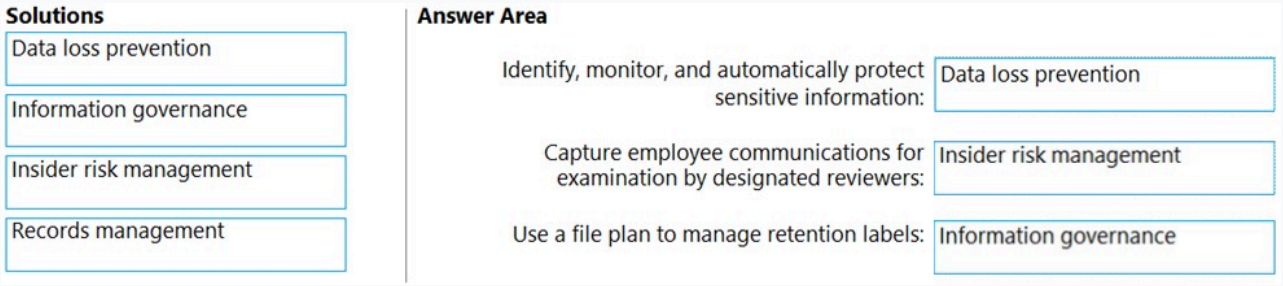
Which solution should you use for each requirement? To answer, drag the appropriate solutions to the correct requirements. Each solution may be used once, more than once, or not at all. You may need to drag the split bat between panes or scroll to view content.

NOTE: Each correct selection is worth one point.

Select and Place:



Suggested Answer:



Reference:

https://docs.microsoft.com/en-us/microsoft-365/compliance/dlp-learn-about-dlp?view=o365-worldwide https://docs.microsoft.com/en-us/microsoft-365/compliance/communication-compliance?view=o365-worldwide https://docs.microsoft.com/en-us/microsoft-365/compliance/file-plan-manager?view=o365-worldwide

JT19760106 Highly Voted 2 years, 11 months ago

Data Loss Prevention

Insider Risk Management

Records Management

upvoted 21 times

prabhjot 1 year, 8 months ago

yes IN-deed RECORD MANAGEMENT as last option (https://learn.microsoft.com/en-us/microsoft-365/compliance/file-plan-manager?view=o365-worldwide)

upvoted 1 times

RenegadeOrange 2 years, 3 months ago

Microsoft Purview menus have changed. If this question is in the exam now it would be:

Data Loss Prevention

Communication Compliance

Records Management

Communication compliance lets you define what communications and users to review and who can review them.

Insider Risk Management lets you find risky activity and from there raise a case which could be escalated to an eDiscovery case to view data if you wanted to argue it could be done.

upvoted 8 times

techtest848 Highly Voted 3 years ago

Use a file plan to manage retention label - I belive the answer to this question is Records Management - https://docs.microsoft.com/en-us/microsoft-365/compliance/file-plan-manager?view=o365-worldwide

upvoted 9 times

jodtzz 3 years ago

I agree: "Although you can create and manage retention labels from Information governance in the Microsoft 365 compliance center, file plan from Records management has additional management capabilities"

upvoted 4 times

VirtualJP 3 years ago

I guess the question comes down to, which would be Microsoft's preferred method. :-/

upvoted 5 times

Durden871 Most Recent 2 years, 5 months ago

Why is it not Information governance?

upvoted 4 times

prabhjot 1 year, 8 months ago

yes IN-deed RECORD MANAGEMENT as last option (https://learn.microsoft.com/en-us/microsoft-365/compliance/file-plan-manager?view=o365-worldwide)

upvoted 1 times

Glorence 2 years, 11 months ago

still valid, it was in my exam last Feb 5, 2022

upvoted 6 times

Question #85 *Topic 1*

HOTSPOT -

You have a Microsoft 365 E5 subscription.

You plan to use Windows Autopilot to deploy 100 new Windows 10 devices.

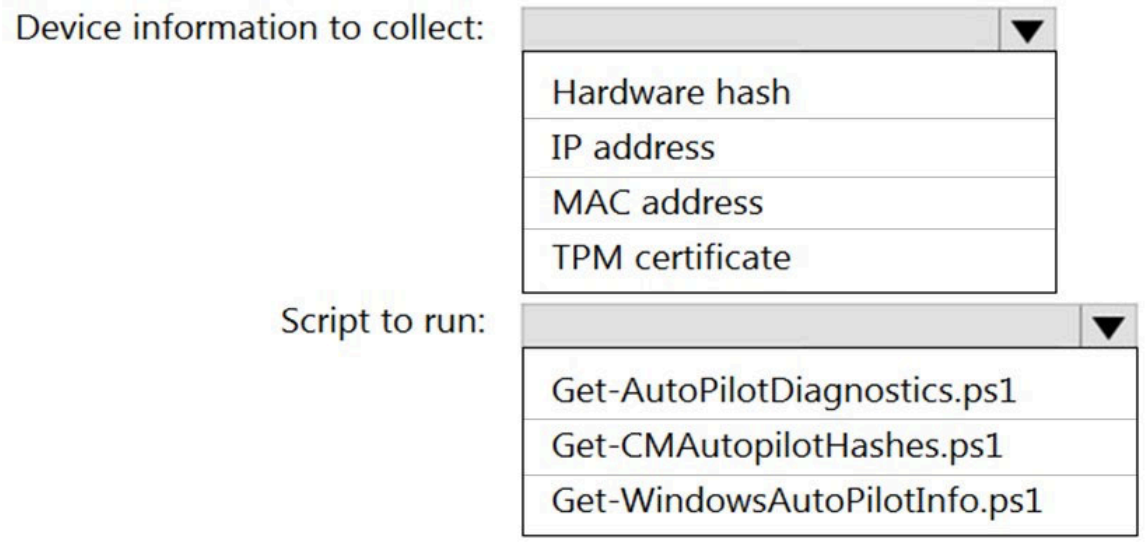
You need to collect device information to register the devices with Autopilot.

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

NOTE: Each correct selection is worth one point.

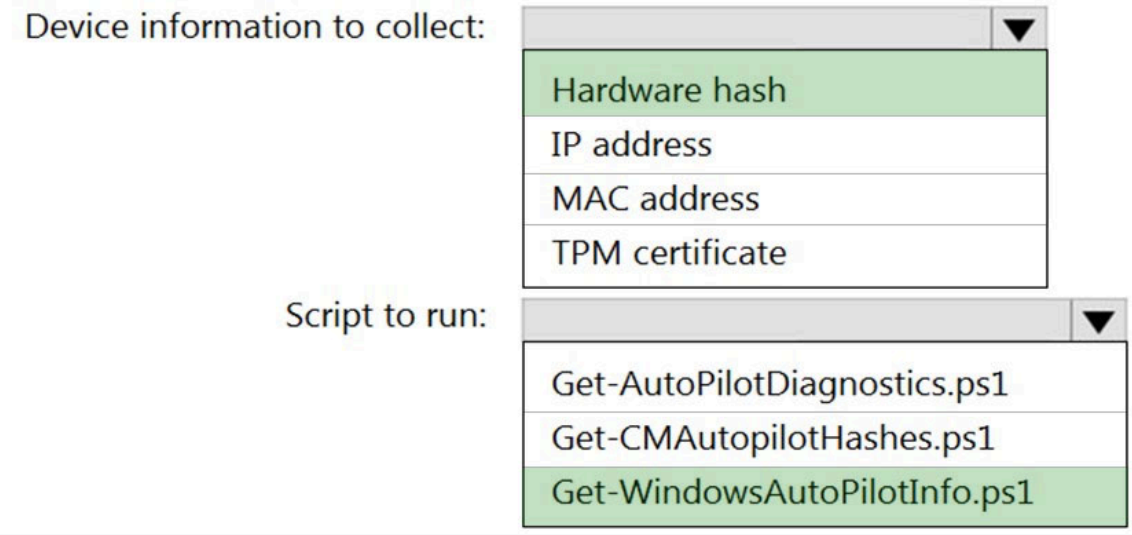
Hot Area:

Answer Area



Suggested Answer:

Answer Area



Reference:

https://docs.microsoft.com/en-us/mem/autopilot/add-devices

Moderator 2 years, 3 months ago

Correct answers given. Provided link is ok.

upvoted 3 times

reastman66 2 years, 4 months ago

This looks correct. Most of the information online shows just running the Get-WindowsAutoPilotInfo.ps1 to get the Hardware Hash.

upvoted 2 times

Question #86 *Topic 1*

You have a Microsoft 365 E5 tenant that contains 500 Windows 10 devices. The devices are enrolled in Microsoft Intune.
You plan to use Endpoint analytics to identify hardware issues.
You need to enable Windows health monitoring on the devices to support Endpoint analytics.
What should you do?

A. Create a configuration profile.

B. Create a compliance policy.

C. Configure the Endpoint analytics baseline regression threshold.

D. Create a Windows 10 Security Baseline profile.

Suggested Answer: *A*
Reference:
https://docs.microsoft.com/en-us/mem/intune/configuration/windows-health-monitoring

Community vote distribution
A (100%)

BigDazza_111 1 year, 4 months ago

Selected Answer: A

yep its A

upvoted 1 times

Moderator 2 years, 3 months ago

Selected Answer: A

Correct answer given. Provided link gives a sufficient explanation

upvoted 4 times

reastman66 2 years, 4 months ago

Configuration Profiles is correct
Create a Windows Health Monitoring profile in Microsoft Intune shows
Sign in to the Microsoft Endpoint Manager --> select Devices --> Configuration Profiles

upvoted 4 times

Question #87 *Topic 1*

You purchase a new computer that has Windows 10, version 2004 preinstalled.
You need to ensure that the computer is up-to-date. The solution must minimize the number of updates installed.
What should you do on the computer?

A. Install the latest feature update and the latest quality update only.

B. Install the latest feature update and all the quality updates released since version 2004.

C. Install all the feature updates released since version 2004 and all the quality updates released since version 2004 only.

D. Install all the feature updates released since version 2004 and the latest quality update only.

Suggested Answer: *B*
Feature updates are typically released twice per year and include new functionality and capabilities as well as potential fixes and security updates. Quality updates are more frequent and mainly include small fixes and security updates. Windows is designed to deliver both kinds of updates to devices through Windows Update.
Reference:
https://support.microsoft.com/en-us/topic/8a903416-6f45-0718-f5c7-375e92dddeb2

Community vote distribution
A (100%)

gmKK Highly Voted 2 years, 3 months ago
Selected Answer: A
Quality updates are cumulative, so installing the latest quality update is sufficient to get all the available fixes for a specific feature update, including any out-of-band security fixes and any servicing stack updates that might have been released previously.
https://docs.microsoft.com/en-us/windows/deployment/update/get-started-updates-channels-tools#types-of-updates
upvoted 13 times

TechMinerUK 2 years, 2 months ago
I concur with gmKK as the quickest way is to install the latest feature update and the latest quality update since quality updates are cummulative.

However I know Windows Update can sometimes attempt to update the system to the latest update by installing previous feature updates beforehand so it is often recommended to use the "Upgrade Assistant" to ensure you "jump" from the current version to the latest Feature Update however this would still lead to answer A being correct
upvoted 2 times

Meebler Most Recent 1 year, 10 months ago
A.

This option will ensure that the computer is up-to-date with the latest version of Windows 10 and the latest quality updates. Installing all the feature updates released since version 2004 may not be necessary, as the latest feature update will typically include all the previous ones. Installing all the quality updates released since version 2004 may also not be necessary, as they may have been superseded by more recent updates. Choosing this option will minimize the number of updates installed while ensuring that the computer is up-to-date.
upvoted 1 times

Fala_Fel 1 year, 11 months ago
Selected Answer: A
Microsoft claim "Quality updates are cumulative; they include all previously released fixes to guard against fragmentation of the operating system (OS)."
So A is the Microsoft answer
https://learn.microsoft.com/en-us/windows/deployment/update/quality-updates
upvoted 1 times

4Shawsy 2 years, 3 months ago
For example... .Net patches are not included in CU patches so they are also required. For that reason, feature update and all quality updates
upvoted 1 times

rrrr5r 2 years, 3 months ago

It should be D.

All feature packs from 2004 and one last quality update because it's cumulative.
upvoted 3 times

ilma_nl 2 years, 4 months ago
nope you need latest feature update and then all quality updates
so answer is correct
upvoted 1 times

A_Blameless_Child 2 years, 4 months ago
I think I must be misunderstanding the MS Docs.

"Feature updates are typically released twice per year and include new functionality and capabilities as well as potential fixes and security updates. Quality updates are more frequent and mainly include small fixes and security updates. Windows is designed to deliver both kinds of updates to devices through Windows Update."

I get that, but if the Quality Updates are cumulative (Including any OOB ones) then I don't understand why you can't get the latest one if it has all of the previous updates included?
upvoted 1 times

A_Blameless_Child 2 years, 4 months ago
Should the answer not be A?

https://docs.microsoft.com/en-us/windows/deployment/update/quality-updates

Quality updates are cumulative so you only need to install the latest one
upvoted 4 times

gmKK 2 years, 3 months ago
https://docs.microsoft.com/en-us/windows/deployment/update/get-started-updates-channels-tools#types-of-updates
"Quality updates are cumulative, so installing the latest quality update is sufficient to get all the available fixes for a specific feature update, including any out-of-band security fixes and any servicing stack updates that might have been released previously."
upvoted 2 times

Question #88 *Topic 1*

DRAG DROP -

You have a Microsoft 365 subscription.

You have the devices shown in the following table.

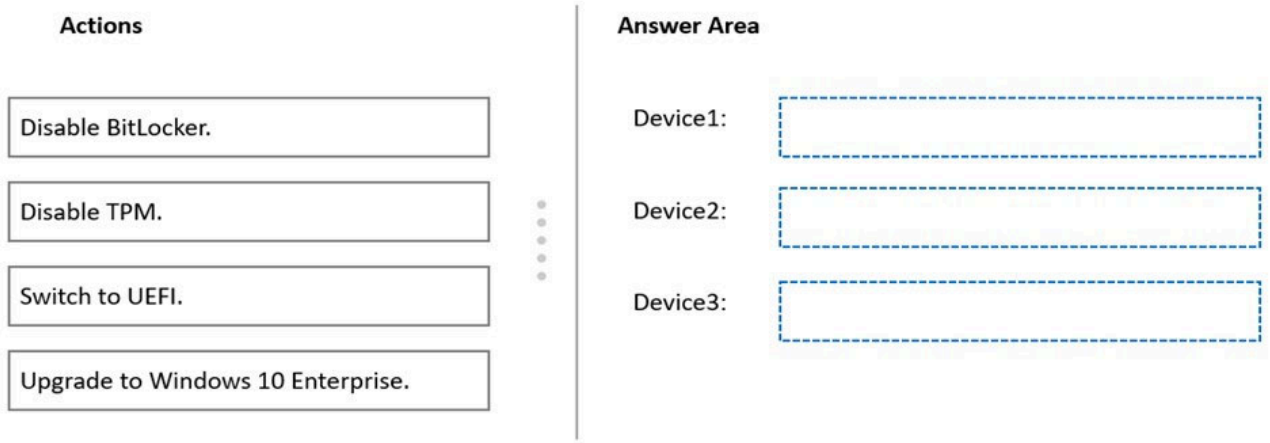
Name	TPM version	Operating system	BIOS/UEFI	BitLocker Drive Encryption (BitLocker)
Device1	TPM 1.2	Windows 10 Pro	BIOS	Enabled
Device2	TPM 2	Windows 10 Home	BIOS	**Not applicable**
Device3	TPM 2	Windows 8.1 Pro	UEFI	Enabled

You plan to join the devices to Azure Active Directory (Azure AD).

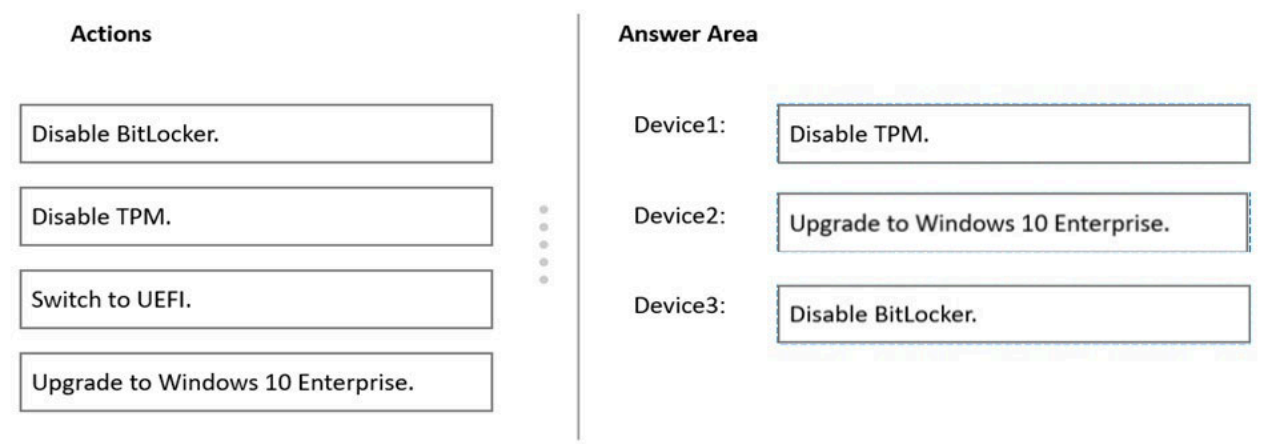
What should you do on each device to support Azure AD join? To answer, drag the appropriate actions to the correct devices. Each action may be used once, more than once, or not at all. You may need to drag the split bar between panes or scroll to view content.

NOTE: Each correct selection is worth one point.

Select and Place:



Suggested Answer:



Box 1: Disable TPM.

Hybrid Azure AD join is supported for FIPS-compliant TPM 2.0 and not supported for TPM 1.2.

If your devices have FIPS-compliant TPM 1.2, you must disable them before proceeding with hybrid Azure AD join.

Box 2: Upgrade to Windows 10 Enterprise

Windows 10 Home edition cannot be joined to a domain. First we must upgrade Windows 10 to Professional or Enterprise.

Box 3: Disable bitlocker -

Azure AD join supports Windows 8.1.

Reference:

https://docs.microsoft.com/en-us/azure/active-directory/devices/hybrid-azuread-join-plan https://www.microsoft.com/en-us/windows/compare-windows-10-home-vs-pro

mackypatio Highly Voted 2 years, 3 months ago

disable TPM
upgrade
upgrade
upvoted 14 times

TechMinerUK Highly Voted 2 years, 2 months ago
I believe the anwer should be the following:

Device 1 - Disable TPM (Whilst I have had devices onboard without a FIPS TPM1.2 chipset it is not supprted by MS)

Device 2 - This would need to be upgraded to Windows 10 Pro or Enterprise before joining to AzureAD

Device 3 - This would also need to be upgraded to Windows 10 Pro or Enterprise as Windows 8.1 only supports AzureAD registration

Source: https://learn.microsoft.com/en-us/azure/active-directory/devices/azureadjoin-plan
upvoted 5 times

TechMinerUK 2 years, 2 months ago
To clarify point 1, I have had plenty of devices enroll via AzureAD Join or Hybrid AzureAD Join with TPM1.2 chipsets without any issues however it seems it is not "officially" supported so for exam purposes it is "Disable TPM"
upvoted 1 times

athadd Most Recent 1 year, 11 months ago
1. Disable TPM
2. Upgrade to Win 10 Enterprise
3. Upgrade to Win 10 Enterprise
upvoted 2 times

KNemeth 1 year, 3 months ago
In such questions it's not possilble to choose the same answer two times
upvoted 1 times

athadd 1 year, 11 months ago
Disable TP
1. Disable TPM
2. Upgrade to Win 10 Enterprise
3. Last should be - Upgrade to Win 10 Enterprise

Details: https://learn.microsoft.com/en-us/azure/active-directory/devices/azureadjoin-plan
Azure AD join:

- Supports Windows 10 and Windows 11 devices.
- Isn't supported on previous versions of Windows or other operating systems. If you have Windows 7/8.1 devices, you must upgrade at least to Windows 10 to deploy Azure AD join.
- Is supported for FIPS-compliant TPM 2.0 but not supported for TPM 1.2. If your devices have FIPS-compliant TPM 1.2, you must disable them before proceeding with Azure AD join. Microsoft doesn't provide any tools for disabling FIPS mode for TPMs as it is dependent on the TPM manufacturer. Contact your hardware OEM for support.
upvoted 3 times

Founiek 2 years, 3 months ago
"Azure AD join isn't supported on previous versions of Windows or other operating systems. If you have Windows 7/8.1 devices, you must upgrade at least to Windows 10 to deploy Azure AD join" (https://docs.microsoft.com/en-us/azure/active-directory/devices/azureadjoin-plan)
Device 3 --> Upgrade to Windows 10 Enterprise
upvoted 5 times

gmKK 2 years, 3 months ago
Why is the option "disable Bitlocker" selected for Windows 8.1? I have not found any article related to this.
upvoted 3 times

rrrr5r 2 years, 3 months ago
1. Disable TPM
2. Upgrade to Win 10 Enterprise
3. Upgrade to Win 10 Enterprise

https://docs.microsoft.com/en-us/azure/active-directory/devices/azureadjoin-plan
upvoted 16 times

Moderator 2 years, 3 months ago
Correct answer :)
upvoted 5 times

HOTSPOT -

You have devices enrolled in Microsoft Intune as shown in the following table.

Name	Platform
Device1	Windows 10
Device2	Windows 10
Device3	iOS/iPadOS

You have the device compliance policies shown in the following table.

Name	Platform	Assignment
Policy1	Windows 10 and later	Device1
Policy2	Windows 10 and later	Device1
Policy3	Windows 10 and later	Device2
Policy4	Windows 10 and later	Device2
Policy5	iOS/iPadOS	Device3
Policy6	iOS/iPadOS	Device3

The device compliance state for each policy is shown in the following table.

Policy	State
Policy1	Compliant
Policy2	In grace period
Policy3	Compliant
Policy4	Not compliant
Policy5	In grace period
Policy6	Compliant

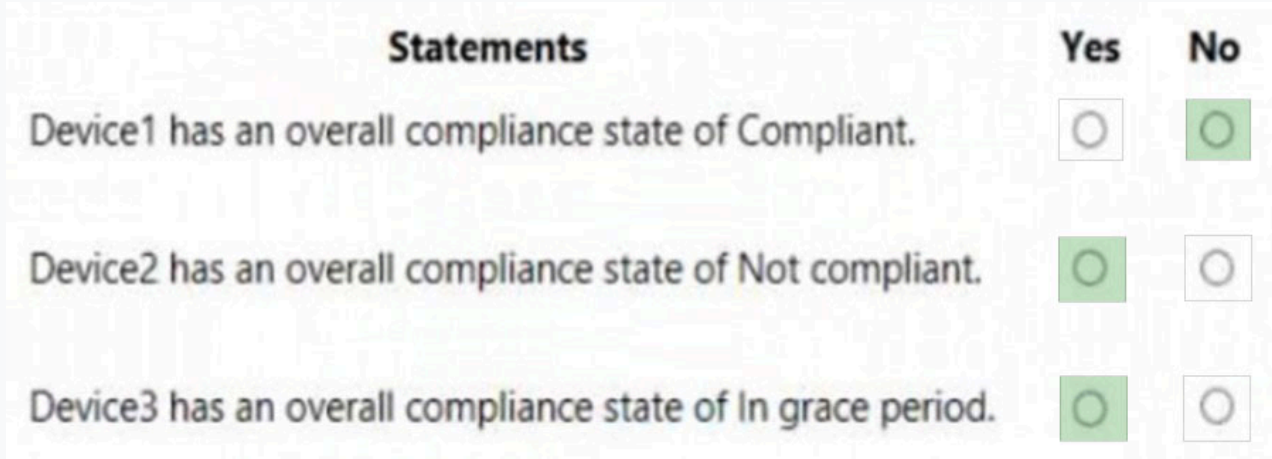
For each of the following statements, select Yes if the statement is true. Otherwise, select No.

NOTE: Each correct selection is worth one point.

Hot Area:

Statements	Yes	No
Device1 has an overall compliance state of Compliant.	○	○
Device2 has an overall compliance state of Not compliant.	○	○
Device3 has an overall compliance state of In grace period.	○	○

Suggested Answer:



Box 1: No -
Descriptions of the different device compliance policy states:
* Compliant: The device successfully applied one or more device compliance policy settings.
* 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.
* Not-compliant: The device failed to apply one or more device compliance policy settings. Or, the user hasn't complied with the policies.

Box 2: Yes -

Box 3: Yes -
Reference:
https://docs.microsoft.com/en-us/mem/intune/protect/compliance-policy-monitor

Fala_Fel 1 year, 11 months ago
Answer given is correct N Y Y
Highest Severity Wins
1 Unknown
2 NotApplicable
3 Compliant
4 InGracePeriod
5 NonCompliant
6 Error
(Just creating a new post in an attempt to get correct answer at top)
upvoted 4 times

sathaporn 2 years, 2 months ago
I think YNN, If there is sort of severity level of a resulting compliance policy status, In the Device3 must choose No, because "Compliant (Severity = 3)" it's high severity level "In grace period (Severity = 4)"?
upvoted 2 times

Arlecchino 1 year, 12 months ago
Its NYY as explained by hcwelcomm.
upvoted 1 times

ajiejeng 2 years, 3 months ago
shouldn't this be YNY? correct me if i'm wrong
upvoted 2 times

hcwelcomm 2 years, 3 months ago
Each compliance status has the following severity level:
ASSIGN A RESULTING COMPLIANCE POLICY STATUS
Status Severity
Unknown 1
NotApplicable 2
Compliant 3
InGracePeriod 4

NonCompliant 5
Error 6
When a device has multiple compliance policies, then the highest severity level of all the policies is assigned to that device.
For example, a device has three compliance policies assigned to it: one Unknown status (severity = 1), one Compliant status (severity = 3), and one
InGracePeriod status (severity = 4). The InGracePeriod status has the highest severity level. So, all three policies have the InGracePeriod compliance
status.
https://docs.microsoft.com/en-us/mem/intune/protect/create-compliance-policy
upvoted 21 times

RenegadeOrange 2 years, 3 months ago
Agree provided answers are correct.
Highest Severity Wins
1 Unknown
2 NotApplicable
3 Compliant
4 InGracePeriod
5 NonCompliant
6 Error
upvoted 7 times

Arlecchino 2 years, 3 months ago
Appreciate your guidance.
upvoted 2 times

JerryZy 2 years, 3 months ago
Nice, you saved my life
upvoted 2 times

Question #90 *Topic 1*

Your on-premises network contains the device types shown in the following table.

Name	Operating system	Drive encryption	BIOS	Image type
Type1	32-bit version of Windows 10 Pro	*None*	Legacy	Standard
Type2	64-bit version of Windows 8.1 Pro	*None*	Legacy	Start from VHD
Type3	64-bit version of Windows 8.1 Pro	BitLocker Drive Encryption (BitLocker)	Legacy	Custom
Type4	64-bit version of Windows 8.1 Pro	BitLocker Drive Encryption (BitLocker)	UEFI	Standard
Type5	64-bit version of Windows 8.1 Pro	*None*	Legacy	Standard

You plan to deploy an in-place upgrade to a 64-bit version of Windows 10 Enterprise by using the Microsoft Deployment Toolkit (MDT).
Which device types will support an in-place upgrade?

A. Type4 and Type5 only

B. Type3, Type4, and Type5 only

C. Type1, Type4, and Type5 only

D. Type1, Type2, and Type5 only

Suggested Answer: *A*
MDT has many useful features, such as:
* UEFI support. Supports deployment to machines using Unified Extensible Firmware Interface (UEFI) version 2.3.1.
* Offline BitLocker. Provides the capability to have BitLocker enabled during the Windows Preinstallation Environment (Windows PE) phase, thus saving hours of encryption time.
* Deploy to VHD. Provides ready-made task sequence templates for deploying Windows into a virtual hard disk (VHD) file.
Incorrect:
Not Type1: The upgrade process cannot change from a 32-bit operating system to a 64-bit due to the possible complications with drivers and applications it may bring.
Not Type2, not Type3: Boot images are the Windows Preinstallation Environment (Windows PE) images that are used to start the deployment.
You're not able to use a custom image of Windows 10 for the In-Place Upgrade scenario. You'd have to use the install.wim image provided with the latest
Windows 10 media that Microsoft has released.
Reference:
https://msendpointmgr.com/2015/10/26/deploy-windows-10-enterprise-using-in-place-upgrade/ https://docs.microsoft.com/en-us/windows/deployment/deploy-windows-mdt/get-started-with-the-microsoft-deployment-toolkit

Community vote distribution
A (100%)

hcwelcomm Highly Voted 2 years, 3 months ago

Selected Answer: A

In-place upgrade differs from computer refresh in that you cannot use a custom image to perform the in-place upgrade. In this article we will add a default Windows 10 image to the production deployment share specifically to perform an in-place upgrade.
https://docs.microsoft.com/en-us/windows/deployment/deploy-windows-mdt/upgrade-to-windows-10-with-the-microsoft-deployment-toolkit
upvoted 6 times

Moderator Most Recent 2 years, 3 months ago

Selected Answer: A

Correct answer and explanation seems fairly accurate as well :)

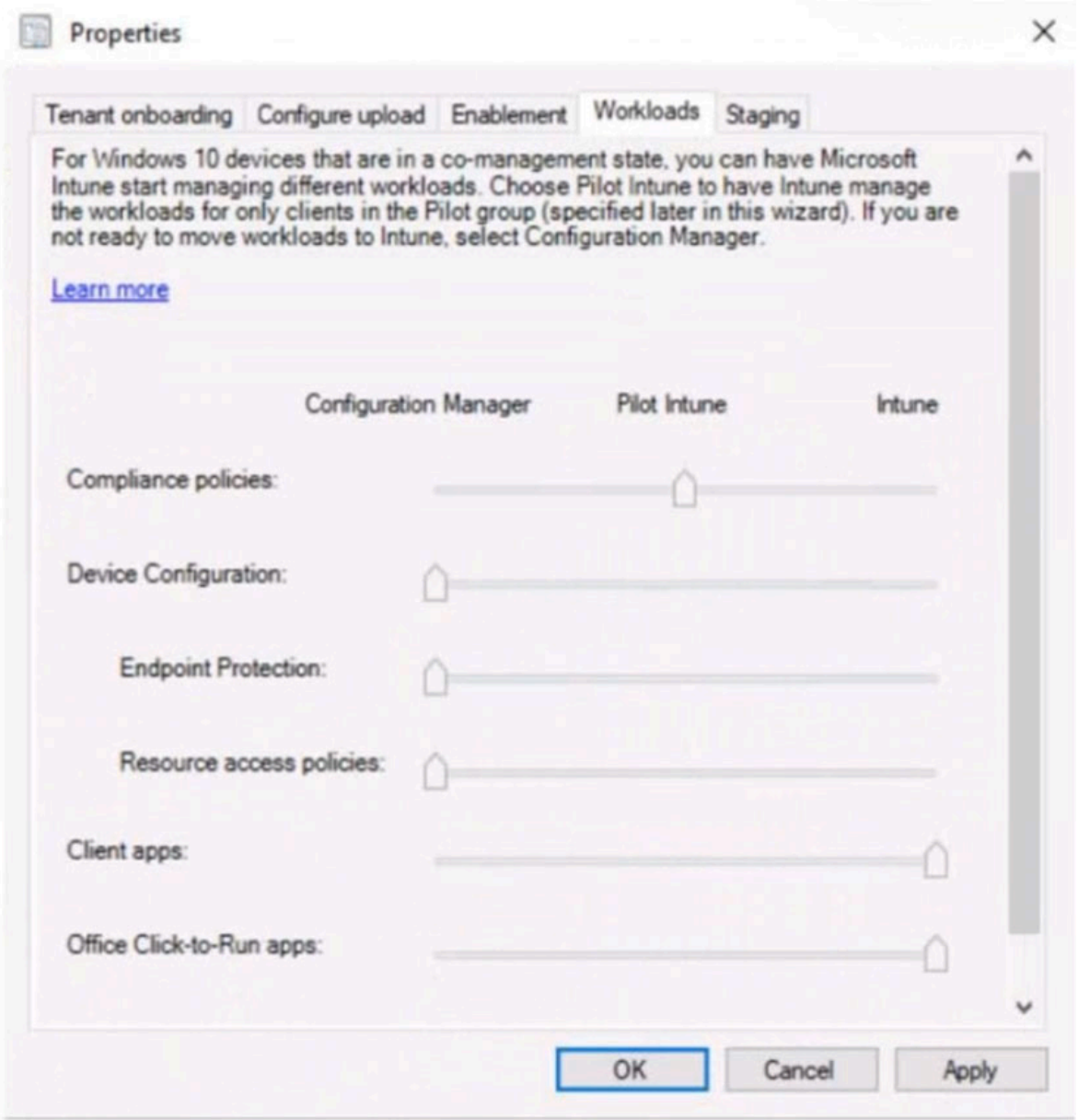
upvoted 4 times

HOTSPOT -

Your network contains an on-premises Active Directory domain and a Microsoft Endpoint Configuration Manager site.

You have a Microsoft 365 E5 subscription that uses Microsoft Intune. Configuration Manager and Intune are configured to support co-management.

The Configuration Manager co-management settings are configured as shown in the following exhibit.



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

NOTE: Each correct selection is worth one point.

Hot Area:

Answer Area

Client apps can be installed on managed devices by using the **[answer choice]**.

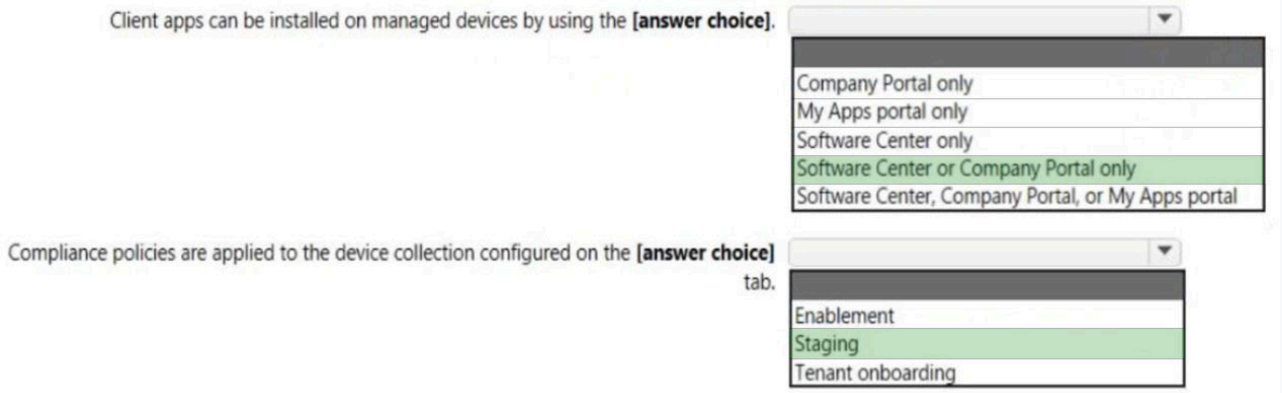
- Company Portal only
- My Apps portal only
- Software Center only
- Software Center or Company Portal only
- Software Center, Company Portal, or My Apps portal

Compliance policies are applied to the device collection configured on the **[answer choice]** tab.

- Enablement
- Staging
- Tenant onboarding

Suggested Answer:

Answer Area



Box 1: Software Center or Company Portal only

Office Click-to-Run apps -
This workload manages Microsoft 365 Apps on co-managed devices.
* After moving the workload, the app shows up in the Company Portal on the device
Apps that you deploy from Configuration Manager are available in Software Center

Box 2: Staging -
What's the difference between Pilot Intune and Intune when I switch workloads?
The difference between Pilot Intune and Intune is subtle but important. Both allow Intune to control a configured workload.
The Pilot Intune setting is used to switch a workload only for the devices in a pilot collection that's created in Configuration Manager. This allows you to test in a staging environment without affecting all Windows 10 devices in the production environment.
The Intune setting is used when you finish testing in the staging environment and are ready to switch a workload for all Windows 10 devices that are enrolled in co-management.
Reference:
https://docs.microsoft.com/en-us/mem/configmgr/comanage/workloads#device-configuration https://docs.microsoft.com/en-us/troubleshoot/mem/intune/troubleshoot-co-management-workloads

gmKK Highly Voted 2 years, 3 months ago
The answer is correct.
Here is what the Enablement Tab looks like: https://youtu.be/rTMZp9DGK0M?t=53
and here is the staging tab: https://www.prajwaldesai.com/wp-content/uploads/2022/06/How-to-Switch-SCCM-workloads-to-Intune-Snap2.jpg
upvoted 5 times

Moderator 2 years, 3 months ago
Answers seem to be correct indeed. Thanks for the link(s).
upvoted 2 times

bac0n Most Recent 2 years ago
I am almost certain the first answer is wrong. If the co-managed devices are managed by Intune for client apps why would they be available from the Software Center? If the workload is handled by Intune only then the apps should be only in the Company portal... If they are configured as Pilot then the answer would be correct.
upvoted 3 times

bac0n 2 years ago
Never mind. This article cleared it up. https://www.anoopcnair.com/software-center-vs-company-portal-differences/

Though, the answer explanation is wrong. Click to run apps WILL be available only from Intune if the co-management workload is moved to Intune only. Client apps will stay available from both portals, and in fact you can install apps from SCCM in Intune as well, but they'll still be available from Software center.
upvoted 4 times

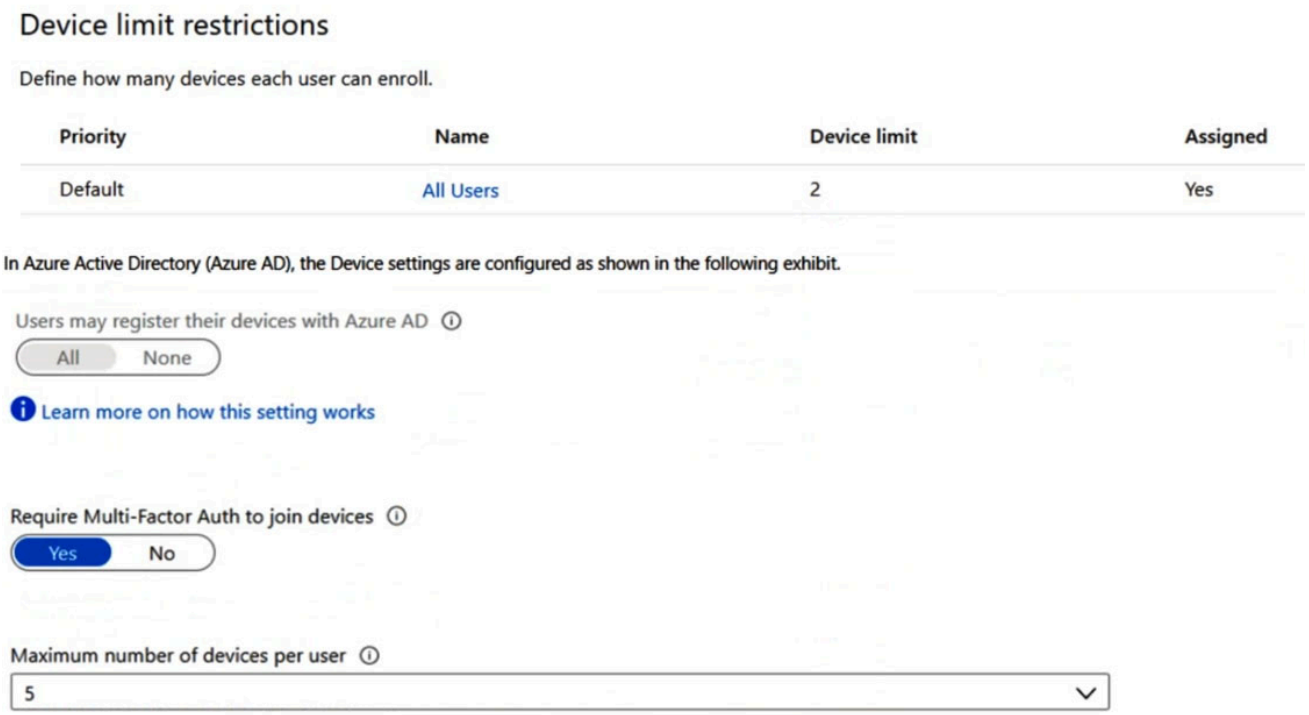
Question #92 *Topic 1*

HOTSPOT -

You have 2,500 Windows 10 devices and a Microsoft 365 E5 tenant that contains two users named User1 and User2. The devices are NOT enrolled in Microsoft

Intune.

In Microsoft Endpoint Manager, the Device limit restrictions are configured as shown in the following exhibit.

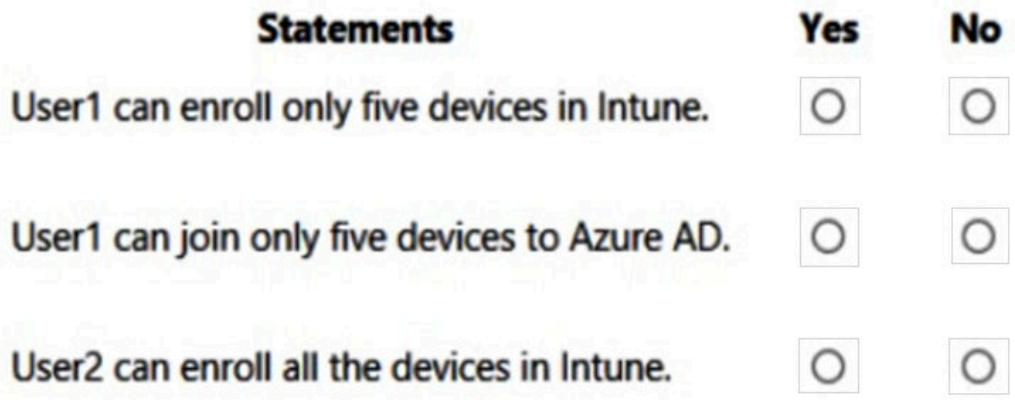


From Microsoft Endpoint Manager, you add User2 as a device enrollment manager (DEM).

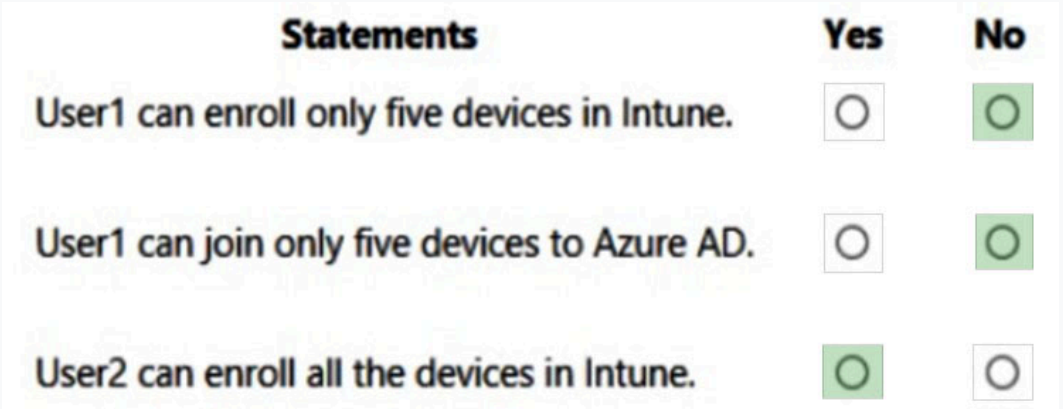
For each of the following statements, select Yes if the statement is true. Otherwise, select No.

NOTE: Each correct selection is worth one point.

Hot Area:



Suggested Answer:



Box 1: No -

The default limit is set to 2.

Box 2: No -
Device enroll limit is set to 2 devices per user.
Note: Maximum number of devices: This setting enables you to select the maximum number of Azure AD joined or Azure AD registered devices that a user can have in Azure AD.

Box 3: Yes -
You can enroll up to 1,000 devices in total with a single Azure Active Directory account by using a device enrollment manager (DEM) account.
Microsoft 365 Device limit restrictions Maximum number of devices per user.
Reference:
https://docs.microsoft.com/en-us/azure/active-directory/devices/device-management-azure-portal https://docs.microsoft.com/en-us/mem/intune/enrollment/device-enrollment-manager-enroll

A_Blameless_Child Highly Voted 2 years, 4 months ago
NYN

Max of 2 to enroll
Users have register/join up to 5
DEM can enroll up to 1,000, but there are 2,500 devices.
upvoted 43 times

rrrr5r 2 years, 3 months ago
https://docs.microsoft.com/en-us/mem/intune/enrollment/device-limit-intune-azure
upvoted 2 times

TechMinerUK 2 years, 2 months ago
Based on this link it suggests A_Blameless_Child is correct however because of the different enrollment methods the question likely needs to provide more information to make sure enrollment methods such as GPO automatic enrollment are not being used as this bypass the Azure restriction etc
upvoted 1 times

Moderator 2 years, 3 months ago
NYN seems correct indeed.
upvoted 7 times

ilma_nl 2 years, 3 months ago
Why not change it then?
it has to be NYN
upvoted 11 times

GotDamnImIn Most Recent 1 year, 8 months ago
I'm going with NYN
upvoted 2 times

shaden2000 1 year, 11 months ago
NYN the explenation is correct the answer is not...
Joining AD is something else then enroll in intune.
So joining 5 is fine enrolling 5 is not.
upvoted 4 times

Question #93 *Topic 1*

You have a Microsoft 365 tenant that contains devices registered for mobile device management. The devices are configured as shown in the following table.

Name	Platform
Device1	MacOS
Device2	Windows 10 Pro for Workstations
Device3	Windows 10 Enterprise
Device4	iOS
Device5	Android

You plan to enable VPN access for the devices.
What is the minimum number of configuration policies required?

A. 1

B. 3

C. 4

D. 5

Suggested Answer: *C*
Create one configuration policies for each platform.
Platform: Choose the platform of your devices. Your options:

Android device administrator -

Android Enterprise -
iOS/iPadOS
macOS

Windows 10 and later -
You create a custom profile for Android device administrator, Android Enterprise, iOS/iPadOS, macOS, and Windows respectively.
Reference:
https://docs.microsoft.com/en-us/mem/intune/configuration/custom-settings-configure https://docs.microsoft.com/en-us/mem/intune/configuration/vpn-settings-configure

in_cloud 1 year, 5 months ago
exam win 10, win 8, android, ios and macos
upvoted 1 times

[Removed] 2 years, 3 months ago
I think the answer should be D because there are 2 configuration profiles for Android with VPN: Android device administrator and Android Enterprise
upvoted 1 times

ilma_nl 2 years, 3 months ago
There is only 1 android device in the list
upvoted 3 times

Futfuyfyjfj 1 year, 8 months ago
Wrong! Only 1 Android is mentioned, you deploy Device Administrator OR Android Enterprise, not both at same time to the same device. (Btw Device Administrator is deprecated already) so provided answer is correct
upvoted 2 times

Question #94 *Topic 1*

HOTSPOT -

Your on-premises network contains an Active Directory domain and a Microsoft Endpoint Configuration Manager site.

You have a Microsoft 365 E5 subscription that uses Microsoft Intune.

You use Azure AD Connect to sync user objects and group objects to Azure Active Directory (Azure AD). Password hash synchronization is disabled.

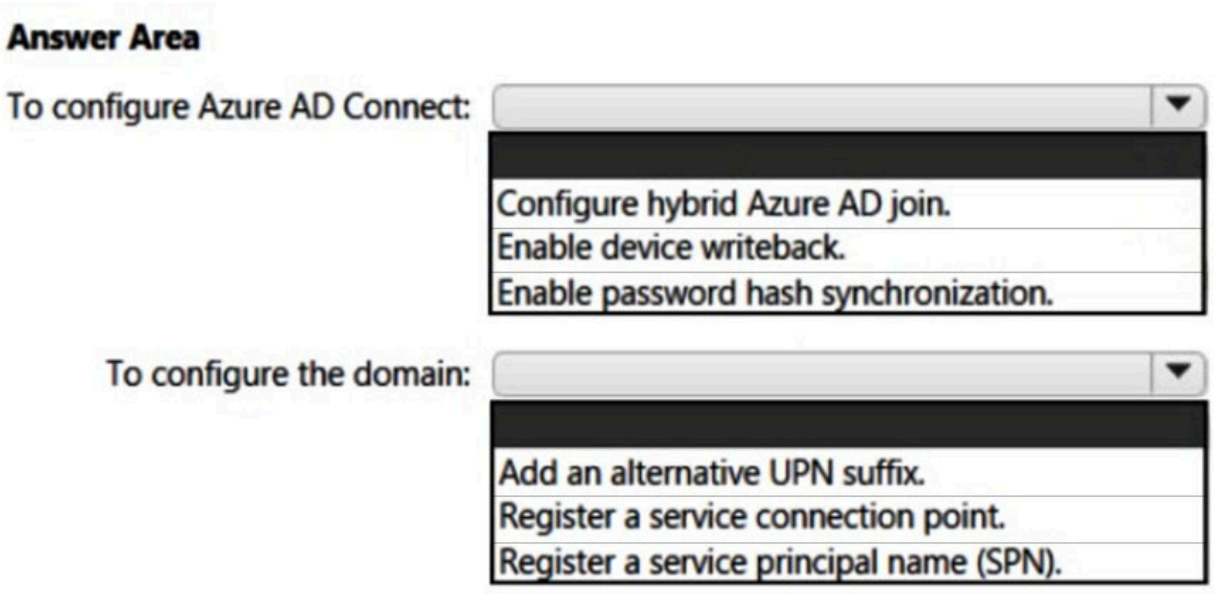
You plan to implement co-management.

You need to configure Azure AD Connect and the domain to support co-management.

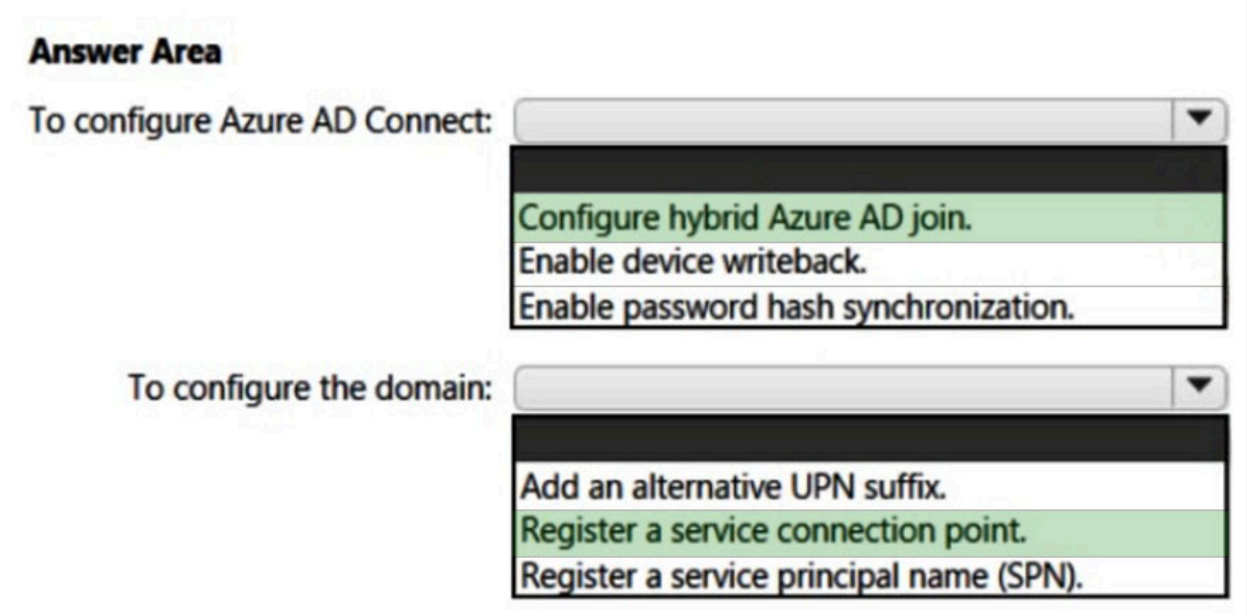
What should you do? To answer, select the appropriate options in the answer area.

NOTE: Each correct selection is worth one point.

Hot Area:



Suggested Answer:



Box 1: Configure Hybrid Azure AD join.

See step 6 below.

Configure a hybrid Azure AD join using Azure AD Connect

1. Get and install the latest version of Azure AD Connect (1.1.819.0 or higher).
2. Launch Azure AD Connect, and then select Configure.
3. On the Additional tasks page, select Configure device options, and then select Next.
4. On the Overview page, select Next.
5. On the Connect to Azure AD page, enter the credentials of a global administrator for Azure AD.
6. On the Device options page, select Configure Hybrid Azure AD join, and then select Next.

7. On the Device operating systems page, select the operating systems used by devices in your Active Directory environment, and then select Next.
8. You can select the option to support Windows downlevel domain-joined devices, but keep in mind that co-management of devices is only supported for
Windows 10 or later.
9. On the SCP page, for each on-premises forest you want Azure AD Connect to configure the service connection point (SCP), do the following steps, and then select Next:
10.Etc.
Box 2: Register a service connection point (SCP)
See step 9 above.
Reference:
https://docs.microsoft.com/en-us/mem/configmgr/comanage/tutorial-co-manage-clients

rrrr5r Highly Voted 2 years, 3 months ago
In Sep 16th 22's exam.
upvoted 7 times

JCkD4Ni3L Most Recent 1 year, 7 months ago
Answers are correct !
upvoted 1 times

Oval61251 2 years ago
Is this MS 100 material....
upvoted 1 times

Moderator 2 years, 2 months ago
Both answers are correct. Supplied link points to the explanation.
upvoted 2 times

Question #95 *Topic 1*

HOTSPOT

-

You have a Microsoft 365 E5 subscription that uses Microsoft Defender for Endpoint and contains the devices shown in the following table.

Name	Operating system	Tag
Device1	Windows 10	Inventory1
Computer1	Windows 10	Inventory2
Device3	Android	Inventory3

Defender for Endpoint has the device groups shown in the following table.

Rank	Name	Matching rule
1	Group1	`Tag Contains Inventory` `And OS in Android`
2	Group2	`Name Starts with Device` `And Tag Contains Inventory`
Last	Ungrouped devices (default)	*Not applicable*

You create an incident email notification rule configured as shown in the following table.

Setting	Value
Name	Rule1
Alert severity	Low
Device group scope	Group1, Group2
Recipient email address	User1@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.

Statements	Yes	No
If a high-severity incident is triggered for Device1, an incident email notification will be sent.	○	○
If a low-severity incident is triggered for Computer1, an incident notification email will be sent.	○	○
If a low-severity incident is triggered for Device3, an incident notification email will be sent.	○	○

Suggested Answer:

Statements	Yes	No
If a high-severity incident is triggered for Device1, an incident email notification will be sent.	○	●
If a low-severity incident is triggered for Computer1, an incident notification email will be sent.	○	●
If a low-severity incident is triggered for Device3, an incident notification email will be sent.	●	○

IPalot Highly Voted 1 year, 12 months ago

No - High severity Alert.

No - Doesn't have 'Device' in name

Yes - Has OS name 'Andriod' and Tag contains 'Inventory'

upvoted 12 times

ChizzyO Most Recent 1 year, 6 months ago

Given answer is correct

No - Device 1 is included in the matching rule but the setting for the alert is low not high, therefore no email is sent

No - Computer 1 does not meet the matching rule as it does not start with device in the name

Yes - Device 3 is included in the matching rule and meets the settings for the email notification

upvoted 1 times

Question #96 *Topic 1*

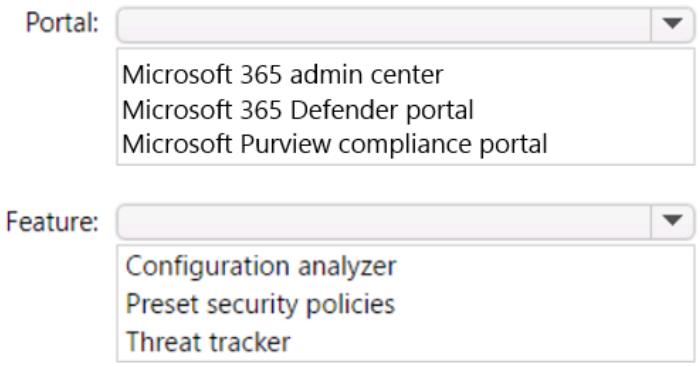
HOTSPOT
-

You have a Microsoft 365 subscription that uses Microsoft Defender for Office 365.

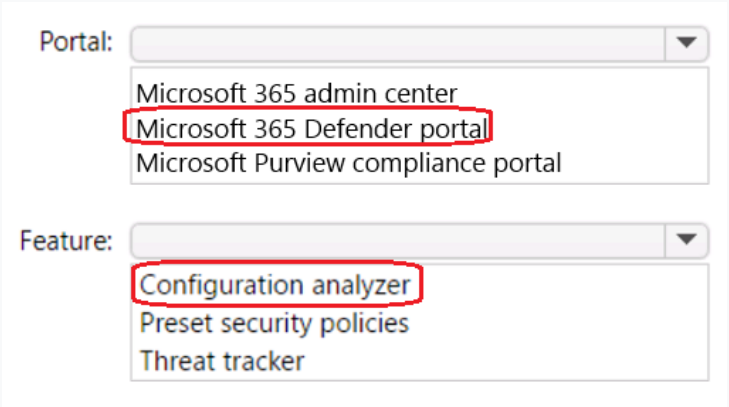
You need to identify the settings that are below the Standard protection profile settings in the preset security policies.

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

NOTE: Each correct selection is worth one point.



Suggested Answer:



IPalot Highly Voted 1 year, 12 months ago
Answer is correct.

https://learn.microsoft.com/en-us/microsoft-365/security/office-365-security/configuration-analyzer-for-security-policies?view=o365-worldwide
upvoted 10 times

Amir1909 Most Recent 11 months ago
Correct
upvoted 1 times

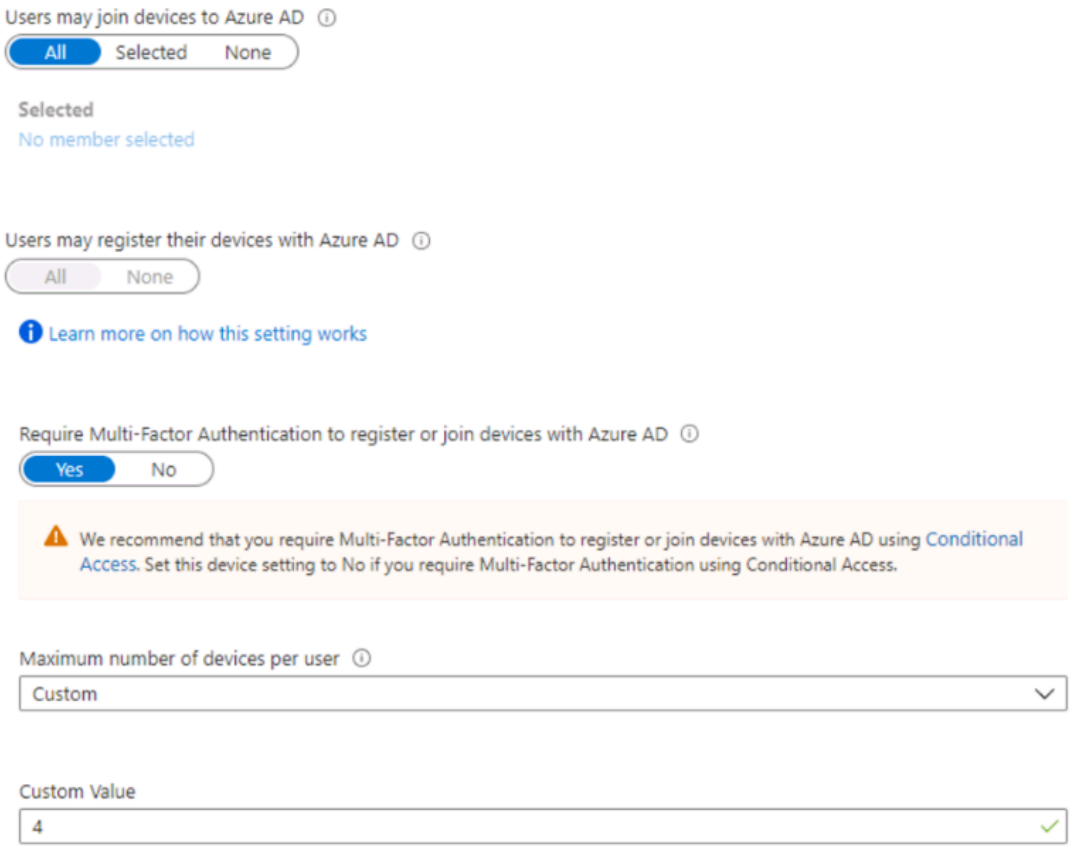
DashP 1 year, 6 months ago
Configuration analyzer in the Microsoft 365 Defender portal provides a central location to find and fix security policies where the settings are below the Standard protection and Strict protection profile settings in preset security policies.
upvoted 2 times

Question #97 *Topic 1*

You have an Azure AD tenant that contains a user named User1. User1 has the devices shown in the following table.

Name	Platform
Device1	Windows 10
Device2	Android
Device3	MacOS
Device4	iOS

The Device settings are configured as shown in the following exhibit.



How many of the devices can User1 join to Azure AD?

A. 1

B. 2

C. 3

D. 4

Suggested Answer: *A*

Community vote distribution

A (68%) D (32%)

JB12340987 Highly Voted 1 year, 12 months ago

Answer is correct. It's in the wording of the question. How many of "the" devices can be joined. Only the windows device from the table can be joined.

upvoted 18 times

IPalot 1 year, 11 months ago

I think you're right, answer should be 1. Oh Microsoft and these questions...

upvoted 3 times

IPalot Highly Voted 1 year, 12 months ago

Selected Answer: D

Here you are defining Azure AD device limits. It is set to 4. So it means there can be for devices registerd in AzureAD

https://learn.microsoft.com/en-us/mem/intune/enrollment/device-limit-intune-azure

upvoted 7 times

alex_p 1 year, 11 months ago

The question is - "How many of THE DEVICES", which means how many of the devices in the table. So I think the answer is 1. Only the Windows 10 device can be joined.

upvoted 13 times

BigDazza_111 Most Recent 1 year, 4 months ago

Selected Answer: A

you can register all the device platforms to AAD, but you can only JOIN windows

upvoted 2 times

itsme12p 1 year, 5 months ago

Selected Answer: A

look at the devices table , only windows can , answer is 1

upvoted 2 times

jecampos2 1 year, 6 months ago

I agree. The correct answer is A.

upvoted 1 times

bernd1976 1 year, 8 months ago

Tricky, but indeed; How many of THE devices; which is actually only Windows 10 device can be joined from that list to Azure AD

upvoted 2 times

GotDamnImIn 1 year, 8 months ago

Selected Answer: A

Only the Windows 10 device can be joined to Azure AD, as it is "one of the" devices. The keywords in Microsoft are so tricky.

upvoted 4 times

fdcpinto 1 year, 8 months ago

Selected Answer: A

Only windows device can be joined

upvoted 4 times

sapt 1 year, 10 months ago

Selected Answer: A

The key is in the first line, User1 has the devices shown in the following table, I think the correct answer is A

upvoted 2 times

RiTh73 1 year, 10 months ago

A - AD Join only support for Winodws10 or later

https://learn.microsoft.com/en-us/azure/active-directory/devices/azureadjoin-plan

upvoted 1 times

theaaronmello 1 year, 10 months ago

Selected Answer: A

Only Windows devices can be joined

upvoted 3 times

MEG 1 year, 11 months ago

Answer is 1.

Check this: https://learn.microsoft.com/en-us/azure/active-directory/devices/concept-azure-ad-join

upvoted 2 times

Mk995 1 year, 11 months ago

Selected Answer: A

User1 can join 4 but only the windows of his devices

upvoted 5 times

Fala_Fel 1 year, 11 months ago

Selected Answer: A

Answer A - Only the windows device can join Azure AD

upvoted 4 times

heinminhtay 1 year, 11 months ago

Azure AD join support for Win 10 device only. Ans was A:

upvoted 5 times

barrypetrol 1 year, 12 months ago

Selected Answer: D

I agree with IPalot, custom limit is set to 4

upvoted 2 times

EsamiTopici 1 year, 11 months ago

but you can JOIN only windows 10-11 devices

upvoted 2 times

FK20850 1 year, 12 months ago

Selected Answer: D

D is correct. Limitations are based on device limits shown in the screenshot

upvoted 3 times

Futfuyfyjfj 1 year, 8 months ago

Great pall, but now tell me how you are going to JOIN a macOS, Android or iOS device to AAD? Exactly, impossible… provided answer is correct

upvoted 1 times

Question #98 *Topic 1*

You have a Microsoft 365 E5 subscription that uses Microsoft Intune.

You need to ensure that during device enrollment in Intune, users are prevented from using their device until all assigned apps and profiles are installed.

What should you configure?

A. a Conditional Access policy

B. a Windows Autopilot deployment profile

C. an enrollment restriction

D. an Enrollment Status Page profile

Suggested Answer: *D*

Community vote distribution

FK20850 1 year, 12 months ago

Selected Answer: D

D is correct

upvoted 2 times

IPalot 1 year, 12 months ago

Selected Answer: D

Correct answer is D

https://learn.microsoft.com/en-us/mem/intune/enrollment/windows-enrollment-status

upvoted 4 times

emanresu 1 year, 11 months ago

Correct. Windows Enrollment - Create Profile, Turn on "Show aoo and profile configuration progress" - new options appear where one is "Block device use until all apps and profiles are installed"

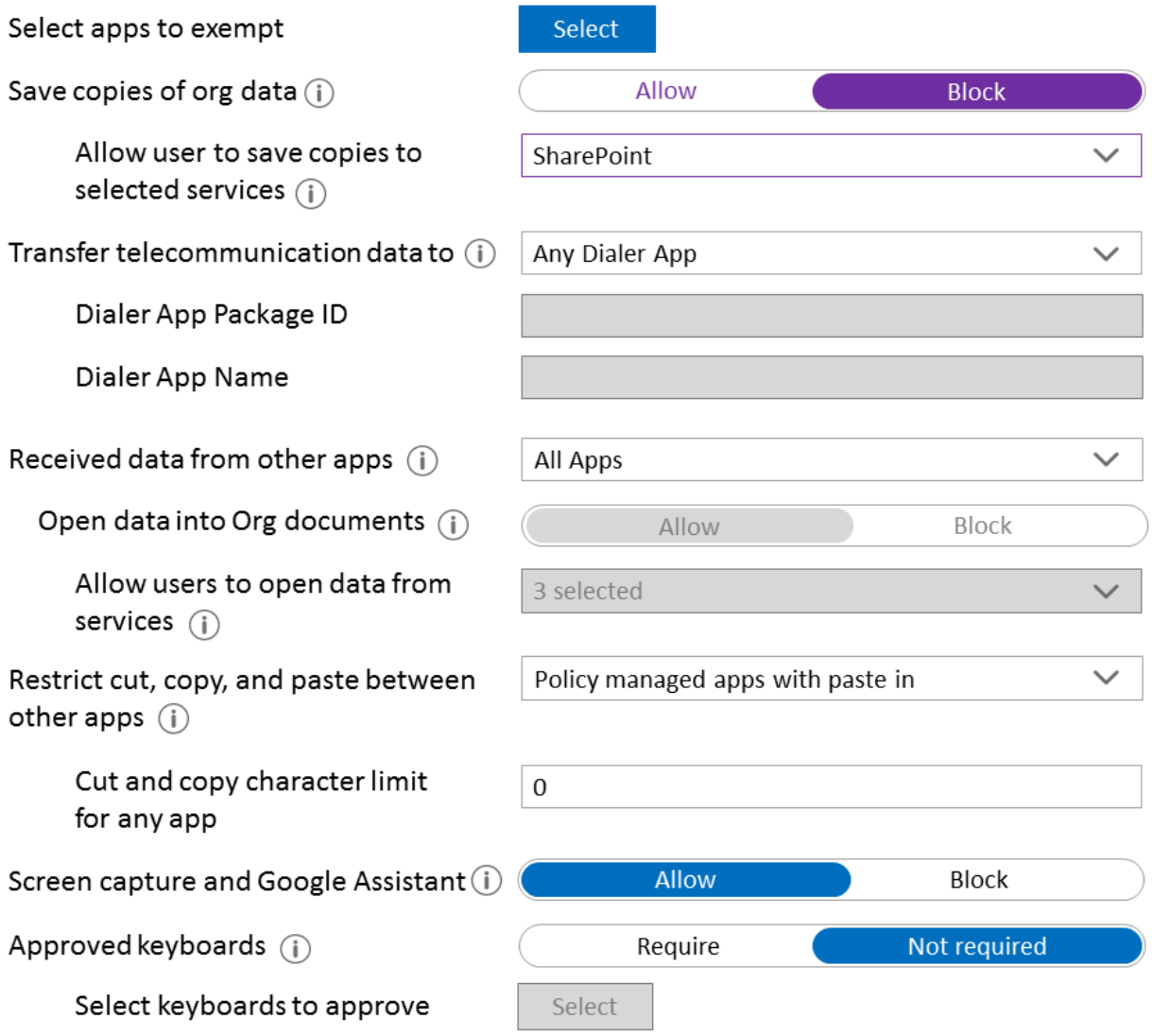
upvoted 2 times

HOTSPOT
-

You have a Microsoft 365 E5 subscription that contains 200 Android devices enrolled in Microsoft Intune.

You create an Android app protection policy named Policy1 that is targeted to all Microsoft apps and assigned to all users.

Policy1 has the Data protection settings shown in the following exhibit.



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

Answer Area

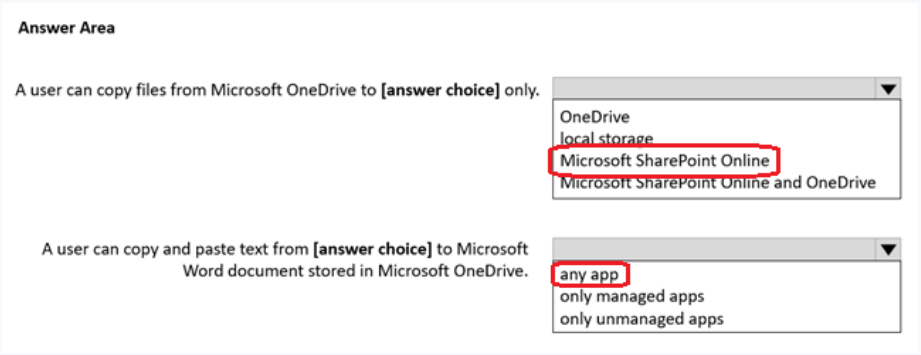
A user can copy files from Microsoft OneDrive to **[answer choice]** only.

- OneDrive
- local storage
- Microsoft SharePoint Online
- Microsoft SharePoint Online and OneDrive

A user can copy and paste text from **[answer choice]** to Microsoft Word document stored in Microsoft OneDrive.

- any app
- only managed apps
- only unmanaged apps

Suggested Answer:



GotDamnImIn 1 year, 8 months ago

Block all except Sharepoint, makes sense. Answer is correct.

upvoted 2 times

Aung2021 1 year, 11 months ago

Yes, I believe the answer is correct.

upvoted 3 times

Fala_Fel 1 year, 11 months ago

agreed

upvoted 1 times

IPalot 1 year, 12 months ago

Wrong.

Allow user to save copies to selected services
Users can save to the selected services (OneDrive for Business, SharePoint, Photo Library, Box, and Local Storage). All other services will be blocked.

Policy managed with paste in: Allow cut or copy between this app and other policy-managed apps. Allow data from any app to be pasted into this app.

upvoted 4 times

QuanN7 1 year, 12 months ago

I believe the answer is correct.

They have to explicitly specify "OneDrive for Business" under app protection policy. Otherwise, they can only save copies of their org data to SharePoint

upvoted 6 times

Arlecchino 1 year, 12 months ago

Can you elaborate please or have a link? the provided answers seem to be correct.

upvoted 1 times

IPalot 1 year, 11 months ago

check this link:

https://learn.microsoft.com/en-us/mem/intune/apps/app-protection-policy-settings-android, search for:

Allow user to save copies to selected services
Users can save to the selected services (OneDrive for Business, SharePoint, Photo Library, Box, and Local Storage). All other services will be blocked.

As earlier stated, the first answer is wrong as per provided link.

upvoted 2 times

IPalot 1 year, 11 months ago

Reading it again... I you're right.
I think you select the service SharePoint which means it shoud block all other services.

upvoted 5 times

Question #100 *Topic 1*

You have a Microsoft 365 E5 subscription. The subscription contains users that have the following types of devices:

• Windows 10
• Android
• iOS

On which devices can you configure the Endpoint DLP policies?

A. Windows 10 only

B. Windows 10 and Android only

C. Windows 10 and iOS only

D. Windows 10, Android, and iOS

Suggested Answer: *A*

Community vote distribution

A (100%)

FK20850 Highly Voted 1 year, 12 months ago

Selected Answer: A

Answer A is correct.

"Endpoint data loss prevention (Endpoint DLP) extends the activity monitoring and protection capabilities of DLP to sensitive items that are physically stored on Windows 10, Windows 11, and macOS (three latest released versions) devices."

https://learn.microsoft.com/en-us/microsoft-365/compliance/endpoint-dlp-learn-about?view=o365-worldwide

upvoted 5 times

Amir1909 Most Recent 11 months ago

Correct

upvoted 1 times

Jakub2023 1 year, 7 months ago

If it says ENDPOINT in the name of the feature then it's about Windows 10/11 or macOS as OS types. :-)

upvoted 4 times

IPalot 1 year, 12 months ago

Correct.

Restricted apps (previously called Unallowed apps) is a list of applications that you create. You configure what actions DLP will take when a user uses an app on the list to access a DLP protected file on a device. It's available for Windows 10 and macOS devices.

upvoted 1 times

Question #101 *Topic 1*

DRAG DROP
-

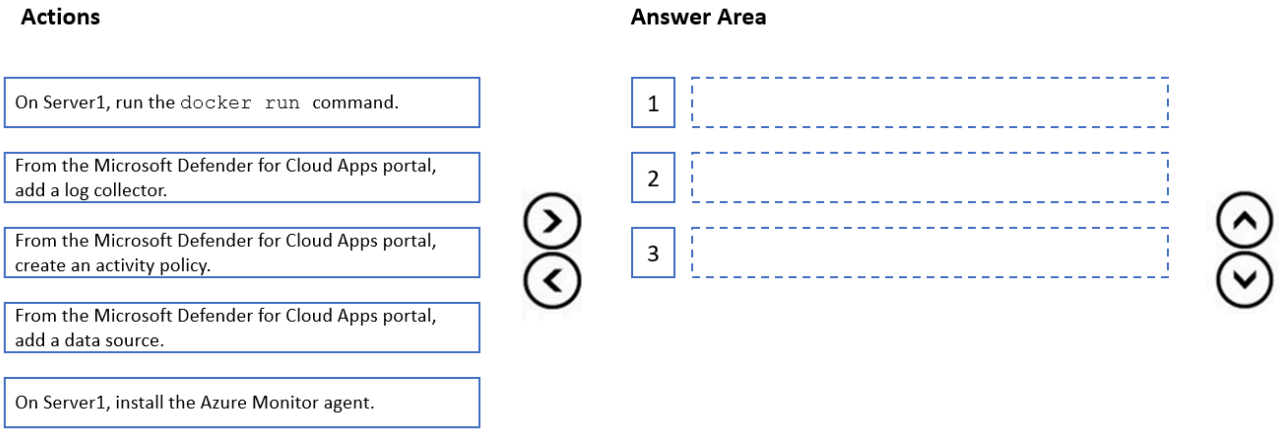
You have a Microsoft 365 E5 subscription and an on-premises server named Server1.

You plan to configure automatic log upload for continuous reports in Microsoft Defender for Cloud Apps.

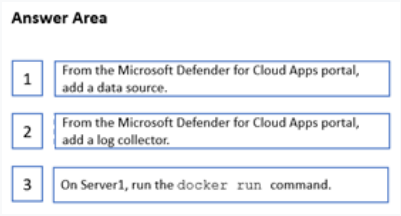
You download a Docker log collector image to Server1.

You need integrate Defender for Cloud Apps with the log collector.

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.



Suggested Answer:



IPalot Highly Voted 1 year, 12 months ago
Correct.

https://learn.microsoft.com/en-us/defender-cloud-apps/discovery-docker-windows
upvoted 9 times

Fala_Fel 1 year, 11 months ago
Thanks, yep all there in your link.
1. Add data Source
2. Add Log Collector
3. Install \ run Docker on Server 1
upvoted 4 times

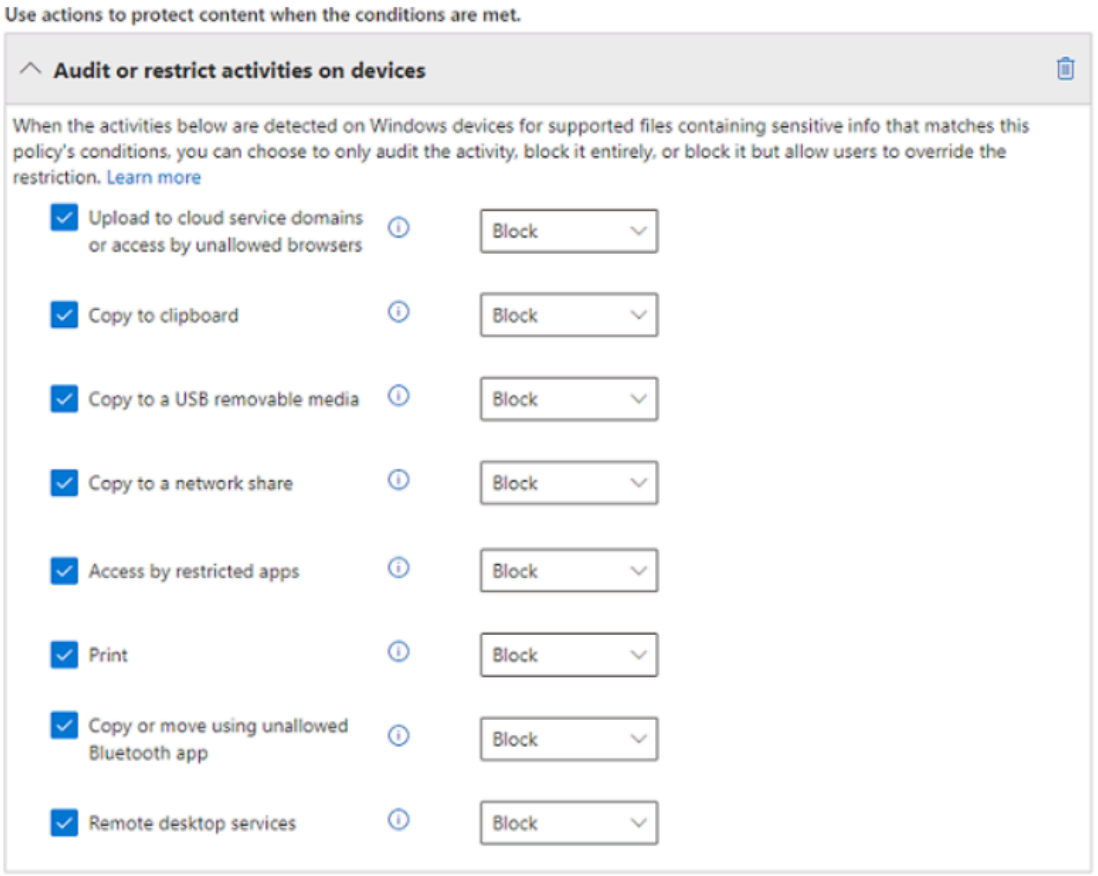
Question #102 *Topic 1*

HOTSPOT
-

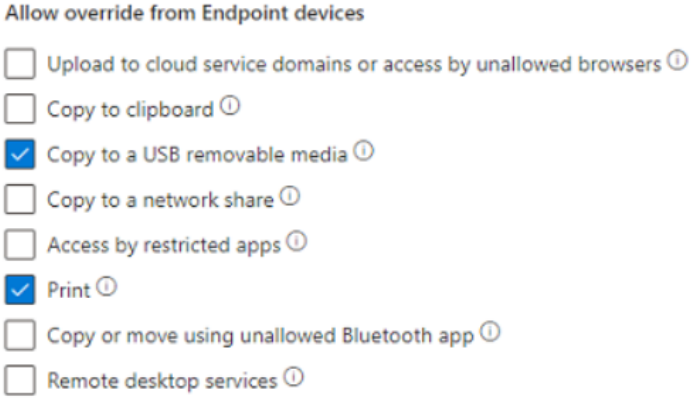
You have a Microsoft 365 subscription that contains an Endpoint data loss prevention (Endpoint DLP) policy named Policy1 and the devices shown in the following table.

Name	Azure AD status	Microsoft Defender for Endpoint status
Device1	Joined	Managed
Device2	Registered	Unmanaged
Device3	Registered	Managed

For Policy1, the Audit or restrict activities on devices settings are configured as shown in the Activities exhibit. (Click the Activities tab.)



For Policy1, the Allow override from Endpoint devices settings are configured as shown in the Devices exhibit. (Click the Devices tab.)



Test users discover that they cannot copy data to their network shares while working remotely.

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

NOTE: Each correct selection is worth one point.

Statements	Yes	No
Users on Device1 can print documents that contain sensitive information.	○	○
Users on Device2 can copy documents that contain sensitive information to USB removable devices.	○	○
Users on Device3 can copy documents that contain sensitive information to network shares.	○	○

Suggested Answer:

Statements	Yes	No
Users on Device1 can print documents that contain sensitive information.	○	●
Users on Device2 can copy documents that contain sensitive information to USB removable devices.	○	●
Users on Device3 can copy documents that contain sensitive information to network shares.	●	○

madfoxmax Highly Voted 1 year, 12 months ago

I expected the opposite of the answer. Device 1 can print, but only after they override. Device 2 is not enrolled in defender, so no policy should apply correct? and device 3 can't save to a network share because it's block and no override is available.

upvoted 23 times

Jakub2023 1 year, 7 months ago

Correct, YYN is the right answer.

- The override setting does allow the user to... override the policy restriction.
- Without Defender for Endpoint enrolment, the policy won't apply.
- AAD joined, AAD registered and Hybrid joined devices are all covered.

upvoted 4 times

egsalvadori Highly Voted 1 year, 12 months ago

I believe that the answer is the opposite: Y-Y-N, anyone care to comment?

upvoted 10 times

Arlecchino 1 year, 11 months ago

At first, I though YNN but now I agree on YYN as madfoxmax explained.

upvoted 2 times

GotDamnImIn Most Recent 1 year, 8 months ago

i think this is Y-Y-N

upvoted 2 times

Lelek 1 year, 10 months ago

OK, that "Allow override from Endpoint devices" screen no longer exists, now this option has entered the "Audit or restrict activities on devices" option, selecting the Block with Block with override option, so the user will receive the warning that the content was blocked, but this warning appears if he wants to, he can print it anyway.

Given this information, the first option should be "YES"

The second option should be "YES", as the device is not managed by Endpoint, so it has no locks.

The third option should be "NO", because the copy network share is blocked and there is no override for this option.

Correct answer is YES, YES, NO

upvoted 5 times

Y2 1 year, 11 months ago

YYN

Device1 -Y override

Device 2 -Y unmanned
Device3 - N No override
upvoted 7 times

Vuuskes 1 year, 11 months ago
I think its also YYN
upvoted 6 times

Jame 1 year, 12 months ago
I think YYN
upvoted 6 times

Question #103 *Topic 1*

You have an on-premises network that has several legacy applications. The applications perform LDAP queries against an existing directory service.

You are migrating the on-premises infrastructure to a cloud-only infrastructure.

You need to recommend an identity solution for the infrastructure that supports the legacy applications. The solution must minimize the administrative effort to maintain the infrastructure.

Which identity service should you include in the recommendation?

A. Azure Active Directory (Azure AD) B2C

B. Active Directory Domain Services (AD DS)

C. Azure Active Directory (Azure AD)

D. Azure Active Directory Domain Services (Azure AD DS)

Suggested Answer: *D*

Community vote distribution

IPalot Highly Voted 1 year, 12 months ago

Selected Answer: D

https://docs.microsoft.com/en-us/azure/active-directory-domain-services/overview

upvoted 5 times

coolbru Most Recent 1 year, 10 months ago

Selected Answer: D

Answer is correct. Azure Active Directory Domain Services (Azure AD DS) supports LDAP = minimal effort.

upvoted 3 times

Question #104 *Topic 1*

HOTSPOT
-

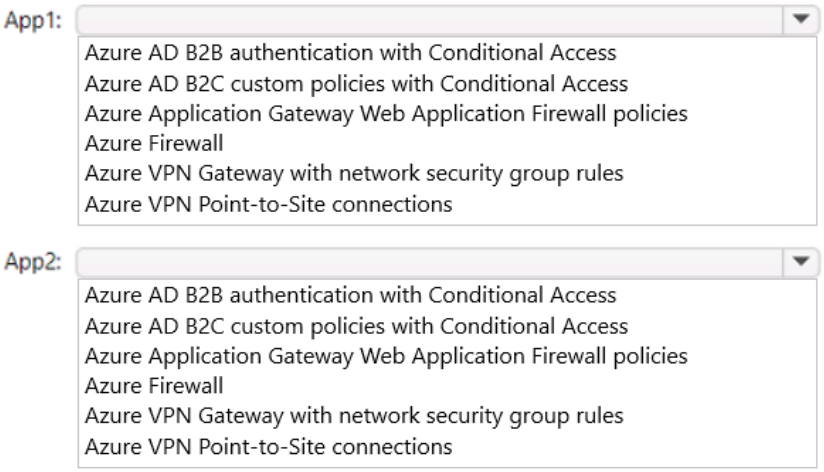
You have a hybrid cloud infrastructure.

You plan to deploy the Azure applications shown in the following table.

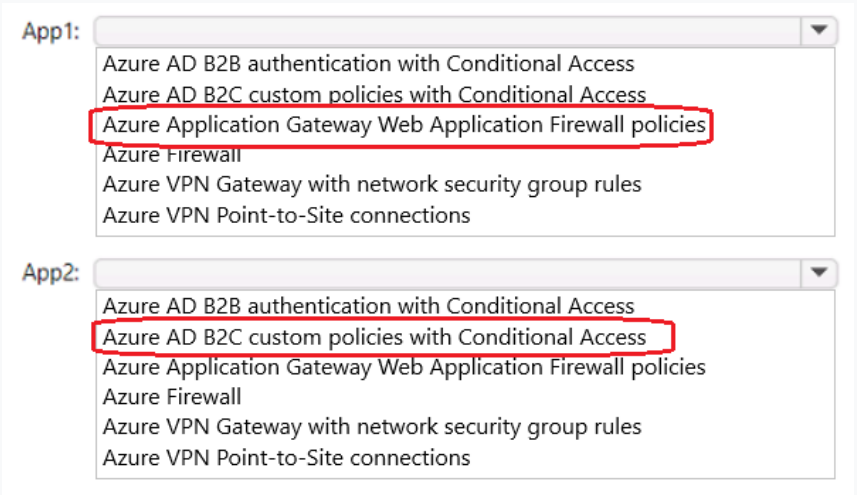
Name	Type	Requirement
App1	An Azure App Service web app accessed from Windows 11 devices on the on-premises network	Protect against attacks that use cross-site scripting (XSS).
App2	An Azure App Service web app accessed from mobile devices	Allow users to authenticate to App2 by using their LinkedIn account.

What should you use to meet the requirement of each app? To answer, select the appropriate options in the answer area.

NOTE: Each correct selection is worth one point.



Suggested Answer:



JCkD4Ni3L 1 year, 7 months ago
Correct ! This is material from SC-100 exam... ;)
upvoted 2 times

master355 1 year, 11 months ago
App2 why not B2B option?
upvoted 1 times

Fala_Fel 1 year, 11 months ago

App2 B2C the clear choice
"Azure Active Directory B2C (Azure AD B2C) is a customer identity access management (CIAM) solution that enables you to sign up and sign in your customers into your apps and APIs. Your customers use their preferred social, enterprise, or local account identities to get single sign-on access to your applications."
https://learn.microsoft.com/en-us/azure/active-directory-b2c/

B2B might work, but sounds like it is being deprecated.
upvoted 2 times

IPalot 1 year, 12 months ago
Correct.
Azure WAF (Web Application Firewall) provides protection for web applications (IaaS, PaaS or on-premises) from common attacks (OWASP Top 10) like SQL injection and XSS (Cross-site scripting).

https://learn.microsoft.com/en-us/azure/active-directory-b2c/identity-provider-linkedin?pivots=b2c-user-flow
upvoted 4 times

HOTSPOT
-

You have a Microsoft 365 E5 subscription that uses Microsoft Intune.

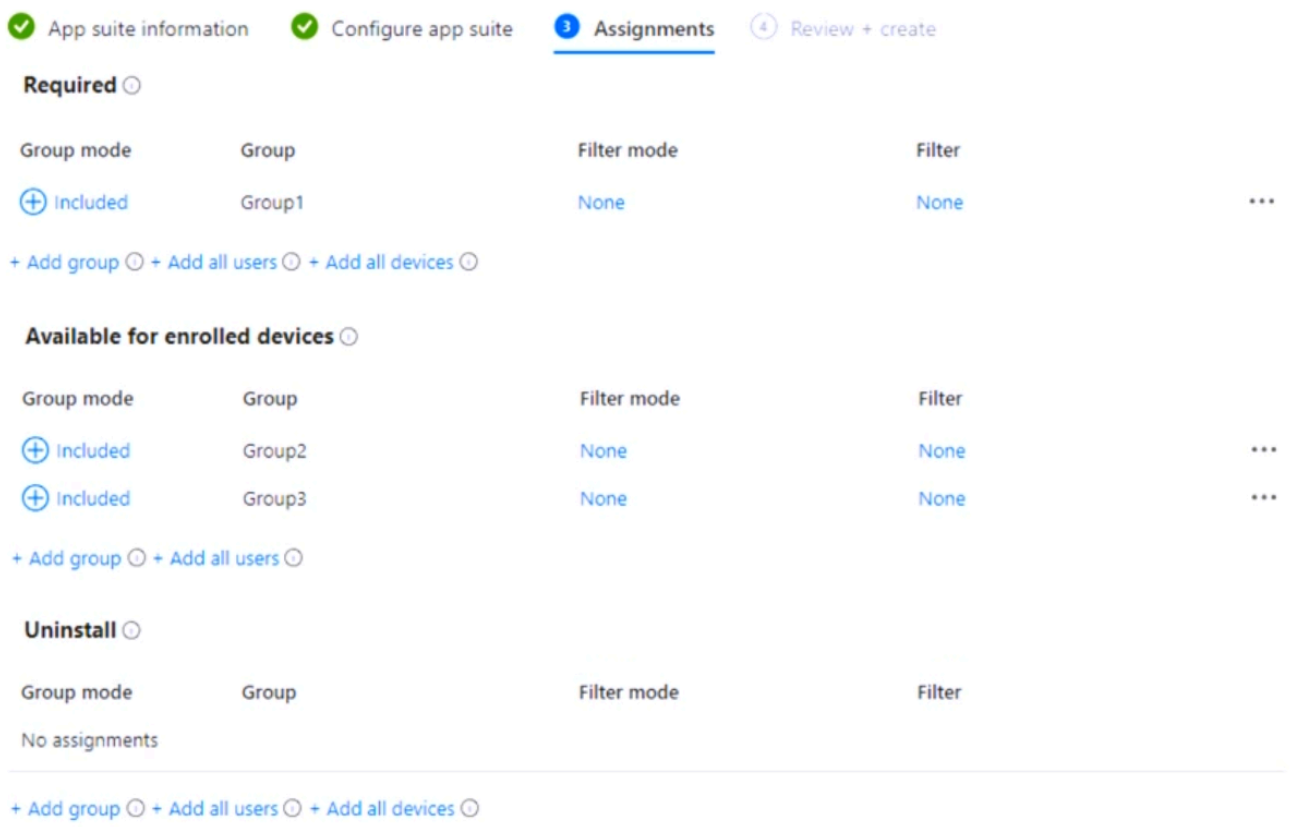
You have the Azure AD security groups shown in the following table.

Name	Member of
Group1	*None*
Group2	Group1
Group3	*None*

You have the Windows 10 devices shown in the following table.

Name	Member of	Intune
Device1	Group2	Enrolled
Device2	Group3	Enrolled
Device3	Group1	Enrolled

You deploy Microsoft 365 Apps for enterprise as shown in the following exhibit.



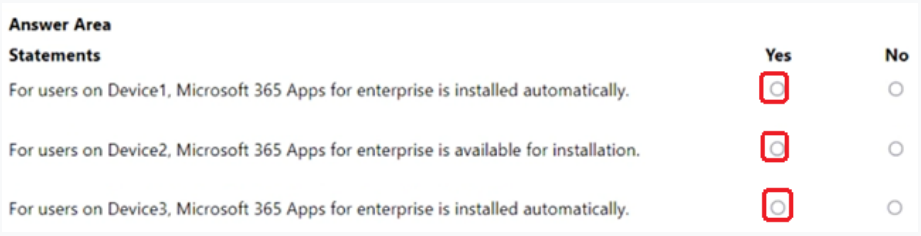
For each of the following statements, select Yes if the statement is true. Otherwise, select No.

NOTE: Each correct selection is worth one point.

Answer Area

Statements	Yes	No
For users on Device1, Microsoft 365 Apps for enterprise is installed automatically.	○	○
For users on Device2, Microsoft 365 Apps for enterprise is available for installation.	○	○
For users on Device3, Microsoft 365 Apps for enterprise is installed automatically.	○	○

Suggested Answer:



JCkD4Ni3L 1 year, 7 months ago

Correct answer is YYY, this MD-101 material.

upvoted 2 times

Lelek 1 year, 10 months ago

I disagree with the answer.

Intune supports nested group, but let's separate the subjects.
The first question is "For users on Device 1". Device1 users are in "Group2", within Group2 are Device3 users as a member, which would be Group1.

In the illustration of the image we can see that Group1 is to perform the automatic installation (Required), therefore only Device3 users will be installed.

It is worth mentioning that the Group2 who is a member is Group1 and not the other way around. If it were Group2 as a member of Group1 the answer would be YES.

In this sense we can say that the answer is NO, YES, YES

upvoted 3 times

Sprocket10 1 year, 8 months ago

Reread the question. Group2 is a member of Group1. Table headings are a little confusing.

upvoted 2 times

QuanN7 1 year, 10 months ago

Intune supports assigning apps to nested groups. For example, if you assigned an app to the "Engineering Global" group and have "Engineering APAC", "Engineering EMEA" and "Engineering US" nested as child groups, the members of those child groups will also be targeted with the assignment.

https://learn.microsoft.com/en-us/mem/intune/apps/apps-deploy

upvoted 1 times

Y2 1 year, 11 months ago

i thought licenses do not support nested groups. -
https://learn.microsoft.com/en-us/azure/active-directory/enterprise-users/licensing-group-advanced#:~:text=Group%2Dbased%20licensing%20currently%20doesn,group%20have%20the%20licenses%20applied.
Group-based licensing currently doesn't support groups that contain other groups (nested groups).

upvoted 1 times

Learner2022 1 year, 11 months ago

Intune supports nested group. https://learn.microsoft.com/en-us/mem/intune/apps/apps-deploy

upvoted 3 times

Jame 1 year, 12 months ago

Correct! YYY

https://learn.microsoft.com/en-us/mem/intune/apps/apps-deploy

Group 1 intent Group 2 intent Resulting intent

User Required User Available Required and Available

upvoted 1 times

FK20850 1 year, 12 months ago

Intune supports nested groups. Correct answer YYY

upvoted 4 times

Question #106 *Topic 1*

You have an Azure AD tenant.

You have 1,000 computers that run Windows 10 Pro and are joined to Azure AD.

You purchase a Microsoft 365 E3 subscription.

You need to deploy Windows 10 Enterprise to the computers. The solution must minimize administrative effort.

What should you do?

A. From the Microsoft Endpoint Manager admin center, create a Windows Autopilot deployment profile. Assign the profile to all the computers. Instruct users to restart their computer and perform a network restart.

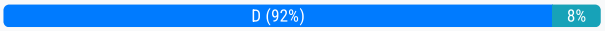
B. Enroll the computers in Microsoft Intune. Create a configuration profile by using the Edition upgrade and mode switch template. From the Microsoft Endpoint Manager admin center, assign the profile to all the computers and instruct users to restart their computer.

C. From Windows Configuration Designer, create a provisioning package that has an EditionUpgrade configuration and upload the package to a Microsoft SharePoint Online site. Instruct users to run the provisioning package from SharePoint Online.

D. From the Azure Active Directory admin center, create a security group that has dynamic device membership. Assign licenses to the group and instruct users to sign in to their computer.

Suggested Answer: *B*

Community vote distribution



EsamiTopici Highly Voted 1 year, 9 months ago

Licenses should be assigned to users not groups, so I think D is wrong.
B is correct
https://learn.microsoft.com/en-us/mem/intune/configuration/edition-upgrade-configure-windows-10

upvoted 5 times

Hazul 1 year, 3 months ago

B is correct.

upvoted 1 times

jecampos2 Most Recent 1 year, 6 months ago

The correct answer is B. Please see the following links:
https://learn.microsoft.com/en-us/mem/intune/fundamentals/licenses
https://learn.microsoft.com/en-us/mem/intune/configuration/edition-upgrade-configure-windows-10

upvoted 2 times

ChizzyO 1 year, 6 months ago

License can be assigned to a security group in Azure
https://learn.microsoft.com/en-us/azure/active-directory/fundamentals/active-directory-licensing-whatis-azure-portal

upvoted 1 times

JCkD4Ni3L 1 year, 7 months ago

Selected Answer: D

D, this is MD-101 material

upvoted 2 times

GotDamnImIn 1 year, 8 months ago

Selected Answer: D

One thing to take note of here is the type of licensing available, since it's an E3, Intune and MEM are out of the picture and you have two options remaining, which D seems to be close unless if there is a typo.

upvoted 3 times

Jakub2023 1 year, 7 months ago

Can you back this up with a link? What limitations in an E3 license make answer B unworkable?
upvoted 1 times

Jimboski 1 year, 8 months ago
I think its D with a typo in play. Microsoft wants subscription activation. We use this and its wonderful
upvoted 1 times

JackeD 1 year, 8 months ago
Selected Answer: D
D, one of the biggest benefits of intune imho
upvoted 2 times

ahmedkmicha 1 year, 8 months ago
Selected Answer: A
By using Windows Autopilot, you can deploy Windows 10 Enterprise to your Azure AD joined devices without the need for physical intervention, minimizing administrative effort. Additionally, Autopilot simplifies the setup and configuration process, ensuring a consistent and standardized deployment across all devices.
upvoted 1 times

ahmedkmicha 1 year, 8 months ago
sorry, Option B is more suitable because it allows you to create a configuration profile in Microsoft Intune that specifically targets the Windows 10 edition upgrade. By using the Edition upgrade and mode switch template, you can directly upgrade the computers from Windows 10 Pro to Windows 10 Enterprise. This minimizes administrative effort as you can centrally manage the upgrade process and simply instruct users to restart their computers.
upvoted 2 times

Florian74 1 year, 8 months ago
Not sure that D is is the good answer : licences can be distributed by dynamics groups, but users should be licenced, not devices. So B appears to be the answer.
upvoted 1 times

jamspurple 1 year, 8 months ago
The answer should be D however I think its written incorrectly.
You can license a group with group based licensing and assign it to the users either manually or using dynamic assignment. Once the USER is licensed they will just need to restart their device for the upgrade to occur. However the answer states that you are using Dynamic DEVICE Membership which won't work (You cant assign a license to a device).

I have a feeling that this is just a typo in the answer.

B cannot be the correct answer, as they have specified you purchased M365 E3 licenses. When using Edition upgrade and mode switch you need to provide a Multiple Activation Key (MAK) or Key Management Server (KMS) key. You would be purchasing additional licenses and it is not the low effort option.
upvoted 3 times

hubran 1 year, 9 months ago
Selected Answer: D
D is correct, in link provided by EsamiTopici they say: "When a licensed user signs in to a device that meets requirements using their Azure AD credentials, Windows steps up from Pro edition to Enterprise. Then all of the Enterprise features are unlocked.
upvoted 2 times

Dislexsick 1 year, 9 months ago
Selected Answer: D
I also think it's D
upvoted 2 times

EsamiTopici 1 year, 9 months ago
I think is D, but correct me:

https://learn.microsoft.com/en-us/windows/deployment/windows-10-subscription-activation#requirements
upvoted 1 times

EsamiTopici 1 year, 9 months ago
Mmmh, re-reading the question, licenses should be assigned to users not groups, so I think D is wrong
upvoted 2 times

Question #107 *Topic 1*

You have a Microsoft 365 E5 subscription that contains 500 users. Two hundred users have personal devices that run either Android, Windows 10, or macOS. Three hundred users have corporate-owned devices that run either Windows 10 or macOS.

You plan to configure device enrollment.

You need to ensure that you can apply separate policies to the corporate-owned devices and the personal devices. The solution must minimize administrative effort.

What should you create first?

A. a dynamic device group

B. a dynamic user group

C. a deployment package

D. a Microsoft 365 group

Suggested Answer: *A*

GotDamnImIn 1 year, 8 months ago

Correct. Very straight-forward.

upvoted 3 times

Question #108 *Topic 1*

HOTSPOT
-

You have a Microsoft 365 E5 subscription that uses Microsoft Intune. The subscription contains the resources shown in the following table.

Name	Type	Member of
User1	User	Group1
Device1	Device	Group2

User1 is the owner of Device1.

You add Microsoft 365 Apps Windows 10 and later app types to Intune as shown in the following table.

Name	Shows in Company Portal	Assignment	Microsoft Office app to install	Day of creation
App1	Yes	Group1 - Required	Word	Monday
App2	Yes	Group2 - Required	Excel	Tuesday
App3	Yes	Group1 - Available	PowerPoint	Wednesday

On Thursday, you review the results of the app deployments.

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
Word is installed on Device1.	○	○
App3 is displayed in the Company Portal.	○	○
Excel is installed on Device1.	○	○

Suggested Answer:

Answer Area

Statements	Yes	No
Word is installed on Device1.	○	◉
App3 is displayed in the Company Portal.	◉	○
Excel is installed on Device1.	◉	○

Kees1990 Highly Voted 1 year, 9 months ago
YYY
https://learn.microsoft.com/en-us/mem/intune/apps/apps-deploy
upvoted 10 times

Feyenoord 1 year, 8 months ago
See: https://learn.microsoft.com/en-us/mem/intune/apps/apps-deploy#how-conflicts-between-app-intents-are-resolved

You are correct!
upvoted 3 times

Roche4ever Most Recent 1 year, 3 months ago
This question is still valid
Was in Exam Today, 25 Sept 23

I think the answer is correct: N,Y,Y. (Note that: User1 is owner of Device 1 but it is in Group 1 instead of Group 2)
upvoted 1 times

zaika 1 year, 7 months ago
Y - User1 in Group1.Y - User1 in Group1. N- User1 owner of Device1. am i right?
upvoted 1 times

zaika 1 year, 7 months ago
Assign to devices - NO (Devices not enrolled with Intune)
upvoted 1 times

GotDamnImIn 1 year, 8 months ago
Correct NYY,
No - Targeting for Device1 is for an object that is a member of Group 2
Yes - Because this has nothing to do with assignment
Yes - Excel is targeted to be installed for a device in Group 2
upvoted 3 times

bartdxxx 1 year, 9 months ago
Why not YYY ?
upvoted 2 times

mario123na 1 year, 9 months ago
Device 1 is inside on group 2
upvoted 1 times

EsamiTopici 1 year, 9 months ago
But intune support meste group, no?
upvoted 1 times

Smeyer 1 year, 9 months ago
Should be YYN
upvoted 2 times

Question #109 *Topic 1*

You have a Microsoft 365 tenant.

You plan to implement device configuration profiles in Microsoft Intune.

Which platform can you manage by using the profiles?

A. Windows 8.1

B. CentOS Linux

C. Windows 10

D. Android Enterprise

Suggested Answer: *ACD*

Community vote distribution

ACD (100%)

Jimboski Highly Voted 1 year, 8 months ago

Ok, I agree with the answer. However, the question is wrote poorly. They do not ask you select more than 1 answer. That needs fixed

upvoted 5 times

hubran Most Recent 1 year, 9 months ago

Selected Answer: ACD

Correct:

When you create a profile (Configuration profiles > Create profile), choose your platform:

Android device administrator

Android Enterprise

iOS/iPadOS

macOS

Windows 10 and later

Windows 8.1 and later

Source: https://learn.microsoft.com/en-us/mem/intune/configuration/device-profile-create

upvoted 2 times

EsamiTopici 1 year, 9 months ago

correct

upvoted 1 times

Question #110 *Topic 1*

You have a Microsoft 365 E5 tenant that contains the devices shown in the following table.

Name	Platform
Device1	Windows 10 Enterprise
Device2	iOS
Device3	Android
Device4	Windows 10 Pro

The devices are managed by using Microsoft Intune.

You plan to use a configuration profile to assign the Delivery Optimization settings.

Which devices will support the settings?

A. Device1 only

B. Device1 and Device4

C. Device1, Device3, and Device4

D. Device1, Device2, Device3, and Device4

Suggested Answer: *B*

NitishKarmakar 1 year, 3 months ago

Correct, Delivery optimization can only be configured for Windows 10 and above. "Delivery Optimization is a reliable HTTP downloader with a cloud-managed solution that allows Windows devices to download those packages from alternate sources if desired (such as other devices on the network and/or a dedicated cache server) in addition to the traditional internet-based servers (referred to as 'HTTP sources' throughout Delivery Optimization documents)." - Applies to Windows 10 and 11.
https://learn.microsoft.com/en-us/windows/deployment/do/waas-delivery-optimization

upvoted 1 times

KNemeth 1 year, 3 months ago

It should be answer A, am I right?

upvoted 1 times

GotDamnImIn 1 year, 8 months ago

Correct, can only create for Windows 10 and/or 11 only

upvoted 2 times

EsamiTopici 1 year, 9 months ago

Correct
https://learn.microsoft.com/en-us/windows/deployment/do/waas-delivery-optimization-reference

upvoted 2 times

Question #111 *Topic 1*

HOTSPOT
-

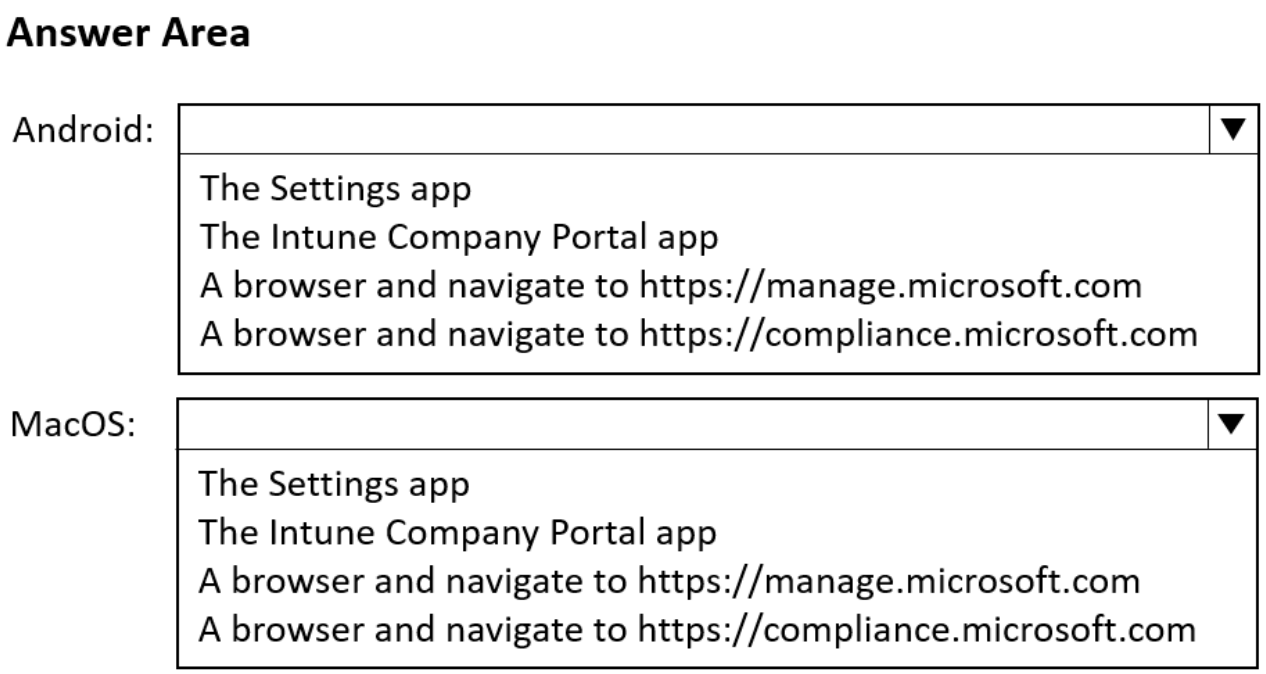
You have a Microsoft 365 E5 subscription that uses device management in Microsoft Endpoint Manager.

You purchase five new Android devices and five new macOS devices.

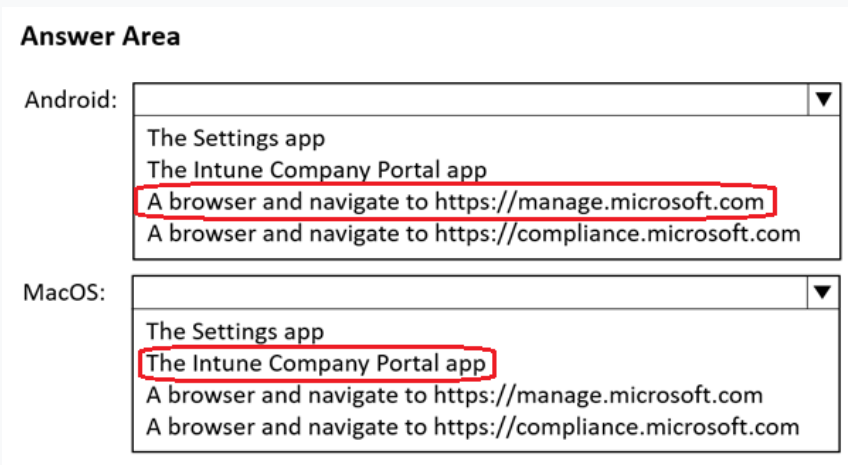
You need to enroll the new devices in Microsoft Intune.

What should you use to enroll each device type? To answer, select the appropriate options in the answer area.

NOTE: Each correct selection is worth one point.



Suggested Answer:



Feyenoord Highly Voted 1 year, 8 months ago

Both Company Portal App: https://learn.microsoft.com/en-us/mem/intune/fundamentals/deployment-guide-enrollment-macos#device-enrollment-end-user-tasks

https://learn.microsoft.com/en-us/mem/intune/fundamentals/deployment-guide-enrollment-android#android-enterprise-personally-owned-devices-with-a-work-profile-end-user-tasks

upvoted 8 times

Amir1909 Most Recent 11 months, 2 weeks ago

- Intune Company Portal app
- Intune Company Portal app

upvoted 1 times

prabhjot 1 year, 8 months ago

for macOS the ans is is correct - https://learn.microsoft.com/en-us/mem/intune/fundamentals/deployment-guide-enrollment-macos

upvoted 2 times

prabhjot 1 year, 8 months ago

https://learn.microsoft.com/en-us/mem/intune/fundamentals/deployment-guide-enrollment Andriod is definitely - Intune Compnay Portal APP

upvoted 1 times

ahmedkmicha 1 year, 8 months ago

Android: Intune Company Portal app

MacOS: https://portal.manage.microsoft.com/

upvoted 1 times

samitri80 1 year, 9 months ago

For Android. Intune Company Portal is the correct answer

upvoted 1 times

Futfuyfyjfj 1 year, 9 months ago

Android answer is wrong. You can browse to portal.manage.microsoft.com you can add your device from there, but you are then forwarded to the Play Store to download the Intune company portal. So I would say use the Intune Company Portal straight away .

upvoted 2 times

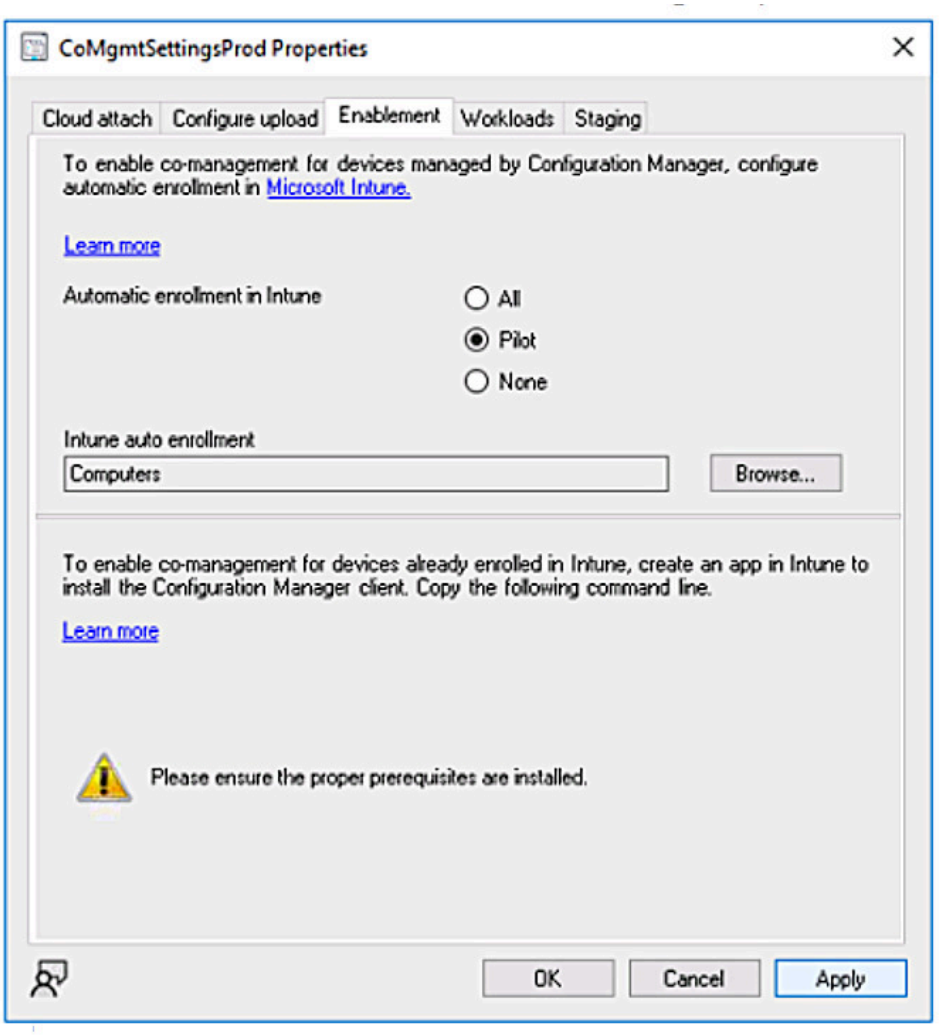
HOTSPOT
-

You use Microsoft Endpoint Configuration Manager for device management.

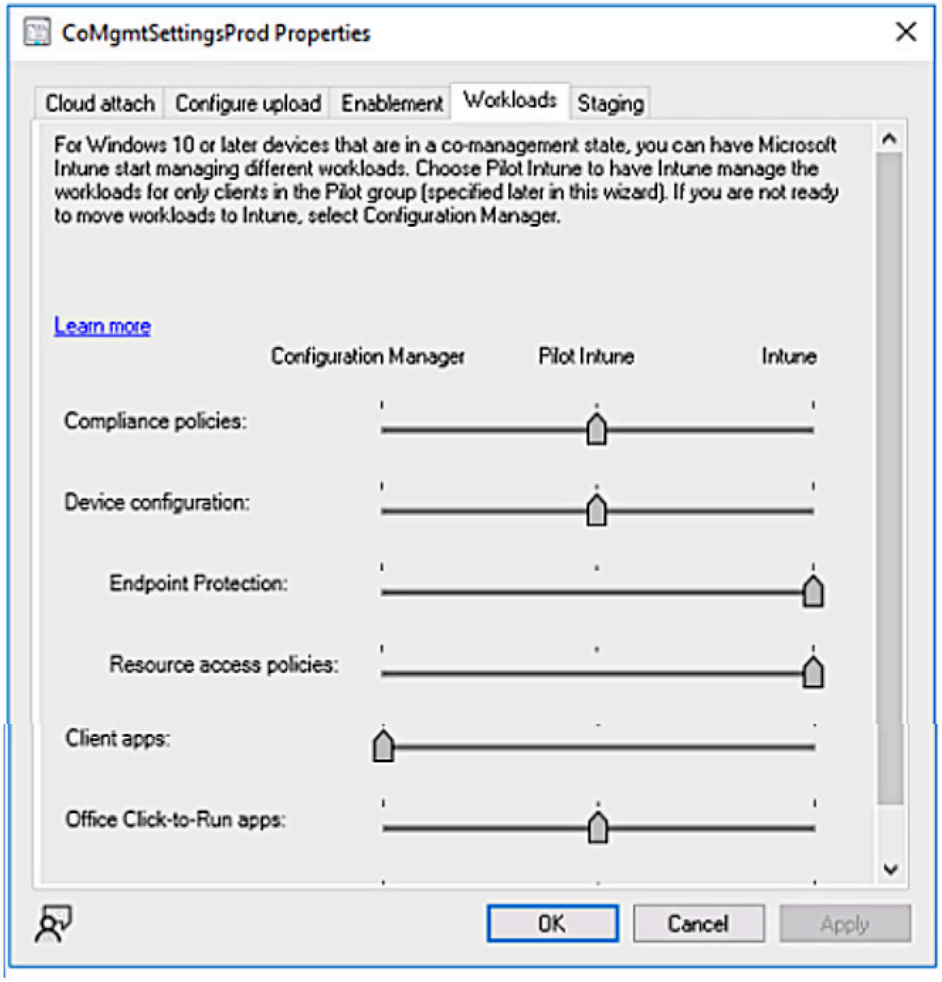
The domain contains the Windows 11 devices shown in the following table.

Name	In collection
Device1	Collection1
Device2	Computers, Collection2

You enable co-management in Configuration Manager as shown in the Enablement exhibit. (Click the Enablement tab.)



You configure the Workloads settings for co-management as shown in the Workloads exhibit. (Click the Workloads tab.)



You configure the Staging settings for co-management as shown in the Staging exhibit. (Click the Staging tab.)

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

NOTE: Each correct selection is worth one point.

Answer Area

Statements	Yes	No
Microsoft Intune manages the compliance policy for Device1.	○	○
Microsoft Intune manages Endpoint Protection for Device2.	○	○
Microsoft Intune manages Microsoft Office Click-to-Run apps for Device2.	○	○

Suggested Answer:

Answer Area

Statements	Yes	No
Microsoft Intune manages the compliance policy for Device1.	○	●
Microsoft Intune manages Endpoint Protection for Device2.	●	○
Microsoft Intune manages Microsoft Office Click-to-Run apps for Device2.	●	○

Jakub2023 1 year, 7 months ago

The answer provided makes sense to me.

upvoted 2 times

Question #113 *Topic 1*

DRAG DROP

-

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

Name	Operating System	Microsoft Intune
Device1	Windows 11 Enterprise	Enrolled
Device2	iOS	Enrolled
Device3	Android	Not enrolled

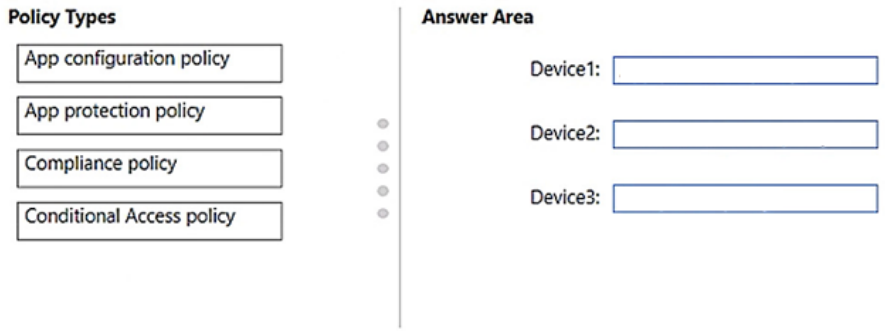
You install Microsoft Word on all the devices.

You plan to configure policies to meet the following requirements:

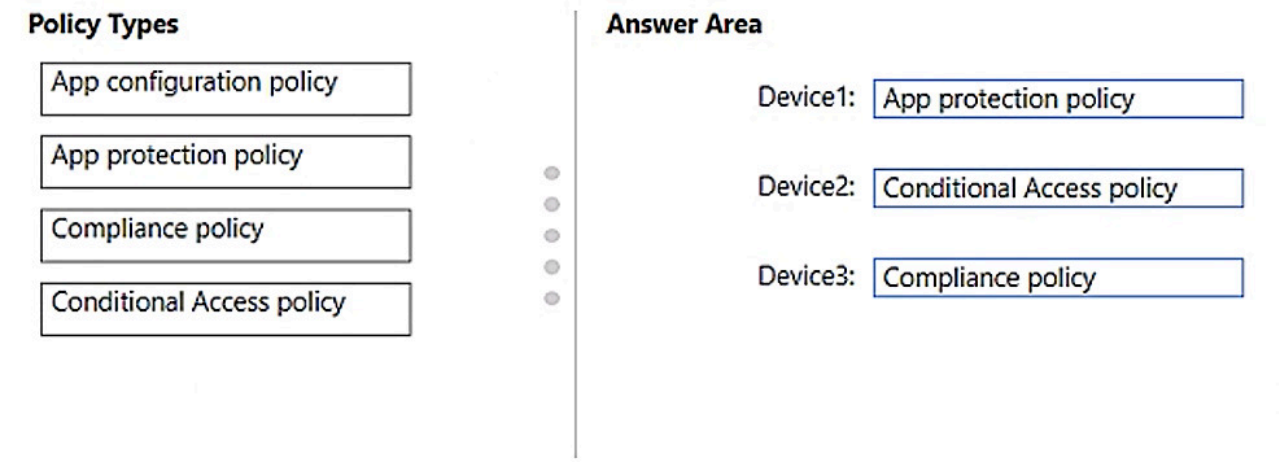
• Word files created by using Windows devices must be encrypted automatically.
• If an Android device becomes jailbroken, access to corporate data must be blocked from Word.
• For iOS devices, users must be prevented from using native or third-party mail clients to connect to Microsoft 365.

Which type of policy should you configure for each device? To answer, drag the appropriate policy types to the correct devices. Each policy type may be used once, more than once, or not at all. You may need to drag the split bar between panes or scroll to view content.

NOTE: Each correct selection is worth one point.



Suggested Answer:



Leo1905tti 1 year, 3 months ago

Device 3 está errado - O correto é App Protection https://learn.microsoft.com/pt-br/mem/intune/apps/app-protection-policy-settings-android

upvoted 1 times

Jo696 1 year, 6 months ago

Just tested this and indeed the answers are correct (I was dubious but they are right)

upvoted 1 times

Jakub2023 1 year, 7 months ago

My take on this:

1) App protection policy

2) Compliance policy

3) Compliance policy

Yes, for 2, you also need a Conditional Access policy - but without the compliance policy setting to define the device status of rooted/jailbroken as non-compliant the conditional access policy won't do anything...

upvoted 3 times

skyline94 1 year, 6 months ago

I think for Device 3, it should be Conditional Access

link: https://learn.microsoft.com/en-us/exchange/clients-and-mobile-in-exchange-online/outlook-for-ios-and-android/secure-outlook-for-ios-and-android#block-all-email-apps-except-outlook-for-ios-and-android-using-conditional-access

upvoted 2 times

Fwekker 1 year, 6 months ago

The android isn't enrolled. So Compliance wouldnt work for the android. In app protection you can detect rooted devices.

upvoted 1 times

Question #1 *Topic 2*

Note: This question is part of a series of questions that present the same scenario. Each question in the series contains a unique solution that might meet the stated goals. Some question sets might have more than one correct solution, while others might not have a correct solution.
After you answer a question in this section, you will NOT be able to return to it. As a result, these questions will not appear in the review screen.
You have a Microsoft 365 subscription.
You discover that some external users accessed content on a Microsoft SharePoint site. You modify the SharePoint sharing policy to prevent sharing outside your organization.
You need to be notified if the SharePoint sharing policy is modified in the future.
Solution: From the Security & Compliance admin center, you create a threat management policy.
Does this meet the goal?

A. Yes

B. No

Suggested Answer: *B*
From the Security & Compliance admin center, Alerts, you create a new alert policy.
Reference:
https://docs.microsoft.com/en-us/microsoft-365/compliance/alert-policies

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

Uglydotcom Highly Voted 5 years, 1 month ago
Correct is B. From the Security & Compliance admin center, Alerts, you create a new alert policy.
https://docs.microsoft.com/en-us/microsoft-365/compliance/alert-policies
upvoted 68 times

LoremanReturns 3 years, 5 months ago
I confirm, tested in my lab
upvoted 3 times

minajahan 4 years, 9 months ago
This is right.
I just tried it with my free trial subscription.
upvoted 6 times

Takloy 3 years, 10 months ago
Agree and tested!
upvoted 5 times

itmp Highly Voted 4 years, 7 months ago
It is an ALERT policy with Threat Management as category - so if it's a typo, than yes, otherwise, no.

SCC-> Alerts -> New alert policy -> Threat Management-> Activity is -> Changed a sharing policy.
upvoted 18 times

Mary_Yvette 4 years, 5 months ago
The answer is No. If I am to create this alert I will categorize this as Data Lost Prevention. Threat Management policies are different from the alert needed here.
upvoted 2 times

Moderator Most Recent 2 years, 3 months ago
Selected Answer: B
B is correct, decent explanations can be found here already.
upvoted 2 times

L33D 2 years, 6 months ago
Still valid, on exam Jun 25, 2022

upvoted 2 times

Rickert 2 years, 8 months ago

Selected Answer: B

It is an alert

upvoted 2 times

JamesM9 2 years, 9 months ago

I have tested this today and from the S&C:

1. S&C center
2. Policies and rules
3. Alert Policy
4. New alert policy
5. Name/assign severity
6. Select category - Threat Management
7. Select Activity - Site Administrations/Changed a Sharing Policy
8. Set alert settings (Every time an activity matches the rule)
9. Set Recipients
10. No limit
11. Create

"An administrator changed a SharePoint sharing policy by using the Office 365 Admin center, SharePoint admin center, or SharePoint Online Management Shell. Any change to the settings in the sharing policy in your organization will be logged. The policy that was changed is identified in the ModifiedProperty field property when you export the search results".

As a result of this, I managed to create an alert policy through the S&C center for when the SharePoint sharing policy is modified.

The answer is A - Yes.

upvoted 2 times

Durden871 2 years, 9 months ago

From Udemy:
Explanation
We can create a threat management policy to alert us when the sharing policy is changed.

Create a new Alert policy > under Category select Threat Management > under ɹ€˜Activity isɹ€™ scroll down to the ɹ€˜Site administration activitiesɹ€™ and select ɹ€˜Changed a sharing policyɹ€™.

upvoted 1 times

Durden871 2 years, 9 months ago

Answer, to them, was "Yes".

upvoted 1 times

Glorence 2 years, 11 months ago

still valid, it was in my exam last Feb 5, 2022

upvoted 2 times

Kalzonee3611 2 years, 10 months ago

Thank you

upvoted 1 times

Panku 2 years, 11 months ago

Answer: B

upvoted 2 times

Coulibaly 2 years, 11 months ago

Selected Answer: A

We can create a threat management policy to alert us when the sharing policy is changed.
Create a new Alert policy > under Category select Threat Management > under 'Activity is' scroll down to the 'Site administration activities' and select 'Changed a sharing policy'

upvoted 1 times

Coulibaly 2 years, 11 months ago

I think Answer is A

We can create a threat management policy to alert us when the sharing policy is changed.
Create a new Alert policy > under Category select Threat Management > under ‘Activity is’ scroll down tothe ‘Site administration activities’ and select ‘Changed a sharing policy’

upvoted 1 times

tf444 3 years ago

Yes:
We can create a threat management policy to alert us when the sharing policy is changed.
Create a new Alert policy > under Category select Threat Management > under 'Activity is' scroll down to the 'Site administration activities' and select 'Changed a sharing policy'.

upvoted 1 times

UWSFish 3 years, 4 months ago

I think of the context of the three questions A is the answer that will get marked correct. Weather the questions has been worded as well as it might have been is up for debate.

upvoted 1 times

Domza 3 years, 4 months ago

Please dont be confused with Threat Management "Category"
This bad boy is in Alerting Policy.

upvoted 2 times

balajim212 3 years, 5 months ago

Answer is B. No - Need to use Alert policies

upvoted 2 times

chenepon 3 years, 6 months ago

Corresct A: test in my tenant dev

upvoted 1 times

Eltooth 3 years, 7 months ago

NO NO NO

upvoted 2 times

Question #2 *Topic 2*

You have a Microsoft 365 subscription.
You need to be notified if users receive email containing a file that has a virus.
What should you do?

A. From the Exchange admin center, create an in-place eDiscovery & hold.

B. From the Security & Compliance admin center, create a safe attachments policy.

C. From the Security & Compliance admin center, create a data loss prevention (DLP) policy.

D. From the Security & Compliance admin center, create an alert policy.

Suggested Answer: *D*
Reference:
https://docs.microsoft.com/en-us/office365/securitycompliance/alert-policies

Sonia33 Highly Voted 4 years, 6 months ago
From the Security & Compliance admin center, create an alert policy.

D. Create alert policy > Category: Threat management > Activity: "Office 365 detected malware in an email message before or after it was delivered."
upvoted 33 times

mgmjtech Highly Voted 4 years, 5 months ago
The answer is D. S&C Alert policies > category mail flow > detected malware in file.
upvoted 7 times

NitishKarmakar Most Recent 1 year, 6 months ago
D. Is the correct answer
Microsoft Security/Defender Portal > Email & Collaboration > New Alert Policy > Severity = Any H/M/L > Category = Mailflow -> Activity is- Detected Malware in Email message
upvoted 1 times

jkklim 3 years, 1 month ago
answer is D - microsoft portal is changing daily, and i wonder when you guys got the latest testging
upvoted 6 times

365admin 3 years, 8 months ago
Alert- Polcies-Email messages containing malware removed after delivery
Generates an alert when any messages containing malware are delivered to mailboxes in your organization. If this event occurs, Microsoft removes the infected messages from Exchange Online mailboxes using Zero-hour auto purge. This policy has an Informational severity setting and automatically triggers automated investigation and response in Office 365.

https://docs.microsoft.com/en-us/microsoft-365/compliance/alert-policies?view=o365-worldwide
upvoted 2 times

Jake1 3 years, 8 months ago
Tested this in my tenant. D is in fact the correct answer. S&C Center > Alert Policies > Create > Name your alert > Create alert settings > Activity is > Detected malware in a file...
upvoted 4 times

moh15 4 years, 5 months ago
I think B
D for : Office 365 detected malware in either a SharePoint or OneDrive file.
upvoted 3 times

melki_zedek 4 years, 2 months ago
B will not give you alert; it will only redirect the email to another address at best
upvoted 1 times

aexlz 4 years, 1 month ago

Alerts are not mentioned. You should be notified, which can be done with B (Email Notification to Administrator)

D is limited to SharePoint and OneDrive, but the question claims an attached file.
upvoted 2 times

slimeycat 3 years, 12 months ago
D - You can set Activity type to Detect malware in an email message
upvoted 2 times

MCSA11 4 years, 8 months ago
From the Exchange admin center, create an anti-malware policy.
upvoted 1 times

Question #3 *Topic 2*

You have a Microsoft 365 E5 subscription.
You plan to deploy Microsoft Defender for Cloud Apps.
You need to ensure that Microsoft Defender for Cloud Apps can differentiate between internal and external users.
What should you do?

A. From the Microsoft 365 admin center, configure the Org settings.

B. From the Microsoft 365 admin center, configure the default domain.

C. From the Microsoft Defender for Cloud Apps portal, add a list of managed domains.

D. From the Microsoft Defender for Cloud Apps portal, configure the Organization details.

Suggested Answer: *C*
Reference:
https://docs.microsoft.com/en-us/defender-cloud-apps/general-setup

Community vote distribution
C (100%)

Moderator Highly Voted 2 years, 3 months ago
Selected Answer: C
Correct answer.

"Make sure you add a list of your Managed domains to identify internal users. Adding managed domains is a crucial step. Defender for Cloud Apps uses the managed domains to determine which users are internal, external, and where files should and shouldn't be shared. This information is used for reports and alerts."

The link provided in the answers is right as well.
https://docs.microsoft.com/en-us/defender-cloud-apps/general-setup
upvoted 8 times

rrrr5r Highly Voted 2 years, 3 months ago
In Sep 16th 22's exam.
upvoted 5 times

Amir1909 Most Recent 11 months ago
D is correct
upvoted 1 times

GotDamnImIn 1 year, 8 months ago
Selected Answer: C
Correct, managed domains will marked as internal, the rest will be internal.
upvoted 2 times

sanz72 1 year, 10 months ago
The portal changed, the correct now is Microsoft 365 Defender - Settings - Cloud Apps - Organization Details - Managed Domains
upvoted 3 times

RenegadeOrange 2 years, 3 months ago
Ah but the tricky part is that "managed domains" is under the "Organizations details" section so both C and D are correct but I guess you have to choose the best answer, probably C...
upvoted 2 times

GotDamnImIn 1 year, 8 months ago
At this point then you should focus on the keyword "managed domains" and ignore the jitter.
upvoted 1 times

Question #4 *Topic 2*

You have a Microsoft Azure Active Directory (Azure AD) tenant.
The organization needs to sign up for Microsoft Store for Business. The solution must use the principle of least privilege.
Which role should you assign to the user?

A. Global administrator

B. Cloud application administrator

C. Application administrator

D. Service administrator

Suggested Answer: *A*
Reference:
https://docs.microsoft.com/en-us/microsoft-store/sign-up-microsoft-store-for-business

Community vote distribution
A (100%)

MomoLomo Highly Voted 3 years, 4 months ago
Least privilege > global admin :'D
upvoted 13 times

Prianishnikov Highly Voted 3 years, 9 months ago
A. Global administrator
upvoted 9 times

Contactfornitish Most Recent 2 years, 4 months ago
Selected Answer: A
Would be helpful if someone was reviewing and removing duplicate questions from examtopics
upvoted 5 times

NikPat3125 3 years, 5 months ago
came in exam 27.07.2021
upvoted 7 times

Question #5 *Topic 2*

Note: This question is part of a series of questions that present the same scenario. Each question in the series contains a unique solution that might meet the stated goals. Some question sets might have more than one correct solution, while others might not have a correct solution.
After you answer a question in this section, you will NOT be able to return to it. As a result, these questions will not appear in the review screen.
You have a Microsoft 365 subscription.
You discover that some external users accessed content on a Microsoft SharePoint site. You modify the SharePoint sharing policy to prevent sharing outside your organization.
You need to be notified if the SharePoint sharing policy is modified in the future.
Solution: From the SharePoint site, you create an alert.
Does this meet the goal?

A. Yes

B. No

Suggested Answer: *A*
From the Security & Compliance admin center, Alerts, you create a new alert policy.
Reference:
https://docs.microsoft.com/en-us/microsoft-365/compliance/alert-policies

Community vote distribution
B (100%)

diggity801 Highly Voted 4 years, 9 months ago
No idea why I linked that but the answer is B. You set an alert for the modification of a SharePoint policy from the Security and Compliance admin center.
upvoted 37 times

BialyFenek 4 years, 9 months ago
+1, all alerta are created in Security & Compliance, not Sharepoint admin center
upvoted 16 times

STFN2019 4 years, 4 months ago
exaclamento
upvoted 4 times

ZakS Highly Voted 4 years, 11 months ago
Correct ans should be A
upvoted 9 times

A365 4 years, 8 months ago
A is definitely not true. Alerts on SharePoint sites allow you to get notified about content changes (eg. new document has been uploaded, a list item changed, ...)
upvoted 23 times

NitishKarmakar 1 year, 3 months ago
Alerts policy has an Activity "Change a Sharing policy" This applies to SharePoint (An administrator changed a SharePoint sharing policy by using the Office 365 Admin center, SharePoint admin center, or SharePoint Online Management Shell. Any change to the settings in the sharing policy in your organization will be logged. The policy that was changed is identified in the ModifiedProperty field property when you export the search results.)
upvoted 1 times

NitishKarmakar Most Recent 1 year, 3 months ago
B. is the correct answer. Here is the following alert available in Defender.
Alerts> New Alert Policy where Alert > Activity is > Changed a sharing policy (An administrator changed a SharePoint sharing policy by using the Office 365 Admin center, SharePoint admin center, or SharePoint Online Management Shell. Any change to the settings in the sharing policy in your organization will be logged. The policy that was changed is identified in the ModifiedProperty field property when you export the search results.)

upvoted 1 times

MasterMans 1 year, 5 months ago

https://support.microsoft.com/en-us/office/manage-view-or-delete-sharepoint-alerts-99dfb19c-9a90-4a8c-aba1-aa8c8afb0de2

upvoted 1 times

Smeyer 1 year, 9 months ago

Selected Answer: B

Create an Alert Policy from the Security & Compliance center.

upvoted 6 times

RNG60FR 2 years ago

Selected Answer: B

Alert for external sharing should be configured in Security portal (Collab Alert Policy or it can be done Cloud App)

upvoted 2 times

Moderator 2 years, 3 months ago

Selected Answer: B

As explained beautifully by several people here already. B is correct.

upvoted 5 times

L33D 2 years, 6 months ago

Still valid, on exam Jun 25, 2022

upvoted 2 times

venwaik 2 years, 7 months ago

Selected Answer: B

Came on Exam 09-05-2022

upvoted 5 times

jkklim 3 years, 1 month ago

NO is correct. Go to SCC -create alert will do. (BTW if you try any categories, you can also see this notified if the SharePoint sharing policy appears in every category)

upvoted 2 times

Domza 3 years, 4 months ago

Here we go, we found the answer to previews question lol

upvoted 1 times

Domza 3 years, 4 months ago

NOT from SharePoint Site.

Its done from "Security & Compliance admin center". Key

upvoted 1 times

Jake1 3 years, 8 months ago

Create an Alert Policy from the Security & Compliance center.

upvoted 4 times

mkoprivnj 3 years, 11 months ago

No is correct!

upvoted 3 times

Mr01z0 4 years, 2 months ago

You need to be notified if the SharePoint sharing policy is modified in the future.

Solution: From the Security & Compliance admin center, you create a threat management policy.

Does this meet the goal?

No.

From the Office 365 Security & Compliance portal you create a "New Alert Policy" with the category "Thread management", you then select "Changed a sharing policy" in the "Activity is" pull down menu.

https://protection.office.com/alertpolicies

upvoted 5 times

AnoniMouse 3 years, 7 months ago

You are 100% right. I've just tested it
upvoted 1 times

Alvaroll 4 years, 2 months ago
Same as MS-100 Topic3-24 https://www.examtopics.com/exams/microsoft/ms-100/view/21/
upvoted 1 times

VTHAR 4 years, 3 months ago
Answer is B.NO

It doesn't meet the goal.
upvoted 1 times

diggity801 4 years, 9 months ago
https://docs.microsoft.com/en-us/microsoft-365/compliance/use-sharing-auditing?view=o365-worldwide
upvoted 1 times

Question #6 *Topic 2*

You have a Microsoft 365 subscription and an on-premises Active Directory domain named contoso.com. All client computers run Windows 10 Enterprise and are joined to the domain.
You need to enable Windows Defender Credential Guard on all the computers.
What should you do?

A. From the Microsoft 365 Defender, configure the DKIM signatures for the domain.

B. From a domain controller, create a Group Policy object (GPO) that enables the Restrict delegation of credentials to remote servers setting.

C. From the Security & Compliance admin center, create a device security policy.

D. From a domain controller, create a Group Policy object (GPO) that enabled the Turn On Virtualization Based Security setting.

Suggested Answer: *D*
Reference:
https://docs.microsoft.com/en-us/windows/security/identity-protection/credential-guard/credential-guard-manage

Community vote distribution
D (100%)

gxsh Highly Voted 3 years, 1 month ago
Correct.
upvoted 7 times

mackzone Highly Voted 2 years, 6 months ago
still valid as of 25/06/22
upvoted 5 times

ServerBrain Most Recent 2 years, 1 month ago
Selected Answer: D
100% correct
upvoted 2 times

Moderator 2 years, 3 months ago
Selected Answer: D
D is the correct answer. The provided link gives the explanation.
upvoted 3 times

ale2197 2 years, 6 months ago
Selected Answer: D
an early question confirm this (D)
upvoted 4 times

Question #7 *Topic 2*

Your company has a Microsoft 365 subscription that uses an Azure Active Directory (Azure AD) tenant named contoso.com.
The company purchases a cloud app named App1 that supports Microsoft Defender for Cloud Apps monitoring.
You configure App1 to be available from the My Apps portal.
You need to ensure that you can monitor App1 from Defender for Cloud Apps.
What should you do?

A. From the Azure Active Directory admin center, create a conditional access policy.

B. From the Azure Active Directory admin center, create an app registration.

C. From the Endpoint Management admin center, create an app protection policy.

D. From the Endpoint Management admin center, create an app configuration policy.

Suggested Answer: *A*

Community vote distribution

A (100%)

B0bacer Highly Voted 2 years, 2 months ago

Selected Answer: A

A. From the Azure Active Directory admin center, create a conditional access policy.

Microsoft Defender for Cloud Apps builds on Azure AD conditional access policies to enable real-time monitoring and control of granular actions with SaaS apps, such as blocking downloads, uploads, copy and paste, and printing.

https://learn.microsoft.com/en-us/microsoft-365/security/office-365-security/mcas-saas-access-policies?view=o365-worldwide

upvoted 9 times

Maroslaw Most Recent 1 year, 5 months ago

A is almost correct, it should be not "conditional access policy" but "conditional access app control"...

upvoted 1 times

RenegadeOrange 2 years, 3 months ago

A is correct.

>

First, in Azure AD, create a new conditional access policy and configure it to "Use Conditional Access App Control." This redirects the request to Defender for Cloud Apps. You can create one policy and add all SaaS apps to this policy.
Next, in Defender for Cloud Apps, create session policies. Create one policy for each control you want to apply.

>

https://learn.microsoft.com/en-us/microsoft-365/security/office-365-security/mcas-saas-access-policies?view=o365-worldwide

upvoted 4 times

Nevermore929 2 years, 3 months ago

It doesn't seem like conditional access would be the answer, but it is:
"To enable CASB in SaaS apps you must configure single sign-on (SSO) of the SaaS app with Defender for Cloud Apps or Azure AD. I recommend you use Azure AD because it is easier as many of you might use Azure AD for SSO already. To set up SSO with Azure AD, you must configure a conditional access policy to trigger session monitoring. Azure AD then passes the session to Defender for Cloud Apps instead of the SaaS app after authenticating the user. Using conditional access requires Azure AD Premium P1. "

upvoted 2 times

ajiejeng 2 years, 3 months ago

so its not inthe choices then?

upvoted 2 times

Question #8 *Topic 2*

HOTSPOT -

You use Microsoft Defender for Endpoint.

You have the Microsoft Defender for Endpoint machine groups shown in the following table.

Name	Rank	Members
Group1	1	Operating system in Windows 10
Group2	2	Name ends with London
Group3	3	Operating system in Windows Server 2016
Ungrouped machines (default)	Last	*Not applicable*

You plan to onboard computers to Microsoft Defender for Endpoint as shown in the following table.

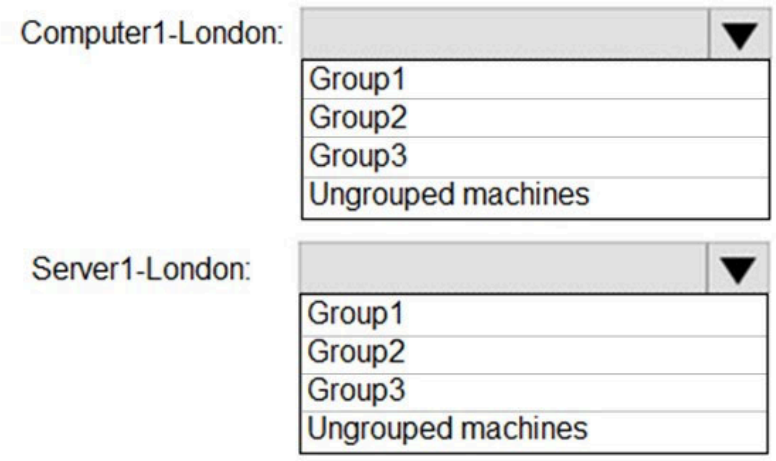
Name	Operating system
Computer1-London	Windows 10
Server1-London	Windows Server 2016

To which machine group will each computer be added? To answer, select the appropriate options in the answer are.

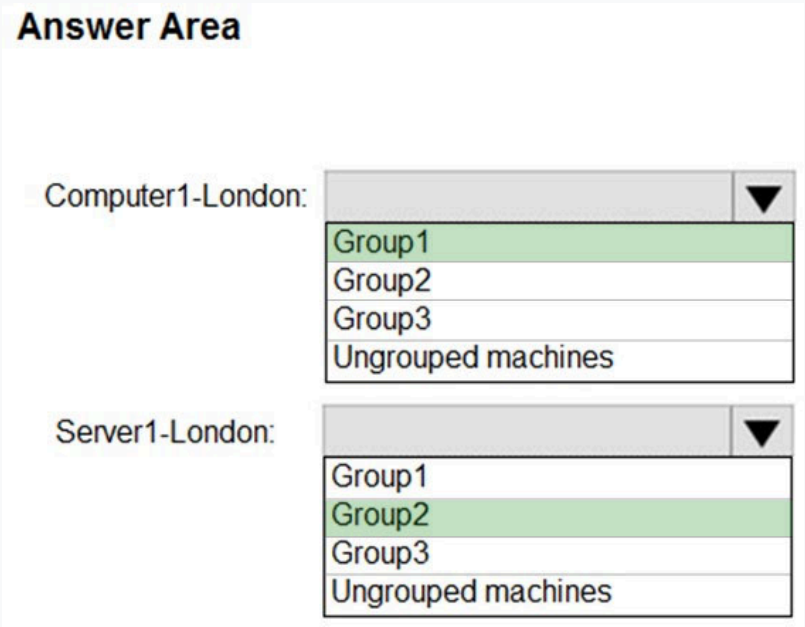
NOTE: Each correct selection is worth one point.

Hot Area:

Answer Area



Suggested Answer:



Amir1909 11 months ago

Correct

upvoted 1 times

Sanjee31 1 year, 6 months ago
in exam 28/6/2023
upvoted 2 times

GotDamnImIn 1 year, 8 months ago
Correct, highest rank determines the grouping.
upvoted 2 times

lchuyen08 2 years, 3 months ago
I think Group1 & Group 2
upvoted 4 times

rrrr5r 2 years, 3 months ago
In Sep 16th 22's exam.
upvoted 3 times

ajiejeng 2 years, 3 months ago
i think current answer is correct ,
upvoted 3 times

Moderator 2 years, 3 months ago
Computer1-London: Group 2
Server1-London: Group 3

The HIGHEST rank determines to which group the devices will be assigned.

https://jeffreyappel.nl/microsoft-defender-for-endpoint-series-configure-defender-for-endpoint-part2/

https://docs.microsoft.com/en-us/microsoft-365/security/defender-endpoint/machine-groups?view=o365-worldwide
upvoted 1 times

RenegadeOrange 2 years, 3 months ago
No.

The given answer is correct, about half way down the article from Microsoft "Moderator" has listed it says "A device group with a rank of 1 is the highest ranked group"
upvoted 4 times

Moderator 2 years, 2 months ago
You're right, I interpreted the ranking system wrong.
Rank 1 is the highest instead of the last number.

That means the answer given is correct after all.
upvoted 3 times

Moderator 2 years, 3 months ago
So imo the currently provided answer is wrong.
upvoted 1 times

extrankie 2 years, 5 months ago
i don't understand the question though
upvoted 1 times

Contactfornitish 2 years, 5 months ago
Groups stablished on dynamic rule and evaluated in order so first match is the group for device. Hope that explains
upvoted 5 times

Kawinho 2 years, 6 months ago
Correct
upvoted 3 times

Question #9 *Topic 2*

Your company has 5,000 Windows 10 devices. All the devices are protected by using Microsoft Defender Advanced Threat Protection (ATP).
You need to create a filtered view that displays which Microsoft Defender ATP alert events have a high severity and occurred during the last seven days.
What should you use in Microsoft Defender ATP?

A. the threat intelligence API

B. Automated investigations

C. Threat analytics

D. Advanced hunting

Suggested Answer: *B*
References:
https://docs.microsoft.com/en-us/windows/security/threat-protection/windows-defender-atp/investigate-alerts-windows-defender-advanced-threat-protection https://docs.microsoft.com/en-us/windows/security/threat-protection/windows-defender-atp/automated-investigations-windows-defender-advanced-threat- protection

Community vote distribution

D (100%)

arai002 Highly Voted 3 years, 5 months ago
The important thing is you need create fileter or not

Topic4 Question #29
ASK:You want to display Microsoft Defender ATP alert events
you don't need create filter*
ANS:B:Automated investigations

Topic2 Qutstion#8
ASK:You need to create a filtered view that displays which Microsoft Defender ATP alert
****you need create *****
ANS:D:Advanced hunting
Advanced hunting can create query and filter
For example:
DeviceAlertEvents
| where Severity == "high"
| where Timestamp > ago(7d)
upvoted 32 times

MiZi Highly Voted 3 years, 7 months ago
As I see, the answer should be D. Advanced Hunting. You can query anything there like in the Azure Log Analytics.
Automated Investigations can give the 7day (1 week) view, but do not show severity.
Please correct me if I am wrong here.
upvoted 24 times

encxorblood Most Recent 2 years ago
B - You need Automated investigations to see alerts
upvoted 1 times

[Removed] 2 years, 1 month ago
I'm going with Automated Investigation.

The link Exam Topics provides a video. Starting at the 2 minute mark, the video even mentions "filtering" days, computer names, etc. within the Automated Investigation app:

https://learn.microsoft.com/en-us/microsoft-365/security/defender-endpoint/automated-investigations?view=o365-worldwide

At 2:12 "...and of course, filter the list..."
upvoted 3 times

gmKK 2 years, 3 months ago
Likely outdated question since this view is available under alerts:
https://docs.microsoft.com/en-us/microsoft-365/security/defender-endpoint/alerts-queue?view=o365-worldwide
upvoted 4 times

RenegadeOrange 2 years, 3 months ago
Agree if its in the exam now one of the solutions will be the "Alerts" section which shows you that stuff by default and allows you to filter. Alternatively it's possible but much more work in Advanced Hunting.
upvoted 1 times

ijskoe 2 years, 5 months ago
Selected Answer: D
as per ms doc
upvoted 1 times

ale2197 2 years, 6 months ago
Selected Answer: D
as other user are telling... D
upvoted 2 times

DARKK 2 years, 8 months ago
Selected Answer: D
D advanced Hunting
upvoted 3 times

JamesM9 2 years, 9 months ago
The answer is B – Automated Investigations, as per the link below (last updated March 25, 2022)

https://docs.microsoft.com/en-us/microsoft-365/security/defender-endpoint/alerts-queue?view=o365-worldwide
upvoted 5 times

ScottT 2 years, 9 months ago
2 mins in to video in https://docs.microsoft.com/en-us/microsoft-365/security/defender-endpoint/automated-investigations?view=o365-worldwide has the answer. The answer is B
upvoted 1 times

TashaGirl 2 years, 10 months ago
There is no correct answer here. Updated docs: https://docs.microsoft.com/en-us/microsoft-365/security/defender-endpoint/alerts-queue?view=o365-worldwide
upvoted 1 times

LillyLiver 2 years, 10 months ago
This is a tough one, and I think that the question answers are out of date. Automated Investigations doesn't seem to be an option in the admin portal anymore (as of 2/20/2022).

I'm going with D. Advanced Hunting.
upvoted 1 times

larnyx 3 years, 4 months ago
Should most surely be, D.

Advanced hunting allows you to create a query that proccesses 30 days of raw data and outputs the info asked for.

Automated investigations handles itself by starting a scan once alerted and remidiates the issue at hand.
upvoted 3 times

gkp_br 3 years, 5 months ago
"D. Advanced hunting". I cant find that filter in Automated investigations blade.
upvoted 3 times

arai002 3 years, 6 months ago

D: Advanced hunting

Question sed "You need to create"
Automated investigations can only filter

Advanced hunting can create query and filter
For example:
DeviceAlertEvents
| where Severity == "high"
| where Timestamp > ago(7d)

That's why Correct Answer : D
upvoted 7 times

LoremanReturns 3 years, 5 months ago
I agree. Automated investigation is used to automate response to specific detection. The answer asks to report specific detections that can be achieved with Advanced Hunting
upvoted 3 times

Pawnzy 3 years, 6 months ago
I think B. Automated investigations is correct because it is asking for a filtered view from something like the Alert Queue rather than creating a query to look for the data then filter
upvoted 3 times

Jake1 3 years, 8 months ago
Automated Investigations is correct. https://docs.microsoft.com/en-us/microsoft-365/security/defender-endpoint/automated-investigations?view=o365-worldwide.
upvoted 1 times

Question #10 *Topic 2*

Note: This question is part of a series of questions that present the same scenario. Each question in the series contains a unique solution that might meet the stated goals. Some question sets might have more than one correct solution, while others might not have a correct solution.
After you answer a question in this section, you will NOT be able to return to it. As a result, these questions will not appear in the review screen.
You have a Microsoft 365 subscription.
You need to prevent users from accessing your Microsoft SharePoint Online sites unless the users are connected to your on-premises network.
Solution: From the Device Management admin center, you create a device configuration profile.
Does this meet the goal?

A. Yes

B. No

Suggested Answer: *B*

Community vote distribution

B (100%)

Jake1 Highly Voted 3 years, 8 months ago

B, No is correct. You need to set up a CA Policy with whitelisted IP addresses to allow access.

upvoted 11 times

atha Most Recent 2 years, 11 months ago

Selected Answer: B

Correct

upvoted 3 times

Goena 3 years ago

No so B.
The other questions are 48 and 60. All are NO.
Create Conditional Access in AD. Conditions: trusted location.

upvoted 3 times

Question #11 *Topic 2*

Note: This question is part of a series of questions that present the same scenario. Each question in the series contains a unique solution that might meet the stated goals. Some question sets might have more than one correct solution, while others might not have a correct solution.
After you answer a question in this section, you will NOT be able to return to it. As a result, these questions will not appear in the review screen.
You have an Azure Active Directory (Azure AD) tenant that contains a user named User1.
Your company purchases a Microsoft 365 subscription.
You need to ensure that User1 is assigned the required role to create file policies and manage alerts in the Defender for Cloud Apps admin center.
Solution: From the Security & Compliance admin center, you assign the Security Administrator role to User1.
Does this meet the goal?

A. Yes

B. No

Suggested Answer: *B*
Security Administrator has the required permissions, but it is not assigned from the Security and Compliance Center.
Reference:
https://docs.microsoft.com/en-us/cloud-app-security/manage-admins

Community vote distribution
B (64%) A (36%)

RenegadeOrange Highly Voted 2 years, 3 months ago
Correct, the in the Security Portal (now M365 Defender) you can view role members but there is a link to the Azure portal to manage role assignments.
Alternatively you can do it in the admin center and exchange admin center.
upvoted 5 times

itsme12p Most Recent 1 year, 5 months ago
Selected Answer: B
B, needs to be done from azure portal
upvoted 1 times

Wired7693 1 year, 6 months ago
Selected Answer: B
You can create custom roles within the Defender portal.
The Defender portal lets you view who is assigned Azure AD roles, but links you through to Azure AD to actually manage membership.
upvoted 3 times

salashow_ 1 year, 7 months ago
Selected Answer: A
Yes we can
upvoted 2 times

Sucxi 1 year, 7 months ago
Selected Answer: A
Yes, you can assign from the Defender portal
https://learn.microsoft.com/en-us/microsoft-365/security/defender-business/mdb-roles-permissions?view=o365-worldwide
upvoted 2 times

Question #12 *Topic 2*

Note: This question is part of a series of questions that present the same scenario. Each question in the series contains a unique solution that might meet the stated goals. Some question sets might have more than one correct solution, while others might not have a correct solution.
After you answer a question in this section, you will NOT be able to return to it. As a result, these questions will not appear in the review screen.
You have an Azure Active Directory (Azure AD) tenant that contains a user named User1.
Your company purchases a Microsoft 365 subscription.
You need to ensure that User1 is assigned the required role to create file policies and manage alerts in the Defender for Cloud Apps admin center.
Solution: From the Azure Active Directory admin center, you assign the Security administrator role to User1.
Does this meet the goal?

A. Yes

B. No

Suggested Answer: *A*
The Security administrator has Full access with full permissions in Defender for Cloud Apps.
Reference:
https://docs.microsoft.com/en-us/cloud-app-security/manage-admins

Community vote distribution
A (100%)

Moderator 2 years, 3 months ago

Selected Answer: A
Correct, Korrekt, Corriger, Corretto.
upvoted 4 times

Question #13 *Topic 2*

Note: This question is part of a series of questions that present the same scenario. Each question in the series contains a unique solution that might meet the stated goals. Some question sets might have more than one correct solution, while others might not have a correct solution.
After you answer a question in this section, you will NOT be able to return to it. As a result, these questions will not appear in the review screen.
You have an Azure Active Directory (Azure AD) tenant that contains a user named User1.
Your company purchases a Microsoft 365 subscription.
You need to ensure that User1 is assigned the required role to create file policies and manage alerts in the Defender for Cloud Apps admin center.
Solution: From the Azure Active Directory admin center, you assign the Compliance administrator role to User1.
Does this meet the goal?

A. Yes

B. No

Suggested Answer: *A*
The Compliance administrator has read-only permissions and can manage alerts, can create and modify file policies, allow file governance actions, and view all the built-in reports under Data Management, but cannot access Security recommendations for cloud platforms.
Reference:
https://docs.microsoft.com/en-us/cloud-app-security/manage-admins

Community vote distribution

Moderator Highly Voted 2 years, 3 months ago

Selected Answer: A

Seems correct.

Compliance administrator: Has read-only permissions and can manage alerts. Can't access Security recommendations for cloud platforms. Can create and modify file policies, allow file governance actions, and view all the built-in reports under Data Management.

Link provided is sufficient to answer this question.

upvoted 10 times

HOTSPOT -

Your company purchases a cloud app named App1.

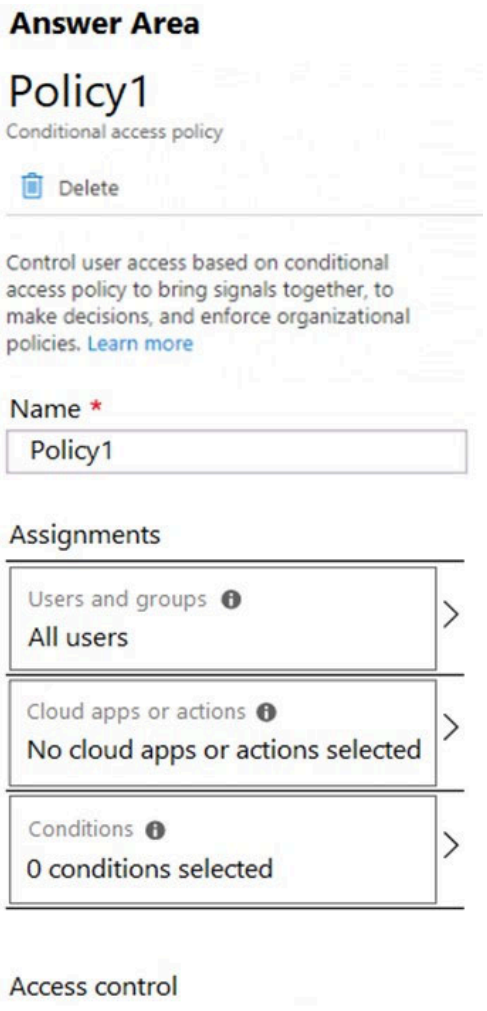
You plan to publish App1 by using a conditional access policy named Policy1.

You need to ensure that you can control access to App1 by using a Microsoft Cloud App Security session policy.

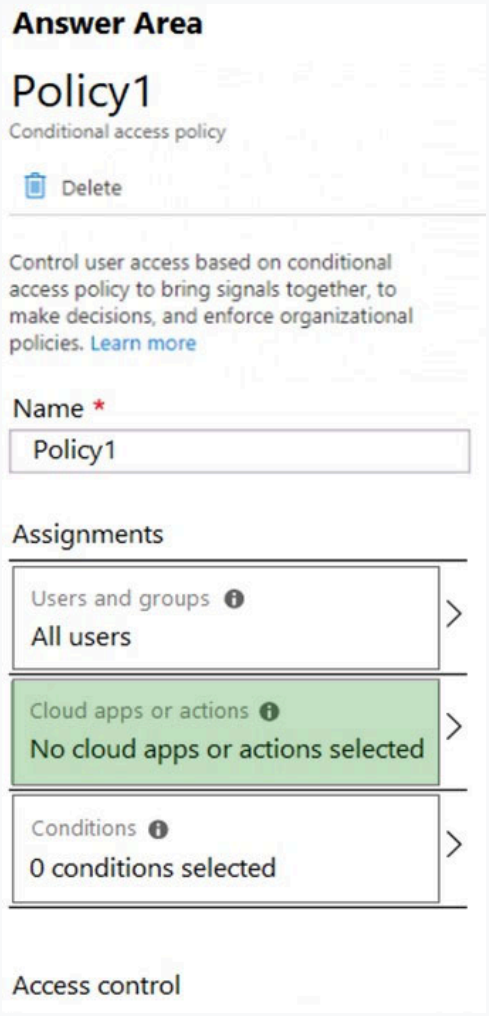
Which two settings should you modify in Policy1? To answer, select the appropriate settings in the answer area.

NOTE: Each correct selection is worth one point.

Hot Area:



Suggested Answer:



Reference:
https://docs.microsoft.com/en-us/cloud-app-security/proxy-deployment-aad

TimurKazan Highly Voted 3 years ago
I would choose "Cloud Apps and Actions " and "Session" to enable Cloud App Access Control. But that is not listed there..
upvoted 13 times

- **TimurKazan** 3 years ago
  I meant Conditional Access App Control
  upvoted 2 times

Glorence Highly Voted 2 years, 11 months ago
still valid, it was in my exam last Feb 5, 2022
upvoted 9 times

Kaloy Most Recent 1 year, 10 months ago
https://www.examtopics.com/discussions/microsoft/view/54363-exam-ms-101-topic-2-question-13-discussion/
upvoted 4 times

JAPo123 3 years ago
2 settings is --> session
upvoted 6 times

B1G_B3N 3 years ago
which 2 settings?? only 1 selected for this answer??
upvoted 4 times

- **True** 3 years ago
  2nd setting: Access controls and select sessions
  upvoted 5 times

- **True** 3 years ago
  Hey bro , see the full diagram and answer here. Hope that helps
  https://www.examtopics.com/discussions/microsoft/view/54363-exam-ms-101-topic-2-question-13-discussion/

upvoted 39 times

Question #15 *Topic 2*

HOTSPOT -

Your company uses Microsoft Defender Advanced Threat Protection (ATP). Microsoft Defender ATP includes the machine groups shown in the following table.

Rank	Machine group	Members
1	Group1	Tag Equals demo And OS In Windows 10
2	Group2	Tag Equals demo
3	Group3	Domain Equals adatum.com
4	Group4	Domain Equals adatum.com And OS In Windows 10
Last	Ungrouped machines (default)	*Not applicable*

You onboard a computer named computer1 to Microsoft Defender ATP as shown in the following exhibit.

Use the drop-down menus to select the answer choice that completes each statement.

NOTE: Each correct selection is worth one point.

Hot Area:

Answer Area

Computer1 will be a member of [**answer choice**].
- Group3 only
- Group4 only
- Group3 and Group4 only
- Ungrouped machines

If you add the tag demo to Computer1, the computer will be a member of [**answer choice**].
- Group1 only
- Group1 and Group2 only
- Group1, Group2, Group3, and Group4
- Ungrouped machines

Suggested Answer:

Answer Area

Computer1 will be a member of [**answer choice**].
- Group3 only
- Group4 only
- **Group3 and Group4 only**
- Ungrouped machines

If you add the tag demo to Computer1, the computer will be a member of [**answer choice**].
- Group1 only
- Group1 and Group2 only
- **Group1, Group2, Group3, and Group4**
- Ungrouped machines

Prianishnikov Highly Voted 3 years, 9 months ago

Computer 1 will be a member of: Group 3 only If you add the tag demo to Computer1, the computer will be a member of: Group 1 only
upvoted 90 times

PP39 3 years, 9 months ago
Agree. Group 3 , Group 1
Higher rank wins
upvoted 24 times

GeraldB 3 years, 9 months ago
so the correct answer is: Group 3 only, Group 3 and Group 1, right?
upvoted 5 times

GeraldB 3 years, 9 months ago
Sorry i meant: Group 3 and Group 1
upvoted 14 times

jjong 3 years, 4 months ago
this is based on - You can promote or demote the rank of a device group so that it's given higher or lower priority during matching. When a device is matched to more than one group, it's added only to the highest ranked group.

https://docs.microsoft.com/en-us/microsoft-365/security/defender-endpoint/machine-groups?view=o365-worldwide#manage-device-groups
upvoted 15 times

barleyhutcher Highly Voted 3 years, 8 months ago
Answer is 3 and 1

When a device is matched to more than one group, it is added only to the highest ranked group. You can also edit and delete groups.

https://docs.microsoft.com/en-us/microsoft-365/security/defender-endpoint/machine-groups?view=o365-worldwide
upvoted 20 times

GotDamnImIn Most Recent 1 year, 8 months ago
I'm going with Group3 and Group1
upvoted 2 times

RiTh73 1 year, 10 months ago
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.

https://learn.microsoft.com/en-us/microsoft-365/security/defender-endpoint/machine-groups#:~:text=You%20can%20promote,and%20delete%20groups.
upvoted 1 times

Lelek 1 year, 10 months ago
I disagree with the answer.

I understand that when Microsoft Defender ATP applies the policy, it applies it to the group with the highest rank. Even to complement the name of Microsoft Defender ATP changed to Microsoft Defender for Endpoint

https://docs.microsoft.com/en-us/microsoft-365/security/defender-endpoint/machine-groups?view=o365-worldwide

But if you look at the question, that's not it. "Computer1 will be a member of", that is, he wants to know from the computer's configuration which group it will be inserted into, in this case the device's dynamic group will be a member, so the answer would be "Group3 and Group4 only". At no point does it ask which policy it will apply for Microsoft Defender ATP.

The same thing when he asks "If you add the tag demo to computer1, the computer will be a member of", that is, again he asks about group members and not what policy will apply in ATP, so the answer would be " Group1, Group2, Group3, and Group4"

Final anwser
1 - Group3 and Group4 only
2 - Group1, Group2, Group3, and Group4

upvoted 3 times

shannon_c0le1 1 year, 6 months ago
I agree, it states which groups computer1 will be a member of and not which policy applies.
upvoted 1 times

Contactfornitish 2 years, 4 months ago
On exam on 13 aug'22
upvoted 2 times

JamesM9 2 years, 9 months ago
"If a device is also matched to other groups, it's added only to the highest ranked device group".

https://docs.microsoft.com/en-us/microsoft-365/security/defender-endpoint/machine-groups?view=o365-worldwide

As a result of this, the answers are Group3 only and Group1 only.
upvoted 3 times

techtest848 3 years ago
Can somone please explain why Computer1 is not matched to Group1 based on the OS (Windows 10)
upvoted 1 times

B1G_B3N 3 years ago
its an AND statement so it must match both conditions - it has no demo tag
upvoted 2 times

techtest848 3 years ago
Thanks B1G_B3N :)
upvoted 1 times

ccadenasa 3 years, 2 months ago
Group 3 and group 1. Someone needs to correct this answer please.
upvoted 3 times

[Removed] 3 years, 2 months ago
Admin, please correct the answer, the correct answer is Group 3 , Group 1
upvoted 3 times

supaman 3 years, 3 months ago
Group 3, Group 1.
Only the highest ranked group will be added.
upvoted 3 times

zakyntos 3 years, 5 months ago
higher rank wins
https://docs.microsoft.com/en-us/microsoft-365/security/defender-endpoint/machine-groups?view=o365-worldwide

To be checked if "WINDOWS 10" filter will cover machine os: "WINDOWS 10 x64" :)
upvoted 5 times

MrDre 3 years, 5 months ago
Answer should be group 3 and group one.
Highest ranked group gets priority.
upvoted 2 times

baseng 3 years, 8 months ago
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.
https://docs.microsoft.com/en-us/microsoft-365/security/defender-endpoint/machine-groups?view=o365-worldwide
Group 3 and group 1 per that article
upvoted 3 times

init2winit 3 years, 8 months ago
Answer should be Group 3 , Group 1
Higher rank wins
upvoted 8 times

Jake1 3 years, 8 months ago

You can only be a member of one group and the highest rank wins (Lowest number).

upvoted 6 times

Question #16 *Topic 2*

HOTSPOT -

You have a Microsoft 365 subscription.

You are planning a threat management solution for your organization.

You need to minimize the likelihood that users will be affected by the following threats:

✑ Opening files in Microsoft SharePoint that contain malicious content

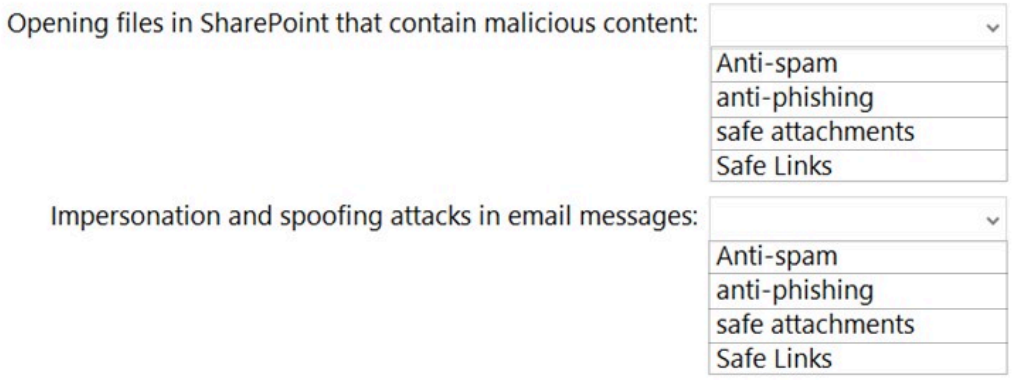
✑ Impersonation and spoofing attacks in email messages

Which policies should you create in the Microsoft 365 Defender? To answer, select the appropriate options in the answer area.

NOTE: Each correct selection is worth one point.

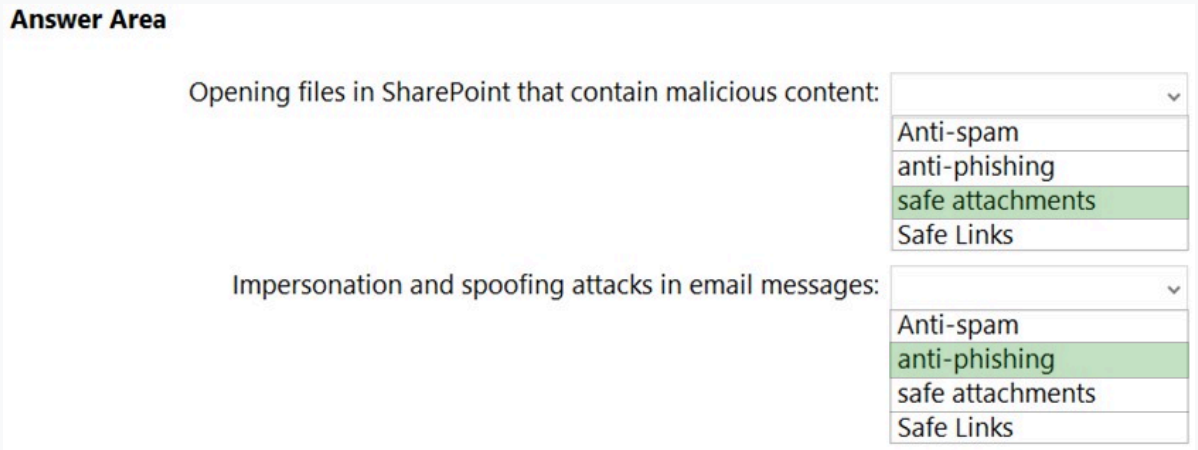
Hot Area:

Answer Area



Suggested Answer:

Answer Area



Box 1: ATP Safe Attachments -

ATP Safe Attachments provides zero-day protection to safeguard your messaging system, by checking email attachments for malicious content. It routes all messages and attachments that do not have a virus/malware signature to a special environment, and then uses machine learning and analysis techniques to detect malicious intent. If no suspicious activity is found, the message is forwarded to the mailbox.

Box 2: ATP anti-phishing -

ATP anti-phishing protection detects attempts to impersonate your users and custom domains. It applies machine learning models and advanced impersonation- detection algorithms to avert phishing attacks.

ATP Safe Links provides time-of-click verification of URLs, for example, in emails messages and Office files. Protection is ongoing and applies across your messaging and Office environment. Links are scanned for each click: safe links remain accessible and malicious links are dynamically blocked.

References:

https://docs.microsoft.com/en-us/microsoft-365/security/office-365-security/office-365-atp#configure-atp-policies

BoxGhost Highly Voted 2 years, 7 months ago

Answers are correct, but explanation for box one is wrong. It should be:

https://docs.microsoft.com/en-us/microsoft-365/security/office-365-security/turn-on-mdo-for-spo-odb-and-teams?view=o365-worldwide

upvoted 11 times

H3adcap Highly Voted 2 years, 4 months ago

Was in exam today 20 Aug 2022

upvoted 6 times

Madskillz13 Most Recent 2 years, 4 months ago

Same here, question featured in exam August 2022

upvoted 3 times

venwaik 2 years, 7 months ago

Answers are correct. Came on exam 09-05-2022

upvoted 5 times

Question #17 *Topic 2*

You have a Microsoft 365 subscription.
All users have their email stored in Microsoft Exchange Online.
In the mailbox of a user named User1, you need to preserve a copy of all the email messages that contain the word ProjectX.
What should you do first?

A. From Microsoft Defender for Cloud Apps, create an access policy.

B. From the Security & Compliance admin center, create an eDiscovery case.

C. From Microsoft Defender for Cloud Apps, create an activity policy.

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

Suggested Answer: *D*
A DLP policy contains a few basic things:
Where to protect the content: locations such as Exchange Online, SharePoint Online, and OneDrive for Business sites, as well as Microsoft Teams chat and channel messages.
When and how to protect the content by enforcing rules comprised of:
Conditions the content must match before the rule is enforced. For example, a rule might be configured to look only for content containing Social Security numbers that's been shared with people outside your organization.
Actions that you want the rule to take automatically when content matching the conditions is found. For example, a rule might be configured to block access to a document and send both the user and compliance officer an email notification.
References:
https://docs.microsoft.com/en-us/microsoft-365/compliance/data-loss-prevention-policies

Community vote distribution
B (100%)

mackypatio Highly Voted 2 years, 3 months ago
I do this a lot. It is B.
upvoted 15 times

Moderator Highly Voted 2 years, 3 months ago
Selected Answer: B
B is correct.

Microsoft Purview --> Create a Case --> Hold --> Create new Hold
upvoted 7 times

Fala_Fel 1 year, 11 months ago
Yep Jan2023 eDiscovery is in Purview. Who knows where it will be next month ;)
Purview > Solutions > eDiscovery > Standard > Create a Case .....
upvoted 3 times

athadd Most Recent 1 year, 11 months ago
Selected Answer: B
https://docs.microsoft.com/en-us/microsoft-365/compliance/create-ediscovery-holds?source=recommendations&view=o365-worldwide
upvoted 1 times

sajlen1414 2 years ago
Selected Answer: B
DLP prevents leaks (like send date of birth via e-mail)
eDiscovery finds and preserves content for a court (or otherwise) case. User can delete message, but it will be still available to admin.
upvoted 6 times

Krystian 2 years, 1 month ago
Selected Answer: B
IMO answer is B
upvoted 1 times

Fefe_ES 2 years, 3 months ago

Selected Answer: B

B answer

upvoted 3 times

FumerLaMoquette 2 years, 3 months ago

Selected Answer: B

Lol b.

upvoted 4 times

gmKK 2 years, 3 months ago

Selected Answer: B

https://docs.microsoft.com/en-us/microsoft-365/compliance/create-ediscovery-holds?source=recommendations&view=o365-worldwide

upvoted 5 times

RenegadeOrange 2 years, 3 months ago

Agree it is B, query-based hold in e-discovery. There are no retention or hold options for DLP.

upvoted 3 times

ahmadalh 2 years, 4 months ago

i think the answer is b

upvoted 2 times

derSchweiger 2 years, 4 months ago

Shouldn't be it B?

upvoted 3 times

A_Blameless_Child 2 years, 4 months ago

Yes, I believe so. Can't find anything about retention for items

https://docs.microsoft.com/en-us/microsoft-365/compliance/dlp-conditions-and-exceptions?view=o365-worldwide#actions-for-dlp-policies

upvoted 2 times

Question #18 *Topic 2*

You have a Microsoft 365 subscription.
From the subscription, you perform an audit log search, and you download all the results.
You plan to review the audit log data by using Microsoft Excel.
You need to ensure that each audited property appears in a separate Excel column.
What should you do first?

A. From Power Query Editor, transform the JSON data.

B. Format the Operations column by using conditional formatting.

C. Format the AuditData column by using conditional formatting.

D. From Power Query Editor, transform the XML data.

Suggested Answer: *A*
After you search the Office 365 audit log and download the search results to a CSV file, the file contains a column named AuditData, which contains additional information about each event. The data in this column is formatted as a JSON object, which contains multiple properties that are configured as property:value pairs separated by commas. You can use the JSON transform feature in the Power Query Editor in Excel to split each property in the JSON object in the
AuditData column into multiple columns so that each property has its own column. This lets you sort and filter on one or more of these properties
References:
https://docs.microsoft.com/en-us/microsoft-365/compliance/export-view-audit-log-records

Community vote distribution
A (100%)

potpal Highly Voted 3 years, 7 months ago
On test 05.10.21
upvoted 44 times

joyyyyyyyyyyyy 3 years, 6 months ago
so what?
upvoted 2 times

otday 3 years, 6 months ago
Are you dumb? They are letting us know its still relevant
upvoted 88 times

Durden871 2 years, 5 months ago
They are, in fact, a thief of joy.
upvoted 4 times

rrrr5r 2 years, 3 months ago
In Sep 16th 22's exam.
upvoted 6 times

LeeM84 Highly Voted 4 years, 7 months ago
You can use the JSON transform feature in Power Query in Excel to split the AuditData column into multiple columns so that each property has its own column. This lets you sort and filter on one or more of these properties
https://docs.microsoft.com/en-us/microsoft-365/compliance/detailed-properties-in-the-office-365-audit-log?view=o365-worldwide
upvoted 23 times

GotDamnImIn Most Recent 1 year, 8 months ago
Selected Answer: A
Was in exam in March 2023
upvoted 1 times

Lelek 1 year, 10 months ago
Selected Answer: A
Answer A is correct

upvoted 1 times

denmaillbox 2 years, 5 months ago

A! https://docs.microsoft.com/en-us/microsoft-365/compliance/export-view-audit-log-records?view=o365-worldwide

upvoted 1 times

junior6995 2 years, 11 months ago

This is the type of question that I'd have gotten wrong if wasn't for examtopics

upvoted 7 times

Durden871 2 years, 5 months ago

I don't even understand the purpose of this question. How relevant is this to the reset of the MS-101? It's so out in left field that it seems like it's purposefully trying to lower your score.

upvoted 2 times

Contactfornitish 2 years, 5 months ago

Not really. Actually a perfectly valid one for practical reasons.

Most details in audit log come into securitydata column and that is in json format. If using powershell then we use convert-fromJSON and if downloading from portal then we need to use power query.

Knowing this makes life easier

upvoted 2 times

Contactfornitish 2 years, 5 months ago

Auditdata column i meant

upvoted 1 times

junior6995 3 years, 1 month ago

Sometimes I don't understand why questions like this one are part of this exam....

upvoted 7 times

us3r 3 years ago

so that dumps have actually a meaning... and they sell them...

upvoted 3 times

Question #19 *Topic 2*

You have a Microsoft 365 subscription.
You need to be notified if users receive email containing a file that has a virus.
What should you do?

A. From the Exchange admin center, create a spam filter policy.

B. From the Security & Compliance admin center, create a data governance event.

C. From the Security & Compliance admin center, create an alert policy.

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

Suggested Answer: *C*
You can create alert policies to track malware activity and data loss incidents. We've also included several default alert policies that help you monitor activities such as assigning admin privileges in Exchange Online, malware attacks, phishing campaigns, and unusual levels of file deletions and external sharing.
The Email messages containing malware removed after delivery default alert generates an alert when any messages containing malware are delivered to mailboxes in your organization.
Incorrect answers:
A: A spam filter policy includes selecting the action to take on messages that are identified as spam. Spam filter policy settings are applied to inbound messages.
B: A data governance event commences when an administrator creates it, following which background processes look for content relating to the event and take the retention action defined in the label. The retention action can be to keep or remove items, or to mark them for manual disposition.
D: You can inspect email attachments in your Exchange Online organization by setting up mail flow rules. Exchange Online offers mail flow rules that provide the ability to examine email attachments as a part of your messaging security and compliance needs. However, mail flow rules are not used to detect malware in emails.
Reference:
https://docs.microsoft.com/en-us/office365/securitycompliance/alert-policies

Community vote distribution
C (100%)

Prianishnikov Highly Voted 3 years, 9 months ago
C. From the Security & Compliance admin center, create an alert policy.
upvoted 15 times

Jake1 Highly Voted 3 years, 8 months ago
You can create an alert for infected email messages sent to users in your organization via the S&C Admin center. Answer is correct.
upvoted 5 times

Fala_Fel Most Recent 1 year, 11 months ago
Selected Answer: C
But now (Jan 2023) in 365 Defender > Email & Collaboration > Policies & Rules > Alert Policy....
I suppose in the exam look for 'alert policy'
I
upvoted 1 times

F_M 3 years, 4 months ago
Answer is correct! If you're trying to replicate this on your tenant, you must have Microsoft Defender for Office365 enabled! Otherwise you won't see the related activity in the list to create the alert.
upvoted 4 times

Question #20 *Topic 2*

DRAG DROP -

You have the Microsoft Azure Advanced Threat Protection (ATP) workspace shown in the Workspace exhibit. (Click the Workspace tab.)

Workspace

Manage Azure ATP user roles

Create Workspace

NAME	TYPE	INTEGRATION	GEOLOCATION
testwrkspace	Primary	Windows Defender ATP	Europe

The sensors settings for the workspace are configured as shown in the Sensors exhibit. (Click the Sensors tab.)

Sensors

Configure Directory Services to install the first Sensor or Standalone Sensor.

NAME	TYPE	DOMAIN CO...	VERSION	SERVICE STATUS	HEALTH
No Sensors registered					

You need to ensure that Azure ATP stores data in Asia.

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

Select and Place:

Actions	Answer Area
Modify the integration setting for the workspace.	
Delete the workspace.	
Regenerate the access keys.	
Create a new workspace.	
Modify the Azure ATP user roles.	

Suggested Answer:

Actions	Answer Area
Modify the integration setting for the workspace.	Delete the workspace.
Delete the workspace.	Create a new workspace.
Regenerate the access keys.	Regenerate the access keys.
Create a new workspace.	
Modify the Azure ATP user roles.	

AnoniMouse Highly Voted 3 years, 7 months ago

The answer is correct. Even more, if you have onboarded computers, you first have to offboard them first!

upvoted 20 times

lucidgreen Highly Voted 3 years, 6 months ago

If you have a workspace for another site, you have to delete it first and create a new one. Regenerate access keys just seems like a logical next step to me.

upvoted 11 times

GotDamnImIn Most Recent 1 year, 8 months ago

Correct

upvoted 1 times

Question #21 *Topic 2*

Your company has five security information and event management (SIEM) appliances. The traffic logs from each appliance are saved to a file share named Logs.
You need to analyze the traffic logs.
What should you do from Microsoft Defender for Cloud Apps?

A. Click Investigate, and then click Activity log.

B. Click Control, and then click Policies. Create a file policy.

C. Click Discover, and then click Create snapshot report.

D. Click Investigate, and then click Files.

Suggested Answer: *C*
Reference:
https://docs.microsoft.com/en-us/cloud-app-security/create-snapshot-cloud-discovery-reports

Community vote distribution
C (100%)

NitishKarmakar 1 year, 3 months ago
C is the correct option. From Cloud Discovery click Create New Report.
upvoted 1 times

Sucxi 1 year, 7 months ago
Selected Answer: C
I think C is correct.
https://learn.microsoft.com/en-us/defender-cloud-apps/set-up-cloud-discovery#snapshot-and-continuous-risk-assessment-reports
upvoted 1 times

Moderator 2 years, 3 months ago
Selected Answer: C
Answer is correct :)
upvoted 4 times

Question #22 *Topic 2*

Note: This question is part of a series of questions that present the same scenario. Each question in the series contains a unique solution that might meet the stated goals. Some question sets might have more than one correct solution, while others might not have a correct solution.
After you answer a question in this section, you will NOT be able to return to it. As a result, these questions will not appear in the review screen.
You have an Azure Active Directory (Azure AD) tenant that contains a user named User1.
Your company purchases a Microsoft 365 subscription.
You need to ensure that User1 is assigned the required role to create file policies and manage alerts in the Defender for Cloud Apps admin center.
Solution: From the Defender for Cloud Apps admin center, you assign the App/instance admin role for all Microsoft Online Services to User1.
Does this meet the goal?

A. Yes

B. No

Suggested Answer: *B*
App/instance admin: Has full or read-only permissions to all of the data in Microsoft Defender for Cloud Apps that deals exclusively with the specific app or instance of an app selected.
Reference:
https://docs.microsoft.com/en-us/cloud-app-security/manage-admins

RenegadeOrange Highly Voted 2 years, 3 months ago
Technically yes that role is able to create policies and manage alerts but onlyl for a specific app, the question does not specify that is has to be for all apps so you could say yes, hopefully the actual exam question has more details.
Compliance Data Administrator would be the lowest role that can create policies and manage alerts. (then Compliance Administrator and Security Administrator)
upvoted 5 times

EsamiTopici 1 year, 11 months ago
The question doesn't specify the app, so no
upvoted 1 times

Ninagalilea Most Recent 2 years, 3 months ago
Antwort: A
upvoted 2 times

Question #23 *Topic 2*

Your company has a Microsoft 365 subscription that uses an Azure Active Directory (Azure AD) tenant named contoso.com.
The tenant is configured to use Azure AD Identity Protection.
You plan to use an application named App1 that creates reports of Azure AD Identity Protection usage.
You register App1 in the tenant.
You need to ensure that App1 can read the risk event information of contoso.com.
To which API should you delegate permissions?

A. Windows Azure Service Management API

B. Windows Azure Active Directory

C. Microsoft Graph

D. Office 365 Management

Suggested Answer: *C*
Reference:
https://docs.microsoft.com/en-us/graph/api/resources/identityprotection-root?view=graph-rest-beta

Community vote distribution
C (100%)

PattiD Highly Voted 4 years ago
C. Microsoft Graph API
upvoted 12 times

us3r Highly Voted 3 years ago
Selected Answer: C
GRAPH
!
upvoted 9 times

chewitt Most Recent 1 year, 12 months ago
Azure Active Directory (Azure AD) Graph is deprecated and will be retired at any time after June 30, 2023, without advance notice, as we announced in September, 2022.
upvoted 3 times

psycho202 1 year, 7 months ago
Azure AD Graph is deprecated and replaced by ... Microsoft Graph.
upvoted 4 times

ServerBrain 2 years, 1 month ago
Selected Answer: C
100% correct
upvoted 2 times

MJQ1 2 years, 12 months ago
Selected Answer: C
correct.
upvoted 4 times

Prianishnikov 3 years, 9 months ago
C. Microsoft Graph
upvoted 6 times

Question #24 *Topic 2*

Your company has a Microsoft 365 subscription that uses an Azure Active Directory (Azure AD) tenant named contoso.com. The tenant contains computers that run Windows 10 Enterprise and are managed by using Microsoft Endpoint Manager. The computers are configured as shown in the following table.

Name	CPU	Cores	RAM	TPM
Computer1	64-bit	2	12 GB	Enabled
Computer2	64-bit	4	12 GB	Enabled
Computer3	64-bit	8	16 GB	Disabled
Computer4	32-bit	4	4 GB	Disabled

You plan to implement Windows Defender Application Guard for contoso.com.
You need to identify on which two Windows 10 computers Windows Defender Application Guard can be installed.
Which two computers should you identify? Each correct answer presents part of the solution.
NOTE: Each correct selection is worth one point.

A. Computer1

B. Computer3

C. Computer2

D. Computer4

Suggested Answer: *BC*
Reference:
https://docs.microsoft.com/en-us/windows/security/threat-protection/windows-defender-application-guard/reqs-wd-app-guard

Community vote distribution
BC (100%)

BenniBenassi Highly Voted 3 years, 9 months ago
HARDWARE REQUIREMENTS
- 64-bit CPU with minimum of 4 cores
- CPU virtualization extensions (VT-x for Intel or AMD-V for AMD)
- Minimal of 8GB Memory
- 5GB free disk space
upvoted 42 times

Jake1 Highly Voted 3 years, 8 months ago
Answer is correct. For Windows Defender Application Guard, you need 64bit CPU with 4 cores, 8GB of RAM, 5GB of disk space, and CPU virtualization extensions (SLAT and VT-x) OR (AMD-V)
upvoted 10 times

Contactfornitish Most Recent 2 years, 4 months ago
On exam on 13 aug'22
upvoted 3 times

venwaik 2 years, 7 months ago
Selected Answer: BC
Answer given, is correct. Came on exam 09-05-2022
upvoted 3 times

L33D 3 years ago
Selected Answer: BC
Answer is correct

https://docs.microsoft.com/en-us/windows/security/threat-protection/microsoft-defender-application-guard/reqs-md-app-guard#hardware-requirements
upvoted 2 times

MomoLomo 3 years, 4 months ago

HARDWARE REQUIREMENTS
- 64-bit CPU with minimum of 4 cores
- CPU virtualization extensions (VT-x for Intel or AMD-V for AMD)
- Minimal of 8 GB Memory
- 5 GB free disk space

Computer4 and Computer1 don't have the requirements
upvoted 2 times

Question #25 *Topic 2*

HOTSPOT -

Your company uses Microsoft Defender for Endpoint.

The devices onboarded to Microsoft Defender for Endpoint are shown in the following table.

Name	Machine group
Device1	ATP1
Device2	ATP1
Device3	ATP2

The alerts visible in the Microsoft Defender for Endpoint alerts queue are shown in the following table.

Name	Machine
Alert1	Device1
Alert2	Device2
Alert3	Device3

You create a suppression rule that has the following settings:

- ✑ Triggering IOC: Any IOC
- ✑ Action: Hide alert
- ✑ Suppression scope: Alerts on ATP1 machine group

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
After you create the suppression rule, Alert1 is visible in the alerts queue.	○	○
After you create the suppression rule, Alert3 is visible in the alerts queue.	○	○
After you create the suppression rule, a new alert triggered on Device2 is visible in the alerts queue.	○	○

Suggested Answer:

Answer Area

Statements	Yes	No
After you create the suppression rule, Alert1 is visible in the alerts queue.	○	○
After you create the suppression rule, Alert3 is visible in the alerts queue.	○	○
After you create the suppression rule, a new alert triggered on Device2 is visible in the alerts queue.	○	○

A suppression rule will not affect alerts that are already in the alerts queue. Only new alerts will be suppressed.

MartiFC Highly Voted 3 years, 2 months ago

When a suppression rule is created, it will take effect from the point when the rule is created. The rule will not affect existing alerts already in the queue, prior to the rule creation. The rule will only be applied on alerts that satisfy the conditions set after the rule is created.

https://docs.microsoft.com/en-us/microsoft-365/security/defender-endpoint/manage-alerts?view=o365-worldwide

So, I tink that the answers are Y,Y,N

upvoted 18 times

Goena Highly Voted 3 years ago

- Yes, alert 1 was already created before suppression was enabled. It won't be suppressed retroactively.
- Yes, Alert 3 was already created and doesn't apply. Either way, it will still show up.
- No, the suppression rule is already in place before the alert can be created.

upvoted 6 times

Contactfornitish Most Recent 2 years, 4 months ago

On exam on 13 aug'22

upvoted 5 times

L33D 2 years, 6 months ago

Still valid, on exam Jun 25, 2022

upvoted 3 times

ZuluHulu 3 years, 2 months ago

Wouldn't the answer to the 3rd question be No? The suppression scope is limited to ATP1.

upvoted 6 times

MartiFC 3 years, 1 month ago

Device2 is ATP1 Machine Group

upvoted 5 times

Question #26 *Topic 2*

HOTSPOT -

Your company has a Microsoft 365 subscription.

You need to configure Microsoft 365 to meet the following requirements:

✑ Malware found in email attachments must be quarantined for 20 days.

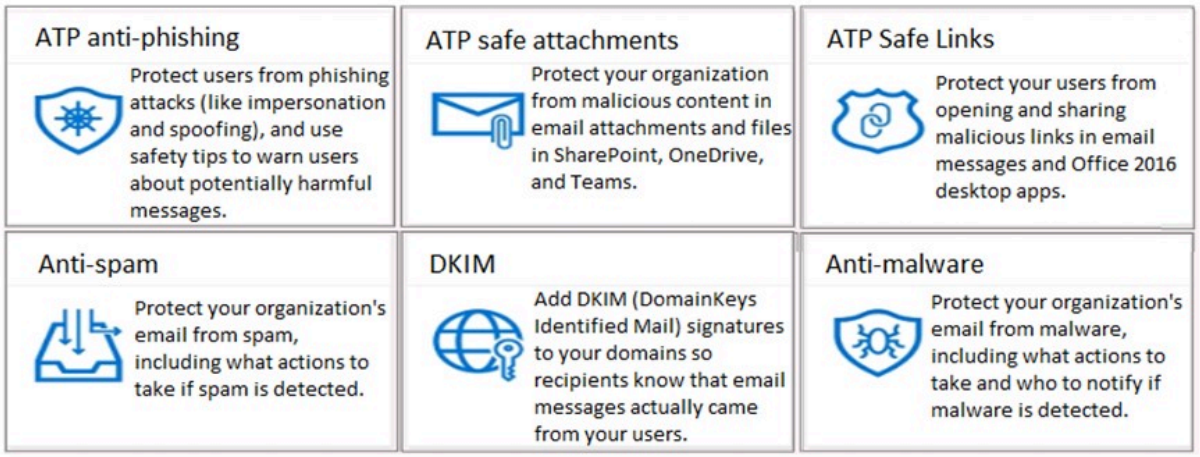
✑ The email address of senders to your company must be verified.

Which two options should you configure in the Security & Compliance admin center? To answer, select the appropriate options in the answer area.

NOTE: Each correct selection is worth one point.

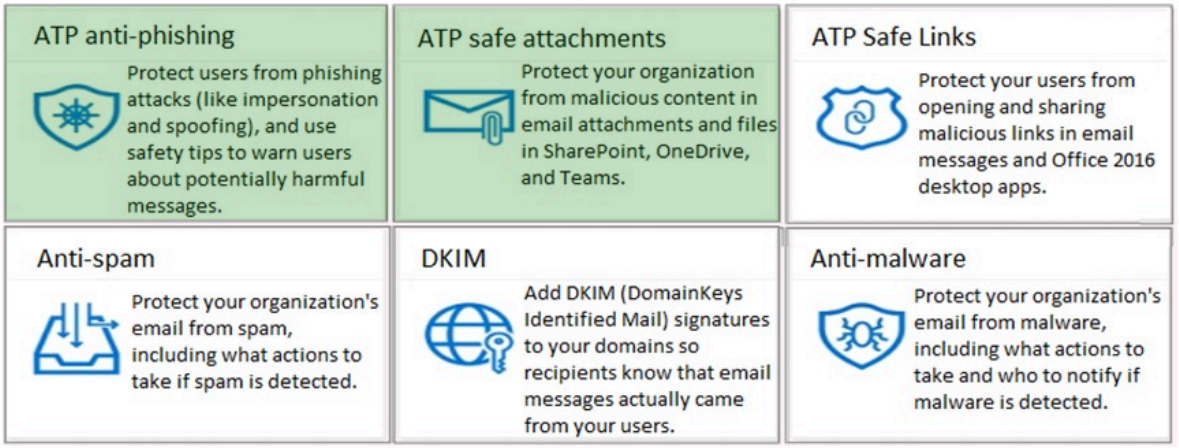
Hot Area:

Answer Area



Suggested Answer:

Answer Area



donathon Highly Voted 3 years, 7 months ago

Anti-Phishing & Anti-Spam.

Safe attachments: 15 days only cannot be changed.

Safe links: does not scan attachments but URLs.

DKIM: is for validation of others that you own the domain and hence is outbound.

Anti-malware: 15 days only cannot be changed.

upvoted 31 times

Alien1981 3 years, 6 months ago

agreed , tested in my tenant

https://security.microsoft.com/threatpolicy

upvoted 3 times

JT19760106 2 years, 11 months ago

Out of Anti-Phishing and Anti-Spam, what's flagging Malware? Reading the document, yes, only Anti-Phishing and Anti-Spam can have a custom quarantine period, but I didn't settings for either of those catching malware?
https://docs.microsoft.com/en-us/microsoft-365/security/office-365-security/quarantine-email-messages?view=o365-worldwide

upvoted 3 times

LK4723 2 years, 3 months ago

I agree with this and below is article that has table for my reasoning.
1) Anti-spam and anti-phishing have customizable retention periods.
2) All other services for email filtering is retention of 30 days and is not customizable.
3) The question requires a 20 day retention not "at least" 20 days of retention.
4) Malware is a type of spam and commonly includes .vbscript and javascript which his detected with anti-spam policies.
5) DKIM is a technology to detect a valid sender but the services that actually picks it up is anti-spam that is what is verifying SPF and DKIM records.

https://docs.microsoft.com/en-us/microsoft-365/security/office-365-security/quarantine-email-messages?view=o365-worldwide

upvoted 4 times

LK4723 2 years, 3 months ago

Update to number 5.
5) DKIM is a technology to detect a valid sender but the services that actually pick it up is anti-phishing and anti-spam when verifying SPF and DKIM records. Anti-phishing can also pickup impersonation in forged headers.

upvoted 2 times

Bulldozzer 2 years, 10 months ago

I don't agree. The anti-spam setting does not apply to malware. So for me, the correct answers are Anti-Phishing and Anti-Malware even though so far there are no settings to customize the quarantine retention period.

upvoted 6 times

Luckyson Highly Voted 3 years, 8 months ago

Antispam + DKIM

upvoted 12 times

themrcox 3 years, 7 months ago

DKIM is a digital signature added to outbound traffic so no, not DKIM.

upvoted 8 times

PersonT 3 years, 8 months ago

Agree...DKIM, offcourse

upvoted 3 times

potpal 3 years, 7 months ago

DKIM is very wrong

upvoted 12 times

lucidgreen 3 years, 5 months ago

DKIM is for email sent from you, not to you. It's so people can't impersonate you. Anti-Phishing/Spoofing is to keep you from getting messages from impersonators/spoofers.

upvoted 4 times

LeGluten Most Recent 1 year, 10 months ago

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.

Link: https://learn.microsoft.com/en-us/microsoft-365/security/office-365-security/quarantine-policies?view=o365-worldwide

upvoted 1 times

lfbservices 2 years, 2 months ago

-The email address of senders to your company must be verified:
I think it should be Anti Spam to verify and filter junk email from legitimate email

upvoted 1 times

Durden871 2 years, 5 months ago

I'm surprised, but I think it's
ATP Anti-Phishing (this one is obvious)

Anti-Spam

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.

If you change the quarantine policy that's assigned to a supported protection feature, the change affects messages that are quarantined after you make the change. Messages that were previously quarantined by that protection feature are not affected by the settings of the new quarantine policy assignment.
https://docs.microsoft.com/en-us/microsoft-365/security/office-365-security/quarantine-policies?view=o365-worldwide
upvoted 2 times

stealthster 2 years, 11 months ago
I think it's anti-phishing and Anti-malware

https://docs.microsoft.com/en-us/microsoft-365/security/office-365-security/safe-attachments?view=o365-worldwide
"Attachments aren't scanned for malware by Safe Attachments. Messages are still scanned for malware by anti-malware protection in EOP."

https://docs.microsoft.com/en-us/microsoft-365/security/office-365-security/manage-quarantined-messages-and-files?view=o365-worldwide

Anti-malware can quarantine messages that contain malware and a quarantine policy can be configured to expire the quarantined message from 1-30 days
upvoted 7 times

FreddyLao 3 years ago
if 20days of quarantine is a must. only Anti-spam can do. Anti-spam did mention can block malware.

https://docs.microsoft.com/en-us/microsoft-365/security/office-365-security/quarantine-email-messages?view=o365-worldwide
Quarantine reason:
Messages quarantined by anti-spam policies: spam, high confidence spam, phishing, high confidence phishing, or bulk.
Default retention period: 15 days:
In the default anti-spam policy.
In anti-spam policies that you create in PowerShell.
30 days in anti-spam policies that you create in the Microsoft 365 Defender portal.
Customizable? Yes

https://docs.microsoft.com/en-us/microsoft-365/security/office-365-security/anti-spam-protection?view=o365-worldwide
EOP anti-spam and anti-phishing technology is applied across our email platforms to provide users with the latest anti-spam and anti-phishing tools and innovations throughout the network. The goal for EOP is to offer a comprehensive and usable email service that helps detect and protect users from junk email, fraudulent email threats (phishing), and malware.
upvoted 1 times

jodtzz 3 years, 1 month ago
This is a touch question, but it's Anti-Phishing and Anti-Spam. Here is the article that tells you: https://docs.microsoft.com/en-us/microsoft-365/security/office-365-security/quarantine-policies?view=o365-worldwide

"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.

If you change the quarantine policy that's assigned to a supported protection feature, the change affects messages that are quarantined after you make the change. Messages that were previously quarantined by that protection feature are not affected by the settings of the new quarantine policy assignment."

So, you have to setup a quarantine policy in anti-spam (or PS) and assign it to the Safe Attachments feature.
upvoted 3 times

zakyntos 3 years, 5 months ago
Anti-Phishing + Anti-Spam
upvoted 4 times

zakyntos 3 years, 5 months ago
Anti-Phishing + Anti-Spam

upvoted 3 times

LoremanReturns 3 years, 5 months ago

The question is not right. The only way to configure quarantine for messages containing a malware is Safe Attachments. Anti-Spam has no options for malware. The default retention period (cannot be modified) for messages quarantined for malware is 15 days. There're no additional options on this, so the answer is wrong.

upvoted 3 times

AnoniMouse 3 years, 7 months ago

Malware found in email attachments must be quarantined for 20 days == SAFE ATTACHMENT

Read the required info carefully [The email address of senders TO your company must be verified]. They key here is the word TO and not FROM. DKIM will add a digital signature to your outgoing emails as a proof of identity, but the question wants the others to prove their identity, hence ANTI-PHISHING, which is the mechanism by which your incoming mail server verifies that the sender is coming from where it should be and not from somewhere else

upvoted 6 times

potpal 3 years, 6 months ago

15 days for files quarantined by Safe Attachments for SharePoint, OneDrive, and Microsoft Teams in Defender for Office 365. Does not meet the requirement.

upvoted 1 times

MiZi 3 years, 7 months ago

I would choose Anti-Phishing & Anti-Spam.
However, in Anti-Spam couldn't find a malware detection rule. There is ZAP (Zero hour auto-purge) which is far from quarantine but affects malware messages that have already been delivered to Exchange Online mailboxes and purge them. But those 20 days... haven't found the option to adjust it elswhere

upvoted 3 times

potpal 3 years, 7 months ago

I had this on test it is Anti-phishing and Anti Spam.
Here's the homework :
The email address of senders to your company must be verified.
https://docs.microsoft.com/en-us/microsoft-365/security/office-365-security/set-up-anti-phishing-policies?view=o365-worldwide#impersonation-settings-in-anti-phishing-policies-in-microsoft-defender-for-office-365

➩ Malware found in email attachments must be quarantined for 20 days
https://docs.microsoft.com/en-us/microsoft-365/security/office-365-security/safe-attachments?view=o365-worldwide
https://docs.microsoft.com/en-us/microsoft-365/security/office-365-security/manage-quarantined-messages-and-files?view=o365-worldwide
15 days for files quarantined by Safe Attachments for SharePoint, OneDrive, and Microsoft Teams in Defender for Office 365.

upvoted 9 times

potpal 3 years, 7 months ago

Anti-spam will allow you to adjust the quarantine to 20 days

upvoted 3 times

365admin 3 years, 8 months ago

Malware found in email attachments must be quarantined for 20 days- ATP Safe attachments.
Agreed the quarantine period is 15 days and there seems to be no way to change it, this solution looks the closest to meet the requirement. Anti-pam does not scan for malware in attachments.

upvoted 1 times

MSGrady 3 years, 8 months ago

ATP Safe attachments policy does block malware n attachments and the message is sent to Quarantine
https://www.imaginet.com/2018/office-365-advanced-threat-protection-101-atp-safe-attachments-policies/#:~:text=Creating%20Your%20First%20ATP%20Safe%20Attachments%20Policy&text=Applies%20to%20the%20imaginet.com,send%20it%20to%20t

upvoted 2 times

Eltooth 3 years, 8 months ago

Anti-phishing and Anti-Spam - checked on tenant and confirmed 30 days is only possible via Anti-Spam policy.

upvoted 2 times

Question #27 *Topic 2*

You have a Microsoft 365 subscription that uses Microsoft Defender Advanced Threat Protection (Microsoft Defender ATP).
All the devices in your organization are onboarded to Microsoft Defender ATP.
You need to ensure that an alert is generated if malicious activity was detected on a device during the last 24 hours.
What should you do?

A. From Alerts queue, create a suppression rule and assign an alert

B. From the Security & Compliance admin center, create an audit log search

C. From Advanced hunting, create a query and a detection rule

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

Suggested Answer: *C*
Reference:
https://docs.microsoft.com/en-us/windows/security/threat-protection/microsoft-defender-atp/custom-detection-rules

VTHAR Highly Voted 4 years, 2 months ago
Answer is correct.
upvoted 30 times

xenmo Highly Voted 2 years, 7 months ago
Correct (although they changed the language from ATP to Defender for Endpoint)
upvoted 6 times

Amir1909 Most Recent 11 months ago
Correct
upvoted 1 times

RiTh73 1 year, 10 months ago
Custom detection rules are rules you can design and tweak using advanced hunting queries. These rules let you proactively monitor various events and system states, including suspected breach activity and misconfigured endpoints. You can set them to run at regular intervals, generating alerts and taking response actions whenever there are matches.
upvoted 1 times

rrrr5r 2 years, 3 months ago
In Sep 16th 22's exam.
upvoted 3 times

Question #28 *Topic 2*

You have an Azure Active Directory (Azure AD) tenant and a Microsoft 365 E5 subscription. The tenant contains the users shown in the following table.

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

You plan to implement Microsoft Defender for Endpoint.
You verify that role-based access control (RBAC) is turned on in Microsoft Defender for Endpoint.
You need to identify which user can view security incidents from the Microsoft Defender Security Center.
Which user should you identify?

A. User1

B. User2

C. User3

D. User4

Suggested Answer: *A*

Community vote distribution

A (86%) 14%

venwaik Highly Voted 2 years, 7 months ago
Answer A. Came on exam 09-05-2022
upvoted 8 times

[Removed] Highly Voted 3 years ago
Selected Answer: A
According to https://docs.microsoft.com/en-us/microsoft-365/security/defender-endpoint/assign-portal-access?view=o365-worldwide i think A is correct.

If you have already assigned basic permissions, you may switch to RBAC anytime. Consider the following before making the switch:
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.
Users that have read-only access (Security Readers) will lose access to the portal until they are assigned a role. Note that only Azure AD user groups can be assigned a role under RBAC.
upvoted 6 times

JonJeff Most Recent 2 years, 8 months ago
The Answer is A.
https://docs.microsoft.com/en-us/azure/active-directory/roles/permissions-reference#security-operator
upvoted 2 times

OneplusOne 2 years, 12 months ago
A

"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."

https://docs.microsoft.com/en-us/microsoft-365/security/defender-endpoint/rbac?view=o365-worldwide
upvoted 5 times

VirtualJP 3 years ago
Selected Answer: C

I'm thinking Security reader would satisfy the requirement to view incidents - https://docs.microsoft.com/en-us/azure/active-directory/roles/permissions-reference#security-reader

upvoted 1 times

Bekkah 2 years, 12 months ago

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

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

Security Reader is not automatically turned on in Defender when RBAC is turned on and the role would have to be assigned in Defender but the Security Admin automatically has access in RBAC from the way I understand the documentation...but I could always be wrong, ha

upvoted 2 times

VirtualJP 2 years, 12 months ago

I think you are right here, so upon reflection A is the more likely answer.

upvoted 3 times

Goena 3 years ago

A. Security Administrator

upvoted 5 times

Question #29 *Topic 2*

Your network contains an on-premises Active Directory domain named contoso.com. The domain contains 1,000 Windows 10 devices.
You perform a proof of concept (PoC) deployment of Microsoft Defender for Endpoint for 10 test devices. During the onboarding process, you configure Microsoft
Defender for Endpoint-related data to be stored in the United States.
You plan to onboard all the devices to Microsoft Defender for Endpoint.
You need to store the Microsoft Defender for Endpoint data in Europe.
What should you do first?

A. Create a workspace.

B. Onboard a new device.

C. Delete the workspace.

D. Offboard the test devices.

Suggested Answer: *D*

Goena Highly Voted 3 years ago
Answer is D: First Offboard the test devices,
delete the workspace, create a workspace in Europe, onboard new devices.
upvoted 13 times

rrrr5r Highly Voted 2 years, 3 months ago
In Sep 16th 22's exam.
upvoted 5 times

Amir1909 Most Recent 11 months ago
D is correct
upvoted 1 times

Tyranttd 1 year ago
We encountered a similar scenario with our tenant. We had to unenroll every endpoint from Microsoft Defender for Endpoint. We then had to work directly with Microsoft to relocate our data storage. After successfully changing the data storage site, we proceeded to re-enroll all the devices.
upvoted 1 times

Tyranttd 1 year ago
so - Answer D :)
upvoted 1 times

k9_bern_001 2 years, 4 months ago
Offboard devices correct
upvoted 2 times

gxsh 3 years ago
Correct.
upvoted 4 times

Question #30 *Topic 2*

You have a Microsoft 365 subscription.
You need to be notified if users receive email containing a file that has a virus.
What should you do?

A. From the Exchange admin center, create an in-place eDiscovery & hold.

B. From the Security & Compliance admin center, create a data loss prevention (DLP) policy.

C. From the Exchange admin center, create an anti-malware policy.

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

Suggested Answer: *C*
Reference:
https://docs.microsoft.com/en-us/office365/servicedescriptions/exchange-online-service-description/anti-spam-and-anti-malware-protection

toontjeharder Highly Voted 3 years, 7 months ago
The same question was in Topic 2 - #28. There were different answers there. The right answer there was "From SCC, create an alert policy."
upvoted 13 times

Gwach Highly Voted 2 years, 11 months ago
Feature no longer in Exchange Admin Center
EAC >Protection >Malware filter : " This feature has moved to the Microsoft 365 Defender. Create and update malware filter policies on the Anti-malware page there. This page has now been retired from Classic Exchange admin center."
Answer is Defender Admin Center > Policies & rules >Threat policies >Anti-malware > Create new
upvoted 12 times

ServerBrain Most Recent 2 years, 1 month ago
https://learn.microsoft.com/en-us/exchange/antispam-and-antimalware/antimalware-protection/antimalware-protection?source=recommendations&view=exchserver-2019
upvoted 1 times

ServerBrain 2 years, 1 month ago
Answer is correct
upvoted 1 times

stealthster 2 years, 11 months ago
Answer is correct.
New-MalwareFilterPolicy -Name "<PolicyName>" [-Action <DeleteMessage | DeleteAttachmentAndUseDefaultAlert | DeleteAttachmentAndUseCustomAlert>] [-AdminDisplayName "<OptionalComments>"] [-CustomNotifications <$true | $false>] [<Inbound notification options>] [<Outbound notification options>] [-QuarantineTag <QuarantineTagName>]
upvoted 2 times

OneplusOne 2 years, 12 months ago
Exchange Online Powershell Anti-Malware policy:

"Notify the administrator admin@contoso.com when malware is detected in a message from an internal sender."

https://docs.microsoft.com/en-us/microsoft-365/security/office-365-security/configure-anti-malware-policies?view=o365-worldwide#use-exchange-online-powershell-or-standalone-eop-powershell-to-configure-anti-malware-policies
upvoted 1 times

Goena 3 years ago
Old Exchange is not an option. Should be SSC.
upvoted 4 times

JhonyTrujillo 3 years, 4 months ago
Select the Old Exchange Admin Center -> Protection -> Malware Filter -> Create New AntiMalware Policy.
upvoted 2 times

balajim212 3 years, 5 months ago

Answer is correct. Standard policy defined with alerts.

upvoted 2 times

jabbrwcky 3 years, 5 months ago

Surely this is incorrect. The Exchange Admin Centre has no access to malware policy; clicking the option to view the classic EAC still works (for now) and you can see the malware policy there but it says "By December 1, 2020 the malware filter experience will be removed from the Exchange admin center. Please use the updated experience in the Security and Compliance Center, Anti-malware page to modify, create and update anti-malware policies." - even that message is so old it's directing to the already-deprecated protection.office.com rather than the new security.microsoft.com!

upvoted 4 times

Boulare 3 years, 6 months ago

FROM SCC? CREATE AN ALERT POLCY !! right

upvoted 4 times

Shooby 3 years, 7 months ago

Answer is correct!

upvoted 1 times

Question #31 *Topic 2*

You have a Microsoft 365 subscription that contains 500 users.
You have several hundred computers that run the 64-bit version of Windows 10 Enterprise and have the following configurations:
✑ Two volumes that contain data
✑ A CPU that has two cores
✑ TPM disabled
✑ 4 GB of RAM
All the computers are managed by using Microsoft Endpoint Manager.
You need to ensure that you can turn on Windows Defender Application Guard on the computers.
What should you do first?

A. Modify the edition of Windows 10.

B. Create an additional volume.

C. Replace the CPU and enable TPM.

D. Replace the CPU and increase the RAM.

Suggested Answer: *D*
The computers need 4 CPU cores and 8GB of RAM.
Reference:
https://docs.microsoft.com/en-us/windows/security/threat-protection/windows-defender-application-guard/reqs-wd-app-guard

MBraga Highly Voted 3 years, 3 months ago
The answer is correct. However, replace the CPU...
upvoted 12 times

Jake1 Highly Voted 3 years, 8 months ago
Answer is correct. You need 8GB of RAM and 4-core CPU.
upvoted 12 times

qcla Most Recent 2 years ago
The answer is correct, but to add RAM and replace CPU for several hundred computers is massive PITA and not worth it.
upvoted 2 times

barleyhutcher 3 years, 8 months ago
answer is correct
upvoted 11 times

Question #32 *Topic 2*

You have a Microsoft 365 E5 subscription that uses Microsoft Defender for Endpoint.
From Microsoft Defender for Endpoint, you turn on the Allow or block file advanced feature.
You need to block users from downloading a file named File1.exe.
What should you use?

A. a suppression rule

B. an indicator

C. a device configuration profile

Suggested Answer: *B*
Reference:
https://docs.microsoft.com/en-us/windows/security/threat-protection/microsoft-defender-atp/respond-file-alerts#allow-or-block-file

Community vote distribution
B (100%)

venwaik Highly Voted 2 years, 7 months ago

Selected Answer: B

Answer B. Came on exam 09-05-2022
upvoted 12 times

gxsh Highly Voted 3 years ago

Answer is correct.
https://docs.microsoft.com/en-us/windows/security/threat-protection/microsoft-defender-atp/respo
nd-file-alerts#allow-or-block-file
upvoted 6 times

[Removed] 3 years ago

Agree: https://docs.microsoft.com/en-us/microsoft-365/security/defender-endpoint/respond-file-alerts?view=o365-worldwide#allow-or-block-file
When you add an indicator hash for a file, you can choose to raise an alert and block the file whenever a device in your organization attempts to run it.
Files automatically blocked by an indicator won't show up in the file's Action center, but the alerts will still be visible in the Alerts queue.
upvoted 8 times

Amir1909 Most Recent 11 months ago

B is correct
upvoted 1 times

VictorSaiz 2 years, 4 months ago

Hello Everyone!! Could anybody explain how to access the Microsoft Defender for Endpoint or wherever the Indicators are? Which is the URL? I cannot find this in Microsoft 365 Defender portal. Thank you very much in advance!
upvoted 2 times

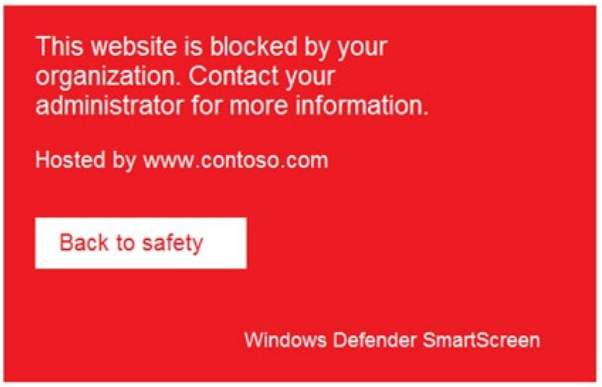
JAPo123 2 years, 10 months ago

https://docs.microsoft.com/en-us/microsoft-365/security/defender-endpoint/indicator-file?view=o365-worldwide#create-an-indicator-for-files-from-the-settings-page
upvoted 1 times

Question #33 *Topic 2*

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

When users attempt to access the portal of a partner company, they receive the message shown in the following exhibit.



You need to enable user access to the partner company's portal.

Which Microsoft Defender for Endpoint setting should you modify?

A. Custom detections

B. Advanced hunting

C. Alert notifications

D. Indicators

E. Alert suppression

Suggested Answer: *D*

Reference:

https://docs.microsoft.com/en-us/microsoft-365/security/defender-endpoint/manage-indicators?view=o365-worldwide

Goena Highly Voted 3 years ago

Indicator: It's possible to override the blocked category in web content filtering to allow a single site by creating a custom indicator policy.

upvoted 6 times

k9_bern_001 Most Recent 2 years, 4 months ago

D is correct

upvoted 2 times

gxsh 3 years ago

Correct.

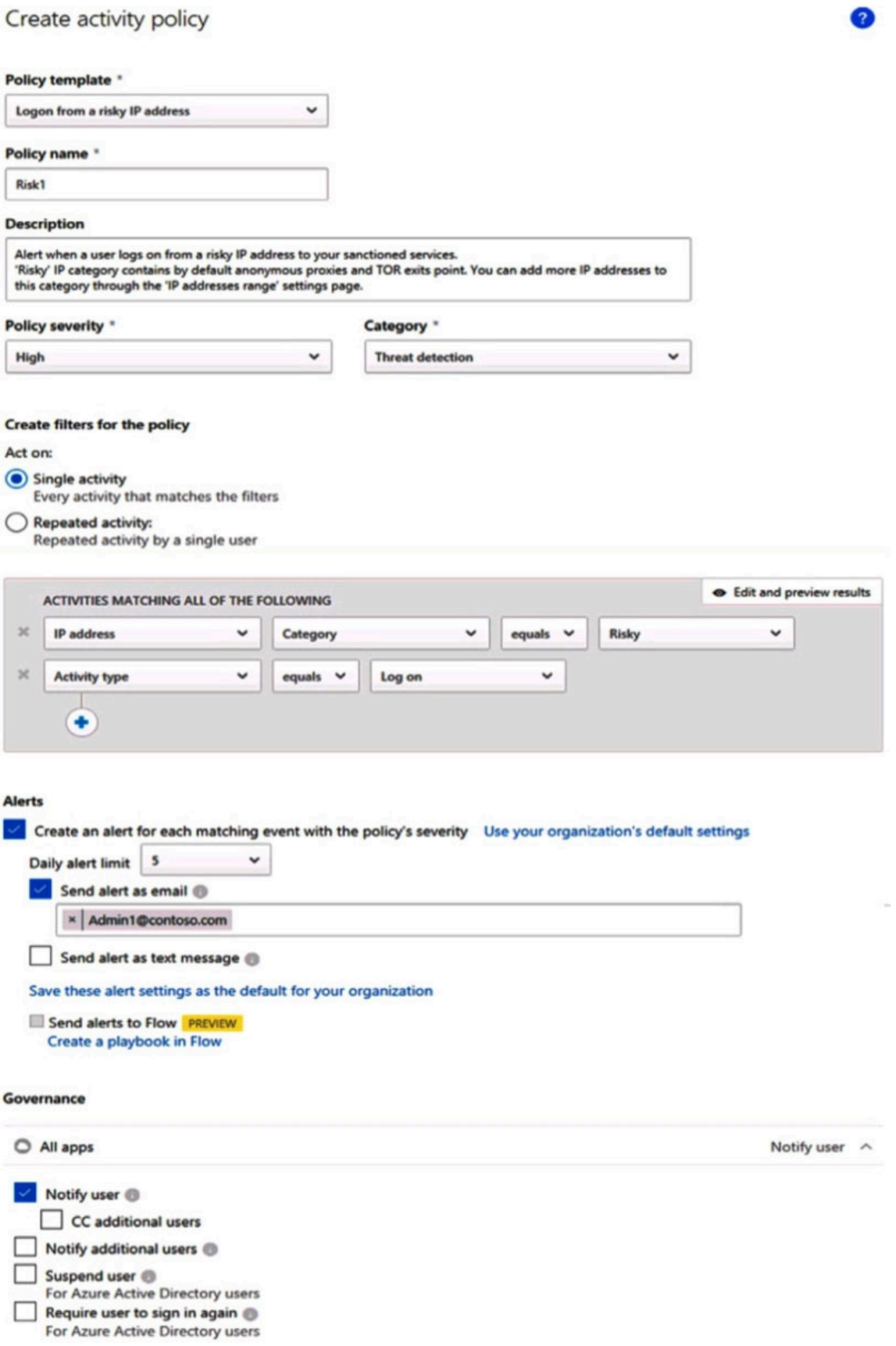
upvoted 2 times

Question #34 *Topic 2*

HOTSPOT -

You have a Microsoft 365 subscription.

You create a Microsoft Defender for Cloud Apps policy named Risk1 based on the Logon from a risky IP address template as shown in the following exhibit.

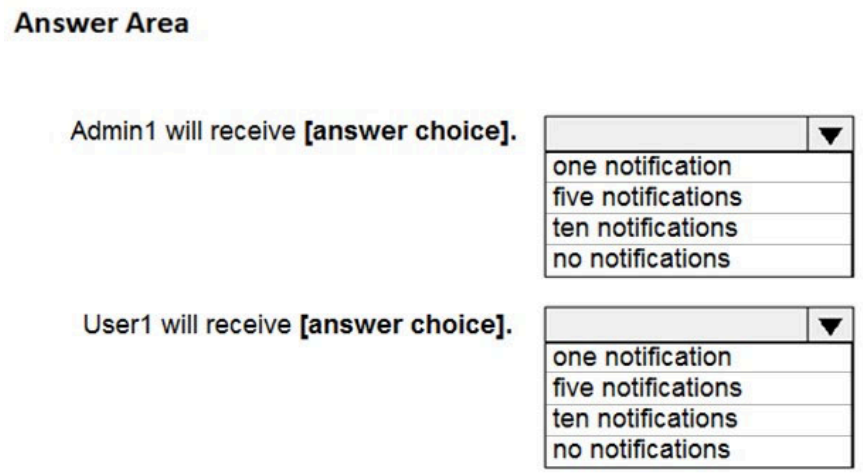


You have two users named User1 and User2. Each user signs in to Microsoft SharePoint Online from a risky IP address 10 times within 24 hours.

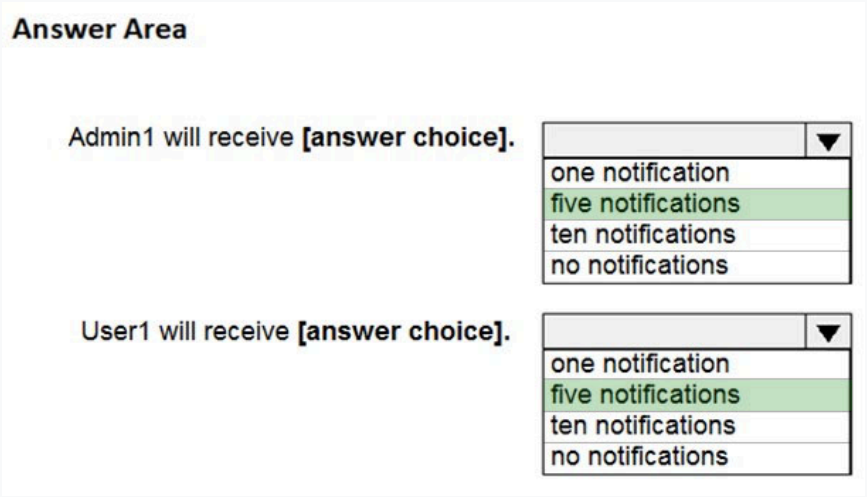
Use the drop-down menus to select the answer choice that completes each statement based on the information presented in the graphic.

NOTE: Each correct selection is worth one point.

Hot Area:



Suggested Answer:



AnoniMouse Highly Voted 3 years, 7 months ago

I have just verified in my environment. The admin will get only 5 as per the settings in the exhibit (no matter how many users try to sign in), and the user himself will get only one per day, so the correct answer is:

5 emails for the admin
1 notification for the user
upvoted 47 times

originalwitness Highly Voted 3 years, 8 months ago

Admin1 will receive 5 notifications. The user will receiver 1 per day. Can't find a URL, but you can hover over the information icon and it'll tell you "1 notification per day"
upvoted 19 times

scottims 3 years, 7 months ago

Verified end user notification in lab.
"The end user is notified when a policy match is detected. A maximum of one notification is sent per day."

The wording seems tricky but if it states maximum of 5 notifications then I suspect Microsoft means that as a hard limit and not a max of 5 per user incident.
upvoted 3 times

jecampos2 Most Recent 1 year, 6 months ago

It says, Act on a single activity. It means the same activity is detected within 24 hours a max of 5 times. Admin = 5, User = 1.
upvoted 1 times

Shadowcatest 1 year, 9 months ago

Was in exam 31.03.2023
upvoted 5 times

StudyBM 1 year, 9 months ago

Admin = 5

User = 1

upvoted 2 times

H3adcap 2 years, 4 months ago

Was in Exam today 20 Aug 2022

upvoted 6 times

rrrr5r 2 years, 3 months ago

In Sep 16th 22's exam.

upvoted 5 times

Sanjee31 1 year, 6 months ago

in exam 28/6/2023

upvoted 1 times

TashaGirl 2 years, 10 months ago

It is Daily alert limit per policy, so this policy, no matter how many users will trigger it, will generate 5 emails to Admin 1.

upvoted 2 times

VirtualJP 3 years, 1 month ago

I'm thinking 10 and 1

upvoted 1 times

VirtualJP 3 years ago

Not sure why I put 10 and 1! But I'm saying now 5 and 1. :-)

upvoted 1 times

Jakub2023 1 year, 7 months ago

Are you sure? ;-)

upvoted 1 times

kmsrajan 3 years, 6 months ago

It is a single activity which means every activity (each activity is considered irrespective of number of users) done by any user. Hence Admin get maximum of 5 email and user1 will get only one notification per day.

Admin 1: 5

User1 : 1

upvoted 5 times

lucidgreen 3 years, 6 months ago

I believe it would be a limit of 5 alerts per user, otherwise, you won't get any alerts about other users.

And the users will get alerted each time.

So 10 and 10?

upvoted 1 times

lucidgreen 3 years, 6 months ago

Never mind.

upvoted 3 times

karthikn 3 years, 7 months ago

Thank you :)

These questions were really helped in cleared the exam

upvoted 1 times

potpal 3 years, 8 months ago

So answer should be Admin -> 10x = 2users 5x each and User 1 - 1 notification based on note tip

upvoted 2 times

Lopsios 3 years, 8 months ago

There are 2 - User1 and User2. Each user signs in to Microsoft SharePoint Online from a risky IP address 10 times within 24 hours:

Admin - 10;

User 1 - 5;

upvoted 2 times

Lopsios 3 years, 8 months ago

User 1 - 1; Test in Lab:)

upvoted 4 times

MSGrady 3 years, 8 months ago

Anyone have a URL to support this?

upvoted 1 times

PersonT 3 years, 9 months ago

5;10..

upvoted 2 times

PersonT 3 years, 9 months ago

autocorrect tablet...should be 5 and 1

The end user is notified when a policy match is detected. A maximum of one otifiication is sent per day...

upvoted 12 times

lucidgreen 3 years, 8 months ago

5 per user to the admin? Or just stop at 5 notifications per day? I'm thinking the former makes more sense, but then, that's a lot of notifications in my environment of 70K+ users and their VPN apps to hide their location! Argh!

10 and 1.

upvoted 3 times

dzits 3 years, 7 months ago

Correct - Tested and Confirmed. Admin will get 5 notifications within mailbox. User1 will get 1 notification custom message (Custom message is missing from Exam question). This can be tested by creating same Cloud App Security however change Risky to your ISP IP address by going to Manage IP address ranges and add you IP address as Corperate and updated Risky to Corperate.

upvoted 2 times

Question #35 *Topic 2*

HOTSPOT -

You have a Microsoft Azure Activity Directory (Azure AD) tenant contains the users shown in the following table.

Name	Member of
User1	Group1
User2	Group2
User3	Group3

Group3 is a member of Group1.

Your company uses Microsoft Defender Advanced Threat Protection (ATP). Microsoft Defender ATP contains the roles shown in the following table.

Name	Permission	Assigned user group
Microsoft Defender ATP administrator (default)	View data, Alerts investigation, Active remediation actions, Manage security settings	*None*
Role1	View data, Alerts investigation	Group1
Role2	View data	Group2

Microsoft Defender ATP contains the device groups shown in the following table.

Rank	Machine group	Machine	User access
1	ATP1	Device1	Group1
Last	Ungrouped machines (default)	Device2	*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
User1 can view Device1 in Microsoft Defender Security Center.	○	○
User2 can sign in to Microsoft Defender Security Center.	○	○
User3 can view Device1 in Microsoft Defender Security Center.	○	○

Suggested Answer:

Answer Area

Statements	Yes	No
User1 can view Device1 in Microsoft Defender Security Center.	○	○
User2 can sign in to Microsoft Defender Security Center.	○	○
User3 can view Device1 in Microsoft Defender Security Center.	○	○

TFou0076 Highly Voted 3 years, 8 months ago

Nested groups are not supported in AAD, so User3 cannot sign in the Security Center.

Answer YYN.

upvoted 38 times

MSGrady 3 years, 8 months ago

is there a place to go to to support this? If the user 3 in Group 3 is a member of Group1 shouldnt user 3 be able to sign in?

upvoted 2 times

SimoneV 3 years, 8 months ago

No nesting. A group can't be added as a member of a role-assignable group.

https://docs.microsoft.com/en-us/azure/active-directory/roles/groups-concept#why-we-enforce-creation-of-a-special-group-for-assigning-it-to-a-role

upvoted 7 times

ALPHA_DELTA Highly Voted 3 years, 9 months ago

Believe this one is Y Y Y

User 2 is part of Group 2 which has view permissions for the Security Center which would allow them to sign in

upvoted 14 times

lucidgreen 3 years, 8 months ago

Nested groups are support in AAD, but are they supported in ATP? If so, Y, Y, Y. If not, Y, Y, N.

upvoted 3 times

lucidgreen 3 years, 6 months ago

I think nested groups for role assignment, if it works, would be a new thing.

upvoted 1 times

Mrawrrr 3 years, 7 months ago

Group nesting in MSDfE works well. I was able to get the same permissions from the nested group as from the parent group.

upvoted 2 times

lucidgreen 3 years, 5 months ago

I think nesting works for certain things, but not for role assignment.

upvoted 1 times

bac0n Most Recent 2 years ago

YYY;

Nested groups are not supported in Azure AD, but they ARE supported for Microsoft Defender for Endpoint. Just make security groups and do not enable the "enable role assignment" option. You can assign the role in the Defender for Endpoint, nest the second security group in the first, add the user to the second security group and boom, they'll have that role. I tested in my demo tenant with a test user, two test security groups with the defender for endpoint Admin role and boom it works.

upvoted 5 times

fpin01 2 years, 1 month ago

https://github.com/MicrosoftDocs/azure-docs/issues/97022

upvoted 1 times

fpin01 2 years, 1 month ago

Last bullet point in this document: https://docs.microsoft.com/en-us/azure/active-directory/roles/groups-concept#how-are-role-assignable-groups-protected states "Group nesting is not supported. A group can't be added as a member of a role-assignable group"

This is not exactly accurate as it is possible to assign a group as a member of a role-assignable group.

upvoted 1 times

KrisCyclo 2 years, 1 month ago

Box 3:

Yes. User3 is in Group3 which is assigned the Windows ATP Administrator role. Someone with a Microsoft Defender ATP Global administrator role has unrestricted access to all machines, regardless of their machine group association and the Azure AD user groups assignments.

upvoted 1 times

alonso_mosley 1 year, 6 months ago

"User3 is in Group3 which is assigned the Windows ATP Administrator role."

Really? Where did you see write this?

upvoted 2 times

Durden871 2 years, 9 months ago

Nesting is not supported for roles. Period.

The following scenarios are not supported with nested groups:

App role assignment, for both access and provisioning. Assigning groups to an app is supported, but any groups nested within the directly assigned group won't have access.

Group-based licensing (assigning a license automatically to all members of a group).

Microsoft 365 Groups.

https://docs.microsoft.com/en-us/azure/active-directory/enterprise-users/directory-service-limits-restrictions

upvoted 2 times

Durden871 2 years, 9 months ago

At this time, the following scenarios are supported with nested groups:
One group can be added as a member of another group, and you can achieve group nesting.
Group membership claims. When an app is configured to receive group membership claims in the token, nested groups in which the signed-in user is a member are included.
Conditional access (when a conditional access policy has a group scope).
Restricting access to self-serve password reset.
Restricting which users can do Azure AD Join and device registration.

https://docs.microsoft.com/en-us/azure/active-directory/enterprise-users/directory-service-limits-restrictions

Group nesting is not supported. A group can't be added as a member of a role-assignable group.
https://docs.microsoft.com/en-us/azure/active-directory/roles/groups-concept

This isn't a CA, this is role-based assignment.
upvoted 2 times

puuyii96 3 years, 4 months ago
YYN
Nesting is not suported for azure ad role assignment:
"Group nesting is not supported. A group can't be added as a member of a role-assignable group."
https://docs.microsoft.com/en-us/azure/active-directory/roles/groups-concept
upvoted 8 times

jkklim 3 years, 1 month ago
Group nesting is not supported. A group can't be added as a member of a role-assignable group. ==> therefore it is YYN
upvoted 2 times

F_M 3 years, 4 months ago
Did some trials. Turns out that ATP (Microsoft Defender for Endpoint, now) supports nested groups role assignment. If you assign a role in ATP to a group, users belonging to nested groups will be assigned that role. Y | Y | Y
upvoted 7 times

encxorblood 3 years, 4 months ago
Group nesting is not supported. A group can't be added as a member of a role-assignable group. Y-Y-N
upvoted 1 times

NikPat3125 3 years, 5 months ago
came in exam 27.07.2021
upvoted 9 times

ferrit 3 years, 5 months ago
I swear during revising today every question that I'm thinking the given answer is wrong and come to review you're here telling me it's in the exam :D
upvoted 12 times

LoremanReturns 3 years, 5 months ago
YYN, group nesting is not supported.
https://docs.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."
upvoted 8 times

MiZi 3 years, 7 months ago
Just tested. Nested groups work (just tested it). So in this scenario, I would select: Y Y Y
upvoted 7 times

Ceuse 3 years, 7 months ago
Is it offically supported though. Cant find information about that anywhere sadly
upvoted 2 times

Durden871 2 years, 9 months ago
I don't think it's officially supported according to the two following links that explicitly say roles don't support nested groups.
https://docs.microsoft.com/en-us/azure/active-directory/roles/groups-concept

https://docs.microsoft.com/en-us/azure/active-directory/enterprise-users/directory-service-limits-restrictions

upvoted 1 times

init2winit 3 years, 8 months ago

YYY - Nested Sec groups is OK

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.

https://docs.microsoft.com/en-us/azure/active-directory/fundamentals/active-directory-groups-membership-azure-portal

upvoted 4 times

Durden871 2 years, 9 months ago

Roles aren't supported for group nesting.

upvoted 1 times

Requi3m 3 years, 5 months ago

Regular security groups can be nested. But when you create a security group with the isAssignableToRole set to true, it can no longer be done.

The question is misleading though, because it says "Group 3 is a member of group 1". This should not be possible if group 1 was created as a role assignable group. So unless ATP roles can be assigned to regular security groups somehow, the answer should be YYN.

https://docs.microsoft.com/en-us/azure/active-directory/roles/groups-concept#why-we-enforce-creation-of-a-special-group-for-assigning-it-to-a-role

upvoted 1 times

MSGrady 3 years, 8 months ago

It is in fact YYN.. TFou0076, you are correct nested groups are not supported in AZure AD

upvoted 3 times

Goseu 3 years, 7 months ago

At this time the following are the supported scenarios with nested groups.
One group can be added as a member of another group and you can achieve group nesting.
Group membership claims (when an app is configured to receive group membership claims in the token, nested groups in which the signed-in user is a member are included)
Conditional access (when a conditional access policy has a group scope)
Restricting access to self-serve password reset
Restricting which users can do Azure AD Join and device registration

The following scenarios DO NOT supported nested groups:
App role assignment (assigning groups to an app is supported, but groups nested within the directly assigned group will not have access), both for access and for provisioning
Group-based licensing (assigning a license automatically to all members of a group)
Microsoft 365 Groups.

upvoted 1 times

slaoui 3 years, 8 months ago

Yes Yes No

User 1 is part of group 1 and group 1 has the role1 permissions for the machine device1
User 2 is part of group 2 and group 2 has has view permissions from role2 so they can sign (it doesn't matter what they can view)
User 3 is not part of any group.
Y, Y, N

upvoted 5 times

HvD 3 years, 7 months ago

Read again: User3 is part of Group3.

upvoted 2 times

eroc1990 3 years, 1 month ago

And for this case, nested groups are not supported and won't pass permissions down from the parent group.

upvoted 1 times

Rens19991 3 years, 8 months ago

I think Yes Yes No here.

upvoted 3 times

MSGrady 3 years, 8 months ago

How can User 3 in group 3 view device 1?

upvoted 1 times

malamos 3 years, 8 months ago

group3 is part group1

upvoted 2 times

bdedecker 3 years, 6 months ago

Can't see where you found that?

upvoted 1 times

bdedecker 3 years, 6 months ago

nevermind, I looked over it ;)

upvoted 2 times

Durden871 2 years, 9 months ago

It shouldn't matter. Nesting isn't supported for roles according to Microsoft.

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

https://docs.microsoft.com/en-us/azure/active-directory/enterprise-users/directory-service-limits-restrictions

upvoted 1 times

Question #36 *Topic 2*

HOTSPOT -

Your company uses Microsoft Defender for Cloud Apps.

You plan to integrate Defender for Cloud Apps and security information and event management (SIEM).

You need to deploy a SIEM agent on a server that runs Windows Server 2016.

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

NOTE: Each correct selection is worth one point.

Hot Area:

Answer Area

First action to perform:
- Install Java 8.
- Install Microsoft .NET Framework 3.5.
- Add the Windows Internal Database feature.
- Add the Setup and Boot Event Collection feature.

Second action to perform:
- Run the Set-MMagent cmdlet.
- Add the Setup and Boot Event Collection feature.
- Run the java command and specify the -jar parameter.
- Run the Install-WindowsFeature cmdlet and specify the -source parameter.

Suggested Answer:

Answer Area

First action to perform:
- Install Java 8.
- Install Microsoft .NET Framework 3.5.
- Add the Windows Internal Database feature.
- Add the Setup and Boot Event Collection feature.

Second action to perform:
- Run the Set-MMagent cmdlet.
- Add the Setup and Boot Event Collection feature.
- Run the java command and specify the -jar parameter.
- Run the Install-WindowsFeature cmdlet and specify the -source parameter.

References:

https://docs.microsoft.com/en-us/office365/securitycompliance/integrate-your-siem-server-with-office-365-cas

Moderator 2 years, 3 months ago

Yes, seem to be the correct answers (Step 1: Install Java 8 | Step 2: Download the JAR file and run it on your server)

upvoted 2 times

sprockets 2 years, 4 months ago

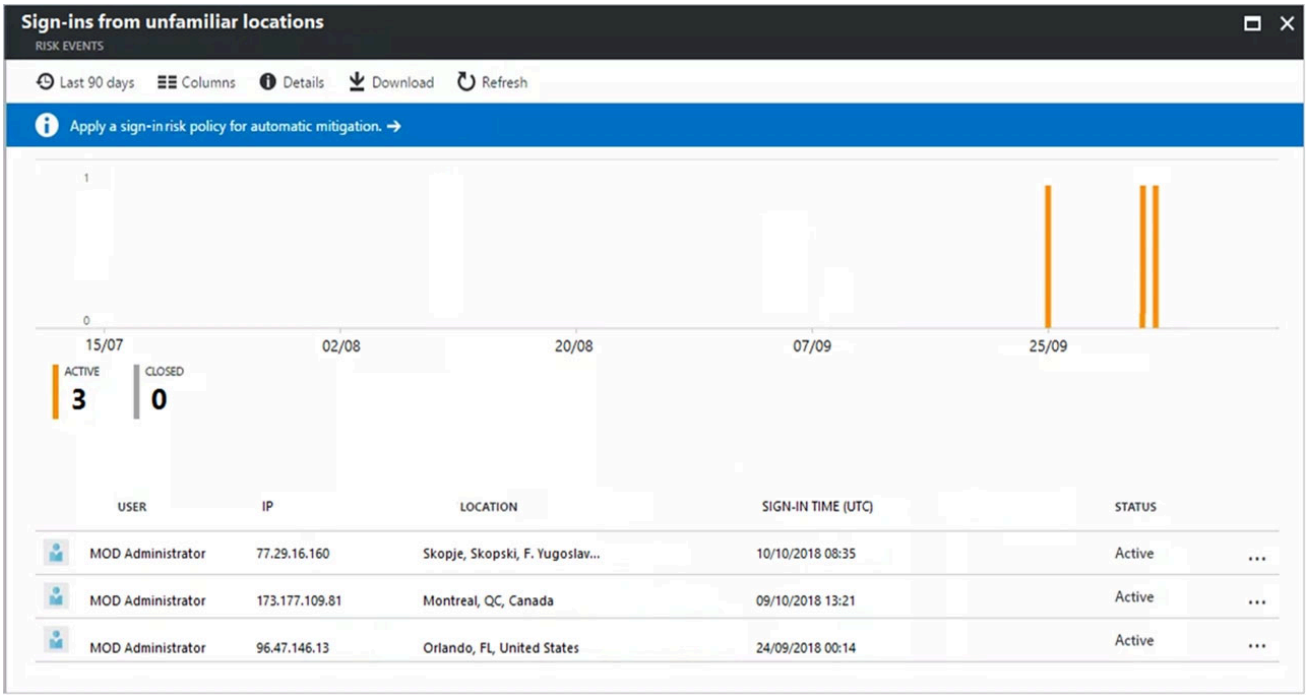
Looks to be correct answer https://docs.microsoft.com/en-us/defender-cloud-apps/siem

upvoted 3 times

Question #37 *Topic 2*

HOTSPOT -

From the Microsoft Azure Active Directory (Azure AD) Identity Protection dashboard, you view the risk events shown in the following exhibit.



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

NOTE: Each correct selection is worth one point.

Hot Area:

Answer Area

To require multi-factor authentication when signing in to unfamiliar locations, you must create a **[answer choice]**.

- named location in Azure AD
- sign-in risk policy
- user risk policy

To avoid generating alerts when signing in to the Montreal location, create **[answer choice]**.

- a named location in Azure AD
- a sign-in risk policy
- a user risk policy

Suggested Answer:

Answer Area

To require multi-factor authentication when signing in to unfamiliar locations, you must create a **[answer choice]**.

- named location in Azure AD
- **sign-in risk policy**
- user risk policy

To avoid generating alerts when signing in to the Montreal location, create **[answer choice]**.

- **a named location in Azure AD**
- a sign-in risk policy
- a user risk policy

References:

https://docs.microsoft.com/en-us/azure/active-directory/authentication/howto-mfa-getstarted https://docs.microsoft.com/en-us/azure/active-directory/identity-protection/howto-sign-in-risk-policy https://docs.microsoft.com/en-us/azure/active-directory/reports-monitoring/quickstart-configure-named-locations

ALPHA_DELTA Highly Voted 3 years, 9 months ago

Answer is correct

upvoted 15 times

Jake1 Highly Voted 3 years, 8 months ago

Given answers are correct. References are correct.

upvoted 10 times

romchik Most Recent 2 years, 2 months ago

Yes, correct

upvoted 3 times

RenegadeOrange 2 years, 3 months ago

Yes agree answer is correct.

upvoted 3 times

Moderator 2 years, 3 months ago

Yes, correct answers :)

upvoted 3 times

Question #38 *Topic 2*

Your company uses Microsoft Defender for Identity and Microsoft 365 Defender for Endpoint.
You need to integrate Microsoft Defender for Identity and Microsoft 365 Defender for Endpoint.
What should you do?

A. From Microsoft Defender for Identity, configure the notifications and reports.

B. From Microsoft Defender for Identity, configure the data sources.

C. From the Microsoft 365 Defender portal, configure general settings for Security center.

D. From the Microsoft 365 Defender portal, configure general settings for Microsoft 365 Defender.

Suggested Answer: *B*
Reference:
https://blog.ahasayen.com/azure-atp-and-windows-defender-atp-integration/

Community vote distribution
B (100%)

emanresu 1 year, 11 months ago
This question seems to be deprecated, checked Microsoft Defender Portal - Settings and none of these answers are correct any more, but B should have been correct
https://learn.microsoft.com/en-us/defender-cloud-apps/mdi-integration
Microsoft Defender for Cloud Apps integrates with Microsoft Defender for Identity to provide user entity behavioral analytics (UEBA) across a hybrid environment
upvoted 2 times

TechMinerUK 2 years, 2 months ago
As mentioned by gmKK should this not be:

MDE: Settings\Endpoints\Advanced Features\Microsoft Defender for Identity
MDI: Configurations\Enable Integration with Defender for Endpoint
upvoted 1 times

RenegadeOrange 2 years, 3 months ago
At the moment this is still correct, one of the last things still in the old portal.atp.azure.com, most things have been moved to the security center security.microsoft.com, under settings... Identities...
upvoted 2 times

gmKK 2 years, 3 months ago
Selected Answer: B
Answer is correct. Updated data source:
https://docs.microsoft.com/en-us/defender-for-identity/classic-integrate-mde#how-to-integrate-defender-for-identity-with-defender-for-endpoint
upvoted 3 times

Question #39 *Topic 2*

HOTSPOT -

You have a Microsoft Azure Activity Directory (Azure AD) tenant that contains the users shown in the following table.

Name	Member of
User1	Group1
User2	Group2
User3	Group3

Your company uses Microsoft Defender for Endpoint. Microsoft Defender for Endpoint contains the roles shown in the following table.

Name	Permission	Assigned user group
Microsoft Defender for Endpoint administrator (default)	View data, Alerts investigation, Active remediation actions, Manage security settings	Group3
Role1	View data, Alerts investigation	Group1
Role2	View data	Group2

Microsoft Defender for Endpoint contains the device groups shown in the following table.

Rank	Machine group	Machine	User access
1	ATP1	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 Device2.	○	○
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 Device2.	○	●
User2 can collect an investigation package from Device2.	○	●
User3 can isolate Device1.	●	○

References:

https://docs.microsoft.com/en-us/windows/security/threat-protection/windows-defender-atp/user-roles-windows-defender-advanced-threat-protection

[Removed] Highly Voted 3 years ago

- No: no access to machine group
- No : no only view data permission, alerts investigation is needed
- Yes : „User groups assigned the microsoft defender for endpoint administrator role have access to all device groups“ checked in M365 Defender Portal.

Infos about the permissions: https://docs.microsoft.com/en-us/microsoft-365/security/defender-endpoint/user-roles?view=o365-worldwide

upvoted 15 times

RenegadeOrange 2 years, 3 months ago

Agree, given answers are correct.

user1 can runs scans with the Alerts Investigation role but does not have access to Device2

upvoted 2 times

Glorence Highly Voted 2 years, 11 months ago

still valid, it was in my exam last Feb 5, 2022

upvoted 8 times

Sanjee31 1 year, 6 months ago

in exam 28/6/2023

upvoted 1 times

Goena Most Recent 3 years ago

- No: User 1 cannot run investigation on Device 2: in the ungrouped machine group which is only accessible by group2 members
- No: User 2 only can view data
- Yes: Nested groups are not supported when assigning roles. So Group 3 is not a member of Group 1 but Group 3 is assigned as (default).

upvoted 5 times

Question #40 *Topic 2*

HOTSPOT -

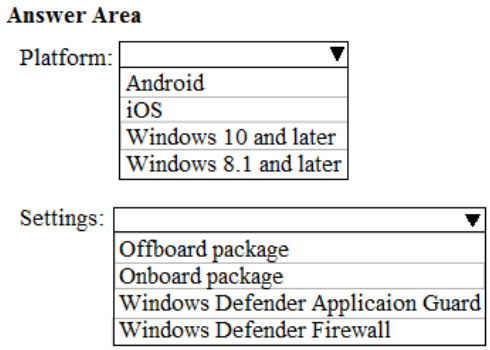
You have a Microsoft 365 subscription. All client devices are managed by Microsoft Endpoint Manager.

You need to implement Microsoft Defender Advanced Threat Protection (ATP) for all the supported devices enrolled in mobile device management (MDM).

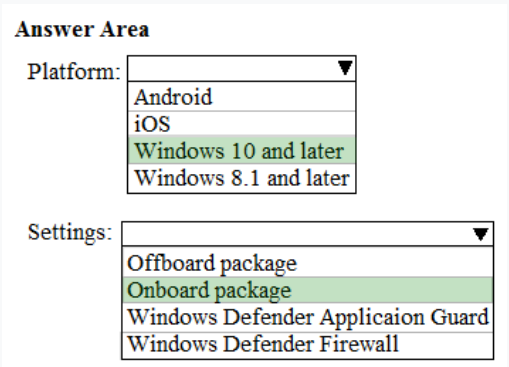
What should you include in the device configuration profile? To answer, select the appropriate options in the answer area.

NOTE: Each correct selection is worth one point.

Hot Area:



Suggested Answer:



Reference:

https://docs.microsoft.com/en-us/intune/advanced-threat-protection

larnyx Highly Voted 3 years, 4 months ago

Defender ATP has changed name to Microsoft defender for endpoint, FYI.

It seems as the devices are already enrolled via MDM and all except Windows 8.1 is supported, so in theory the answer should be Android, iOS and Windows 10..

But as the question states the DEVICE CONFIGURATION it points to the answer being only Windows 10, otherwise you deploy the app and use an APP CONFIGURATION for mobile devices.

Anyone else want to chime in with their thoughts?

upvoted 13 times

F_M 3 years, 3 months ago

I agree with you! Except for two details:

1) To enroll mobile devices you have to deploy an app, not an app configuration policy (or not only that)

2) It's still possible to enroll older Windows and Windows Server versions, just not with MEM/Intune. Check here: https://docs.microsoft.com/it-it/microsoft-365/security/defender-endpoint/onboard-downlevel?view=o365-worldwide

upvoted 2 times

LK4723 2 years, 3 months ago

I agree with your comment that the answer is correct and all info is in this link.

1) Create the device configuration profile to onboard Windows devices. (Displayed in article at bottom)

2) Onboard iOS/iPadOS devices using app configuration policy(this is different than device configuration as you advised and displayed in

article at bottom)
3) Onboard Android devices using app configuration policy(this appears to be the most complicated and they link to other articles for this work and one is: https://docs.microsoft.com/en-us/microsoft-365/security/defender-endpoint/android-intune?view=o365-worldwide
4) Windows 8.1 is not supported per article and is listed at the top of article in regards to onboarding.

Main article for 1, 2, and 4: https://docs.microsoft.com/en-us/mem/intune/protect/advanced-threat-protection-configure

https://docs.microsoft.com/en-us/mem/intune/protect/advanced-threat-protection-configure
upvoted 4 times

JAPo123 Most Recent 2 years, 10 months ago
Keywords
"..in mobile device management (MDM)"

https://docs.microsoft.com/en-us/mem/intune/enrollment/windows-enroll
Applies to:
Windows 10
Windows 11
upvoted 4 times

TimurKazan 3 years ago
this clearly states that all mentioned OS are supported...https://docs.microsoft.com/en-us/microsoft-365/security/defender-endpoint/minimum-requirements?view=o365-worldwide

+onboard
upvoted 2 times

TimurKazan 3 years ago
if we mention device configuration profile - I would choose win 10 + onboarding package
upvoted 3 times

Fcnet 3 years, 5 months ago
Microsoft Defender for Endpoint = Defender ATP
Microsoft Defender for Endpoint works with devices that run:
Android
iOS/iPadOS
Windows 10 or later
upvoted 1 times

teamspirate 3 years, 6 months ago
Shouldn't answer for Platform be: Android, IOS and Windows 10 and later?
Based on link: https://docs.microsoft.com/en-us/mem/intune/protect/advanced-threat-protection#prerequisites
"The following platforms are supported for Intune with Microsoft Defender for Endpoint:

Android
iOS/iPadOS
Windows 10 (Hybrid Azure Active Directory Joined or Azure Active Directory Joined)"
upvoted 1 times

lebaron 3 years, 5 months ago
Question states "Microsoft Defender Advanced Threat Protection" not "Microsoft Defender for Endpoint" as stated in the article you linked?.
upvoted 3 times

TimurKazan 3 years ago
it was renamed..
upvoted 3 times

Jake1 3 years, 7 months ago
Answer is correct. Onboarding is needed to complete the deployment. https://docs.microsoft.com/en-us/mem/intune/protect/advanced-threat-protection-configure
upvoted 2 times

ALPHA_DELTA 3 years, 9 months ago
Answer is correct

upvoted 4 times

Question #41 *Topic 2*

You have a Microsoft 365 subscription.
Your company purchases a new financial application named App1.
From Cloud Discovery in Microsoft Defender for Cloud Apps, you view the Discovered apps page and discover that many applications have a low score because they are missing information about domain registration and consumer popularity.
You need to prevent the missing information from affecting the App1 score.
What should you configure from the Cloud Discover settings?

A. Organization details

B. Default behavior

C. Score metrics

D. App tags

Suggested Answer: *C*
Reference:
https://docs.microsoft.com/en-us/cloud-app-security/getting-started-with-cloud-app-security

Community vote distribution
C (100%)

ServerBrain 2 years, 1 month ago

Selected Answer: C
100% correct!
upvoted 3 times

RenegadeOrange 2 years, 3 months ago
C is probably the correct answer.

An apps score is categorized by Microsoft from the General (domains etc), Security (mfa, encryption etc), Compliance & Legal properties of the App.
If you edit the App and add domain information (lets say it was missing) then you get a few points depending on the domain.
The only option in this question however that could increase the score would be to adjust the actual score metrics for each those four categories for your tenancy.

The above is a summary from this article:

https://learn.microsoft.com/en-us/defender-cloud-apps/risk-score
upvoted 3 times

Question #42 *Topic 2*

You have a Microsoft 365 E5 subscription.
You need to be notified if users receive email containing a file that has a virus.
What should you do?

A. From the Exchange admin center, create an in-place eDiscovery & hold.

B. From the Exchange admin center, create a spam filter policy.

C. From the Exchange admin center, create an anti-malware policy.

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

Suggested Answer: *C*
Reference:
https://docs.microsoft.com/en-us/office365/servicedescriptions/exchange-online-service-description/anti-spam-and-anti-malware-protection

Community vote distribution
C (100%)

Contactfornitish Highly Voted 2 years, 4 months ago
Selected Answer: C
If duplicate questions were removed then this cert on examtopics was less than 300 or even 250 easily
upvoted 9 times

Jake1 Highly Voted 3 years, 7 months ago
Correct. Create a Threat Management Policy for Anti-malware from the Security Admin Center.
upvoted 7 times

jkklim Most Recent 3 years, 1 month ago
Answer was C in exchange admin center - because in the old cloud portal, you can create anti-malware policy.

Now of course, you go to SCC
upvoted 2 times

jabbrwcky 3 years, 5 months ago
This looks like a duplicate of Q29, I noted the same there. It's definitely not on EAC.
upvoted 3 times

MiZi 3 years, 7 months ago
Malware filter has a new home and improved functionality. By December 1, 2020 – the malware filter experience will be removed from the Exchange admin center. Please use the updated experience in the Security and Compliance Center, Anti-malware page to modify, create and update anti-malware policies
upvoted 3 times

Goseu 3 years, 7 months ago
Correct ,but not from EAC but from SAC
upvoted 3 times

Question #43 *Topic 2*

HOTSPOT -

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

A user named User1 stores documents in Microsoft OneDrive.

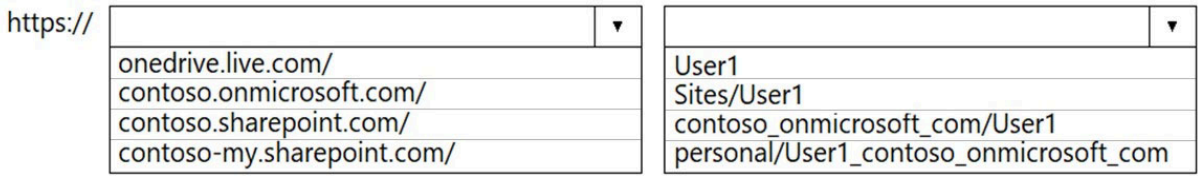
You need to place the contents of User1's OneDrive account on an eDiscovery hold.

Which URL should you use for the eDiscovery hold? To answer, select the appropriate options in the answer area.

NOTE: Each correct selection is worth one point.

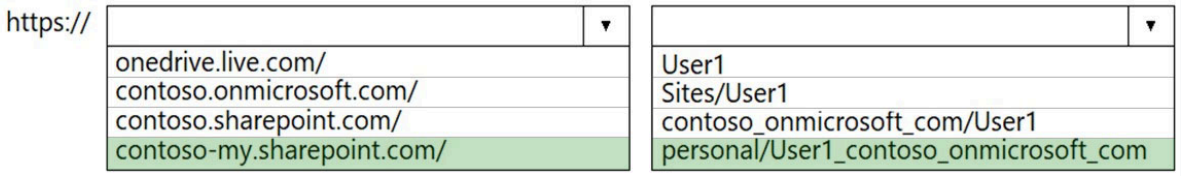
Hot Area:

Answer Area



Suggested Answer:

Answer Area



Reference:

https://docs.microsoft.com/en-us/microsoft-365/compliance/create-ediscovery-holds

PersonT Highly Voted 3 years, 9 months ago

Here's an example of a URL for a user's OneDrive site: https://contoso-my.sharepoint.com/personal/sarad_contoso_onmicrosoft.com.

upvoted 21 times

DiscGolfer 3 years, 2 months ago

https://docs.microsoft.com/en-us/microsoft-365/compliance/create-ediscovery-holds?view=o365-worldwide#preserve-content-in-onedrive-accounts

upvoted 3 times

barleyhutcher Highly Voted 3 years, 8 months ago

Correct - tested

upvoted 9 times

ARYMBS Most Recent 2 years, 3 months ago

Super Easy:

URL starts with "-my." always.

Personal Onedrive starts with "personal/"

upvoted 3 times

H3adcap 2 years, 4 months ago

Was in exam today 20 Aug 2022

upvoted 4 times

us3r 3 years ago

easy peasy

upvoted 1 times

balajim212 3 years, 5 months ago

Correct

upvoted 2 times

Question #44 *Topic 2*

HOTSPOT -

You have a Microsoft 365 E5 subscription linked to an Azure Active Directory (Azure AD) tenant. The tenant contains a group named Group1 and the users shown in the following table:

Name	Role
Admin1	Conditional Access administrator
Admin2	Security administrator
Admin3	User administrator

The tenant has a conditional access policy that has the following configurations:

✑ Name: Policy1

✑ Assignments:

- Users and groups: Group1
- Cloud aps or actions: All cloud apps

✑ Access controls:

✑ Grant, require multi-factor authentication

✑ Enable policy: Report-only

You set Enabled Security defaults to Yes for the tenant.

For each of the following settings 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 set Enable policy for Policy1 to **On**.	○	○
Admin2 can set Enable policy for Policy1 to **Off**.	○	○
Admin3 can set Users and groups for Policy1 to **All users**.	○	○

Suggested Answer:

Answer Area

Statements	Yes	No
Admin1 can set Enable policy for Policy1 to **On**.	○	○
Admin2 can set Enable policy for Policy1 to **Off**.	○	○
Admin3 can set Users and groups for Policy1 to **All users**.	○	○

Report-only mode is a new Conditional Access policy state that allows administrators to evaluate the impact of Conditional Access policies before enabling them in their environment. With the release of report-only mode:

✑ Conditional Access policies can be enabled in report-only mode.

✑ During sign-in, policies in report-only mode are evaluated but not enforced.

✑ Results are logged in the Conditional Access and Report-only tabs of the Sign-in log details.

✑ Customers with an Azure Monitor subscription can monitor the impact of their Conditional Access policies using the Conditional Access insights workbook.

Reference:

https://docs.microsoft.com/en-us/azure/active-directory/conditional-access/concept-conditional-access-report-only

Dan_Turnbull Highly Voted 3 years, 8 months ago

You need to turn security defaults off before you can enable the policy:

"It looks like you're about to manage your organization's security configurations. That's great! You must first disable Security defaults before enabling a Conditional Access policy."

"Security defaults must be disabled to enable Conditional Access policy."

I believe the answer is:

No, Yes, No
upvoted 54 times

bac0n 2 years ago
Tested and confirmed.
upvoted 1 times

JFRigot Highly Voted 3 years, 9 months ago
Yes, yes, no
upvoted 41 times

Prianishnikov 3 years, 9 months ago
Agree with you, tested this case.
upvoted 5 times

RenegadeOrange 2 years, 3 months ago
I tested this, with the conditional access policy set to report-only you can turn on security defaults, when you go to turn on the policy however it won't let you and gives you an error that security defaults must be disabled first.

No, Yes, No
upvoted 3 times

GotDamnImIn Most Recent 1 year, 8 months ago
No - Security defaults need to be off before enabling
Yes - Has access to do so, no warnings
No - Does not have access, cannot even see the policy
upvoted 3 times

ElmarK 2 years, 1 month ago
Correct answer is:
NO : you cannot enable a policy when security default are enabled.
Yes: report-only to off is allowed
No: User adminstrator has in addition no rights.
upvoted 1 times

RazielLycas 2 years, 5 months ago
as soon as you activate default the conditional policy will become ineffective and not accessible so N-N-N
upvoted 3 times

JamesM9 2 years, 9 months ago
"If you're using Conditional Access and have Conditional Access policies enabled in your environment, security defaults won't be available to you"

https://docs.microsoft.com/en-us/azure/active-directory/fundamentals/concept-fundamentals-security-defaults#deployment-considerations

Therefore, as a result of this the answer is NNN.
upvoted 8 times

TashaGirl 2 years, 10 months ago
The scenario is impossible to achieve: if you have a policy in conditional access you cannot enable security defaults - "It looks like you have Identity Protection policies enabled. Enabling Identity Protection policies prevents you from enabling Security defaults." If you have Security Defaults enabled, you cannot save the conditional access policy.
upvoted 4 times

LillyLiver 2 years, 10 months ago
Just tested this scenario in my tenant. Replicated the question and with the Security Defaults set to "Yes" none of the users could enable the policy.

So the answer is N, N, N.
upvoted 10 times

Bulldozzer 2 years, 10 months ago
You're right. N,N,N

upvoted 3 times

Ahema 3 years, 4 months ago

Y-Y-N is the answer

User admin don't have access to edit conditional access policies guys

upvoted 8 times

Domza 3 years, 4 months ago

Darkwing Duck to the rescue :)

Answers are correct. Caz you can have Read Only or OFF - Policy status. To test Conditional policy before applying them.

As soon as you switch Policy ON you will get a message "Security defaults must be disabled to enable Conditional Access policy."

upvoted 3 times

Bouncy 2 years, 8 months ago

Which makes it NYN according to your arguments instead of "Answers are correct" ;)

upvoted 3 times

encxorblood 3 years, 4 months ago

N-Y-N

1. No - Can not set to on. Before the Security defaults must be disabled
2. Yes - Off ist ok with Security defaults must be disabled
3. No - No rights to edit CA

upvoted 13 times

Kanta 3 years, 4 months ago

NYN

and agreed with below:

Because you set Enabled Security defaults to Yes for the tenant...

N Conditional access policy can not be changed from report-only to on

Y conditional access policy can be changed from report-only to off

N user admin role doesn't have rights to modify conditional access policy

upvoted 9 times

TesterDude 3 years, 5 months ago

This is a trick question, it's no to all of them. If you enable security defaults you can't use conditional access rules until it's disabled

Sources:

https://docs.microsoft.com/en-us/azure/active-directory/fundamentals/concept-fundamentals-security-defaults#deployment-considerations

If you're using Conditional Access and have Conditional Access policies enabled in your environment, security defaults won't be available to you. If you have a license that provides Conditional Access but don't have any Conditional Access policies enabled in your environment, you are welcome to use security defaults until you enable Conditional Access policies.

https://techcommunity.microsoft.com/t5/azure-active-directory-identity/introducing-security-defaults/ba-p/1061414

You can't enable Security Defaults if you're already using conditional access policies or other settings which conflict

upvoted 7 times

TesterDude 3 years, 5 months ago

After testing it is No Yes No because you can change conditional access from report-only to Off but not to On while security defaults are enabled

upvoted 8 times

TechMinerUK 2 years, 2 months ago

I agree with TesterDude, you can turn a Conditional Access policy off when Security Baselines is on however you can not enable them without disablng Security Baselines first

upvoted 1 times

GiJoe1987 3 years, 6 months ago

Security defaults must be set to off to modify/ create or turn on a conditional access policy

upvoted 4 times

BGM_YKA 3 years, 7 months ago

Because you set Enabled Security defaults to Yes for the tenant...
N Conditional access policy can not be changed from report-only to on
Y conditional access policy can be changed from report-only to off
N user admin role doesn't have rights to modify conditional access policy
upvoted 10 times

Matajare 3 years, 7 months ago
Neither can turn anything on or off. Security Default is active, so conditional access policies are disabled.
NO-NO-NO
upvoted 1 times

Matajare 3 years, 7 months ago
Sorry, I don't see "Report-Only" mode.
YES-YES-NO
upvoted 2 times

bellorg 3 years, 8 months ago
Tested on my LAB, don't need to turn off Security Defaults
yes, yes. no
upvoted 1 times

Dan_Turnbull 3 years, 8 months ago
I've tested it too.

I had to disable security defaults before enabling:

https://docs.microsoft.com/en-us/azure/active-directory/fundamentals/concept-fundamentals-security-defaults#:~:text=Organizations%20that%20choose%20to%20implement,defaults%20must%20disable%20security%20defaults.&text=in%20your%20dire

"Organizations that choose to implement Conditional Access policies that replace security defaults must disable security defaults."
upvoted 4 times

Question #45 *Topic 2*

Your network contains an on-premises Active Directory domain.
Your company has a security policy that prevents additional software from being installed on domain controllers.
You need to monitor a domain controller by using Microsoft Defender for Identity.
What should you do? More than one answer choice may achieve the goal. Choose the BEST answer.

A. Deploy a Microsoft Defender for identity sensor, and then configure port mirroring.

B. Deploy a Microsoft Defender for identity sensor, and then configure detections.

C. Deploy a Microsoft Defender for Identity standalone sensor, and then configure detections.

D. Deploy a Microsoft Defender for Identity standalone sensor, and then configure port mirroring.

Suggested Answer: *D*
We cannot install additional software on the domain controllers. Azure ATP Standalone Sensor is a full agent installed on a dedicated server that can monitor traffic from multiple domain controllers. This is an alternative to those that do not wish to install an agent directly on a domain controller.
Incorrect Answers:
A, B: Azure ATP Sensor is a lightweight agent installed directly on a domain controller to monitor and report traffic. However, we cannot install additional software on the domain controllers
Reference:
https://docs.microsoft.com/en-us/azure-advanced-threat-protection/install-atp-step5 https://docs.microsoft.com/en-us/defender-for-identity/configure-port-mirroring https://blog.enablingtechcorp.com/secure-and-monitor-domain-controllers-with-azure-atp

Community vote distribution
D (100%)

Contactfornitish Highly Voted 2 years, 4 months ago
On exam on 13 aug'22
upvoted 9 times

venwaik Highly Voted 2 years, 7 months ago
Selected Answer: D
Answer D. Came on exam 09-05-2022
upvoted 7 times

jonny_sins Most Recent 1 year, 4 months ago
asked Chat GPT and the answer is A.
upvoted 1 times

Tyreece 2 years, 2 months ago
Ms-100 question
upvoted 2 times

mackzone 2 years, 6 months ago
came on exam on 25-06-2022
upvoted 5 times

gxsh 3 years, 1 month ago
According to the question the answer is correct.
upvoted 4 times

RenegadeOrange 2 years, 3 months ago
Agreed
upvoted 3 times

Question #46 *Topic 2*

Your company has digitally signed applications.
You need to ensure that Microsoft Defender for Endpoint considers the digitally signed applications safe and never analyzes them.
What should you create in the Microsoft Defender Security Center?

A. a custom detection rule

B. an allowed/blocked list rule

C. an alert suppression rule

D. an indicator

Suggested Answer: *D*
Reference:
https://docs.microsoft.com/en-us/windows/security/threat-protection/microsoft-defender-atp/manage-indicators

Community vote distribution
D (100%)

Goena Highly Voted 3 years ago
Correct answer D:
Create indicators that define detection prevention and exclusion of entities and define an action to be taken and duration for when to apply the action.
upvoted 10 times

RenegadeOrange 2 years, 3 months ago
Agreed
upvoted 5 times

Sucxi Most Recent 1 year, 7 months ago
Selected Answer: D
These indicators are kinda confusing. You can create a Indicator for a certificate.

https://learn.microsoft.com/en-us/microsoft-365/security/defender-endpoint/indicator-certificates?view=o365-worldwide
upvoted 1 times

Question #47 *Topic 2*

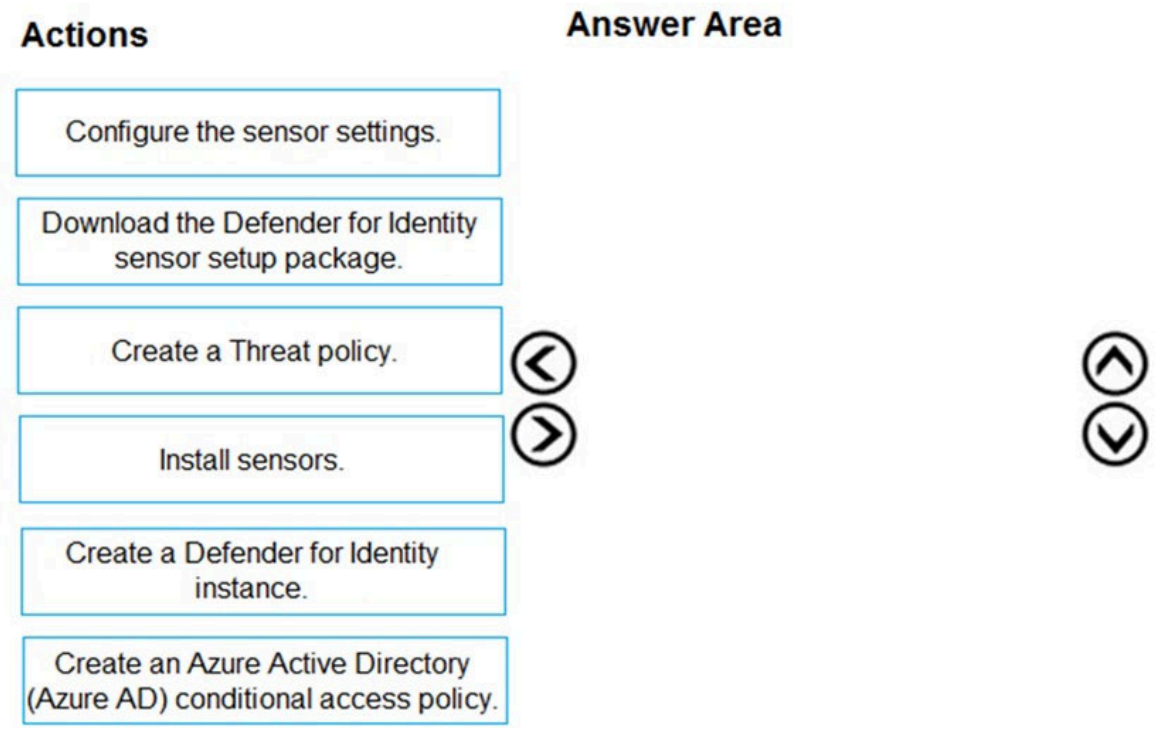
DRAG DROP -

You create a Microsoft 365 subscription.

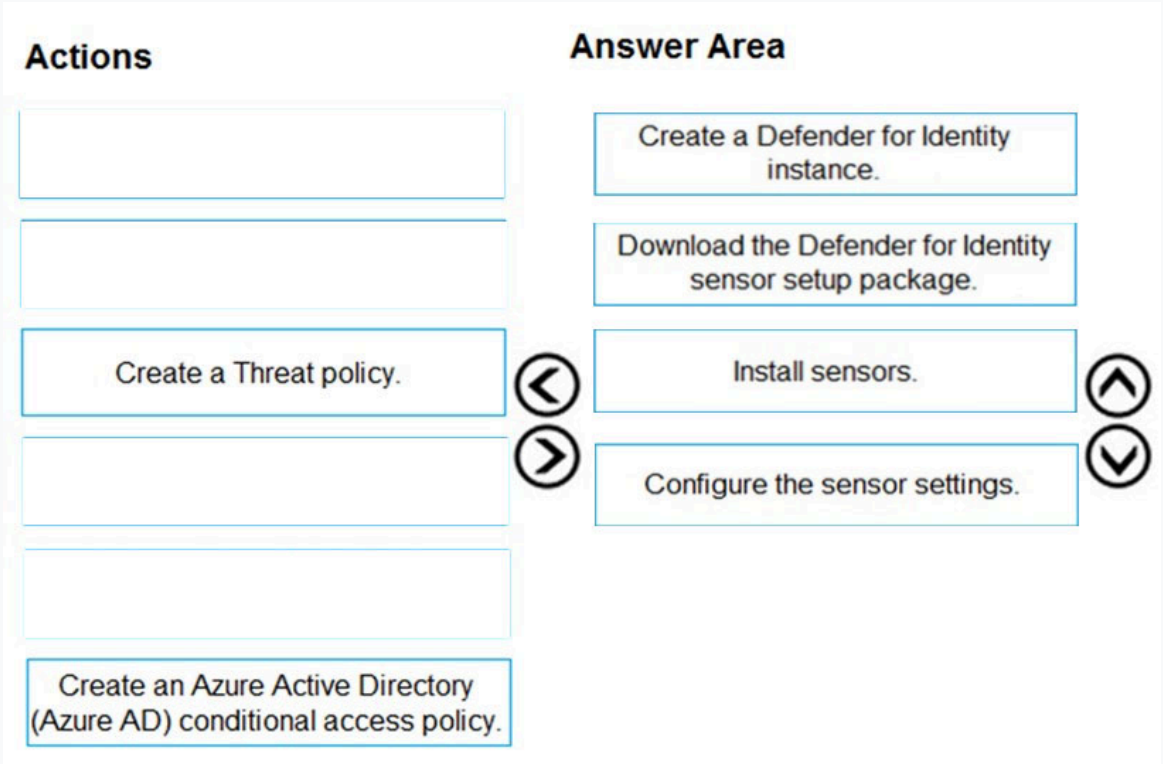
You need to create a deployment plan for Microsoft Defender for Identity.

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

Select and Place:



Suggested Answer:



Reference:

https://docs.microsoft.com/en-us/defender-for-identity/install-step1 https://docs.microsoft.com/en-us/defender-for-identity/install-step3 https://docs.microsoft.com/en-us/defender-for-identity/install-step4

jkklim Highly Voted 3 years, 1 month ago

ansswers correct

upvoted 7 times

BryanL332 Highly Voted 3 years, 2 months ago

Question is about Defender for EndPoint but answer is about Defender for Identity. Hope this won't come out in exam

upvoted 5 times

RenegadeOrange Most Recent 2 years, 3 months ago

by "Configure Sensor settings" does it mean configure the Directory services accounts? I don't see any settings to configure under Sensors in the new Defender for Identity, during the installation you need to provide the Access Key you copy when you download the installer... unless you want to say that is "configuring the sensor" but that's part of the install.

Out of the given answers though those are the best choice.

upvoted 1 times

ccadenasa 3 years, 2 months ago

This should be Microsoft Endpoint for Identity. Someone needs to correct the question

upvoted 2 times

Question #48 *Topic 2*

You have a Microsoft 365 E5 subscription that uses Azure Advanced Threat Protection (ATP).
You need to create a detection exclusion in Azure ATP.
Which tool should you use?

A. the Security & Compliance admin center

B. Microsoft Defender Security Center

C. the Microsoft 365 admin center

D. the Azure Advanced Threat Protection portal

E. the Defender for Cloud Apps portal

Suggested Answer: *D*
Reference:
https://docs.microsoft.com/en-us/defender-for-identity/what-is https://docs.microsoft.com/en-us/defender-for-identity/excluding-entities-from-detections

Community vote distribution
B (100%)

RenegadeOrange Highly Voted 2 years, 3 months ago
In the old portal.atp.azure.com which still exists there is an exclusions section but it's limited to certain types of exclusions and you can add a user, pc or IP under those.

The new place is now in security.microsoft.com (Microsoft 365 Defender) under Settings...Identities... Global excluded entities

There you can just add a User/Domain/Device or IP as a direct global exclusion.
upvoted 6 times

EliasMartinelli Most Recent 2 years, 1 month ago
Selected Answer: B
old question new is the MD portal.
B is right
upvoted 2 times

sliix 2 years, 2 months ago
Selected Answer: B
See Fefe_ES
upvoted 3 times

Fefe_ES 2 years, 3 months ago
Old. Now is on MD portal:
https://learn.microsoft.com/en-us/microsoft-365/security/defender-identity/exclusions?view=o365-worldwide
upvoted 3 times

Moderator 2 years, 3 months ago
Selected Answer: B
My guess would be B: https://docs.microsoft.com/en-us/defender-for-identity/exclusions
upvoted 2 times

Question #49 *Topic 2*

Note: This question is part of a series of questions that present the same scenario. Each question in the series contains a unique solution that might meet the stated goals. Some question sets might have more than one correct solution, while others might not have a correct solution.
After you answer a question in this section, you will NOT be able to return to it. As a result, these questions will not appear in the review screen.
You have a Microsoft 365 subscription.
You need to prevent users from accessing your Microsoft SharePoint Online sites unless the users are connected to your on-premises network.
Solution: From the Endpoint Management admin center, you create a device configuration profile.
Does this meet the goal?

A. Yes

B. No

Suggested Answer: *B*
You need to create a trusted location and a conditional access policy.

Community vote distribution
B (100%)

potpal Highly Voted 3 years, 7 months ago
On test 05.10.21
upvoted 9 times

bk_apex Highly Voted 3 years, 3 months ago
Details can be found here: https://docs.microsoft.com/en-us/azure/active-directory/conditional-access/location-condition
upvoted 8 times

DFFECT Most Recent 2 years, 4 months ago
Correct
upvoted 2 times

Contactfornitish 2 years, 4 months ago
Selected Answer: B
Repeat question
upvoted 2 times

Question #50 *Topic 2*

Note: This question is part of a series of questions that present the same scenario. Each question in the series contains a unique solution that might meet the stated goals. Some question sets might have more than one correct solution, while others might not have a correct solution.
After you answer a question in this section, you will NOT be able to return to it. As a result, these questions will not appear in the review screen.
You have a Microsoft 365 E5 subscription.
You create an account for a new security administrator named SecAdmin1.
You need to ensure that SecAdmin1 can manage Microsoft Defender for Office 365 settings and policies for Microsoft Teams, SharePoint, and OneDrive.
Solution: From the Azure Active Directory admin center, you assign SecAdmin1 the Security administrator role.
Does this meet the goal?

A. Yes

B. No

Suggested Answer: *A*
Reference:
https://docs.microsoft.com/en-us/microsoft-365/security/office-365-security/office-365-atp?view=o365-worldwide

Contactfornitish Highly Voted 2 years, 4 months ago
On exam on 13 aug'22
upvoted 6 times

RenegadeOrange Most Recent 2 years, 3 months ago
Correct.

Additionally it can be done in:

Admin Center - Roles section
Exchange Admin Center - Roles section
Microsoft 365 Defender (security.microsoft.com) - Permissions section
upvoted 3 times

tejb 2 years, 7 months ago
correct
upvoted 3 times

Question #51 *Topic 2*

Note: This question is part of a series of questions that present the same scenario. Each question in the series contains a unique solution that might meet the stated goals. Some question sets might have more than one correct solution, while others might not have a correct solution.
After you answer a question in this section, you will NOT be able to return to it. As a result, these questions will not appear in the review screen.
You have a Microsoft 365 E5 subscription.
You create an account for a new security administrator named SecAdmin1.
You need to ensure that SecAdmin1 can manage Microsoft Defender for Office 365 settings and policies for Microsoft Teams, SharePoint, and OneDrive.
Solution: From the Microsoft 365 admin center, you assign SecAdmin1 the SharePoint admin role.
Does this meet the goal?

A. Yes

B. No

Suggested Answer: *B*
You need to assign the Security Administrator role.
Reference:
https://docs.microsoft.com/en-us/microsoft-365/security/office-365-security/office-365-atp?view=o365-worldwide

Contactfornitish 2 years, 4 months ago
On exam on 13 aug'22
upvoted 4 times

mavexamtops 2 years, 5 months ago
Correct!
upvoted 2 times

Question #52 *Topic 2*

Note: This question is part of a series of questions that present the same scenario. Each question in the series contains a unique solution that might meet the stated goals. Some question sets might have more than one correct solution, while others might not have a correct solution.
After you answer a question in this section, you will NOT be able to return to it. As a result, these questions will not appear in the review screen.
You have a Microsoft 365 E5 subscription.
You create an account for a new security administrator named SecAdmin1.
You need to ensure that SecAdmin1 can manage Microsoft Defender for Office 365 settings and policies for Microsoft Teams, SharePoint, and OneDrive.
Solution: From the Azure Active Directory admin center, you assign SecAdmin1 the Teams Administrator role.
Does this meet the goal?

A. Yes

B. No

Suggested Answer: *B*
You need to assign the Security Administrator role.
Reference:
https://docs.microsoft.com/en-us/microsoft-365/security/office-365-security/office-365-atp?view=o365-worldwide

Contactfornitish 2 years, 4 months ago
On exam on 13 aug'22
upvoted 3 times

mavexamtops 2 years, 5 months ago
Correct!
upvoted 2 times

Question #53 *Topic 2*

You have a Microsoft 365 subscription.
You need to be notified if users receive email containing a file that has a virus.
What should you do?

A. From the Exchange admin center, create an in-place eDiscovery & hold.

B. From the Security & Compliance admin center, create a data governance event.

C. From the Exchange admin center, create an anti-malware policy.

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

Suggested Answer: *C*
Reference:
https://docs.microsoft.com/en-us/office365/servicedescriptions/exchange-online-service-description/anti-spam-and-anti-malware-protection

Community vote distribution
C (100%)

lucidgreen Highly Voted 3 years, 8 months ago
Is this the 3rd time I've seen this question?
upvoted 30 times

harburn422 2 years, 10 months ago
3rd times a charm.
upvoted 6 times

jabbrwcky 3 years, 5 months ago
The third time I've seen this incorrect question!
upvoted 9 times

m43s 2 years, 1 month ago
Yes, I was trying to write the same comment
upvoted 1 times

Jake1 Highly Voted 3 years, 7 months ago
Yes but from Security Admin Center for the 10th time!
upvoted 17 times

Oval61251 Most Recent 2 years ago
dj khaled.....Another one..
Why is this question on here 3 times?!
upvoted 2 times

EliasMartinelli 2 years, 1 month ago
another one haha
upvoted 1 times

Contactfornitish 2 years, 4 months ago
Selected Answer: C
Another repeat question
upvoted 2 times

Pawnzy 3 years, 6 months ago
SAC is the new location, it used to be in EAC
upvoted 6 times

Goseu 3 years, 7 months ago
SAC not EAC
upvoted 5 times

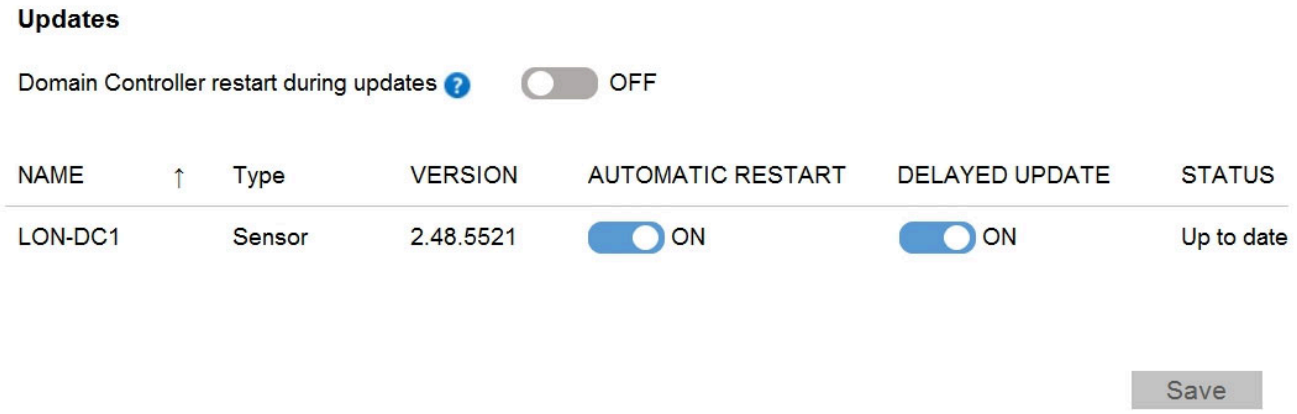
lucidgreen 3 years, 5 months ago
SAC has been separated. It would be just in Security.

upvoted 6 times

Question #54 *Topic 2*

You implement Microsoft Defender for Identity.

You have a Defender for Identity sensor configured as shown in the following exhibit.



How long after the Azure ATP cloud service is updated will the sensor update?

A. 72 hours

B. 12 hours

C. 48 hours

D. 7 days

E. 20 hours

Suggested Answer: *A*

Sensors set to Delayed update are updated on a delay of 72 hours.

References:

https://docs.microsoft.com/en-us/defender-for-identity/sensor-update

Community vote distribution

A (100%)

gxsh Highly Voted 3 years, 1 month ago

Correct, I've seen this on MS-100.

upvoted 6 times

ale2197 2 years, 6 months ago

Me too. Some question seems 1:1 from MS-100 or a clone (same scenario, but different answer

upvoted 2 times

arg_007 Highly Voted 2 years, 10 months ago

Selected Answer: A

Sensors not selected for delayed update are updated automatically, each time the Defender for Identity service is updated. Sensors set to Delayed update are updated on a delay of 72 hours, following the official release of each service update.

upvoted 6 times

L33D Most Recent 2 years, 6 months ago

Still valid, on exam Jun 25, 2022

upvoted 3 times

ATLGATOR688 2 years, 9 months ago

Selected Answer: A

Correct!

upvoted 3 times

Question #55 *Topic 2*

HOTSPOT -

Your company uses Microsoft Defender Advanced Threat Protection (ATP). Microsoft Defender ATP contains the device groups shown in the following table.

Rank	Machine group	Member
1	Group1	Name starts with COMP
2	Group2	Name starts with Comp And OS In Windows 10
3	Group3	OS In Windows Server 2016
Last	Ungrouped machines (default)	*Not applicable*

You onboard computers to Microsoft Defender ATP as shown in the following table.

Name	Operating system
Computer1	Windows 10
Computer2	Windows Server 2016

Of which groups are Computer1 and Computer2 members? To answer, select the appropriate options in the answer area.

NOTE: Each correct selection is worth one point.

Hot Area:

Answer Area

Computer1: ▼
- Group1 only
- Group2 only
- Group1 and Group2
- Ungrouped machines

Computer2: ▼
- Group1 only
- Group3 only
- Group1 and Group3

Suggested Answer:

Answer Area

Computer1: ▼ Group1 only

Computer2: ▼ Group1 only

When a device is matched to more than one group, it is added only to the highest ranked group.

Reference:

https://docs.microsoft.com/en-us/microsoft-365/security/defender-endpoint/machine-groups?view=o365-worldwide

Prianishnikov Highly Voted 3 years, 9 months ago

group 1 for both

upvoted 37 times

Therion90 Highly Voted 3 years, 8 months ago

Indeed Group 1 for both.
https://docs.microsoft.com/en-us/microsoft-365/security/defender-endpoint/machine-groups?view=o365-worldwide half way on the page: When a device is matched to more than one group, it is added only to the highest ranked group.

upvoted 14 times

lucidgreen 3 years, 6 months ago

https://docs.microsoft.com/en-us/microsoft-365/security/defender-endpoint/machine-groups?view=o365-worldwide#manage-device-groups

upvoted 2 times

Powerplay27 Most Recent 1 year, 6 months ago

Case sensitive no?

So for me:

Computer 1 = Group 2 "And statement removes Comp 2"
Computer 2 = Group 3

upvoted 1 times

GotDamnImIn 1 year, 8 months ago

Correct: Group1 and Group1 because only the highest rank applies, you ignore the rest.

upvoted 2 times

Lelek 1 year, 10 months ago

I disagree with the answer.

I understand that when Microsoft Defender ATP applies the policy, it applies it to the group with the highest rank.

https://docs.microsoft.com/en-us/microsoft-365/security/defender-endpoint/machine-groups?view=o365-worldwide

But if you look at the question, that's not it. "Of which groups are Computer1 and Computer2 members?", that is, he wants to know in which group inserted in the computer, so the answer would be "Computer1 - Group1 and Group2". At no point does it ask which policy it will apply for Microsoft Defender ATP, If it were this question, I agree that it would be group1 only.

The same thing when he asks "Computer2", that is, again he asks about group members and not what policy will apply in ATP, so the answer would be " Group1 and Group3"

Final anwser
Computer1 - Group1 and Group2
Computer2 - Group1 and Group3

upvoted 3 times

ChizzyO 1 year, 6 months ago

I had the same thinking like you did and had to look at the question as well as the link: https://docs.microsoft.com/en-us/microsoft-365/security/defender-endpoint/machine-groups?view=o365-worldwide#manage-device-groups

The question asks of which groups are Computer 1 and Computer 2 members which requires the groups the computers plurally are members of. Here, you take Computer 1 and start matching to the device groups and the rule takes precedence. We do the same for Computer 2 and end up with Group 1 as answers for both computers.

upvoted 1 times

vanr2000 1 year, 8 months ago

Trying to confuse people?

upvoted 4 times

encxorblood 2 years ago

Group 1 and Group 1 - If a device in this group matches groups with a higher rank, it will show in the preview but will only be added to the group with the highest rank.

upvoted 2 times

Crixsus 2 years, 2 months ago

On exam today 23 Oct 2022. I answered group 1 and 2, then 1 and 3. Think I got this wrong but I passed. I must have missed the ranks column.

upvoted 2 times

rrrr5r 2 years, 3 months ago

In Sep 16th 22's exam.

upvoted 5 times

venwaik 2 years, 7 months ago

Group 1 for both. Came on exam 09-05-2022

upvoted 4 times

AlexBa 3 years ago

Group 1 for both.

For the group detection we are " Start with" or "Equal", so no sensitive in this case.

upvoted 2 times

MartiFC 3 years, 2 months ago

Isn't case sensitive? COMP vs Comp

upvoted 7 times

TechMinerUK 2 years, 2 months ago

It's not case sensitive from personal experience as most items relating to searching computer names are not case sensitive due to the issues it would cause

upvoted 4 times

Domza 3 years, 4 months ago

Grp 1 for both. As many of you point out, "If a device is also matched to other groups, it's added only to the highest ranked device group". Thx you all.

upvoted 5 times

LoremanReturns 3 years, 5 months ago

The right answer is Group 1 only for both: https://docs.microsoft.com/en-us/microsoft-365/security/defender-endpoint/machine-groups?view=o365-worldwide "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."

upvoted 5 times

EngrTahir 3 years, 6 months ago

Computer1 Group2 Only, Computer2 Group3 Only

upvoted 3 times

toontjeharder 3 years, 7 months ago

Isn't it Group 2 for Computer1? Because it starts with comp AND had Windows 10 OS and not just comp?

upvoted 1 times

Jake1 3 years, 9 months ago

I don't think the names are case sensitive. That would require multiple policies or a renaming requirement for devices. I go with Group 1 for both.

upvoted 6 times

ALPHA_DELTA 3 years, 9 months ago

"You can promote or demote the rank of a device group so that it is given higher or lower priority during matching. When a device is matched to more than one group, it is added only to the highest ranked group."

I believe group matching is case sensitive as well. So the answers should be Group 2 only and Group 3 only

https://docs.microsoft.com/en-us/microsoft-365/security/defender-endpoint/machine-groups?view=o365-worldwide

upvoted 3 times

ALPHA_DELTA 3 years, 9 months ago

I was wrong. Just found this thread on whether groups are case sensitive. They are not.

Should be group 1 for both

https://www.examtopics.com/discussions/microsoft/view/9954-exam-ms-101-topic-2-question-20-discussion/

upvoted 14 times

Question #56 *Topic 2*

You have Windows 10 devices that are managed by using Microsoft Endpoint Manager.
You need to configure the security settings in Microsoft Edge.
What should you create in Microsoft Endpoint Manager?

A. an app configuration policy

B. an app

C. a device configuration profile

D. a device compliance policy

Suggested Answer: *C*
Reference:
https://docs.microsoft.com/en-us/deployedge/configure-edge-with-intune

Goena Highly Voted 3 years, 6 months ago
The answer is correct: C
upvoted 15 times

DiscGolfer 3 years, 1 month ago
Correct Answer is C
https://docs.microsoft.com/en-us/deployedge/configure-edge-with-intune#use-administrative-templates-to-create-a-policy-for-microsoft-edge
upvoted 6 times

mustafanot Most Recent 1 year, 11 months ago
was in the exam on December 22
upvoted 2 times

RenegadeOrange 2 years, 3 months ago
Correct and as mentioned in other comments you can also do it with Endpoint Security...Security baselines... Microsoft Edge Baseline
upvoted 2 times

LillyLiver 2 years, 10 months ago
So, what's the difference between the app configuration policy and a device configuration policy? is the app config policy only for Android and iOS?

That's what it seems according to https://docs.microsoft.com/en-us/mem/intune/apps/app-configuration-policies-overview#:~:text=App%20configuration%20policies%20can%20help%20you%20eliminate%20app,device%2C%20and%20end-users%20don%27t%20need%20to%20take%20action.
upvoted 3 times

TechMinerUK 2 years, 2 months ago
AppConfiguration policies are used for iOS and Android devices to configure specific settings for an app e.g. change themes in Outlook, focussed inbox and also to grant permissions for the app on the device.

There is no AppConfiguration policy for Windows or macOS meaning any configurations need to be done via OMA-URI, Administrative Template or Device Restriction policies all of which are Device Configuration policies
upvoted 5 times

goape 3 years ago
Not sure this is still valid? Edge Security Baseline under Endpoint Security > Baselines would surely cover Edge security settings...
upvoted 3 times

Csed 2 years, 11 months ago
You are right, baselines are in the Endpoint security area, however when you go there rather than to Configuration Profiles in Devices, you will see that you are still creating a "Configuration Profile" same settings assignments, etc. Also the settings for edge are in the Settings catalog and are marked as Preview as of 25 Jan 2022.
upvoted 2 times

Question #57 *Topic 2*

HOTSPOT -

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

Name	Role
User1	Global admin
User2	*None*
User3	*None*

You provision the private store in Microsoft Store for Business.

You assign Microsoft Store for Business roles to the users as shown in the following table.

Name	Role
User1	*None*
User2	Purchaser
User3	Basic Purchaser

You need to identify which users can add apps to the private store, and which users can assign apps from Microsoft Store for Business.

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

Can add apps to the private store:
- User2 only
- User1 and User2 only
- User2 and User3 only
- User1, User2, and User3

Can assign apps from Microsoft Store for Business:
- User2 only
- User1 and User2 only
- User2 and User3 only
- User1, User2, and User3

Suggested Answer:

Answer Area

Can add apps to the private store:
- User2 only
- **User1 and User2 only**
- User2 and User3 only
- User1, User2, and User3

Can assign apps from Microsoft Store for Business:
- User2 only
- User1 and User2 only
- User2 and User3 only
- **User1, User2, and User3**

Reference:

https://docs.microsoft.com/en-us/microsoft-store/roles-and-permissions-microsoft-store-for-business https://docs.microsoft.com/en-us/education/windows/education-scenarios-store-for-business#basic-purchaser-role

sh_gu Highly Voted 3 years, 5 months ago

Answer 1. User1, User2

Answer 2. User1, User2
Microsoft Store for Business only Purchaser, Global admin
Basic Purchaser is Microsoft Store for "EDUCATION"

Right?
upvoted 24 times

JT19760106 2 years, 11 months ago
No, it may have been the case 6 months ago, but as of 1/18/2022 Basic Purchaser is available in the Microsoft Store for BUSINESS and they can assign apps to users.
Answer given is correct:
Answer 1. User 1, User 2
Answer 2. User 1, User 2, User 3
upvoted 9 times

JT19760106 2 years, 11 months ago
Answer 2. User 1, User 2, while Basic Purchaser role is available they can only procure apps for themselves and cannot assign apps.
upvoted 3 times

LillyLiver 2 years, 10 months ago
According to the test I just did in my tenant, the Basic Purchaser (BP) can't the current state of the Microsoft Store (whether for Business, or Business and Education). The BP can't assign apps from the public store.

So I would answer User1/2 for both.
upvoted 7 times

Bulldozzer 2 years, 10 months ago
I agree. These are the correct answers.
upvoted 3 times

TechMinerUK 2 years, 2 months ago
I agree with sh_gu it is 1&2 for both answers as Purchaser role allows the user to add any apps which they have purchased (But not already purchased apps) and although Basic Purchaser may work on Education tenants Microsoft cleared it up a few months back that it in fact is still missing the functionality on standard Business tenants
upvoted 1 times

junior6995 Highly Voted 2 years, 11 months ago
Very likely this question is not valid anymore, BASIC PURCHASER doesn't exist anymore, please check the updated roles for MS Store

https://docs.microsoft.com/en-us/microsoft-store/roles-and-permissions-microsoft-store-for-business
upvoted 9 times

RenegadeOrange Most Recent 2 years, 3 months ago
I doubt this question will be on the exam:

Starting on April 14th, 2021, only free apps will be available in Microsoft Store for Business and Education.

With regards to the answer, I'd say User1, User2, User3 for both because a basic purchaser can purchase and assign apps (but only those they purchase themselves, not those purchased by others) and the question does not mention apps purchased by others.

https://learn.microsoft.com/en-us/microsoft-store/microsoft-store-for-business-overview
upvoted 2 times

ilma_nl 2 years, 3 months ago
both are user1 and user2
https://docs.microsoft.com/en-us/microsoft-store/microsoft-store-for-business-overview
basic purchaser only for education and own apps
upvoted 1 times

AVR31 2 years, 5 months ago
Global Admins can add apps to the store.
"Global Administrator and Billing Administrator - IT Pros with these accounts have full access to Microsoft Store. They can do everything allowed in the Microsoft Store Admin role, plus they can sign up for Microsoft Store."

from here:
https://docs.microsoft.com/en-us/microsoft-store/roles-and-permissions-microsoft-store-for-business

So both answers are "all users".
upvoted 1 times

haazybanj 2 years, 11 months ago
By default, when a teacher with a work or school account signs up for Microsoft Store for Education, the Basic Purchaser role is assigned to them. Basic Purchaser role allows
teachers to:

https://docs.microsoft.com/en-us/education/windows/education-scenarios-store-for-business#basic-purchaser-role

Answer 1: User 1 and 2
Answer2: User 1 ,2 and 3
upvoted 2 times

JT19760106 2 years, 11 months ago
Enough with the teacher/Education talk. This is Microsoft Store for BUSINESS and YES the basic purchaser role is available and can assign apps. I've tested this in my lab.
upvoted 3 times

us3r 3 years ago
According the below link, only the MS Store for business Admin can add apps to the private store. I assume that GA is MS Store for Business admin, so answers below:

Can add apps to private store: User1 (not in the answers, I believe it is a typo)
Can assign apps to Microsoft Store for Business: USer1 and User2

****
Distribute apps - Distribute apps that are in your inventory.

Admins can assign apps to people, add apps to the private store, or use a management tool.
Purchasers can assign apps to people.
***

https://docs.microsoft.com/en-us/microsoft-store/roles-and-permissions-microsoft-store-for-business
upvoted 2 times

FreddyLao 3 years ago
from your link.
acquire app = add app.
both GA and MS Store Admin can Acquire apps & Distribute apps.
so both answers are User 1 & User 2.
since User 3 is Basic Purchaser role, he has nothing to do in MS Store for Business here.
upvoted 3 times

allesglar 3 years ago
The answers are correct. This setting exists also for "MS Store for Business" and wouldn't make sense if this role wasn't also there available. Make everyone a Basic Purchaser Allow everyone in your organization to automatically become a Basic Purchaser. This allows them to purchase apps and manage them. For more information, see Make everyone a Basic Purchaser. Settings - Shop

https://docs.microsoft.com/en-us/microsoft-store/settings-reference-microsoft-store-for-business
upvoted 1 times

TimurKazan 3 years ago
user 1 and user 2 for both.
upvoted 2 times

jkklim 3 years, 1 month ago

BASIC PURCHASER ROLE available in Education Store only.
upvoted 4 times

JT19760106 2 years, 11 months ago
BASIC PURCHASER ROLE is available in the BUSINESS Store too, but they can't assign apps to other users.
upvoted 2 times

Domza 3 years, 4 months ago
Boys and girls, this is ONLY "private store in MS for Business".
>Basic Purchaser is for Teachers only. (as many of you point out)
There is NO "Education" in the question. Please read carefully.
upvoted 3 times

haazybanj 2 years, 11 months ago
Is there any link for this?
upvoted 1 times

JT19760106 2 years, 11 months ago
https://docs.microsoft.com/en-us/microsoft-store/microsoft-store-for-business-overview#set-up
upvoted 1 times

larnyx 3 years, 4 months ago
I'd go for User 1 & 2 on both answers as Basic Purchaser is only valid in the Education version of the store and not Business
upvoted 2 times

MomoLomo 3 years, 4 months ago
yup same
upvoted 1 times

donathon 3 years, 4 months ago
Both are user1 and user 2. User1 is a GA so he can do anything. Since there is no such option as User1 only, we assume that allow everyone to shop is disabled. Basic Purchaser is only for Microsoft Store for Education. https://docs.microsoft.com/en-us/microsoft-store/acquire-apps-microsoft-store-for-business#allow-users-to-shop
https://docs.microsoft.com/en-us/microsoft-store/roles-and-permissions-microsoft-store-for-business
upvoted 1 times

LoremanReturns 3 years, 5 months ago
Basic Purchaser is for Microsoft Store for Education only.
Can acquire and manage Minecraft: Education Edition, and other apps from Store for Education
Can only manage (assign and reclaim licenses) for apps that they purchased. They can't manage apps purchased by people with Purchaser or Admin roles.
The question is generic on the ability to add and assing Apps, in my opinion answer is: User1, User2 and User3 on both
upvoted 1 times

LoremanReturns 3 years, 5 months ago
Sorry read the question with more attention, the second one asks for Microsoft Store for Business. Answers are correct
upvoted 3 times

LoremanReturns 3 years, 5 months ago
Answer 1 User1, User2 and User3
Answer 2 User1 and User2 only
upvoted 2 times

lucidgreen 3 years, 6 months ago
It seems the difference between a basic purchaser and purchaser is that they can only manage apps they've purchased. All other apps in the store would be available to those assigned by the Global Admin or Purchaser. It would make sense that they couldn't add them to the global store. Perhaps a sub category store place within the business or education store?
upvoted 5 times

lucidgreen 3 years, 5 months ago
The answers are correct, btw.
upvoted 1 times

lucidgreen 3 years, 5 months ago
Basic Purchaser role may be coming to the Microsoft Store for Business in 2023, I think. This role is meant for teachers to be able to assign apps to their students. It would make sense if we let managers assign apps to their employees, but as an IT guy, this makes me

cringe with horror stories of the Wild West.
If we're going by the fact that Basic Purchaser doesn't exist in the store for business, then it would still be 1 and 2, but I don't know why they say they can assign the role. They try to trick you with stupid stuff like this.
Long story shortened, I've seen current documentation that says this role isn't available for Enterprise but it is available for Education.
upvoted 2 times

MomoLomo 3 years, 4 months ago
btw i always look for your answers on the questions

keep rocking dude
upvoted 5 times

MomoLomo 3 years, 4 months ago
that was 1 month ago now if u see the docs

Microsoft Store for Business and Microsoft Store for Education will be retired in the first quarter of 2023. You can continue to use the current capabilities of free apps until that time. For more information about this change, see Evolving the Microsoft Store for Business and Education.
upvoted 2 times

Question #58 *Topic 2*

DRAG DROP -

You have a Microsoft 365 subscription.

You have the devices shown in the following table.

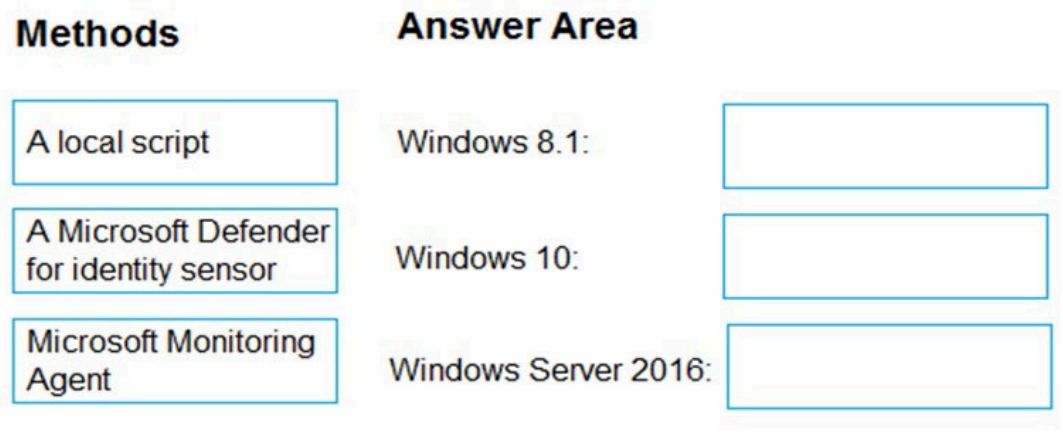
Operating system	Quantity
Windows 8.1	5
Windows 10	5
Windows Server 2016	5

You need to onboard the devices to Microsoft Defender for Endpoint. The solution must avoid installing software on the devices whenever possible.

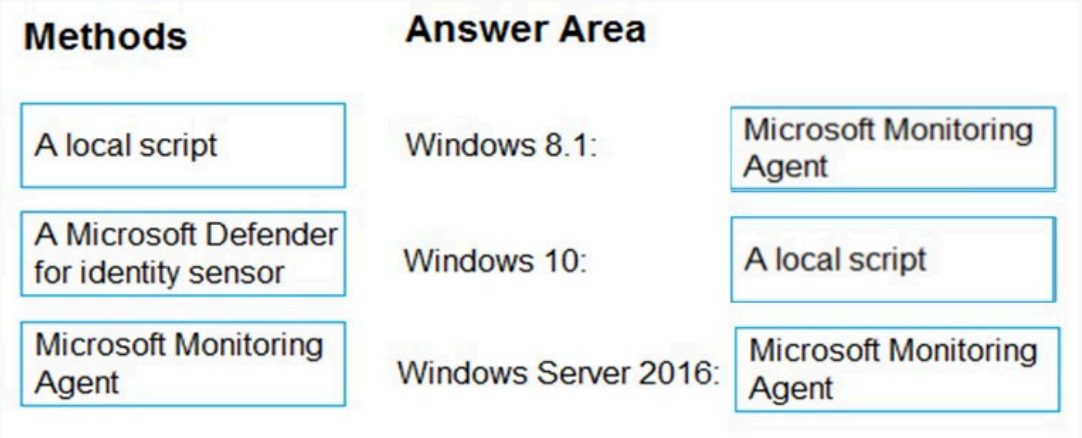
Which onboarding method should you use for each operating system? To answer, drag the appropriate methods to the correct operating systems. Each method may be used once, more than once, or not at all. You may need to drag the split bar between panes or scroll to view content.

NOTE: Each correct selection is worth one point.

Select and Place:



Suggested Answer:



Reference:

https://docs.microsoft.com/en-us/microsoft-365/security/defender-endpoint/onboard-downlevel?view=o365-worldwide

https://docs.microsoft.com/en-us/microsoft-365/security/defender-endpoint/configure-endpoints?view=o365-worldwide

https://docs.microsoft.com/en-us/microsoft-365/security/defender-endpoint/configure-server-endpoints?view=o365-worldwide

ubt Highly Voted 3 years, 1 month ago

As per link supplied in Answer

MMA - Win8.1

Local Script - Win10 / Server 2016

https://docs.microsoft.com/en-us/microsoft-365/security/defender-endpoint/configure-endpoints?view=o365-worldwide

upvoted 28 times

ajiejeng 2 years, 3 months ago

thanks! looks correct from the referral link itself

upvoted 1 times

Feyenoord 1 year, 8 months ago

https://learn.microsoft.com/en-us/microsoft-365/security/defender-endpoint/onboard-windows-server?view=o365-worldwide#windows-server-onboarding-overview

upvoted 1 times

Contactfornitish Highly Voted 2 years, 4 months ago

On exam on 13 aug'22

upvoted 7 times

Debadatta Most Recent 1 year, 5 months ago

MMA

Local Script

Local Script

https://learn.microsoft.com/en-us/microsoft-365/security/defender-endpoint/onboard-windows-client?view=o365-worldwide

upvoted 1 times

Jame 1 year, 12 months ago

MMA

Local Script

MMA

These offboarding instructions for other Windows server versions also apply if you are running the previous Microsoft Defender for Endpoint for Windows Server 2016 and Windows Server 2012 R2 that requires the MMA. Instructions to migrate to the new unified solution are at Server migration scenarios in Microsoft Defender for Endpoint.

https://learn.microsoft.com/en-us/microsoft-365/security/defender-endpoint/configure-server-endpoints?view=o365-worldwide

upvoted 1 times

JakeLi 1 year, 11 months ago

Correct.

The previous implementation (before April of 2022) of onboarding Windows Server 2012 R2 and Windows Server 2016 required the use of Microsoft Monitoring Agent (MMA).

The new unified solution package makes it easier to onboard servers by removing dependencies and installation steps. It also provides a much expanded feature set.

upvoted 2 times

EsamiTopici 1 year, 10 months ago

MMA

Local Script

Local Script

https://learn.microsoft.com/en-us/microsoft-365/security/defender-endpoint/onboard-windows-client?view=o365-worldwide

no?

upvoted 5 times

encxorblood 2 years ago

MMA - Script - Script

upvoted 2 times

TechMinerUK 2 years, 2 months ago

This question seems to be missing out information as based on new information from Microsoft you can onboard Windows 10 via script (For 10 or fewer devices) and for Windows Server 2012 R2 and 2016 you can use the "Unified Solution" as mentioned here:

https://learn.microsoft.com/en-us/microsoft-365/security/defender-endpoint/configure-server-endpoints?view=o365-worldwide

Now the answer for script for Windows 10 and Windows Server 2016 would depend on if you define the Unified Solution as a script or an app. On the Defender portal it defines it as a script which would lead to MMA, Script, Script being correct

Personally I believe for this particular question it would be MMA for Windows Server 2012 R2 and Windows Server 2016 as it comes from a time when there was no Unified Solution, if it were asked on an exam now I would imagine it would be phrased differently or have different options to choose from

upvoted 1 times

reastman66 2 years, 6 months ago

As of right now it looks like Window 8.1 is Install Monitoring Agent, Windows 10 Local Script up to 10 devices and Windows 2012R2 and 2016 Local Script up to 10 devices.
upvoted 2 times

L33D 2 years, 6 months ago
Still valid, on exam Jun 25, 2022
upvoted 4 times

L33D 2 years, 6 months ago
The previous implementation of onboarding Windows Server 2012 R2 and Windows Server 2016 required the use of Microsoft Monitoring Agent (MMA). The new unified solution package makes it easier to onboard servers by removing dependencies and installation steps.
https://docs.microsoft.com/en-us/microsoft-365/security/defender-endpoint/configure-server-endpoints?view=o365-worldwide#new-windows-server-2012-r2-and-2016-functionality-in-the-modern-unified-solution
upvoted 1 times

JAPo123 2 years, 10 months ago
Microsoft Defender Security --> Settings --> Device management --> Onboarding --> Select Windows Server 2008.....and 2016 --> Step 2 is Install Microsoft Monitoring Agent
upvoted 2 times

LillyLiver 2 years, 10 months ago
This question may be updated in the 101 exam since 2/18/2022. For Server 12R2 and 16 there is a new "Unified solution" and the Monitoring Agent may not be the correct answer. Watch for that in the exam...

https://docs.microsoft.com/en-us/microsoft-365/security/defender-endpoint/configure-server-endpoints?view=o365-worldwide
upvoted 4 times

TimurKazan 3 years ago
had this question in MS-100 exam a while ago. Answer is correct
upvoted 3 times

JT19760106 2 years, 11 months ago
I'm curious, how would you know it's correct based on seeing it in the MS-100? Did you get a 1000 on that exam?
upvoted 19 times

[Removed] 3 years ago
friggin MS!! This question should of mentioned whether it POC or Production - Scripts are for POC only. Also, Microsoft Monitoring Agent is now Azure Log Analytics agent, it will change in the exam so watch for it!
upvoted 1 times

veteran_tech 2 years, 4 months ago
Azure Log Analytics agent will soon replace Azure Monitor Agent. https://docs.microsoft.com/en-us/azure/azure-monitor/agents/azure-monitor-agent-migration
upvoted 1 times

jkklim 3 years, 1 month ago
windows 8.1 ==> MMA
WINDOWS 10 ==> LOCAL SCRIPT up to 10 machines
windows 2016 ==> local script

local script max total of 10 machines (requirements of the question is The solution must avoid installing software on the devices whenever possible), therefore Windows server2016 cannot use MSI to install (which is recommended by MS)

NOTE: A local script is suitable for a proof of concept but should not be used for production deployment. For a production deployment, we recommend using Group Policy, Microsoft Endpoint Configuration Manager, or Intune.
upvoted 2 times

helpdeskinfra 3 years, 1 month ago
Windows 81 --> Microsoft Monitoring Agent (MMA)
Windows 10 & Server 2016 --> Local script
As there are 10 devices in W10 and Win2016, we can use local scripts which is the upper.

If more, you must use another method.
https://docs.microsoft.com/en-us/microsoft-365/security/defender-endpoint/switch-to-microsoft-defender-onboard?view=o365-worldwide
upvoted 2 times

Question #59 *Topic 2*

The users at your company use Dropbox Business to store documents. The users access Dropbox Business by using the MyApps portal. You need to ensure that user access to Dropbox Business is authenticated by using a Microsoft 365 identity. The documents must be protected if the data is downloaded to a device that is not trusted.
What should you do?

A. From the Azure Active Directory admin center, configure conditional access settings.

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

C. From the Azure Active Directory admin center, configure organizational relationships settings.

D. From the Endpoint Manager admin center, configure device enrollment settings.

Suggested Answer: *A*
Reference:
https://docs.microsoft.com/en-us/microsoft-365/campaigns/m365-campaigns-conditional-access?view=o365-worldwide
https://docs.microsoft.com/en-us/azure/active-directory/conditional-access/concept-conditional-access-conditions

Community vote distribution
A (100%)

FleurJ Highly Voted 3 years ago
Selected Answer: A
https://docs.microsoft.com/en-us/defender-cloud-apps/use-case-proxy-block-session-aad#create-a-block-download-policy-for-unmanaged-devices
upvoted 9 times

[Removed] 3 years ago
Great stuff, thx. You need a conditional access policy AND a microsoft defender for cloud apps (mcas) session policy.
upvoted 7 times

ServerBrain Most Recent 2 years, 1 month ago
Selected Answer: A
Key words - " ensure that user access to Dropbox Business is authenticated "
Answer is correct..
upvoted 1 times

Chris_Rock 3 years, 3 months ago
All answers seem to be wrong here. This is Azure Active Directory's Application Proxy. Which allow you single Sing on to azure AD and then access cloud app or local app
upvoted 1 times

JT19760106 2 years, 11 months ago
You are funny Chris Rock. AAD App Proxy is used as a reverse proxy to internal resources. MCAS Session Policy coupled with Azure AD Conditional Access Policy can be used as a proxy for SaaS apps.
upvoted 8 times

rfox321 3 years, 3 months ago
I believe the answer is correct. You can create a conditional access policy, apply it to the cloud app "Drop Box" after it's registered, then make the condition "Non-compliant devices," and Deny access.
upvoted 17 times

Question #60 *Topic 2*

Note: This question is part of a series of questions that present the same scenario. Each question in the series contains a unique solution that might meet the stated goals. Some question sets might have more than one correct solution, while others might not have a correct solution.
After you answer a question in this section, you will NOT be able to return to it. As a result, these questions will not appear in the review screen.
You have a Microsoft 365 subscription.
You discover that some external users accessed content on a Microsoft SharePoint site. You modify the SharePoint sharing policy to prevent sharing outside your organization.
You need to be notified if the SharePoint sharing policy is modified in the future.
Solution: From the SharePoint admin center, you modify the sharing settings.
Does this meet the goal?

A. Yes

B. No

Suggested Answer: *B*

Myko Highly Voted 4 years, 4 months ago
Create an alert policy, and select "Changed a sharing policy" as the activity.
upvoted 17 times

neo124t Highly Voted 4 years, 7 months ago
Answer: No
Use Audit logs
upvoted 13 times

Contactfornitish Most Recent 2 years, 4 months ago
On exam on 13 aug'22
upvoted 4 times

L33D 2 years, 6 months ago
Still valid, on exam Jun 25, 2022
upvoted 2 times

airairo 3 years, 7 months ago
- Policy -> Sharing

File and folder links
Choose the type of link that's selected by default when users share files and folders in SharePoint and OneDrive.
1- Specific ppl
2- only ppl in your org.
3- anyone with the link
upvoted 1 times

mkoprivnj 3 years, 11 months ago
No is correct!
upvoted 5 times

Mr01z0 4 years, 2 months ago
You need to be notified if the SharePoint sharing policy is modified in the future.
Solution: From the SharePoint admin center, you modify the sharing settings.
Does this meet the goal?

No

From https://security.microsoft.com/securitypolicies Create an Office 365 alert policy, and select "Changed a sharing policy" as the activity. and select to be notified trough an email every time this happens.

upvoted 10 times

ajna_ 2 years, 10 months ago

Thank you.

upvoted 1 times

Alvaroll 4 years, 2 months ago

Same as MS-100 Topic3-25 https://www.examtopics.com/exams/microsoft/ms-100/view/21/

upvoted 3 times

diggity801 4 years, 9 months ago

https://docs.microsoft.com/en-us/microsoft-365/compliance/use-sharing-auditing?view=o365-worldwide

upvoted 2 times

Question #61 *Topic 2*

Note: This question is part of a series of questions that present the same scenario. Each question in the series contains a unique solution that might meet the stated goals. Some question sets might have more than one correct solution, while others might not have a correct solution.
After you answer a question in this section, you will NOT be able to return to it. As a result, these questions will not appear in the review screen.
You have a Microsoft 365 subscription.
You need to prevent users from accessing your Microsoft SharePoint Online sites unless the users are connected to your on-premises network.
Solution: From the Device Management admin center, you create a trusted location and a compliance policy
Does this meet the goal?

A. Yes

B. No

Suggested Answer: *B*
Conditional Access in SharePoint Online can be configured to use an IP Address white list to allow access.
References:
https://techcommunity.microsoft.com/t5/Microsoft-SharePoint-Blog/Conditional-Access-in-SharePoint-Online-and-OneDrive-for/ba-p/46678

potpal Highly Voted 3 years, 7 months ago
On test 05.10.21
upvoted 10 times

NitishKarmakar Most Recent 1 year, 3 months ago
Yes, we can do it now. DMAC moved to Azure (somewhere in 2018 or later) and then to Intune (Now).

https://techcommunity.microsoft.com/t5/microsoft-365-admin-center/device-management-portal/m-p/162752

From Intune, you can create both named locations and a Conditional Access policy. Tested and verified in the tenant as of 28-Sep-2023.
Intune > Home > Devices |Conditionala access > Conditional Access
upvoted 1 times

Jake1 3 years, 9 months ago
TonySuccess is correct. From AAD Security you create the named location and CAP.
upvoted 3 times

TechMinerUK 2 years, 2 months ago
It should be known as well you can create a Conditional Access policy from the endpoint.microsoft.com portal however the answer in the question is still incorrect since it mentions compliance and not Conditional Access
upvoted 1 times

DeeJayU 3 years, 11 months ago
This is another possible solution to implement the restriction: https://docs.microsoft.com/en-US/sharepoint/control-access-based-on-network-location
upvoted 2 times

TaSpanja 4 years, 5 months ago
why not yes this works i do it all the time?
upvoted 2 times

TonySuccess 4 years, 5 months ago
Because you create the Conditional Access Policy from the Security and Compliance Admin Centre, not the DMAC.
upvoted 9 times

TonySuccess 4 years, 5 months ago
I meant to type Azure Active Directory Admin Centre (portal.azure.com - Security). Clearly been at the laptop too long today.

Create the named location and then CAP.

upvoted 8 times

test123123 4 years ago

:D good catch

upvoted 1 times

diggity801 4 years, 9 months ago

Yes, it does?

upvoted 2 times

diggity801 4 years, 9 months ago

nevermind, B is correct.

upvoted 3 times

Question #62 *Topic 2*

Note: This question is part of a series of questions that present the same scenario. Each question in the series contains a unique solution that might meet the stated goals. Some question sets might have more than one correct solution, while others might not have a correct solution.
After you answer a question in this section, you will NOT be able to return to it. As a result, these questions will not appear in the review screen.
You have a Microsoft 365 subscription.
You need to prevent users from accessing your Microsoft SharePoint Online sites unless the users are connected to your on-premises network.
Solution: From the Microsoft 365 admin center, you configure the Organization profile settings.
Does this meet the goal?

A. Yes

B. No

Suggested Answer: *B*
Conditional Access in SharePoint Online can be configured to use an IP Address white list to allow access.
References:
https://techcommunity.microsoft.com/t5/Microsoft-SharePoint-Blog/Conditional-Access-in-SharePoint-Online-and-OneDrive-for/ba-p/46678A

Community vote distribution
B (100%)

Snaypi Highly Voted 3 years, 10 months ago
B - Correct answer ;)
upvoted 8 times

Lelek Most Recent 1 year, 10 months ago
Selected Answer: B
B is correct Answer
upvoted 1 times

Question #63 *Topic 2*

Note: This question is part of a series of questions that present the same scenario. Each question in the series contains a unique solution that might meet the stated goals. Some question sets might have more than one correct solution, while others might not have a correct solution.
After you answer a question in this section, you will NOT be able to return to it. As a result, these questions will not appear in the review screen.
You have a Microsoft 365 subscription.
You need to prevent users from accessing your Microsoft SharePoint Online sites unless the users are connected to your on-premises network.
Solution: From the Azure Active Directory admin center, you create a trusted location and a conditional access policy.
Does this meet the goal?

A. Yes

B. No

Suggested Answer: *A*
Conditional Access in SharePoint Online can be configured to use an IP Address white list to allow access.
References:
https://docs.microsoft.com/en-us/azure/active-directory/conditional-access/location-condition
https://techcommunity.microsoft.com/t5/Microsoft-SharePoint-Blog/Conditional-Access-in-SharePoint-Online-and-OneDrive-for/ba-p/46678

zzuk01 Highly Voted 4 years, 12 months ago
Answer is A, you create a Conditional Access policy from the Azure Active directory admin centre
upvoted 41 times

Sonia33 Highly Voted 4 years, 7 months ago
It's A, you use a conditional access policy after defining your trusted location. At the Cloud apps tab, you select only Sharepoint Online. So the statement is correct, YES.
upvoted 9 times

VTHAR Most Recent 4 years, 2 months ago
Answer is A.YES it does meet the goal. Conditional Access policy and Named Location (Trusted location) can make SPO only accessible from on-perm network. This is the last of a series of questions in which all prior answers are B. NO. This last one meets the goal.
upvoted 4 times

PJR 3 years, 11 months ago
This is a very sneaky question as immediately people think it must be a CA policy thats needed; however in the SharePoint Online admin center there is a section called Access Control where you can specify the network locations able to access SharePoint Online sites from.

More info here - https://docs.microsoft.com/en-us/sharepoint/control-access-based-on-network-location

So you could achieve this using that and not a CA policy - HOWEVER I still think the Answer is as VTHAR has pointed out, this is the 4th Q in a series and with these types of questions there are always 3 wrong answers and 1 correct.

Plus this question is also shown on this site (Q13) https://www.itexams.com/exam/MS-101#:~:text=You%20need%20to%20prevent%20users,and%20a%20conditional%20access%20policy and shows A as being correct.
upvoted 1 times

itmp 3 years, 10 months ago
why are we talking about other ways to achieve this ?
Does this meet the goal? - yes. Nothing "sneaky" about the question/answer.
upvoted 5 times

TaSpanja 4 years, 5 months ago
this works and you can do it from azure ad, intune and device management all 3 have the options available, i work with these on a daily basis and we do these kinds of policies all the time.
upvoted 3 times

ginsahec 4 years, 8 months ago

The correct answer is A,you can see it at this link:
Q29
https://www.examtopics.com/exams/microsoft/ms-100/view/22/
upvoted 2 times

diggity801 4 years, 9 months ago
I think the most correct answer is B because if you use CA to block Sharepoint Online, it not only block sites, but also blocks teams and planner and myanalytics and newsfeed. Both answers technically can block users based on location but answer A also blocks all of the dependency apps, not just a SharePoint site.
upvoted 3 times

diggity801 4 years, 9 months ago
This is the text CA policies show you when you choose SharePoint online to block: "Selecting SharePoint Online will also affect apps such as Microsoft Teams, Planner, Delve, MyAnalytics, and Newsfeed."
upvoted 1 times

diggity801 4 years, 9 months ago
But CA does technically met the requirement so who knows what they want.
upvoted 2 times

CARO54 4 years, 9 months ago
I think it 's A
upvoted 2 times

SCT 4 years, 10 months ago
Answer is No, This solution applies to users accessing Azure Active Directory, not to users accessing SharePoint Online. Conditional Access in SharePoint Online can be configured to use an IP Address white list to allow access.
upvoted 1 times

hitten_za 4 years, 9 months ago
Don't agree with you here. In the CA policy you specify SharePoint Online as the Cloud App and you set your Location under Conditions. In doing so you're specifying that you must be in a Safe Location in order to gain access to SharePoint Online, so A would be correct.
upvoted 18 times

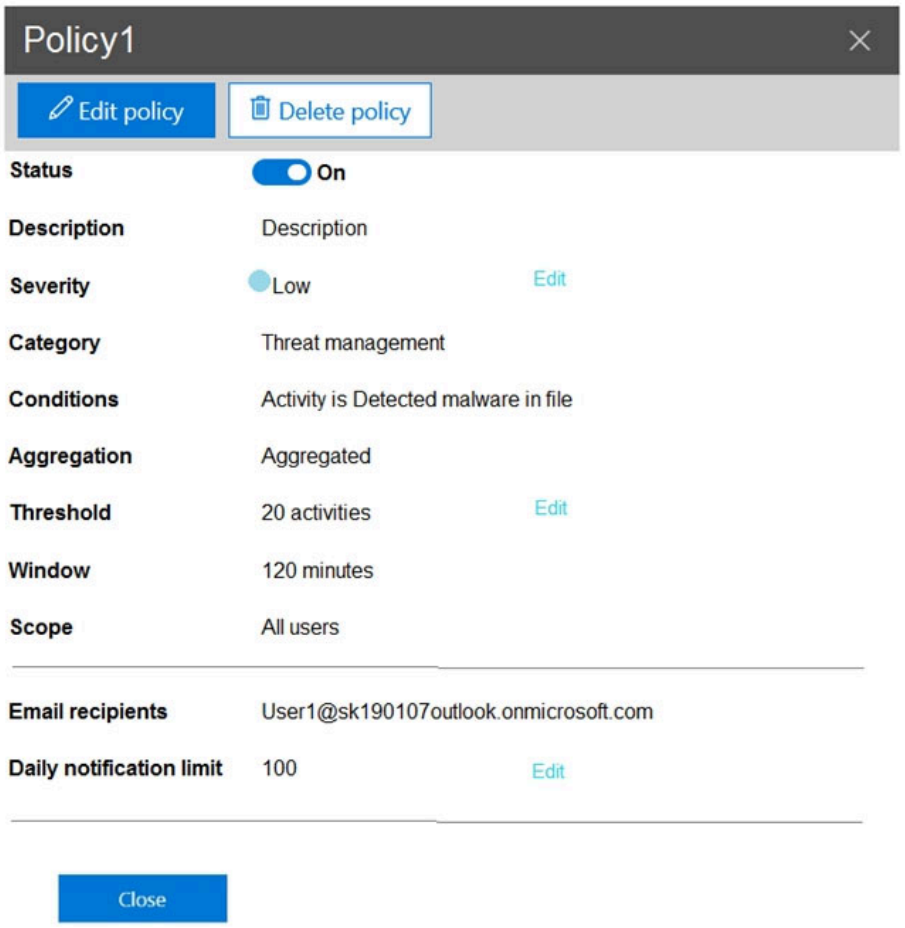
a0977185 5 years ago
Why not Answer A?
upvoted 4 times

Question #64 *Topic 2*

HOTSPOT -

You have Microsoft 365 subscription.

You create an alert policy as shown in the following exhibit.



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

NOTE: Each correct selection is worth one point.

Hot Area:

Answer Area

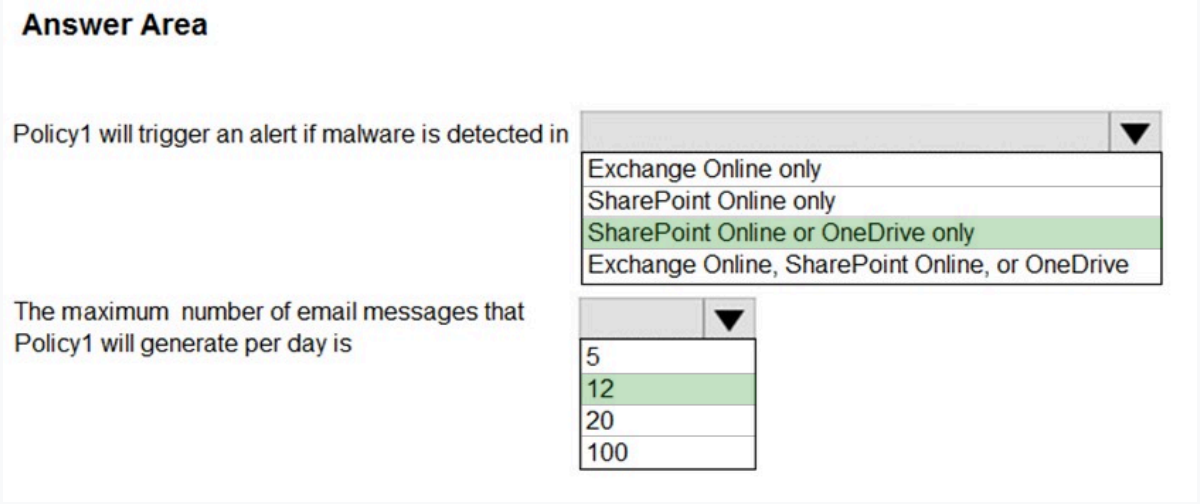
Policy1 will trigger an alert if malware is detected in

- Exchange Online only
- SharePoint Online only
- SharePoint Online or OneDrive only
- Exchange Online, SharePoint Online, or OneDrive

The maximum number of email messages that Policy1 will generate per day is

- 5
- 12
- 20
- 100

Suggested Answer:



Note: The Aggregation settings has a 120 minute window

Jake1 Highly Voted 3 years, 8 months ago

Tested this on my tenant. It's for sure Sharepoint and One Drive only. Every 2 hours it's checked so max 12 alerts a day.

upvoted 41 times

AnoniMouse 3 years, 7 months ago

You are right I have just verified. "Detect malware in file" applies only to SharePoint and OneDrive, so Exchange is excluded here

upvoted 12 times

PersonT Highly Voted 3 years, 9 months ago

mailware in file: Sharepoint & Onedrive

upvoted 11 times

PersonT 3 years, 9 months ago

Daily notification limit 100

upvoted 2 times

Prianishnikov 3 years, 9 months ago

Yes, Agree with you

upvoted 1 times

lucidgreen 3 years, 5 months ago

It's an aggregate alert, with a threshold of so many instances before sending an alert which can only be sent once every 2 hours every day.

The most it can send in a 24-hour period is be 12.

To send 100 messages, it would have to be able to send them every 14 minutes and 24 seconds. Clearly the policy won't allow this.

upvoted 5 times

Prianishnikov 3 years, 9 months ago

Yes, Agree with you

upvoted 1 times

PP39 3 years, 9 months ago

Agree should be sharepoint and onedrive only

upvoted 1 times

ALPHA_DELTA 3 years, 9 months ago

SharePoint Online or One Drive Only

I think the answer is not correct because when you select "Detect malware in file", you will see the explanation which says "Office 365 detected malware in either a SharePoint or OneDrive file". If you want a policy which protect Exchange, I think we need to select "Detect malware in an email message"

12

The policy triggers when there are 20 activities within 120 min (2 hours)

So every 2 hours, the policy checks and if there are more than 20 activities, it sends 1 alert. Since we have 24hours/day, the policy can send a maximum of 1alert/2hours or 12alerts/24hours.

upvoted 13 times

Amir1909 Most Recent 11 months ago

- SharePoint Online or OneDrive only

- 100

upvoted 1 times

Sanjee31 1 year, 6 months ago

in exam 28.6.2023

upvoted 1 times

petersonal 1 year, 10 months ago

Came on exam 2023 February. Answer is correct.

upvoted 1 times

H3adcap 2 years, 4 months ago

Was in exam today 20 Aug 2022

upvoted 7 times

mackzone 2 years, 6 months ago

Came on exam 25-06-2022

upvoted 4 times

rrrr5r 2 years, 3 months ago

In Sep 16th 22's exam.

upvoted 4 times

venwaik 2 years, 7 months ago

Provided answer is correct.. Came on exam 09-05-2022

upvoted 2 times

encxorblood 3 years, 6 months ago

Only Sharepoint and Onedrive. Detect malware in file. Exchange is a other rule as Detect Malware in a email message

upvoted 6 times

lucidgreen 3 years, 5 months ago

This is exactly what I needed to know to get this straight in my head. Thank you!

upvoted 1 times

lucidgreen 3 years, 6 months ago

Saw this one on the test in June.

upvoted 3 times

Question #65 *Topic 2*

You have a Microsoft 365 subscription.
All users have their email stored in Microsoft Exchange Online.
In the mailbox of a user named User1, you need to preserve a copy of all the email messages that contain the word ProjectX.
What should you do?

A. From the Security & Compliance admin center, create a label and a label policy.

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

C. From the Security & Compliance admin center, start a message trace.

D. From Exchange admin center, start a mail flow message trace.

Suggested Answer: *A*
References:
https://docs.microsoft.com/en-us/azure/information-protection/configure-policy-classification

encxorblood Highly Voted 3 years, 6 months ago
Question is older. Now one anser is A. From the Security & Compliance admin center, create an eDiscovery case. And this is correct.
upvoted 31 times

MSGrady Highly Voted 3 years, 8 months ago
Agreed.. mail flow rules also does in place holds and litigation holds
upvoted 7 times

lucidgreen 3 years, 8 months ago
Mail flow doesn't have a functionality to retain a message.
upvoted 10 times

potpal Most Recent 3 years, 7 months ago
On test 05.10.21
upvoted 5 times

lucidgreen 3 years, 8 months ago
Seems A is the most logical answer.
From Security & Compliance:
Classification > Retention labels.
Information governance > Retention.
upvoted 5 times

365admin 3 years, 8 months ago
Mail flow rules applies to messages in transit and not at rest. So i think most likely answer is A
upvoted 2 times

MiZi 3 years, 8 months ago
I would say the hold is a domain of the eDiscovery from the Office 365 Security & Compliance. First, you create a case, then hold selecting places and keywords.
upvoted 4 times

lucidgreen 3 years, 8 months ago
See question 28.
Apparently, there is more than one way to skin this cat...
upvoted 6 times

potpal 3 years, 7 months ago
Both are right one has ediscovery and one has label as an option
upvoted 5 times

TFou0076 3 years, 8 months ago
You want to retain mail containing the word ProjectX, so you need to tag those mails with a label, Answer A.
upvoted 3 times

lucidgreen 3 years, 8 months ago

It would be a if it were "Create a retention label and a retention policy." But I don't think you can do both of those in the same place.

upvoted 2 times

barleyhutcher 3 years, 9 months ago

is it not C?

upvoted 1 times

Rens19991 3 years, 9 months ago

Yes I also think B

upvoted 2 times

Prianishnikov 3 years, 9 months ago

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

https://docs.microsoft.com/en-us/office365/servicedescriptions/exchange-online-service-description/message-policy-and-compliance#mail-flow-rules

upvoted 5 times

Luckyson 3 years, 8 months ago

Mail flow rule will not "preserve copy", you can use it for FW/CC to another mailbox etc., so I guess A is here the right answer.

upvoted 3 times

MSGrady 3 years, 8 months ago

Preserve could mean "archive" and a mail flow rule can do this ... I think

upvoted 1 times

Question #66 *Topic 2*

HOTSPOT -

You have a new Microsoft 365 subscription.

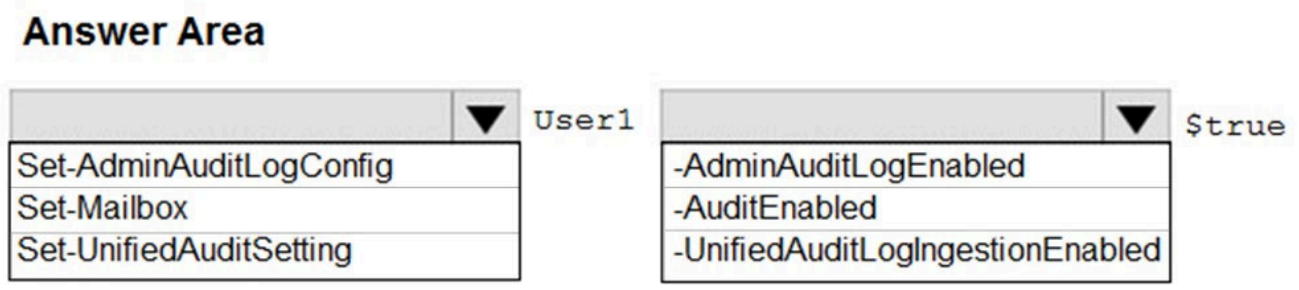
A user named User1 has a mailbox in Microsoft Exchange Online.

You need to log any changes to the mailbox folder permissions of User1.

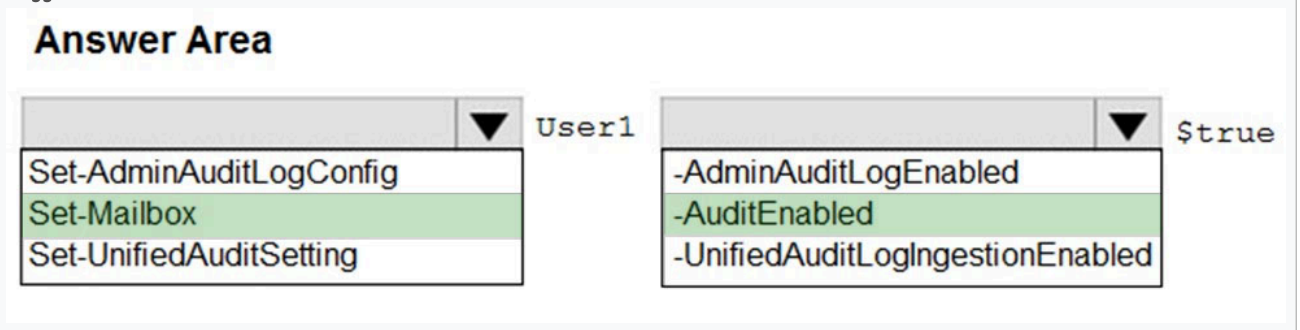
Which command should you run? To answer, select the appropriate options in the answer area.

NOTE: Each correct selection is worth one point.

Hot Area:



Suggested Answer:



To enable auditing for a single mailbox (in this example, belonging to Holly Sharp), use this PowerShell command: Set-Mailbox username -AuditEnabled $true

References:

https://support.microsoft.com/en-us/help/4026501/office-auditing-in-office-365-for-admins https://docs.microsoft.com/en-us/powershell/module/exchange/mailboxes/set-mailbox?view=exchange-ps

potpal Highly Voted 3 years, 7 months ago

On test 05.10.21

upvoted 13 times

gxsh Highly Voted 3 years ago

Answer is correct.

upvoted 6 times

vanr2000 Most Recent 1 year, 8 months ago

The answer is right

The AuditEnabled parameter must be set to $true to enable mailbox audit logging.

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

upvoted 1 times

ServerBrain 2 years, 1 month ago

Correct .. PowerShell 101

upvoted 1 times

EliasMartinelli 2 years, 1 month ago

CORRECT! - On MS-100 Test xx.11.2022

upvoted 1 times

MigrationEndpoint 2 years, 8 months ago

So, Holly Sharp = User1 ;)

upvoted 2 times

Question #67 *Topic 2*

You have a Microsoft 365 subscription.
You recently configured a Microsoft SharePoint Online tenant in the subscription.
You plan to create an alert policy.
You need to ensure that an alert is generated only when malware is detected in more than five documents stored in SharePoint Online during a period of 10 minutes.
What should you do first?

A. Enable Microsoft Office 365 Defender for Cloud Apps.

B. Deploy Microsoft Defender Advanced Threat Protection (Microsoft Defender ATP)

C. Enable Microsoft Office 365 Analytics.

Suggested Answer: *A*
Reference:
https://docs.microsoft.com/en-us/cloud-app-security/use-case-admin-quarantine

Community vote distribution
A (100%)

Moderator Highly Voted 2 years, 3 months ago

Selected Answer: A

Answer A is correct.
https://[tenant].portal.cloudappsecurity.com --> Control --> Policies --> Create Policy --> Activity Policy --> Repeated Activity

https://ibb.co/xqfYyJc
upvoted 5 times

Lelek Most Recent 1 year, 10 months ago

Selected Answer: A

This question could be pulled from the exam as the Microsoft Defender for Cloud Apps portal is moving to the Microsoft 365 Defender portal (https://security.microsoft.com)

https://learn.microsoft.com/en-us/microsoft-365/security/defender/microsoft-365-security-center-defender-cloud-apps?view=o365-worldwide

The answer in this case would be A.
upvoted 1 times

Question #68 *Topic 2*

DRAG DROP -

Your company has a Microsoft 365 E5 tenant.

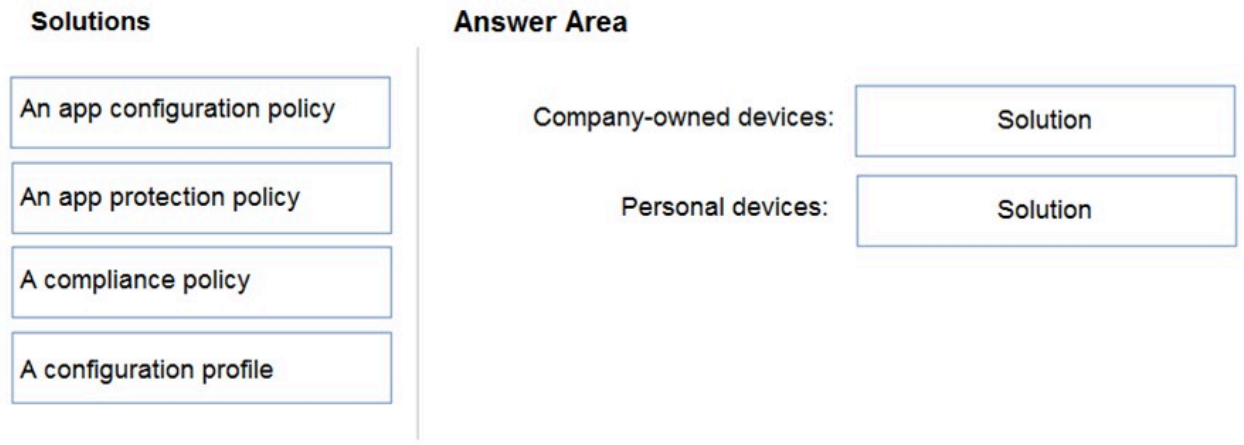
Users access resources in the tenant by using both personal and company-owned Android devices. Company policies requires that the devices have a threat level of medium or lower to access Microsoft Exchange Online mailboxes.

You need to recommend a solution to identify the threat level of the devices and to control access of the devices to the resources.

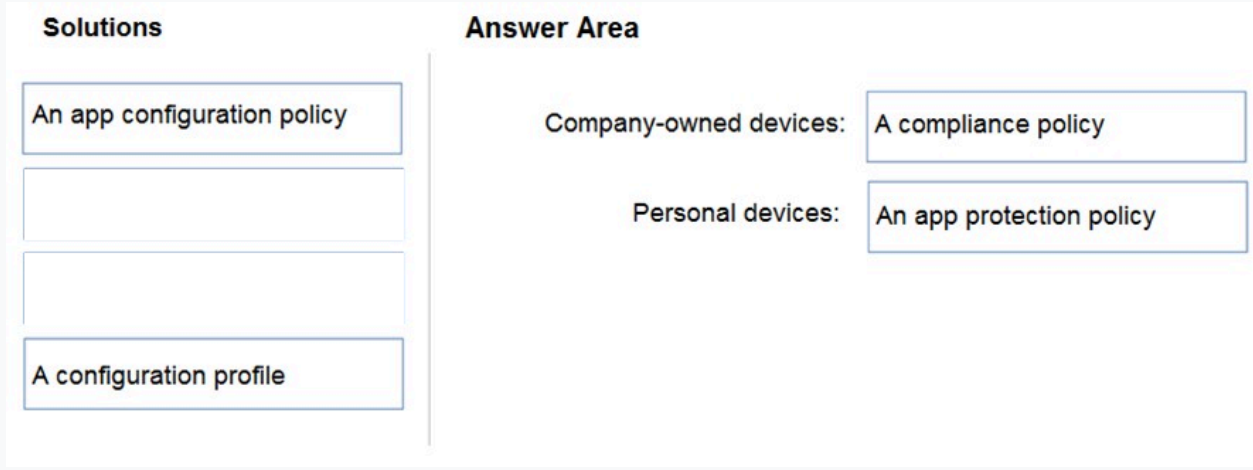
What should you include in the solution for each device type? To answer, drag the appropriate components to the correct devices. Each component may be used once, more than once, or not at all. You may need to drag the split bar between panes or scroll to view content.

NOTE: Each correct selection is worth one point.

Select and Place:



Suggested Answer:



L33D Highly Voted 2 years, 6 months ago

Still valid, on exam Jun 25, 2022

upvoted 11 times

Contactfornitish Highly Voted 2 years, 4 months ago

On exam on 13 aug'22

upvoted 6 times

Mujja Most Recent 1 year, 6 months ago

App Protection for both?

Nothing says the company device is enrolled. Device needs to be enrolled for Compliance policies. Also, compliance policy will alone won't prevent access to resources which is one of the requirments.

upvoted 1 times

TechMinerUK 2 years, 2 months ago

I'm confused here as the question states:

"Company policies requires that the devices have a threat level of medium or lower"

This to me means that both personal and corporate devices would need the Microsoft Defender app installing and an acompanying compliance policy to confirm they are below the acceptable risk level.

An AppProtection policy could be used if the business is only bothered about managing security controls (We do this regularly) and it makes more sense to do this however it would not meet the questions goal of confirming the devices threat level as AppProtection is MAM only and not managing the threat level of the device, only monitoring the security configuration such as PIN, biometric, OS version and rooted/jailbreak state
upvoted 1 times

TechMinerUK 2 years, 2 months ago
Wait, disregard my comment, the question is right as there was functionality I didn't realise was present.

Based on: https://learn.microsoft.com/en-us/mem/intune/protect/mtd-app-protection-policy

There is an additonal option in AppProtection policies under the "Device Conditions" area called "Max allowed device theat level"

Now the bit which is cheeky, this requires a MTD such as Microsoft Defender still to be installed on the device however it would mean the device doesn't have to be enrolled which is the preferred state even though there are BYOD profiles for Android and you can have personal iOS devices enrolled into Intune.

Bit tricky but knowing that the functionality is there it makes sense for the answer to be correct now
upvoted 3 times

TimurKazan 3 years ago
app protection and compliance policies for both
upvoted 2 times

[Removed] 3 years ago
Could you please elaborate why? I think they prefer not to enroll the BYOD. In the App Protection Policy on step „Conditional Launch“ you can set „max allowed device threat level“. Then the Info box for Mobile Threat Defense pops up: https://docs.microsoft.com/en-us/mem/intune/protect/mtd-add-apps-unenrolled-devices
Im still with:
1: compliance policy
2 app protection policy
:/
upvoted 6 times

KornienkoBoris 2 years, 11 months ago
for iOS, where is the type of the device defined
upvoted 1 times

KornienkoBoris 2 years, 11 months ago
nevermind, for Android also
upvoted 1 times

jkklim 3 years, 1 month ago
answer is correct
upvoted 3 times

jfuem 3 years, 4 months ago
Why not Compliance and App-Protection policy for both ?
upvoted 1 times

helpdeskinfra 3 years, 1 month ago
I think that BYOD will not be enroled in Intune so you have to configure MAM App protection policy.
Then, the CA policy will not permit access to EXO unless you use Outlook.
upvoted 5 times

F_M 3 years, 4 months ago
I would say both compliance policy. BYOD enrollment is supported in Intune and defines every device, both corporate owned and private, as compliant or not. I'm saying this because an app protection policy can protect some apps but not every possible different way to access an exchange online mailbox. If the organization uses Outlook App what about browser? And how many different browser are there for Android? You can't include each one in an app protection policy...
upvoted 2 times

F_M 3 years, 4 months ago

Forget this, you can set an app protection policy and create a conditional access policy to enforce the access only from app protected by a policy.

https://docs.microsoft.com/en-us/mem/intune/protect/tutorial-protect-email-on-unmanaged-devices

upvoted 5 times

Question #69 *Topic 2*

HOTSPOT -

You have a Microsoft 365 E5 tenant that contains five devices enrolled in Microsoft Intune as shown in the following table.

Name	Platform
Device1	Windows 10
Device2	Android 8.1.0
Device3	Android 10
Device4	iOS 12
Device5	iOS 14

All the devices have an app named App1 installed.

You need to prevent users from copying data from App1 and pasting the data into other apps.

Which policy should you create in Microsoft Endpoint Manager, and what is the minimum number of required policies? To answer, select the appropriate options in the answer area.

NOTE: Each correct selection is worth one point.

Hot Area:

Answer Area

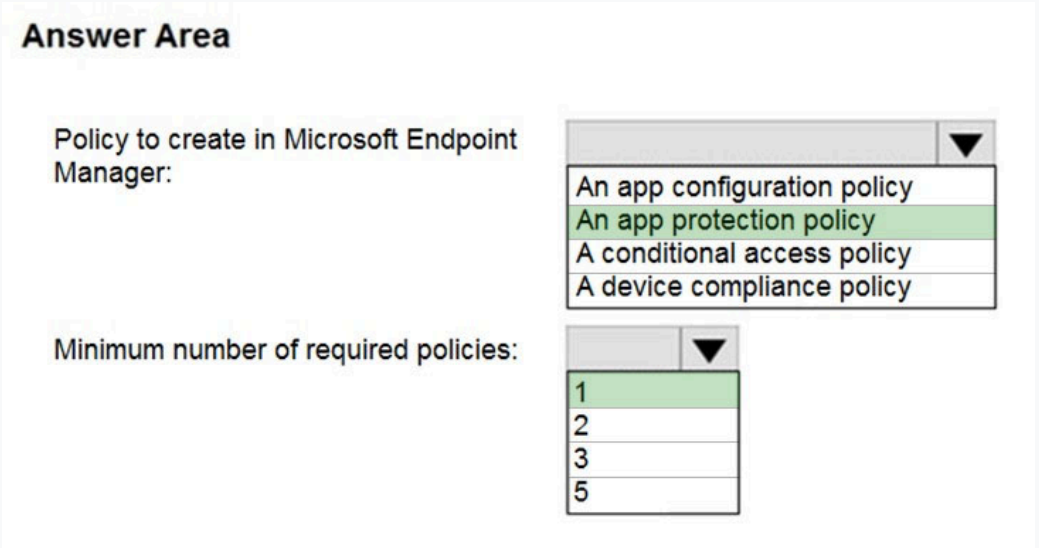
Policy to create in Microsoft Endpoint Manager:

- An app configuration policy
- An app protection policy
- A conditional access policy
- A device compliance policy

Minimum number of required policies:

- 1
- 2
- 3
- 5

Suggested Answer:



Reference:

https://docs.microsoft.com/en-us/mem/intune/apps/app-protection-policy

encxorblood Highly Voted 3 years, 6 months ago

Wrong answer 2 - Need 3 Policies Windows + Anroid + IOS/IpadOS

upvoted 58 times

[Removed] 3 years, 2 months ago

I do agree

upvoted 9 times

AzureExpertwannabe Highly Voted 3 years, 5 months ago

Can someone confirm the answer here:
App protection Policy
Minimum policies required 3

??

upvoted 19 times

rrrr5r Most Recent 2 years, 3 months ago

In Sep 16th 22's exam.

upvoted 6 times

RenegadeOrange 2 years, 3 months ago

Really? with Windows as one of the OS? WIP is being deprecated from July 2022 so if it's in the exam it would be a trick question and potentially the answer is 2, one for IOS and one for Android since you need to use Purview DLP to do it for Windows 10 and 11.

upvoted 2 times

RenegadeOrange 2 years, 3 months ago

https://learn.microsoft.com/en-us/windows/security/information-protection/windows-information-protection/protect-enterprise-data-using-wip

upvoted 1 times

Steverae 2 years, 2 months ago

I agree that WIP is being depreciated, however this will only be not available for new versions of windows where the recommendation is to use Purview DLP - this question does not state you are adding new devices, but have existing devices so still believe the answer is 3 policy's

upvoted 1 times

TechMinerUK 2 years, 2 months ago

Whilst WIP is being deprecated for new devices the functionality to edit existing policies is also being removed from what I understand as Microsoft are favouring Purview DLP.

As such it seems confusing to still be answering questions on WIP since the Microsoft recommended solution is to migrate all policies to the newer alternatives that are available in Purview since the old WIP system will essentially be "locked" in its current state (Which based on what I have read will be similar to Windows 7 and 8 policies in Intune after they were retired)

upvoted 1 times

rajpatel007 2 years, 9 months ago

An app protection policy
3 (Windows, Android, and iOS)

upvoted 3 times

JamesM9 2 years, 9 months ago

Tested - the answer is App Protection Policy + 3 (Windows, IOS, Android).

upvoted 4 times

ajna_ 2 years, 9 months ago

You need 3 app configuration profiles. 1-Windows, 1-iOS, 1-Android.

upvoted 3 times

70mach1 3 years, 2 months ago

I run this very thing in my organization and its 3 app protection policies.

upvoted 8 times

managerofendpoints 3 years, 3 months ago

Answer is 3x app protection policies - Android/iOS will get 'not applicable' upon receiving a Windows policy and vice versa

upvoted 2 times

encxorblood 3 years, 4 months ago

Answer 2 is 3. For Windows, IOS and Anroid. Android ist supported from Version 6 ans IOS from version 12.

upvoted 4 times

doctorcarter 3 years, 4 months ago

Confimed, 3 minimum policy needed. In endpoint protection manager when you add an app configuration policy you need to select from dropdown list Windows - Android or IOS

upvoted 3 times

AzureExpertwannabe 3 years, 5 months ago

So is it 3 or 1???

upvoted 2 times

jabbrwcky 3 years, 5 months ago

Confirmed. As soon as you click the Create Policy button in MEM App Protection Policies you get a drop-down to choose between Windows, iOS / iPadOS or Android.

upvoted 4 times

Question #70 *Topic 2*

You have a Microsoft 365 tenant.
You plan to manage incidents in the tenant by using the Microsoft 365 Defender.
Which Microsoft service source will appear on the Incidents page of the Microsoft 365 Defender?

A. Microsoft Defender for Cloud Apps

B. Azure Sentinel

C. Azure Web Application Firewall

D. Azure Information Protection

Suggested Answer: *A*
Reference:
https://docs.microsoft.com/en-us/microsoft-365/security/defender/investigate-alerts?view=o365-worldwide

jonny_sins 1 year, 4 months ago
incorrect. correct answer is B according to ChatGPT daddy
upvoted 1 times

RenegadeOrange 2 years, 3 months ago
Correct.

Alert sources
Microsoft 365 Defender alerts may come from solutions like Microsoft Defender for Endpoint, Microsoft Defender for Office 365, Microsoft Defender for Cloud Apps, and the app governance add-on for Microsoft Defender for Cloud Apps.

https://learn.microsoft.com/en-us/microsoft-365/security/defender/investigate-alerts?view=o365-worldwide
upvoted 3 times

ThanishNoor 2 years, 3 months ago
correct answer
upvoted 3 times

Question #71 *Topic 2*

You have a Microsoft 365 tenant.
You plan to manage incidents in the tenant by using the Microsoft 365 Defender.
Which Microsoft service source will appear on the Incidents page of the Microsoft 365 Defender portal?

A. Microsoft Sentinel

B. Azure Web Application Firewall

C. Microsoft Defender for Cloud

D. Microsoft Defender for Identity

Suggested Answer: *D*
Reference:
https://docs.microsoft.com/en-us/microsoft-365/security/defender/investigate-alerts?view=o365-worldwide

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

robertcornette Highly Voted 2 years, 3 months ago
Maybe the face that App is left off is a point - answer only "D"
upvoted 5 times

gills Most Recent 1 year, 5 months ago
Selected Answer: D
Defender for Cloud is for Azure workloads.
upvoted 1 times

sanz72 1 year, 10 months ago
Only D, Microsoft Defender for Cloud is another tool and acessed using Azure portal (https://portal.azure.com/#view/Microsoft_Azure_Security/SecurityMenuBlade/~/0), not Microsoft 365 Defender
upvoted 1 times

Gillactus 1 year, 10 months ago
Selected Answer: D
The correct answer is D
upvoted 1 times

MEG 1 year, 11 months ago
Selected Answer: D
Microsoft Defender for Cloud should be Microsoft Defender for Cloud "Apps". Apps is missing. Only Microsoft Defender for Identity is correct.
upvoted 2 times

Vinniel83 1 year, 11 months ago
The correct answer is D
upvoted 2 times

RenegadeOrange 2 years, 3 months ago
Both C and D (well if they used the correct name for C that is... Cloud Apps not just "Cloud")

Alert source Prepended character
Microsoft Defender for Office 365 fa{GUID}
Example: fa123a456b-c789-1d2e-12f1g33h445h6i
Microsoft Defender for Endpoint da or ed for custom detection alerts
Microsoft Defender for Identity aa{GUID}
Example: aa123a456b-c789-1d2e-12f1g33h445h6i
Microsoft Defender for Cloud Apps ca{GUID}
Example: ca123a456b-c789-1d2e-12f1g33h445h6i

https://learn.microsoft.com/en-us/microsoft-365/security/defender/investigate-alerts?view=o365-worldwide

upvoted 1 times

ajiejeng 2 years, 3 months ago

Selected Answer: C

correct me if im wrong but i think its C

upvoted 2 times

natazar 2 years, 2 months ago

if that would be for "cloud apps" instead of "cloud" you would be right.

upvoted 2 times

Question #72 *Topic 2*

You have a Microsoft 365 E5 subscription.
All users have Mac computers. All the computers are enrolled in Microsoft Endpoint Manager and onboarded to Microsoft Defender Advanced Threat Protection
(Microsoft Defender ATP).
You need to configure Microsoft Defender ATP on the computers.
What should you create from the Endpoint Management admin center?

A. a Microsoft Defender ATP baseline profile

B. a device configuration profile

C. an update policy for iOS

D. a mobile device management (MDM) security baseline profile

Suggested Answer: *B*
Reference:
https://docs.microsoft.com/en-us/mem/intune/protect/advanced-threat-protection-configure

TesterDude Highly Voted 3 years, 5 months ago
The answer is B, you need to assign a device configuration profile to configure Defender ATP on Macs
https://docs.microsoft.com/en-us/microsoft-365/security/defender-endpoint/mac-preferences?view=o365-worldwide#configuration-profile-deployment
upvoted 9 times

managerofendpoints Most Recent 3 years, 3 months ago
Technically correct but you can also set up an Endpoint Security > EDR policy
upvoted 4 times

Fcnet 3 years, 5 months ago
Answer B
After you connect Intune and Microsoft Defender for Endpoint, Intune receives an onboarding configuration package from Microsoft Defender for Endpoint. You use a device configuration profile for Microsoft Defender for Endpoint to deploy the package to your Windows devices.
https://docs.microsoft.com/en-us/mem/intune/protect/advanced-threat-protection-configure
upvoted 4 times

ruchita89 3 years, 5 months ago
Devices are already onboarded to MEM & Defender. To configure defender on the device, you need to setup a defender profile from MEM. Correct Answer is A!!
upvoted 4 times

MomoLomo 3 years, 4 months ago
https://docs.microsoft.com/en-us/microsoft-365/security/defender-endpoint/mac-preferences?view=o365-worldwide#summary
The answer is correct
upvoted 3 times

adaniel89 3 years, 5 months ago
Answer is correct
https://docs.microsoft.com/en-us/mem/intune/protect/advanced-threat-protection
upvoted 4 times

Question #73 *Topic 2*

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

Name	Severity	Status	Comment	Category
Alert1	Medium	Active	Comment1	Threat management
Alert2	Low	Resolved	Comment2	Other

Which properties of the alerts can you modify?

A. Status only

B. Status and Comment only

C. Status and Severity only

D. Status, Severity, and Comment only

E. Status, Severity, Comment and Category

Suggested Answer: *B*
Reference:
https://docs.microsoft.com/en-us/microsoft-365/security/defender-endpoint/update-alert?view=o365-worldwide#limitations

TimurKazan Highly Voted 3 years ago
correct
upvoted 6 times

Amir1909 Most Recent 11 months ago
B is correct
upvoted 1 times

Wired7693 1 year, 6 months ago
Currently you can change: status, comment, assign to and classification (True Positive, Informational, False Positive) for an alert
upvoted 1 times

psp65 1 year, 11 months ago
On exam on 30 dic 2022
upvoted 1 times

Contactfornitish 2 years, 4 months ago
On exam on 13 aug'22
upvoted 4 times

AlexBa 3 years ago
Yes B :

Property Type Description
Status String Specifies the current status of the alert. The property values are: 'New', 'InProgress' and 'Resolved'.
assignedTo String Owner of the alert
Classification String Specifies the specification of the alert. The property values are: 'Unknown', 'FalsePositive', 'TruePositive'.
Determination String Specifies the determination of the alert. The property values are: 'NotAvailable', 'Apt', 'Malware', 'SecurityPersonnel', 'SecurityTesting', 'UnwantedSoftware', 'Other'
Comment String Comment to be added to the alert.
upvoted 2 times

Johnnien 3 years, 1 month ago
Submission of comment is available with or without updating properties.

Updatable properties are: status, determination, classification and assignedTo.
upvoted 3 times

Question #74 *Topic 2*

DRAG DROP -

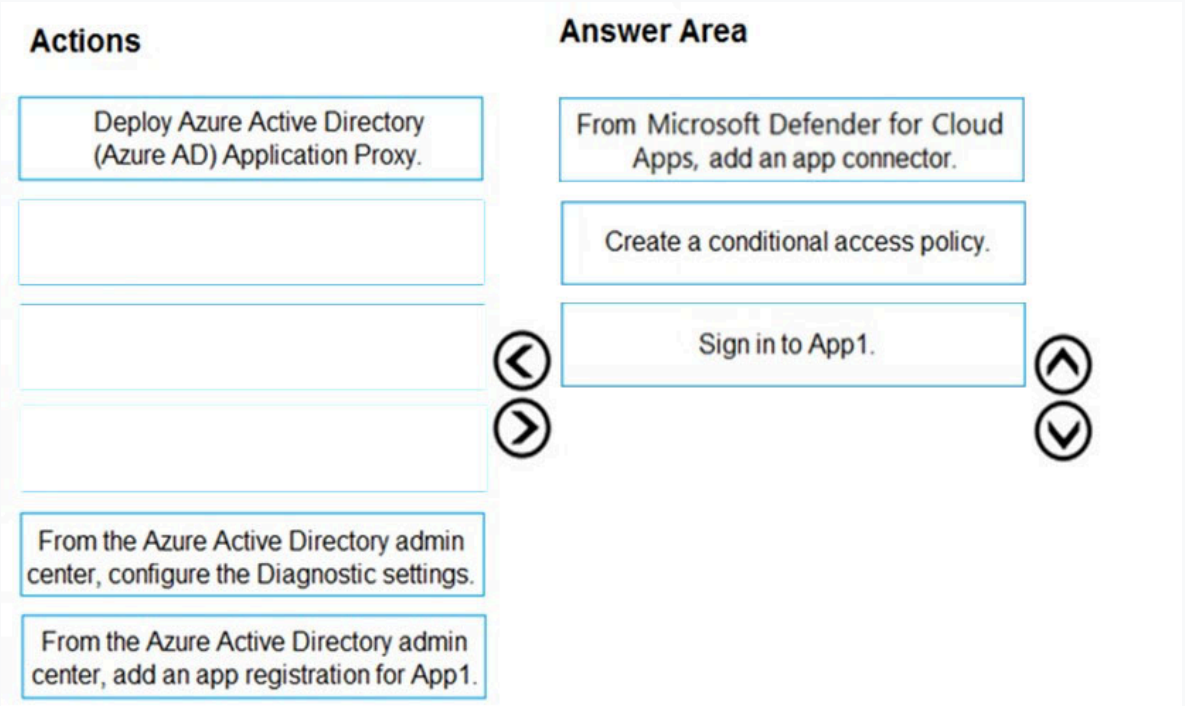
Your company purchases a cloud app named App1.

You need to ensure that you can use Microsoft Defender for Cloud Apps to block downloads in App1. App1 supports session controls.

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:

Suggested Answer:



Reference:

https://docs.microsoft.com/en-us/cloud-app-security/getting-started-with-cloud-app-security https://docs.microsoft.com/en-us/defender-for-identity/integrate-mde

RenegadeOrange Highly Voted 2 years, 3 months ago

Correct, reading through that first article those are the steps available in the answer area.

-Required task: Connect apps
-Recommended task: Enable file monitoring and create file policies
-Required task: Create policies
-Required task: Enable Defender for Cloud Apps to view your cloud app use
-Recommended task: Deploy Conditional Access App Control for catalog apps

Onboard apps onto access and session controls.
From the settings cog, select Conditional Access App Control.
Sign in to each app using a user scoped to the policy
Refresh the Conditional Access App Control page and to view the app.
Verify the apps are configured to use access and session controls
upvoted 6 times

RNG60FR Most Recent 2 years ago
I disagree with proposed Answer. Following https://learn.microsoft.com/en-us/defender-cloud-apps/proxy-deployment-aad, i would propose :
1) from AAD Admin Center, Add an App Registration for App1
2) Create a conditional Access Policy
3) Sign-In to App1
upvoted 4 times

Learner2022 1 year, 11 months ago
The URL provided shows another way of achieving the same goal. However, from AAD admin centre, it's not "add an App registration for App1", it should configure SSO. So the given answer is correct.
upvoted 2 times

Question #75 *Topic 2*

You have a Microsoft 365 E5 subscription that has Microsoft Defender for Endpoint integrated with Microsoft Endpoint Manager.
Devices are onboarded by using Microsoft Defender for Endpoint.
You plan to block devices based on the results of the machine risk score calculated by Microsoft Defender for Endpoint.
What should you create first?

A. a device configuration policy

B. a device compliance policy

C. a conditional access policy

D. an endpoint detection and response policy

Suggested Answer: *B*
Reference:
https://docs.microsoft.com/en-us/mem/intune/protect/advanced-threat-protection-configure

Community vote distribution
B (100%)

maikel87 Highly Voted 3 years ago
Important, "What should you create first"

Begin with device compliance policy, after that conditional access to block high risk devices.
upvoted 16 times

Johnnien Highly Voted 3 years, 1 month ago
To configure integration of Microsoft Defender for Endpoint with Intune.
Configuration includes the following general steps:

Enable Microsoft Defender for Endpoint for your tenant
Onboard devices that run Android, iOS/iPadOS, and Windows 10/11
Use compliance policies to set device risk levels
Use conditional access policies to block devices that exceed your expected risk levels
Android and iOS/iPadOS, use app protection policies that set device risk levels. App protection polices work with both enrolled and unenrolled devices.
upvoted 6 times

Amir1909 Most Recent 11 months ago
B is correct
upvoted 1 times

MEG 1 year, 11 months ago
Selected Answer: B
Use compliance policies to set device risk levels
upvoted 1 times

Darisha 3 years ago
Selected Answer: B
https://docs.microsoft.com/en-us/mem/intune/protect/advanced-threat-protection-configure

in this article there is stated "Use conditional access policies to block devices that exceed your expected risk levels"
upvoted 3 times

Darisha 3 years ago
So wrong, I thought for C, it's definitely conditional access.
upvoted 1 times

[Removed] 3 years ago
FIRST a compliance policy, then a confitional access policy

upvoted 3 times

Goena 3 years ago

Selected Answer: B

compliance policy

upvoted 5 times

AlexBa 3 years ago

B

Create and assign compliance policy to set device risk level

For Android, iOS/iPadOS, and Windows devices, the compliance policy determines the level of risk that you consider as acceptable for a device.

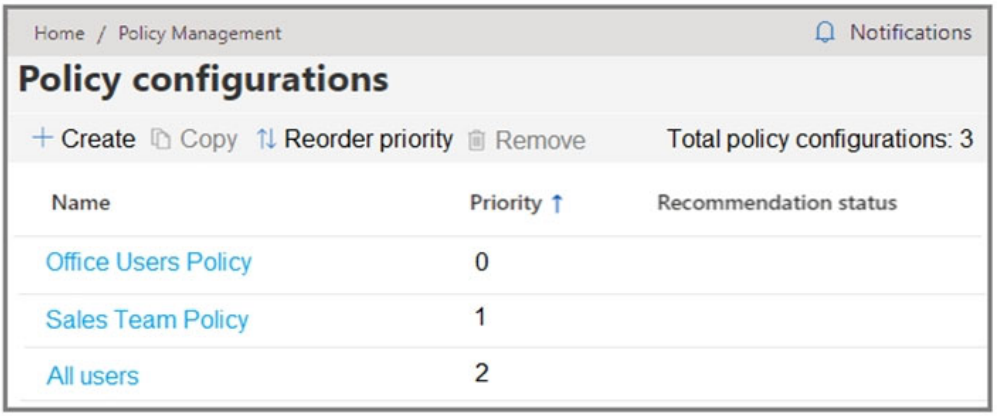
upvoted 6 times

HOTSPOT -

You have a Microsoft 365 subscription that contains three groups named All users, Sales team, and Office users, and two users shown in the following table.

Name	Member of
User1	All users, Sales team
User2	All users, Office users

In Microsoft Endpoint Manager, you have the Policies for Office apps settings shown in the following exhibit.



The policies use the settings shown in the following table.

Policy	Default Shared Folder Location	Default Office Theme
All users	https://sharepoint.contoso.com/addins_all_users	Colorful
Office Users Policy	https://sharepoint.contoso.com/addins_office_users	White
Sales Team Policy	https://sharepoint.contoso.com/addins_sales_team_users_	Dark Gray

What is the default share folder location for User1 and the default Office theme for User2? To answer, select the appropriate options in the answer area.

NOTE: Each correct selection is worth one point.

Hot Area:

Answer Area

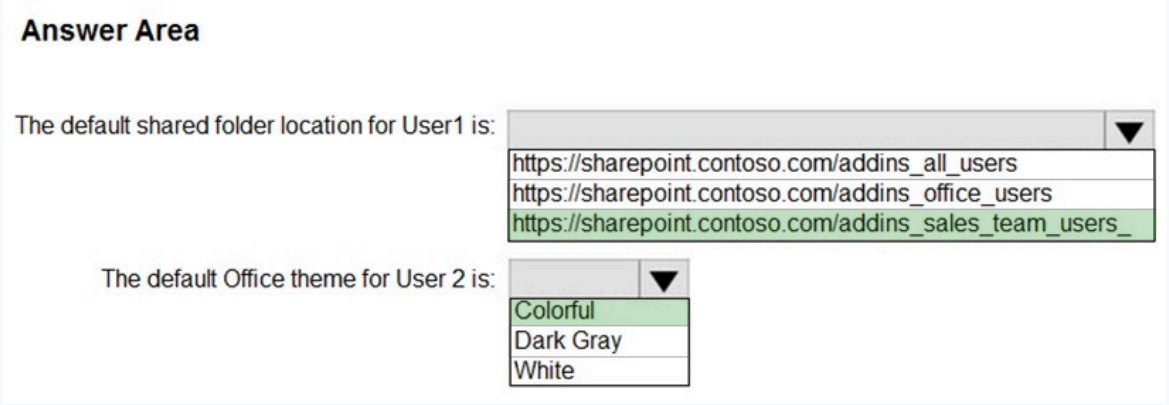
The default shared folder location for User1 is:

- https://sharepoint.contoso.com/addins_all_users
- https://sharepoint.contoso.com/addins_office_users
- https://sharepoint.contoso.com/addins_sales_team_users_

The default Office theme for User 2 is:

- Colorful
- Dark Gray
- White

Suggested Answer:



Reference:
https://docs.microsoft.com/en-us/deployoffice/overview-office-cloud-policy-service

BryanL332 Highly Voted 3 years, 2 months ago

2nd question should be 'White'. If the user is a member of multiple AAD groups with conflicting policy settings, priority is used to determine which policy setting is applied. The highest priority is applied, with "0" being the highest priority that you can assign

upvoted 67 times

ccadenasa 3 years, 2 months ago

You are correct. Admin, can you please modify the answer.

upvoted 19 times

BluMoon 3 years ago

They won't change the answer because this site is used by MS to help the cert testing software detect who is using these dumps. Trust only what gets the most votes and is VERIFIABLE.

upvoted 6 times

Toschu 2 years, 9 months ago

The same dumps with the answers are used on many websites. This is one of the only sites where people are actually discussing every question. I don't think MS likes examtopics.com :P

upvoted 10 times

venwaik Highly Voted 2 years, 7 months ago

Box1: Provided answer is correct

Box2: should be " White". Priority of the office users is higher.

Came on exam 09-05-2022

upvoted 9 times

Mshaty Most Recent 1 year, 7 months ago

how is All users taking precedence whilst it has lower priority than Office users

upvoted 1 times

GotDamnImIn 1 year, 8 months ago

Second answer is White because the policy with the lowest priority will apply first.

upvoted 1 times

DCT 2 years ago

second answer is white bro~

upvoted 1 times

Fefe_ES 2 years, 3 months ago

white 2nd

upvoted 3 times

H3adcap 2 years, 4 months ago

Was in exam today 20 Aug 2022

upvoted 5 times

Nargoo 3 years ago

should be white

upvoted 5 times

AlexBa 3 years ago

Yes priority for "office user" > "all users" so correct answer is White

upvoted 4 times

haazybanj 3 years, 1 month ago

Answer to the 2nd question should be White

upvoted 6 times

Question #77 *Topic 2*

You have a Microsoft 365 tenant that contains a Windows 10 device. The device is onboarded to Microsoft Defender for Endpoint.
From Microsoft Defender Security Center, you perform a security investigation.
You need to run a PowerShell script on the device to collect forensic information.
Which action should you select on the device page?

A. Initiate Live Response Session

B. Initiate Automated Investigation

C. Collect investigation package

D. Go hunt

Suggested Answer: *A*
Reference:
https://docs.microsoft.com/en-us/microsoft-365/security/defender-endpoint/live-response?view=o365-worldwide

Community vote distribution
A (100%)

Johnnien Highly Voted 3 years, 1 month ago
Live response gives security operations teams instantaneous access to a device (also referred to as a machine) 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 your security operations team to collect forensic data, run scripts, send suspicious entities for analysis, remediate threats, and proactively hunt for emerging threats.
upvoted 15 times

venwaik Highly Voted 2 years, 7 months ago
Selected Answer: A
Came on Exam 09-05-2022
upvoted 6 times

Amir1909 Most Recent 11 months ago
A is correct
upvoted 1 times

RenegadeOrange 2 years, 3 months ago
Selected Answer: A
Agree A is correct.
upvoted 2 times

mackzone 2 years, 6 months ago
Came on Exam on 25-06-2022
upvoted 5 times

shivam1 2 years, 11 months ago
The Answer is Correct
upvoted 3 times

Question #78 *Topic 2*

You have a Microsoft 365 E5 subscription.
You plan to implement Microsoft 365 compliance policies to meet the following requirements:
✑ Identify documents that are stored in Microsoft Teams and SharePoint Online that contain Personally Identifiable Information (PII).
✑ Report on shared documents that contain PII.
What should you create?

A. an alert policy

B. a data loss prevention (DLP) policy

C. a retention policy

D. a Microsoft Defender for Cloud Apps policy

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

Community vote distribution
B (100%)

Johnnien Highly Voted 3 years, 1 month ago
In Microsoft 365, you implement data loss prevention by defining and applying DLP policies. With a DLP policy, you can identify, monitor, and automatically protect sensitive items across:

Microsoft 365 services such as Teams, Exchange, SharePoint, and OneDrive
Office applications such as Word, Excel, and PowerPoint
Windows 10 endpoints
non-Microsoft cloud apps
on-premises file shares and on-premises SharePoint.
upvoted 6 times

Amir1909 Most Recent 11 months ago
Correct
upvoted 1 times

RenegadeOrange 2 years, 3 months ago
Selected Answer: B
DLP
https://learn.microsoft.com/en-us/compliance/regulatory/gdpr-discovery-protection-reporting-in-office365-dev-test-environment
upvoted 1 times

Toschu 2 years, 9 months ago
A bit tricky. In the conditions of a DLP policy, you can set a condition to either internally or externally shared but not both.
The question doesn't tell you which one.

I would say a Cloud App Security File policy could be the solution but I can't check at the moment.
File Policies allow you to enforce a wide range of automated processes using the cloud provider's APIs. Policies can be set to provide continuous compliance scans, legal eDiscovery tasks, DLP for sensitive content shared publicly, and many more use cases. Defender for Cloud Apps can monitor any file type based on more than 20 metadata filters (for example, access level, file type).
upvoted 2 times

Question #79 *Topic 2*

HOTSPOT -

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

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

In Microsoft Endpoint Manager, you have the Policies for Office apps settings shown in the following table.

Name	Priority	Applies to
Policy1	0	Group1
Policy2	1	Group2
Policy3	2	Group3

The policies use the settings shown in the following table.

Name	Cursor movement	Clear cache on close
Policy1	Logical	Disabled
Policy2	Not configured	Enabled
Policy3	Visual	Enabled

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 has their cache cleared on close.	○	○
User2 has Cursor movement set to Visual.	○	○
User3 has Cursor movement set to Visual.	○	○

Suggested Answer:

Answer Area

Statements	Yes	No
User1 has their cache cleared on close.	○	○
User2 has Cursor movement set to Visual.	○	○
User3 has Cursor movement set to Visual.	○	○

Reference:

https://docs.microsoft.com/en-us/deployoffice/overview-office-cloud-policy-service

Bakje Highly Voted 3 years, 1 month ago

User 2 cursor movement shoud be visual = yes.

User 2 has policy 2 and 3 assigned with policy2 having higher priority but a "not configured" state. Because of this policy 3, which has cursor movement set to Visual, applies.

upvoted 19 times

ChaBum 3 years, 1 month ago

The setting for the Cursor movement is not configured, does not mean the policy won't apply.

upvoted 12 times

goape 3 years, 1 month ago

Policy 2 will apply, but there is no clash of settings, so the settings of Policy 3 will also be applied.

upvoted 7 times

hans333 2 years, 9 months ago
I agree.
So the answer is: NYN
Source: https://serverfault.com/questions/934183/does-enabled-policy-in-gpo-take-precedence-over-gpo-that-is-not-configured-for-t
upvoted 5 times

jodtzz Highly Voted 3 years, 1 month ago
NNN
"If the user is a member of multiple AAD groups with conflicting policy settings, priority is used to determine which policy setting is applied. The highest priority is applied, with "0" being the highest priority that you can assign. You can set the priority by choosing Reorder priority on the Policy configurations page."
https://docs.microsoft.com/en-us/deployoffice/admincenter/overview-office-cloud-policy-service
upvoted 16 times

Bouncy 2 years, 7 months ago
Your source says "which policy SETTING is applied", not "which POLICY is applied". Hence it will process the lower priority policy as well to check for conflicting settings and not stop at the first policy match.
NYN
upvoted 4 times

Jakub2023 1 year, 7 months ago
The site reads:
- "If the user is a member of multiple Azure AD groups with conflicting policy settings, priority is used to determine which policy setting is applied. The [policy with the] highest priority is applied, with "0" being the highest priority that you can assign."
- "If the user is in multiple security groups that have policy configurations assigned to them, then the priority of the policy configurations determines which policies take effect."

This is not ambiguous. The correct answer is NNN.
upvoted 1 times

TimurKazan 3 years ago
so,in this case it would be N-Y-N
upvoted 17 times

Roche4ever Most Recent 1 year, 3 months ago
I think the Answer is correct: N,N,N
Was in Exam today, 25 Sept 23
upvoted 1 times

Kees1990 1 year, 9 months ago
it's NNN
policy selection is determined before applying. So policy3 will never reach the user/device.

https://learn.microsoft.com/en-us/microsoftteams/assign-policies-users-and-groups
upvoted 1 times

EsamiTopici 1 year, 9 months ago
Why Teams?
upvoted 1 times

Learner2022 1 year, 11 months ago
Should be NNN, “not configured” is in conflict of “visual” as it is a different state. So Policy 2 takes precedence
upvoted 1 times

hubran 1 year, 10 months ago
I disagree. "Not configured" is basically every setting that you don't touch and leave it at its default value, so it doesn't create conflicts. This means the correct answer is NYN
upvoted 1 times

thuba_TD 2 years, 1 month ago
No Nut November
upvoted 6 times

RenegadeOrange 2 years, 3 months ago

NYN

I first thought NNN because the policy with the highest priority wins if there are conflicting settings, BUT, there is not conflicting setting because it's not configured at all so user2 will get the setting on the only policy which is configured!

upvoted 1 times

Contactfornitish 2 years, 4 months ago

On exam on 13 aug'22

upvoted 2 times

Contactfornitish 2 years, 4 months ago

Its NNN

If the user is a member of multiple Azure AD groups with conflicting policy settings, priority is used to determine which policy setting is applied. The highest priority is applied, with "0" being the highest priority that you can assign.

ref: https://docs.microsoft.com/en-us/deployoffice/admincenter/overview-cloud-policy

upvoted 2 times

LillyLiver 2 years, 10 months ago

I'm in the N,N,N camp myself. Policy2 in a higher priority than Policy3 for user 2. So Policy3 won't even be considered.

also, I thought nested groups weren't allowed. From the provided link:
"If users are located in nested groups and the parent group is targeted for policies, the users in the nested groups will receive the policies."

upvoted 3 times

Notorious19 2 years, 11 months ago

N-Y-N correct answer, read BAKJE"s explanation

upvoted 5 times

haazybanj 3 years, 1 month ago

answer is NNN

upvoted 2 times

jkklim 3 years, 1 month ago

nyy

apply common sense

upvoted 1 times

JT19760106 2 years, 11 months ago

It's either NNN or NYN, not sure what "common sense" gets you to NYY

upvoted 11 times

Kalzonee3611 2 years, 10 months ago

What a useless comment, well done.

upvoted 5 times

Question #80 *Topic 2*

You have a Microsoft 365 E5 tenant that contains the devices shown in the following table.

Name	Platform
Device1	MacOS
Device2	Windows 10 Pro
Device3	Windows 10 Enterprise
Device4	Ubuntu 18.04 LTS

You plan to implement attack surface reduction (ASR) rules.
Which devices will support the ASR rules?

A. Device1, Device2, Device3, and Device4

B. Device1, Device2, and Device3 only

C. Device2 and Device3 only

D. Device3 only

Suggested Answer: *C*
Reference:
https://docs.microsoft.com/en-us/microsoft-365/security/defender-endpoint/enable-attack-surface-reduction?view=o365-worldwide#requirements

Community vote distribution
C (83%) D (17%)

BryanL332 Highly Voted 3 years, 2 months ago
Correct, ASR can only run on:
Windows 10 Pro, version 1709 or later
Windows 10 Enterprise, version 1709 or later
Windows Server, version 1803 (Semi-Annual Channel) or later
Windows Server 2019
Windows Server 2016
Windows Server 2012 R2
Windows Server 2022
upvoted 20 times

DiscGolfer 3 years, 1 month ago
https://docs.microsoft.com/en-us/microsoft-365/compliance/dlp-learn-about-dlp?view=o365-worldwide
upvoted 1 times

harburn422 2 years, 10 months ago
https://docs.microsoft.com/en-us/microsoft-365/security/defender-endpoint/enable-attack-surface-reduction?view=o365-worldwide
upvoted 1 times

ChizzyO Most Recent 1 year, 6 months ago
The given answer is correct as they want to know the device that supports ASR

Attack surface reduction features across Windows versions

You can set attack surface reduction rules for devices that are running any of the following editions and versions of Windows:

Windows 11 Pro
Windows 11 Enterprise
Windows 10 Pro, version 1709 or later
Windows 10 Enterprise, version 1709 or later
Windows Server, version 1803 (Semi-Annual Channel) or later
Windows Server 2012 R2
Windows Server 2016

Windows Server 2019
Windows Server 2022

To use the entire feature-set of attack surface reduction rules, you need:

Microsoft Defender Antivirus as primary AV (real-time protection on)
Cloud-Delivery Protection on (some rules require that)
Windows 10 Enterprise E5 or E3 License

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

freeq 2 years ago
On the exam 30.12.2022
upvoted 3 times

LillyLiver 2 years, 10 months ago
Selected Answer: C
The answer is in the first couple lines of he link.
upvoted 2 times

LillyLiver 2 years, 10 months ago
Given the provided link (updated yesterday, 2/22/2022) Win 10 Pro. and Ent are targetable. And in my tenant it states Win 10 or later. So I am inclined to agree with the provided answer.
upvoted 1 times

tagada 2 years, 11 months ago
Selected Answer: C
Correct.
upvoted 3 times

amymay101 3 years ago
Selected Answer: D
win10 enterprise
upvoted 1 times

edzio 3 years ago
"To use the entire feature-set of attack surface reduction rules, you need:

- Windows Defender Antivirus as primary AV (real-time protection on)
- Cloud-Delivery Protection on (some rules require that)
- Windows 10 Enterprise E5 or E3 License"

But they do not ask about entire feature-set of ASR rules. W10 PRO is enough to set ASR.
So C.
upvoted 3 times

Question #81 *Topic 2*

You have a Microsoft 365 tenant.
You plan to enable BitLocker Disk Encryption (BitLocker) automatically for all Windows 10 devices that enroll in Microsoft Intune.
What should you use?

A. an attack surface reduction (ASR) policy

B. an app configuration policy

C. a device compliance policy

D. a device configuration profile

Suggested Answer: *D*
Reference:
https://docs.microsoft.com/en-us/mem/intune/protect/encrypt-devices

Community vote distribution
D (100%)

AlexBa Highly Voted 3 years ago
Selected Answer: D
https://docs.microsoft.com/en-us/mem/intune/protect/encrypt-devices#create-a-device-configuration-profile-for-bitlocker
upvoted 5 times

Roche4ever Most Recent 1 year, 3 months ago
Answer is correct: D
Was in Exam Today, 25 Sept 23
upvoted 1 times

[Removed] 3 years ago
It's a config, Answer is D, you can find it in the Endpoint Protection template for Windows 10, it's under windows encryption and it must be set to require, Compliance would just check for it if you wanted to apply a rule.
upvoted 3 times

Rocky83 3 years, 1 month ago
I think the answer is correct
upvoted 2 times

TheWallPTA 3 years, 1 month ago
I just checked and i can see Bitlocker under Compliance Policies...So think im going to go with C
upvoted 1 times

VirtualJP 3 years ago
The Compliance policy just checks for the presence of Bitlocker and its state, it does not actually perform the function of enabling Bitlocker and settings. For this you would need a configuration profile either via Device | Configuration profile or by using Endpoint security | Disk encryption
upvoted 8 times

Johnnien 3 years, 1 month ago
Use one of the following policy types to configure BitLocker on your managed devices

Endpoint security disk encryption policy for BitLocker. The BitLocker profile in Endpoint security is a focused group of settings that is dedicated to configuring BitLocker.

View the BitLocker settings that are available in BitLocker profiles from disk encryption policy.

Device configuration profile for endpoint protection for BitLocker. BitLocker settings are one of the available settings categories for Windows 10/11 endpoint protection.
upvoted 4 times

Question #82 *Topic 2*

You have a Microsoft 365 tenant.
You plan to implement Endpoint Protection device configuration profiles.
Which platform can you manage by using the profiles?

A. Android Enterprise

B. Windows 10

C. Windows 8.1

D. Android

Suggested Answer: *B*
Intune device configuration profiles can be applied to Windows 10 devices and macOS devices
Note:
There are several versions of this question in the exam. The question has two possible correct answers:
1. Windows 10
2. macOS
Other incorrect answer options you may see on the exam include the following:
1. Ubuntu Linux
2. iOS
Reference:
https://docs.microsoft.com/en-us/mem/intune/protect/endpoint-protection-configure

Johnnien Highly Voted 3 years, 1 month ago
ntune can manage for each supported platform:

macOS settings
Windows settings
upvoted 9 times

rnd3131 Most Recent 2 years, 4 months ago
windows 11 also
upvoted 2 times

Question #83 *Topic 2*

You have a Microsoft 365 tenant that contains 500 Windows 10 devices and a Microsoft Endpoint Manager device compliance policy.
You need to ensure that only devices marked as compliant can access Microsoft Office 365 apps.
Which policy type should you configure?

A. conditional access

B. account protection

C. attack surface reduction (ASR)

D. Endpoint detection and response

Suggested Answer: *A*
Reference:
https://docs.microsoft.com/en-us/mem/intune/protect/device-compliance-get-started

DiscGolfer Highly Voted 3 years, 1 month ago
Conditional Access
https://docs.microsoft.com/en-us/mem/intune/protect/device-compliance-get-started#integrate-with-conditional-access
upvoted 10 times

Question #84 *Topic 2*

You have a Microsoft 365 tenant that contains a Windows 10 device named Device1 and the Microsoft Endpoint Manager policies shown in the following table.

Name	Type	Block execution of potentially obfuscated scripts (js/vbs/ps)
Policy1	Attack surface reduction (ASR)	Audit mode
Policy2	Microsoft Defender ATP Baseline	Disable
Policy3	Device configuration profile	Not configured

The policies are assigned to Device1.
Which policy settings will be applied to Device1?

A. only the settings of Policy1

B. only the settings of Policy2

C. only the settings of Policy3

D. no settings

Suggested Answer: *C*

Community vote distribution

A (58%) D (42%)

mnak Highly Voted 3 years, 2 months ago

This rule is only applicable to ASR. Device Configuration Profile -> Endpoint protection template -> Microsoft Defender Exploit Guard -> Attack Surface Reduction. Though the question is the height of obfuscation itself, I believe the answer is A. Policy 2 is related to email, Policy 3 is not defining any setting.

upvoted 26 times

qhuy199 11 months, 1 week ago

Disable and not configure are same stage disable. Source: https://docs.microsoft.com/en-us/mem/intune/protect/security-baseline-settings-defender-atp?pivots=atp-december-2020#attack-surface-reduction-rules

upvoted 1 times

Bakje Highly Voted 3 years, 1 month ago

D: No settings

Attack surface reduction rules support a merger of settings from different policies, to create a superset of policy for each device. Only the settings that are not in conflict are merged, while those that are in conflict are not added to the superset of rules.

Source: https://docs.microsoft.com/en-us/mem/intune/protect/security-baseline-settings-defender-atp?pivots=atp-december-2020#attack-surface-reduction-rules

upvoted 24 times

OneplusOne 2 years, 11 months ago

Agreed, D

Note

Conflict handling:

"If you assign a device two different ASR policies, the way conflict is handled is rules that are assigned different states, there is no conflict management in place, and the result is an error.
Non-conflicting rules will not result in an error, and the rule will be applied correctly. The result is that the first rule is applied, and subsequent non-conflicting rules are merged into the policy."

https://docs.microsoft.com/en-us/microsoft-365/security/defender-endpoint/enable-attack-surface-reduction?view=o365-worldwide#mem

upvoted 3 times

us3r 3 years ago

disagree. The merge can happen on the ASR rules only, not in the Microsoft Endpoint manager policies.

Most probably the correct answer is A (Policy1)

upvoted 2 times

amymay101 3 years ago

I agree, all these settings are in conflict so none of them will apply

upvoted 3 times

lamrandom 2 years, 7 months ago

Disagree. That paragraph is related to two asr policies.
You missed the most important statement:

Policy Conflict

If a conflicting policy is applied via MDM and GP, the setting applied from MDM will take precedence.

Reference: https://github.com/MicrosoftDocs/microsoft-365-docs/blob/public/microsoft-365/security/defender-endpoint/enable-attack-surface-reduction.md

upvoted 2 times

Feyenoord Most Recent 1 year, 7 months ago

Look at this discussion: https://techcommunity.microsoft.com/t5/microsoft-intune/difference-between-quot-devices-gt-configuration-profiles-quot/m-p/3260865

There someone tested it and confirmed that a setting in a Device Configuration Profile took precedence over a ASR policy.

So for me answer is Policy 1, Answer A

upvoted 1 times

prabhjot 1 year, 8 months ago

IT IS A - Ans

upvoted 1 times

EsamiTopici 1 year, 9 months ago

Can anyone explain why it should be D? D should apply when there are multiple asr policies, there is only one asr, shouldn't policy 1 win?

upvoted 1 times

Lelek 1 year, 10 months ago

Selected Answer: D

The Answer D. No Settings

https://techcommunity.microsoft.com/t5/microsoft-intune/best-practice-for-multiple-configuration-policies/m-p/275893

upvoted 1 times

hufflepuff 1 year, 10 months ago

Selected Answer: D

See Bakje's answer.

upvoted 1 times

hufflepuff 1 year, 10 months ago

Selected Answer: D

No settings apply due to policy conflicts as previously stated - see Bakje's answer. Dont get misdirected mistaking the values of the settings with the policies themselves. The values are set to Audit or Disabled, not if the policy itself is audit or disabled.

upvoted 2 times

psp65 1 year, 11 months ago

Answer is D because the setting about "Block obfuscation of potentially obfuscated scripts" has 3 conflicting values, so it will no applied (https://learn.microsoft.com/en-us/mem/intune/protect/security-baseline-settings-defender-atp?pivots=atp-december-2020#attack-surface-reduction-rules)

upvoted 2 times

bac0n 2 years ago

https://docs.microsoft.com/en-us/mem/intune/protect/security-baseline-settings-defender-atp?pivots=atp-december-2020#attack-surface-reduction-rules

The key here is that this rule, "Block obfuscation of potentially obfuscated scripts" is an attack surface reduction rule. You can configure it from the three places the article is talking about. Therefore, the statement in the article applies;

When two or more policies have conflicting settings, the conflicting settings are not added to the combined policy, while settings that don't conflict are added to the superset policy that applies to a device.

The answer is D.
upvoted 2 times

4Shawsy 2 years, 1 month ago

Selected Answer: D

Conflicting Settings so D
upvoted 1 times

soydlm 2 years, 5 months ago

D: No Settings.
When two or more policies have conflicting settings, the conflicting settings are not added to the combined policy, while settings that don't conflict are added to the superset policy that applies to a device.
upvoted 1 times

AZalan 2 years, 8 months ago

Audit, Disable & Not Configured for the same setting are in conflict >>> will not be applied
Answer = D
upvoted 2 times

Kalzonee3611 2 years, 10 months ago

I feel this should be “A” - anybody agree?
upvoted 2 times

JAPo123 2 years, 10 months ago

Policy 3 is assigned to device 1, but the settings have no value.
Therefore answer C.
upvoted 2 times

LK4723 2 years, 3 months ago

I would agree this. There are only four values that an ASR policy can have listed below. This would make the first two in conflict and not apply leaving only the last policy to apply as not configured is not an ASR value.

0 : Disable (Disable the ASR rule)
1 : Block (Enable the ASR rule)
2 : Audit (Evaluate how the ASR rule would impact your organization if enabled)
6 : Warn (Enable the ASR rule but allow the end-user to bypass the block)
upvoted 2 times

Joshycannon 2 years, 11 months ago

Selected Answer: A

I think A as well. Auditing is not actively doing anything on the policy, but it's still tracking and pulling logs for the device it attached to and that is "something"
upvoted 3 times

Llex 3 years ago

Selected Answer: A

A please
upvoted 4 times

Question #85 *Topic 2*

HOTSPOT -

You have a Microsoft 365 E5 tenant that contains 100 Windows 10 devices.

You plan to attack surface reduction (ASR) rules for the Windows 10 devices.

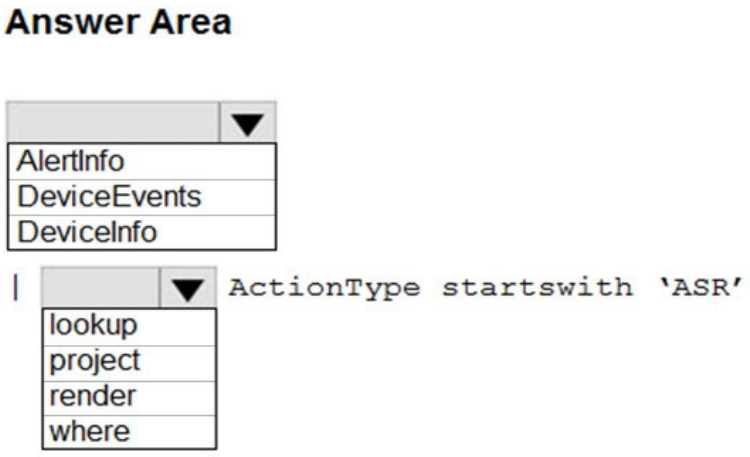
You configure the ASR rules in audit mode and collect audit data in a Log Analytics workspace.

You need to find the ASR rules that match the activities on the devices.

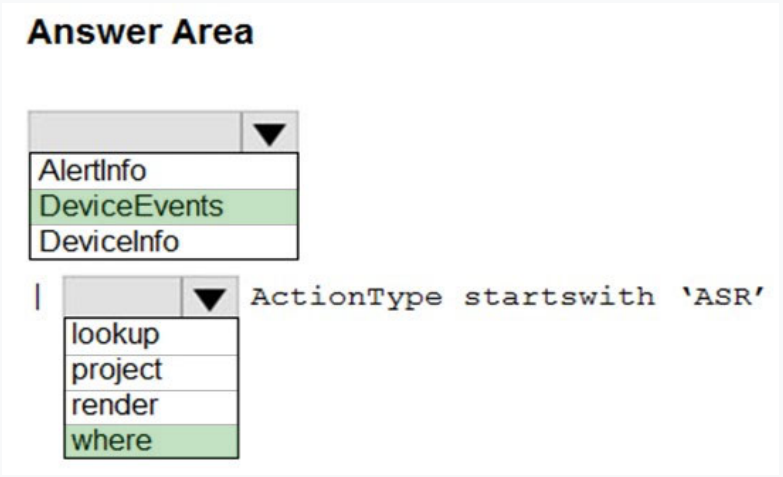
How should you complete the Kusto query? To answer, select the appropriate options in the answer area.

NOTE: Each correct selection is worth one point.

Hot Area:



Suggested Answer:



Reference:

https://techcommunity.microsoft.com/t5/microsoft-defender-for-endpoint/demystifying-attack-surface-reduction-rules-part-3/ba-p/1360968

hans333 Highly Voted 2 years, 9 months ago

DeviceEvents | where ActionType startswith 'Asr'

upvoted 11 times

AlexBa Highly Voted 3 years ago

https://docs.microsoft.com/fr-fr/microsoft-365/security/defender-endpoint/attack-surface-reduction?view=o365-worldwide#review-attack-surface-reduction-events-in-the-microsoft-365-defender-portal

upvoted 10 times

NitishKarmakar Most Recent 1 year, 6 months ago

https://learn.microsoft.com/en-us/microsoft-365/security/defender-endpoint/attack-surface-reduction?view=o365-worldwide#review-attack-surface-reduction-events-in-the-microsoft-365-defender-portal

upvoted 1 times

Question #86 *Topic 2*

HOTSPOT -

You have a Microsoft 365 E5 tenant that connects to Microsoft Defender for Endpoint.

You have devices enrolled in Microsoft Intune as shown in the following table.

Name	Platform
Device1	Windows 10
Device2	Windows 8.1
Device3	iOS
Device4	Android

You plan to use risk levels in Microsoft Defender for Endpoint to identify whether a device is compliant. Noncompliant devices must be blocked from accessing corporate resources.

You need to identify which devices can be onboarded to Microsoft Defender for Endpoint, and which Endpoint security policies must be configured.

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

NOTE: Each correct selection is worth one point.

Hot Area:

Answer Area

Devices that can onboarded to Microsoft Defender for Endpoint:

- Device 1 only
- Device 1 and Device 2 only
- Device 1 and Device 3 only
- Device 1 and Device 4 only
- Device 1, Device 2, and Device 4 only
- Device 1, Device 2, Device 3, and Device 4

Endpoint security policies that must be configured:

- A conditional access policy only
- A device compliance policy only
- A device configuration profile only
- A device configuration profile and a conditional access policy only
- Device configuration profile, device compliance policy, and conditional access policy

Suggested Answer:

Answer Area

Devices that can onboarded to Microsoft Defender for Endpoint:

- Device 1 only
- Device 1 and Device 2 only
- Device 1 and Device 3 only
- Device 1 and Device 4 only
- Device 1, Device 2, and Device 4 only
- Device 1, Device 2, Device 3, and Device 4

Endpoint security policies that must be configured:

- A conditional access policy only
- A device compliance policy only
- A device configuration profile only
- A device configuration profile and a conditional access policy only
- Device configuration profile, device compliance policy, and conditional access policy

Reference:

https://docs.microsoft.com/en-us/microsoft-365/security/defender-endpoint/configure-machines-onboarding?view=o365-worldwide

ZuluHulu Highly Voted 3 years, 1 month ago

I believe the answer to the second question is device configuration policy, device compliance policy and conditional access.

upvoted 39 times

amymay101 3 years, 1 month ago

I agree, surely all 3 need to be configured to provide a complete solution
upvoted 10 times

jkklim Highly Voted 3 years, 1 month ago
https://docs.microsoft.com/en-us/mem/intune/protect/advanced-threat-protection#onboard-devices-by-using-a-configuration-profile

To be successful, you'll use the following configurations in concert:

Establish a service-to-service connection between Intune and Microsoft Defender for Endpoint. This connection lets Microsoft Defender for Endpoint collect data about machine risk from supported devices you manage with Intune.
Use a device configuration profile to onboard devices with Microsoft Defender for Endpoint. You onboard devices to configure them to communicate with Microsoft Defender for Endpoint and to provide data that helps assess their risk level.
Use a device compliance policy to set the level of risk you want to allow. Risk levels are reported by Microsoft Defender for Endpoint. Devices that exceed the allowed risk level are identified as noncompliant.
Use a conditional access policy to block users from accessing corporate resources from devices that are noncompliant.
upvoted 13 times

ubt 2 years, 11 months ago
However, this doesn't show Win8.1 as an option and there is no answer that has all devices over then Win8.1...
upvoted 1 times

Amir1909 Most Recent 11 months ago
- Device1, Device2, Device3, and Device4
- Device configuration Profile, device compliance policy, and conditional access policy
upvoted 1 times

BigDazza_111 1 year, 3 months ago
In question #82 apparently only MacOS and Windows devices can be configured with MS Endpoint config profiles. and now in this questions they say all devives can be applied to device config profile. WTF thanks for teaching me the meaning of the word 'obsfucate' ET's!
upvoted 1 times

Mshaty 1 year, 7 months ago
You plan to use risk levels in Microsoft Defender for Endpoint to identify whether a device is compliant. this is where you draw your answer from.. the policy is to identify whether its compliant or not
upvoted 1 times

ACTOSA 1 year, 9 months ago
So I was torn but I think I understand why.

You need a compliance policy and a conditional access policy. However the conditional access is for the application rather than the endpoint. The question states what endpoint policies would need to be implemented.

A configuration profile is irrelevant to this question.
upvoted 1 times

Lelek 1 year, 10 months ago
The answer should be
1 - Device1, Device2, Device3 and Device 4
2 - Device Configuration profile, device compliance policy, and conditional access policy

If you look at Microsoft's official documentation, it says that it supports Windows 8.1, in addition to supporting iOS and Android, in addition to Windows 10. You can confirm at the link:
https://learn.microsoft.com/en-us/microsoft-365/security/defender-endpoint/minimum-requirements?view=o365-worldwide

As for the second question, it asks "security policies that must be configured", if you look at the beginning of the question, you will find the text "Noncompliant devices must be blocked from accessing corporate resources.", so to meet this demand, we first need to configure the Complaince Policy to mark whether the device is compliant or non-compliant, but still need to block if device is non-compliant, so we use Conditioanl Access. And finally the Configuration Profile is for onboarding with the MDE.
upvoted 3 times

hufflepuff 1 year, 10 months ago

Ok, think I've sorted out the confusion, I hope this helps. Please flag if I've missed something.

Endpoint supports all the listed devices(include 8.1), however intune only supports: Android, iOS/iPadOS, Windows 10/11

Use compliance policies to set device risk levels.
Use conditional access policies to block devices that exceed your expected risk levels.
The above two policies would be enough if we excluded windows 8.1, but to support that device - "You can manage Defender for Endpoint security configurations on devices that aren't enrolled with Intune"

So my answer:
1) device1, device2, device3, device4
2) device configuration policy, device compliance policy and conditional access.

References:
https://learn.microsoft.com/en-us/microsoft-365/security/defender-endpoint/minimum-requirements?view=o365-worldwide
https://learn.microsoft.com/en-us/mem/intune/protect/advanced-threat-protection-configure
https://learn.microsoft.com/en-us/mem/intune/protect/advanced-threat-protection#onboard-devices-by-using-a-configuration-profile
upvoted 2 times

EsamiTopici 1 year, 10 months ago
But is Windows 8.1 correct in the first answer?
upvoted 1 times

chrys 2 years, 4 months ago
You would need config, compliance, and conditional access policies according to this MS doc:

Use the information and procedures in this article to configure integration of Microsoft Defender for Endpoint with Intune. Configuration includes the following general steps:

- Enable Microsoft Defender for Endpoint for your tenant
- Onboard devices that run Android, iOS/iPadOS, and Windows 10/11
- Use compliance policies to set device risk levels
- Use conditional access policies to block devices that exceed your expected risk levels

Android and iOS/iPadOS, use app protection policies that set device risk levels. App protection polices work with both enrolled and unenrolled devices.

https://docs.microsoft.com/en-us/mem/intune/protect/advanced-threat-protection-configure
upvoted 5 times

EsamiTopici 1 year, 10 months ago
so the first answer is wrong(?) windows 8.1 not supported
upvoted 1 times

itmaster 2 years, 8 months ago
Configuration profile is only needed if you want to onbaord devices through intune. The right answer for second question should be: "compliance policy and conditional access policy only". However, this is not an option, so I am thinking the question is asking for a solution for both on boadrding devices and controlling access through intune, and if this is the case the second question would be okay to include "configuraiton profile" in it, but in that case the answer for the first qustion should be "device 1 only", because it is not onbaord Android,IOS, and windows 8 thorugh "configuration profiles".
upvoted 2 times

itmaster 2 years, 8 months ago
correction.... because it is not supported* to* onbaord Android,IOS, and windows 8 through "configuration profiles"
upvoted 1 times

itmaster 2 years, 8 months ago
https://docs.microsoft.com/en-us/mem/intune/protect/advanced-threat-protection-configure#:~:text=There%20isn%27t%20a%20configuration%20package%20for%20devices%20that%20run%20iOS/iPadOS
upvoted 1 times

itmaster 2 years, 8 months ago

https://docs.microsoft.com/en-us/mem/intune/protect/advanced-threat-protection-configure#:~:text=There%20isn%27t%20a%20configuration%20package%20for%20devices%20that%20run%20Android

upvoted 1 times

jkklim 3 years, 1 month ago

Devices managed with Intune:

The following platforms are supported for Intune with Microsoft Defender for Endpoint:

Android

iOS/iPadOS

Windows 10/11 (Hybrid Azure Active Directory Joined or Azure Active Directory Joined)

upvoted 3 times

jkklim 3 years, 1 month ago

https://docs.microsoft.com/en-us/microsoft-365/security/defender-endpoint/minimum-requirements?view=o365-worldwide

for answer 1 ==> all devices

upvoted 7 times

goape 3 years, 1 month ago

jkklim is linked a good document here. Win10/11, Android and iOS devices can be onboarded. We'd need all 3 policy types to set this up.

upvoted 2 times

Johnnien 3 years, 1 month ago

https://docs.microsoft.com/en-us/microsoft-365/security/defender-endpoint/onboard-configure?view=o365-worldwide

upvoted 1 times

[Removed] 3 years, 1 month ago

There's no need to create a configuration policy. You only need to block access when a device is not compliant.

But that's not an option so the answer is we need to setup all profiles

upvoted 2 times

Question #87 *Topic 2*

You have a Microsoft 365 tenant that contains the groups shown in the following table.

Name	Type
Group1	Distribution
Group2	Mail-enabled security
Group3	Security

You plan to create a new Windows 10 Security Baseline profile.
To which groups can you assign to the profile?

A. Group3 only

B. Group1 and Group3 only

C. Group2 and Group3 only

D. Group1, Group2, and Group3

Suggested Answer: *A*
Reference:
https://docs.microsoft.com/en-us/mem/intune/protect/security-baselines-configure#create-the-profile https://docs.microsoft.com/en-us/microsoft-365/admin/create-groups/compare-groups?view=o365-worldwide

Community vote distribution
C (90%) 10%

goape Highly Voted 3 years ago
Selected Answer: C
Tested in dev tenant. You have to create the mail enabled group in another portal, like O365, but you can then select it when assigning the policy.
upvoted 26 times

us3r Highly Voted 3 years ago
Selected Answer: C
sec & email-enabled sec
upvoted 7 times

vanr2000 Most Recent 1 year, 8 months ago
Selected Answer: A
Mail-enabled security groups function the same as regular security groups, except that they cannot be dynamically managed through Azure Active Directory and cannot contain devices.

They include the ability to send mail to all the members of the group.

Mail-enabled security groups can be added to a team.

https://learn.microsoft.com/en-us/microsoft-365/admin/create-groups/compare-groups?view=o365-worldwide#mail-enabled-security-groups
upvoted 2 times

jaycenornin 1 year, 8 months ago
The crux of the question is "You plan to create a new Windows 10 Security Baseline profile."
The question is implying that you're creating a *DEVICE* Baseline profile, in which case only a security group will work because mail-enabled security groups cannot contain devices. QED: A.
upvoted 3 times

bac0n 2 years ago
Tested and confirmed, the answer is C.
upvoted 1 times

TimLyrical 2 years, 3 months ago
Selected Answer: C
both work on my tenant

upvoted 1 times

JamesM9 2 years, 9 months ago

A very tricky question from Microsoft here - the link below specifies that you can apply the baseline to groups of both users and devices.

https://docs.microsoft.com/en-us/mem/intune/protect/security-baselines

Therefore, this makes the answer C - group 2 and 3.

upvoted 4 times

Toschu 2 years, 9 months ago

C:
https://docs.microsoft.com/en-us/mem/intune/protect/security-baselines
"You deploy security baselines to groups of users or devices in Intune, and the settings apply to devices that run Windows 10/11."
The email enabled security group can be used.

upvoted 2 times

BluMoon 2 years, 10 months ago

Selected Answer: A

I agree that it's A. It's a tricky one. Read the post that OneplusOne cites and you'll find this:
"Mail-enabled security groups function the same as regular security groups, except that they cannot be dynamically managed through Azure Active Directory and cannot contain devices."

upvoted 2 times

Bulldozzer 2 years, 10 months ago

This is not a problem because a Windows 10 security Baseline profile can be assigned to either a devices or a users.

upvoted 3 times

Toschu 2 years, 9 months ago

Correct.
"You deploy security baselines to groups of users or devices in Intune, and the settings apply to devices that run Windows 10/11."
https://docs.microsoft.com/en-us/mem/intune/protect/security-baselines

upvoted 2 times

ubt 2 years, 11 months ago

Selected Answer: C

I have just tested this

upvoted 2 times

haazybanj 2 years, 11 months ago

Tested=== Security and Mail enabled Security groups

upvoted 2 times

OneplusOne 2 years, 11 months ago

A:

"Mail-enabled security groups function the same as regular security groups, except that they cannot be dynamically managed through Azure Active Directory and cannot contain devices."
https://docs.microsoft.com/en-us/microsoft-365/admin/create-groups/compare-groups?view=o365-worldwide

upvoted 2 times

BluMoon 2 years, 10 months ago

I agree that it's A. It's a tricky one. Read the post that OneplusOne cites and you'll find this:
"Mail-enabled security groups function the same as regular security groups, except that they cannot be dynamically managed through Azure Active Directory and cannot contain devices."

upvoted 1 times

VirtualJP 3 years ago

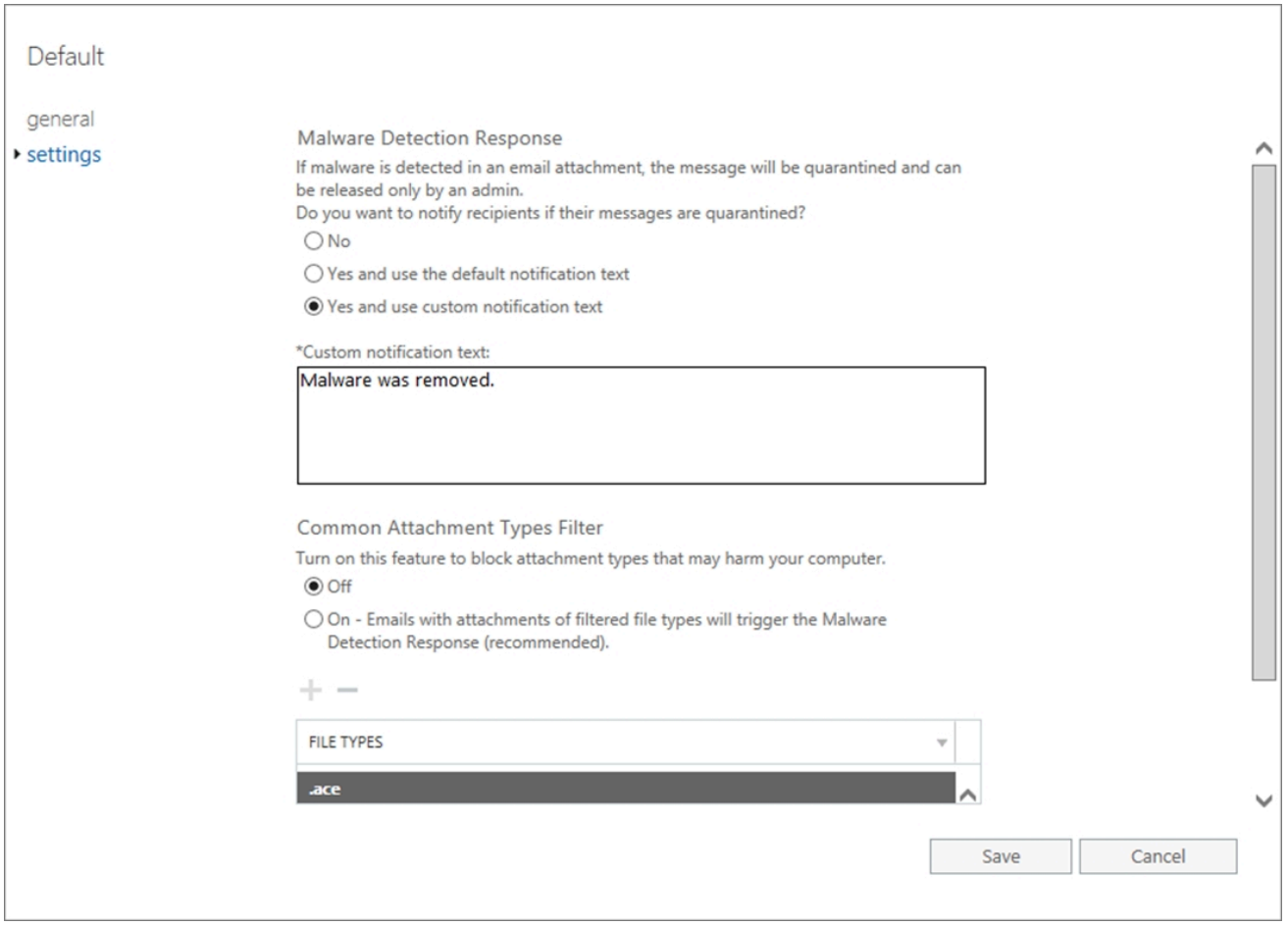
This is one of those questions where both security group types can be used but what is not clear is which is "best practice" in Microsoft's eyes and thus hard to know what the correct answer should be.

upvoted 3 times

Question #88 *Topic 2*

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

The subscription has a single anti-malware policy as shown in the following exhibit.



An email message that contains text and two attachments is sent to User1. One attachment is infected with malware.

How will the email message and the attachments be processed?

A. Both attachments will be removed. The email message will be quarantined, and User1 will receive an email message without any attachments and an email message that includes the following text: ɔ€Malware was removed.ɔ€

B. The email message will be quarantined, and the message will remain undelivered.

C. Both attachments will be removed. The email message will be quarantined, and User1 will receive a copy of the message containing the original text and a new attachment that includes the following text: ɔ€Malware was removed.ɔ€

D. The malware-infected attachment will be removed. The email message will be quarantined, and User1 will receive a copy of the message containing only the uninfected attachment.

Suggested Answer: *C*

Reference:

https://docs.microsoft.com/en-us/microsoft-365/security/office-365-security/anti-malware-protection?view=o365-worldwide#anti-malware-policies

Community vote distribution

C (87%) 13%

VirtualJP Highly Voted 3 years ago

Selected Answer: C

After careful consideration and review of Anti-malware policy behaviour I too will go with C.

upvoted 7 times

us3r Highly Voted 3 years ago

Selected Answer: C

Recipient notifications: By default, a message recipient isn't told that a message intended for them was quarantined due to malware. But, you can enable recipient notifications in the form of delivering ****the original message***** with all attachments removed and replaced by a single file named Malware Alert Text.txt

https://docs.microsoft.com/en-us/microsoft-365/security/office-365-security/anti-malware-protection?view=o365-worldwide#anti-malware-policies

upvoted 6 times

psp65 Most Recent 1 year, 9 months ago

Selected Answer: A

I think that actually the only possible answer is A according to:
https://learn.microsoft.com/en-us/microsoft-365/security/office-365-security/quarantine-quarantine-notifications?view=o365-worldwide

upvoted 2 times

RenegadeOrange 2 years, 3 months ago

It says the message will be quarantined, the user just get's a notification.
It does not say remove attachment and don't quarantine the email...

upvoted 2 times

Doinitza 2 years, 3 months ago

Outdated question, you cannot notify the recipient about a quarantined message with a single anti-malware policy:

* The quarantine policy named NotificationEnabledPolicy is not present in all environments. You'll have the NotificationEnabledPolicy quarantine policy if your organization meets both of the following requirements:
• Your organization existed before the quarantine policy feature was turned on (late July/early August 2021).
• You had one or more anti-spam policies (the default anti-spam policy or custom anti-spam policies) where the Enable end-user spam notifications setting was turned on.

Link: https://docs.microsoft.com/en-us/microsoft-365/security/office-365-security/quarantine-policies?view=o365-worldwide#full-access-permissions-and-quarantine-notifications

So, the right answer would be the “B”

upvoted 5 times

RenegadeOrange 2 years, 3 months ago

Agree question is also outdated so probably won't be in the exam in this format.

upvoted 2 times

TimNov 2 years, 6 months ago

If you read the question closely the message must first be released by an admin and this is never implied to be the case so I would say B.

upvoted 4 times

Goena 3 years ago

I go for answer A.
According the given link: Recipient notifications: By default, a message recipient isn't told that a message intended for them was quarantined due to malware. But, you can enable recipient notifications in the form of delivering the original message with all attachments removed and replaced by a single file named Malware Alert Text.txt that contains the text.

upvoted 3 times

Spacedust 3 years ago

That sounds like answer C to me. Answer A will send 2 separate emails to the recipient

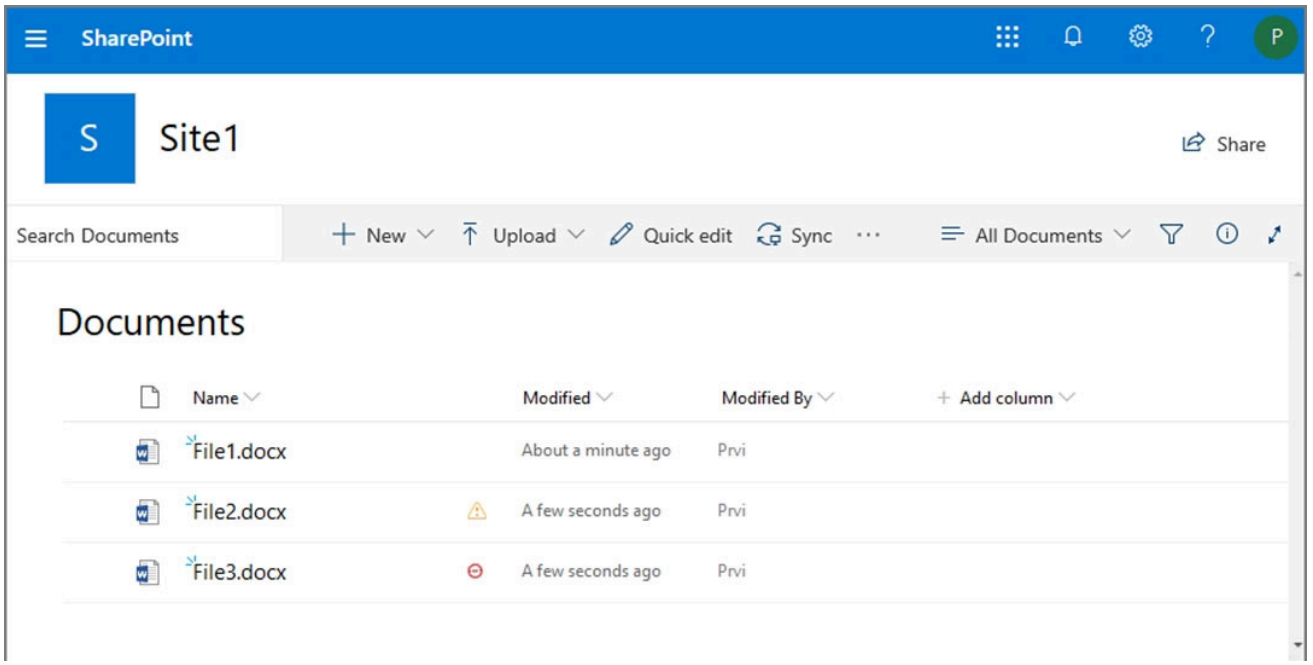
upvoted 5 times

HOTSPOT -

From the Microsoft 365 compliance center, you configure a data loss prevention (DLP) policy for a Microsoft SharePoint Online site named Site1. Site1 contains the roles shown in the following table.

Role	Member
Site owner	Prvi
Site member	User1
Site visitor	User2

Prvi creates the files shown in the exhibit. (Click the Exhibit tab.)



Which files can User1 and User2 open? To answer, select the appropriate options in the answer area.

NOTE: Each correct selection is worth one point.

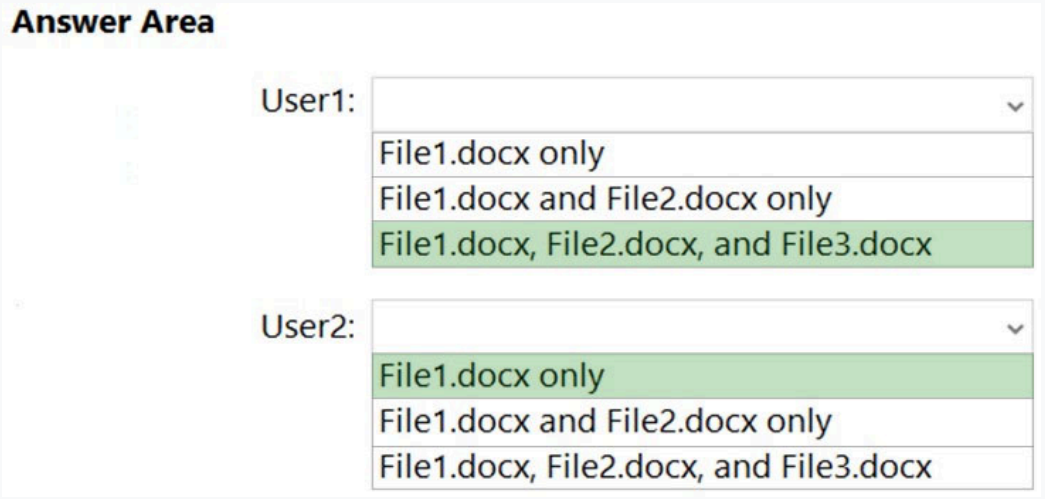
Hot Area:

Answer Area

User1:
- File1.docx only
- File1.docx and File2.docx only
- File1.docx, File2.docx, and File3.docx

User2:
- File1.docx only
- File1.docx and File2.docx only
- File1.docx, File2.docx, and File3.docx

Suggested Answer:



Reference:
https://sharepointmaven.com/4-security-roles-of-a-sharepoint-site/ https://gcc.microsoftcrmportals.com/blogs/office365-news/190220SPIcons/

allesglar Highly Voted 3 years ago

File3 cannot be access by anyone apart from the owner, last user modified the document and site owner.
File2 seems to only have a notification and not block applied. Visitor or member does not play a role in this case. Therefore I believe the right answer is File1 and File2 for both users.
upvoted 39 times

[Removed] 3 years ago

Block users from accessing shared SharePoint, OneDrive, and Teams content
Block everyone. Only the content owner, last modifier, and site admin will continue to have access.
https://docs.microsoft.com/en-us/microsoft-365/compliance/dlp-policy-reference?view=o365-worldwide#actions
Agree with you
upvoted 5 times

us3r Highly Voted 3 years ago

File1 and File2 for both users.

The only available info for the warning icon is following:

If the rule sends a notification about the file, the warning icon appears.
If the rule blocks access to the document, the blocked icon appears..
https://docs.microsoft.com/en-us/microsoft-365/compliance/use-notifications-and-policy-tips?view=o365-worldwide
upvoted 19 times

Amir1909 Most Recent 11 months ago

- File1.docx, File2.docx, and File3.docx
- File1.docx, File2.docx, and File3.docx
upvoted 1 times

Hriz2019 1 year, 4 months ago

Seen in exam aug 2023
upvoted 3 times

BigDazza_111 1 year, 4 months ago

User 1 all files. User 2 file one only.
From this article below, the DLP icons you see in the sharepoint site, are for the DLP policy tips. A member of the site, can override the DLP policy with justification. A guest cannot access files that have sesitive info contain controlled by a DLP policy. https://learn.microsoft.com/en-au/purview/use-notifications-and-policy-tips?redirectSourcePath=%252fen-us%252farticle%252fsend-email-notifications-and-show-policy-tips-for-dlp-policies-87496bc5-9601-4473-8021-cb05c71369c1
upvoted 1 times

Jo696 1 year, 7 months ago

Very little information on this answer, ideally more on what DLP policy was applied and restrictions. However going on the icons alone, File 3 is blocked so only the owner would have access, so I agree with consensus, File 1 and 2 for both users. Question either needs more information is poorly worded.
upvoted 1 times

bleroblero 1 year, 8 months ago
Seen in exam on 2 May 2023
upvoted 3 times

hubran 1 year, 10 months ago
From the presented screenshots this question cannot be answered. Please update the exhibit with the missing image of the DLP policy.
upvoted 1 times

Contactfornitish 2 years, 4 months ago
User2 would be able to access file 1&2 while user1 can access all three. Warning only send notification , doesn't block. File3 is blocked due to sensitive content but in no sense it would be blocked for owner himself
upvoted 3 times

Burki_71 2 years, 3 months ago
User 1 is not the owner of File3 ?
upvoted 3 times

bushwick2002 2 years, 1 month ago
Owner is Prvi; not User 1 or 2
upvoted 1 times

H3adcap 2 years, 5 months ago
Got this question in the MS 500 exam
upvoted 5 times

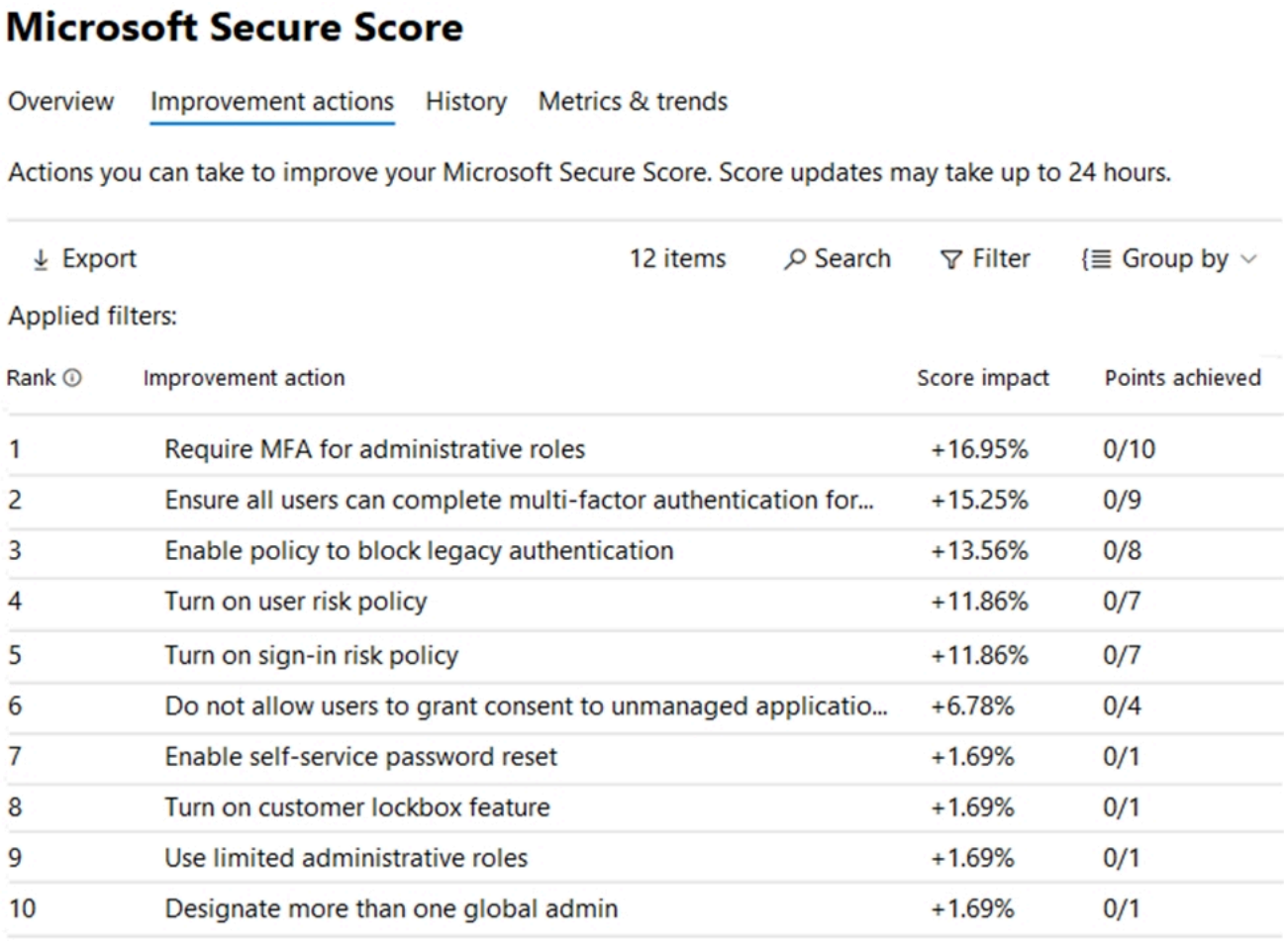
Gwach 2 years, 11 months ago
File 3 can only be accessed by Prvi
Until the sensitive information has been removed, the document access will be restricted to its owner, last modified and the Site owner.
https://social.technet.microsoft.com/wiki/contents/articles/36527.implement-data-loss-prevention-dlp-in-sharepoint-online.aspx
upvoted 4 times

techtest848 3 years ago
Does anyone have a Microsoft Documentation link to support the answers??
upvoted 6 times

Question #90 *Topic 2*

You have a Microsoft 365 E5 tenant.

The Microsoft Secure Score for the tenant is shown in the following exhibit.



Microsoft Secure Score

Overview | Improvement actions | History | Metrics & trends

Actions you can take to improve your Microsoft Secure Score. Score updates may take up to 24 hours.

Export | 12 items | Search | Filter | Group by

Applied filters:

Rank	Improvement action	Score impact	Points achieved
1	Require MFA for administrative roles	+16.95%	0/10
2	Ensure all users can complete multi-factor authentication for...	+15.25%	0/9
3	Enable policy to block legacy authentication	+13.56%	0/8
4	Turn on user risk policy	+11.86%	0/7
5	Turn on sign-in risk policy	+11.86%	0/7
6	Do not allow users to grant consent to unmanaged applicatio...	+6.78%	0/4
7	Enable self-service password reset	+1.69%	0/1
8	Turn on customer lockbox feature	+1.69%	0/1
9	Use limited administrative roles	+1.69%	0/1
10	Designate more than one global admin	+1.69%	0/1

You plan to enable Security defaults for Azure Active Directory (Azure AD).

Which three improvement actions will this affect?

A. Require MFA for administrative roles.

B. Ensure all users can complete multi-factor authentication for secure access

C. Enable policy to block legacy authentication

D. Enable self-service password reset

E. Use limited administrative roles

Suggested Answer: *ABC*

Reference:

https://docs.microsoft.com/en-us/azure/active-directory/fundamentals/concept-fundamentals-security-defaults

Community vote distribution

ABC (100%)

SQL_Student Highly Voted 3 years ago

correct

upvoted 10 times

us3r Highly Voted 3 years ago

Selected Answer: ABC

correct

Requiring all users to register for Azure AD Multi-Factor Authentication.

Requiring administrators to do multi-factor authentication.

Blocking legacy authentication protocols.
Requiring users to do multi-factor authentication when necessary.
Protecting privileged activities like access to the Azure portal.
upvoted 10 times

Amir1909 Most Recent 11 months ago
A, B and C is correct
upvoted 1 times

NitishKarmakar 1 year, 3 months ago
correct
MFA for All users
MFA for Admins
Block legacy auth methods.

https://learn.microsoft.com/en-us/azure/active-directory/fundamentals/concept-fundamentals-security-defaults
upvoted 1 times

Roche4ever 1 year, 3 months ago
Answer is correct: ABC
Was in Exam today, 25 Sept 23
upvoted 1 times

jonny_sins 1 year, 4 months ago
ABCD u dumb fuc
upvoted 1 times

psp65 1 year, 11 months ago
ABC
https://learn.microsoft.com/en-us/azure/active-directory/fundamentals/concept-fundamentals-security-defaults
upvoted 1 times

lusis987 2 years, 3 months ago
In exam 30.09.2022
Pass with 755
upvoted 2 times

H3adcap 2 years, 4 months ago
Was in Exam today 20 Aug 22
upvoted 4 times

Contactfornitish 2 years, 4 months ago
On exam on 13 aug'22
upvoted 2 times

L33D 2 years, 6 months ago
Still valid, on exam Jun 25, 2022
upvoted 1 times

Tuvshinjargal 2 years, 7 months ago
Selected Answer: ABC
022/05/26 Came on today's exam.
upvoted 2 times

venwaik 2 years, 7 months ago
Selected Answer: ABC
Came on exam 09-05-2022
upvoted 2 times

Glorence 2 years, 11 months ago
still valid, it was in my exam last Feb 5, 2022
upvoted 4 times

Question #91 *Topic 2*

You have a Microsoft 365 E5 subscription.
You need to identify which users accessed Microsoft Office 365 from anonymous IP addresses during the last seven days.
What should you do?

A. From the Defender for Cloud Apps admin center, select Users and accounts.

B. From the Microsoft 365 Defender, view the Threat tracker.

C. From the Microsoft 365 admin center, view the Security & compliance report.

D. From the Azure Active Directory admin center, view the Risky sign-ins report.

Suggested Answer: *A*

Community vote distribution

D (98%)

allesglar Highly Voted 3 years ago

Selected Answer: D

There is no way to filter based on the IP in users and accounts of cloud app security.
I believe the answer is D the there is also a 7 day filter for anonymous IPs.

upvoted 26 times

tagada Highly Voted 3 years ago

Selected Answer: D

i think correct answer is D.

upvoted 9 times

Amir1909 Most Recent 11 months ago

D is correct

upvoted 1 times

BigDazza_111 1 year, 3 months ago

Selected Answer: A

Look under heading 'Activity from anonymous IP address' half way down page https://learn.microsoft.com/en-us/azure/active-directory/identity-protection/concept-identity-protection-risks#activity-from-anonymous-ip-address

upvoted 1 times

Jo696 1 year, 7 months ago

Selected Answer: D

Always Azure AD, Risky sign in

upvoted 1 times

DilythiumCrystal 1 year, 10 months ago

That being said the use of users does not seem right as it is a policy that you set up to then see a threat detection from Cloudapps/Control/Policies/threat detections which has now been hidden somewhere in Defender

upvoted 1 times

DilythiumCrystal 1 year, 10 months ago

Correct Answer was A. https://learn.microsoft.com/en-us/defender-cloud-apps/anomaly-detection-policy.

However they have changed the portal so there is no way of knowing if it is still the case.

upvoted 1 times

KrisDeb 2 years, 2 months ago

Selected Answer: D

D, Risky sign-in

upvoted 2 times

Burki_71 2 years, 3 months ago

Selected Answer: D

I think D, Risky Sign-In

upvoted 1 times

mackzone 2 years, 6 months ago

Came on exam 25-06-2022

upvoted 1 times

venwaik 2 years, 7 months ago

Selected Answer: D

Answer D. Came on exam 09-05-2022

upvoted 2 times

JamesM9 2 years, 9 months ago

Tested today - the criteria is met within the risky sign-ins report found within the Azure Active Directory.

Therefore, the answer is D.

upvoted 1 times

ScottT 2 years, 9 months ago

Looking at Risk Detections in https://docs.microsoft.com/en-us/azure/active-directory/identity-protection/howto-identity-protection-investigate-risk . You can see reported Anonymous IP Addresses. This isn't strictly Risky Sign-ins but compared to the other answers it is in the right area. I go with D.

upvoted 2 times

edzio 2 years, 11 months ago

Selected Answer: D

D is correct

upvoted 2 times

Goena 3 years ago

Correct answer is D.

upvoted 4 times

Question #92 *Topic 2*

HOTSPOT -

You have a Microsoft 365 tenant that contains 100 Windows 10 devices. The devices are managed by using Microsoft Endpoint Manager.

You plan to create two attack surface reduction (ASR) policies named ASR1 and ASR2. ASR1 will be used to configure Microsoft Defender Application Guard.

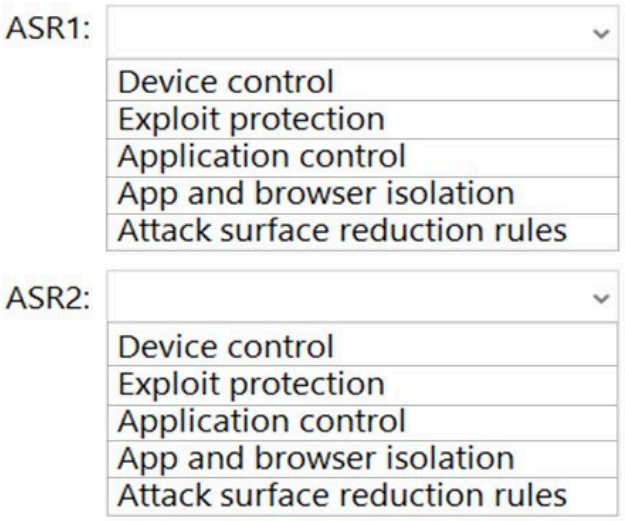
ASR2 will be used to configure Microsoft Defender SmartScreen.

Which ASR profile type should you use for each policy? To answer, select the appropriate options in the answer area.

NOTE: Each correct selection is worth one point.

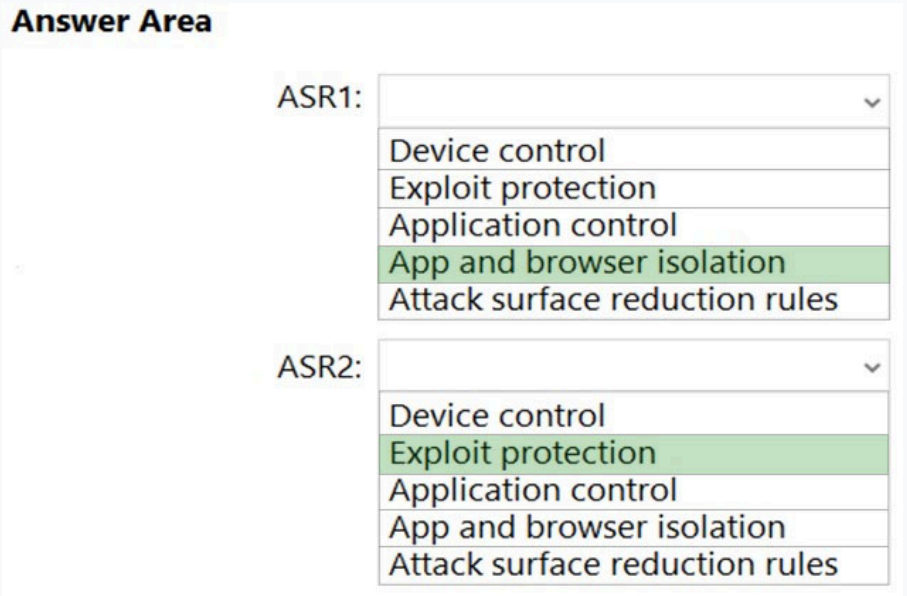
Hot Area:

Answer Area



Suggested Answer:

Answer Area



Reference:

https://docs.microsoft.com/en-us/mem/intune/protect/endpoint-security-asr-policy

JT19760106 Highly Voted 3 years ago

ASR 1 = App and browser isoloation

ASR 2 = Application control

Tested this and application control has an option to "Turn on Windows SmartScreen"

upvoted 24 times

Glorence Highly Voted 2 years, 11 months ago

still valid, it was in my exam last Feb 5, 2022

upvoted 11 times

athadd Most Recent 1 year, 11 months ago

ASR1 - App and Browser isolation
ASR2 - Application Control

https://docs.microsoft.com/en-us/mem/intune/protect/endpoint-security-asr-profile-settings
upvoted 2 times

psp65 1 year, 11 months ago
ASR 1 = App and browser isoloation
ASR 2 = Application control
https://learn.microsoft.com/en-us/mem/intune/protect/endpoint-security-asr-profile-settings?source=recommendations
upvoted 1 times

H3adcap 2 years, 4 months ago
Was in Exam today 20 Aug 2022
upvoted 4 times

venwaik 2 years, 7 months ago
Came on exam 09-05-2022
upvoted 5 times

JamesM9 2 years, 9 months ago
https://docs.microsoft.com/en-us/mem/intune/protect/endpoint-security-asr-profile-settings

1 - App and Browser isolation
2 - Application control
upvoted 4 times

ajna_ 2 years, 9 months ago
ASR 2 | This should be "application control".
upvoted 4 times

FreddyLao 3 years ago
https://docs.microsoft.com/en-us/mem/intune/protect/endpoint-security-asr-profile-settings

App and browser isolation for App Guard
App control for Samrtscreen
upvoted 4 times

SQL_Student 3 years ago
ASR 1 = correct
ASR 2 = Should be "Web protection (Microsoft Edge Legacy)"

I went into that blade in Intune and checked. There is a smartscreen setting under "Web protection (Microsoft Edge Legacy)"
upvoted 1 times

SQL_Student 3 years ago
ASR 2 = Application control
There is a setting for smartScreen there too. I agree with TimurKazan
upvoted 5 times

TimurKazan 3 years ago
Iwould go with
ASR1.App and Browser isolation
ASR2. Application Control
upvoted 4 times

OneplusOne 2 years, 11 months ago
The functionality 'Exploit control' does not exist for Windows Defender for Endpoint.
Application control is correct.
upvoted 4 times

Question #93 *Topic 2*

You have a Microsoft 365 tenant.
You plan to implement Endpoint Protection device configuration profiles.
Which platform can you manage by using the profiles?

A. Ubuntu Linux

B. macOS

C. iOS

D. Android

Suggested Answer: *B*
Intune device configuration profiles can be applied to Windows 10 devices and macOS devices
Note:
There are several versions of this question in the exam. The question has two possible correct answers:
1. Windows 10
2. macOS
Other incorrect answer options you may see on the exam include the following:
1. Android Enterprise
2. Windows 8.1
Reference:
https://docs.microsoft.com/en-us/mem/intune/protect/endpoint-protection-configure

RenegadeOrange Highly Voted 2 years, 3 months ago
Answer is correct...

"Intune device configuration profiles can be applied to Windows 10 devices and macOS devices"
well... device configuration profiles can be applied to all OS types... but... only Win10 and MacOS have the Template called "EndPoint Protection"

Alternatively you now have a new section in Intune called "EndPoint Security" where in there is an "Antivirus" section where you can create the policies, Win10 and MacOS are the only options in there when creating a policy.
upvoted 7 times

psp65 1 year, 11 months ago
I agree with everything, tested in my lab
upvoted 1 times

BigDazza_111 Most Recent 1 year, 3 months ago
wrong. all of them.
upvoted 1 times

m43s 2 years, 3 months ago
Very nice explaination, ty examtopics.
upvoted 1 times

L33D 2 years, 6 months ago
Still valid, on exam Jun 25, 2022
upvoted 1 times

Question #94 *Topic 2*

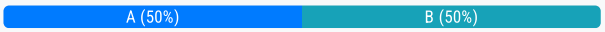
Note: This question is part of a series of questions that present the same scenario. Each question in the series contains a unique solution that might meet the stated goals. Some question sets might have more than one correct solution, while others might not have a correct solution.
After you answer a question in this section, you will NOT be able to return to it. As a result, these questions will not appear in the review screen.
You have a Microsoft 365 E5 subscription that contains a user named User1.
You need to enable User1 to create Compliance Manager assessments.
Solution: From the Microsoft 365 admin center, you assign User1 the Compliance data admin role.
Does this meet the goal?

A. Yes

B. No

Suggested Answer: *B*
Reference:
https://github.com/MicrosoftDocs/microsoft-365-docs/blob/public/microsoft-365/security/office-365-security/permissions-in-the-security-and-compliance-center.md

Community vote distribution



RenegadeOrange Highly Voted 2 years, 3 months ago

Selected Answer: A

Ok now I'm thinking A is actually correct, looking at this article is maps the "Compliance Data Administrator" as an AzureAD role that can ? Manage assessments, templates, and tenant data; assign improvement actions"

https://learn.microsoft.com/en-us/microsoft-365/compliance/compliance-manager-setup?view=o365-worldwide#set-user-permissions-and-assign-roles

upvoted 8 times

RenegadeOrange 2 years, 3 months ago

Ok went ahead and tested it, I was able to create an assessment with a user who I assigned the Compliance Data Administrator role.
Answer is A!

upvoted 7 times

RenegadeOrange Highly Voted 2 years, 3 months ago

Selected Answer: B

B is correct.
Only users who hold a Global Administrator, Compliance Manager Administration, or Compliance Manager Assessor role can create and modify assessments.

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

upvoted 5 times

RenegadeOrange 2 years, 3 months ago

Sorry please ignore, answer is actually A!

upvoted 1 times

Swimpy Most Recent 1 year, 5 months ago

Selected Answer: B

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

upvoted 1 times

Jo696 1 year, 7 months ago

Tested and you can create an assessment. It seems odd as all three answers are correct around this question.

upvoted 2 times

Mshaty 1 year, 7 months ago

Selected Answer: B

https://learn.microsoft.com/en-us/microsoft-365/security/office-365-security/scc-permissions?view=o365-worldwide. Compliance Data manager does not have the permissions however Compliance Admin has

upvoted 2 times

Mshaty 1 year, 7 months ago

compliance manager admin sorry

upvoted 2 times

Projector 1 year, 8 months ago

Ans is No: https://learn.microsoft.com/en-us/microsoft-365/compliance/microsoft-365-compliance-center-permissions?view=o365-worldwide

upvoted 2 times

prabhjot 1 year, 8 months ago

ANS IS B (no)

Role- Compliance data admin

Description - View and edit settings and reports for compliance features.

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

upvoted 2 times

Meebler 1 year, 10 months ago

yes,

The Compliance data admin role is a built-in role in Microsoft 365 that allows users to manage compliance-related data and perform various compliance-related tasks, including creating Compliance Manager assessments. This role provides access to the data and features needed to create and manage assessments, without granting excessive privileges that could compromise the security or compliance of your organization.

On the other hand, the Compliance admin role is a higher-level role that includes all the permissions of the Compliance data admin role, as well as additional permissions to manage compliance settings and policies across your organization. While this role would also enable User1 to create Compliance Manager assessments, it would grant additional privileges that may not be necessary for this specific task.

Therefore, it is recommended to assign the Compliance data admin role to User1 to ensure that they have the appropriate level of access to create Compliance Manager assessments without compromising the security or compliance of your organization.

upvoted 1 times

MEG 1 year, 10 months ago

Selected Answer: B

Only users who hold a Global Administrator, Compliance Manager Administration, or Compliance Manager Assessor role can create and modify assessments.

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

upvoted 2 times

EsamiTopici 1 year, 10 months ago

The answer is A

https://learn.microsoft.com/en-us/microsoft-365/compliance/compliance-manager-setup?view=o365-worldwide#set-user-permissions-and-assign-roles

upvoted 1 times

IPalot 1 year, 11 months ago

Selected Answer: A

Ok, let's clear this up.

Compliance roles which can be added from M365 portal:
- Compliance Data administrator
- Compliance Administrator

Answer is YES.

upvoted 1 times

Y2 1 year, 11 months ago

B Compliance data admin role is not assigned through 365 admin portal!!!

upvoted 2 times

getatit 1 year, 11 months ago

Yes it is. I just added that role to a user via 365 admin portal.

upvoted 3 times

Y2 1 year, 11 months ago

apologises you're right i didn't click the show all by category option

upvoted 3 times

sliix 2 years, 2 months ago

Selected Answer: A

See RenegadeOrange

upvoted 1 times

ercluff 2 years, 6 months ago

B. No Compliance Manager Assessments are conducted by Compliance Manager Administrators and Compliance manager Assessors Reference: https://github.com/MicrosoftDocs/microsoft-365-docs/blob/public/microsoft-365/security/office-365-security/permissions-in-the-security-and-compliance-center.md

upvoted 2 times

Question #95 *Topic 2*

Note: This question is part of a series of questions that present the same scenario. Each question in the series contains a unique solution that might meet the stated goals. Some question sets might have more than one correct solution, while others might not have a correct solution.
After you answer a question in this section, you will NOT be able to return to it. As a result, these questions will not appear in the review screen.
You have a Microsoft 365 E5 subscription that contains a user named User1.
You need to enable User1 to create Compliance Manager assessments.
Solution: From the Microsoft 365 admin center, you assign User1 the Compliance admin role.
Does this meet the goal?

A. Yes

B. No

Suggested Answer: *B*
Reference:
https://github.com/MicrosoftDocs/microsoft-365-docs/blob/public/microsoft-365/security/office-365-security/permissions-in-the-security-and-compliance-center.md

Community vote distribution
A (54%) B (46%)

Swimpy 1 year, 5 months ago
Selected Answer: B
https://learn.microsoft.com/en-us/microsoft-365/security/office-365-security/scc-permissions?view=o365-worldwide
upvoted 1 times

Jo696 1 year, 7 months ago
I have just tested this. In the M365 Admin center, added a user with Compliance Administrator and the user can make new assessments
upvoted 1 times

prabhjot 1 year, 8 months ago
Ans is B (NO) -
Role -= Compliance Administrator
Description =Members can manage settings for device management, data loss prevention, reports, and preservation.
https://learn.microsoft.com/en-us/microsoft-365/security/office-365-security/scc-permissions?view=o365-worldwide
upvoted 2 times

Meebler 1 year, 10 months ago
Compliance data admin role.

The Compliance data admin role is a built-in role in Microsoft 365 that allows users to manage compliance-related data and perform various compliance-related tasks, including creating Compliance Manager assessments. This role provides access to the data and features needed to create and manage assessments, without granting excessive privileges that could compromise the security or compliance of your organization.

On the other hand, the Compliance admin role is a higher-level role that includes all the permissions of the Compliance data admin role, as well as additional permissions to manage compliance settings and policies across your organization. While this role would also enable User1 to create Compliance Manager assessments, it would grant additional privileges that may not be necessary for this specific task.

Therefore, it is recommended to assign the Compliance data admin role to User1 to ensure that they have the appropriate level of access to create Compliance Manager assessments without compromising the security or compliance of your organization.
upvoted 1 times

aims123456 1 year, 10 months ago
No.. Check Compliance Administrator details on this page - https://learn.microsoft.com/en-us/microsoft-365/security/office-365-security/scc-permissions?view=o365-worldwide
upvoted 1 times

EsamiTopici 1 year, 10 months ago

I think is yes also for this question:
https://learn.microsoft.com/en-us/microsoft-365/compliance/compliance-manager-setup?view=o365-worldwide#set-user-permissions-and-assign-roles

upvoted 1 times

MEG 1 year, 10 months ago

Selected Answer: B

Only users who hold a Global Administrator, Compliance Manager Administration, or Compliance Manager Assessor role can create and modify assessments.

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

upvoted 2 times

Feyenoord 1 year, 7 months ago

Look at this: https://learn.microsoft.com/en-us/microsoft-365/security/office-365-security/scc-permissions?view=o365-worldwide#role-groups-in-microsoft-defender-for-office-365-and-microsoft-purview-compliance

upvoted 1 times

IPalot 1 year, 11 months ago

Ok, let's clear this up.

Compliance roles which can be added from M365 portal:
- Compliance Data administrator
- Compliance Administrator

Answer is YES.

upvoted 1 times

Feyenoord 1 year, 8 months ago

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

upvoted 1 times

emanresu 1 year, 11 months ago

Selected Answer: B

B is correct answer
M365 portal allows to assign only below Admin access
Exchange Admin
Global Admin
Global Reder
Helpdesk Admin
Service Support Admin
SharePoint Admin
Teams Admin
Users Admin

upvoted 2 times

Y2 1 year, 11 months ago

Correct!!!

upvoted 1 times

owenMS 1 year, 10 months ago

There is a "Show all by category" drop down which has additional admin roles available to assign to the users.

upvoted 2 times

JCVDB 2 years ago

Selected Answer: B

Following reastman66
Only users who hold a Global Administrator, Compliance Manager Administration, or Compliance Manager Assessor role can create and modify assessments.

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

upvoted 1 times

RenegadeOrange 2 years, 3 months ago

Selected Answer: A

A is correct although the role is called "Compliance Administrator" not "Compliance Admin"

upvoted 2 times

DaDaDave 2 years, 2 months ago

That detail makes me doubt, technically the "Compliance Admin" role does not exist, only the "Compliance Administrator" one

upvoted 1 times

KemalM 2 years, 4 months ago

Selected Answer: A

You can assign from M365 admin center as well

upvoted 2 times

k9_bern_001 2 years, 4 months ago

A is correct, from MS admin center you can assign a user compliance manager role. Its included in security and compliance sub-category

upvoted 2 times

reastman66 2 years, 4 months ago

A is correct as the Admin Center now has it so you can assign roles for AAD, Exchange and Intune.

upvoted 2 times

reastman66 2 years, 4 months ago

Btw this question is saying that assigning the Compliance Administrator role so this is a different solution than question 95

upvoted 1 times

reastman66 2 years, 4 months ago

I guess searching even more would have helped but I found this to support the answer be NO

Only users who hold a Global Administrator, Compliance Manager Administration, or Compliance Manager Assessor role can create and modify assessments.

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

upvoted 3 times

Rickert 2 years, 8 months ago

Answer is correct, see the given link

upvoted 1 times

Starz0rz 2 years, 8 months ago

Selected Answer: A

According to the link hereunder, this would be yes. There is a better role which gives less rights, however, in the Compliance Manager Assessors role.

https://github.com/MicrosoftDocs/microsoft-365-docs/blob/public/microsoft-365/security/office-365-security/permissions-in-the-security-and-compliance-center.md

upvoted 3 times

BoxGhost 2 years, 7 months ago

Trick question, as per the link:

As per the link:
Role groups in the "Security & Compliance Center"

The question states they are trying to assign the role via the 365 admin centre which isn't possible. Therefore the answer is no.

upvoted 7 times

Question #96 *Topic 2*

Note: This question is part of a series of questions that present the same scenario. Each question in the series contains a unique solution that might meet the stated goals. Some question sets might have more than one correct solution, while others might not have a correct solution.
After you answer a question in this section, you will NOT be able to return to it. As a result, these questions will not appear in the review screen.
You have a Microsoft 365 E5 subscription that contains a user named User1.
You need to enable User1 to create Compliance Manager assessments.
Solution: From the Microsoft 365 compliance center, you add User1 to the Compliance Manager Assessors role group.
Does this meet the goal?

A. Yes

B. No

Suggested Answer: *A*
Reference:
https://github.com/MicrosoftDocs/microsoft-365-docs/blob/public/microsoft-365/security/office-365-security/permissions-in-the-security-and-compliance-center.md

Community vote distribution
A (100%)

prabhjot 1 year, 8 months ago
Role=Compliance Manager Assessors
description =Create assessments, implement improvement actions, and update test status for improvement actions.
https://learn.microsoft.com/en-us/microsoft-365/security/office-365-security/scc-permissions?view=o365-worldwide
upvoted 1 times

MEG 1 year, 10 months ago
Selected Answer: A
Only users who hold a Global Administrator, Compliance Manager Administration, or Compliance Manager Assessor role can create and modify assessments.

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

IPalot 1 year, 11 months ago
Ok, let's clear this up.

Compliance roles which can be added from M365 portal:
- Compliance Data administrator
- Compliance Administrator

Answer is NO.
upvoted 3 times

IPalot 1 year, 11 months ago
Disregard my comment, it says "Compliance portal" instead of M365 admin center.

Answer should be yes.
upvoted 2 times

RenegadeOrange 2 years, 3 months ago
Selected Answer: A
Correct
upvoted 1 times

Boeroe 2 years, 6 months ago

Selected Answer: A

In the Compliance Center (Purview) under Permissions you can assign the Microsoft Purview solution roles (Compliance Administrator and Compliance manager Assessor)

upvoted 3 times

ercluff 2 years, 6 months ago

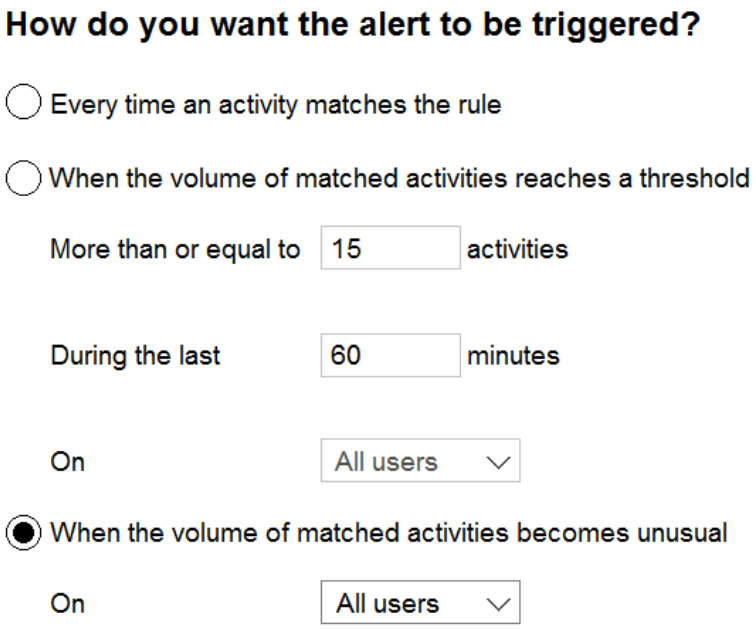
As in Question #94, the role of Compliance manager Assessor is correct for the task. However, that role is assigned through the Security and Compliance admin center, not the Microsoft 365 admin center.

upvoted 2 times

HOTSPOT -

You have a Microsoft 365 E5 subscription.

You configure a new alert policy as shown in the following exhibit.



You need to identify the following:

➪ How many days it will take to establish a baseline for unusual activity.

➪ Whether alerts will be triggered during the establishment of the baseline.

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

NOTE: Each correct selection is worth one point.

Hot Area:

Answer Area

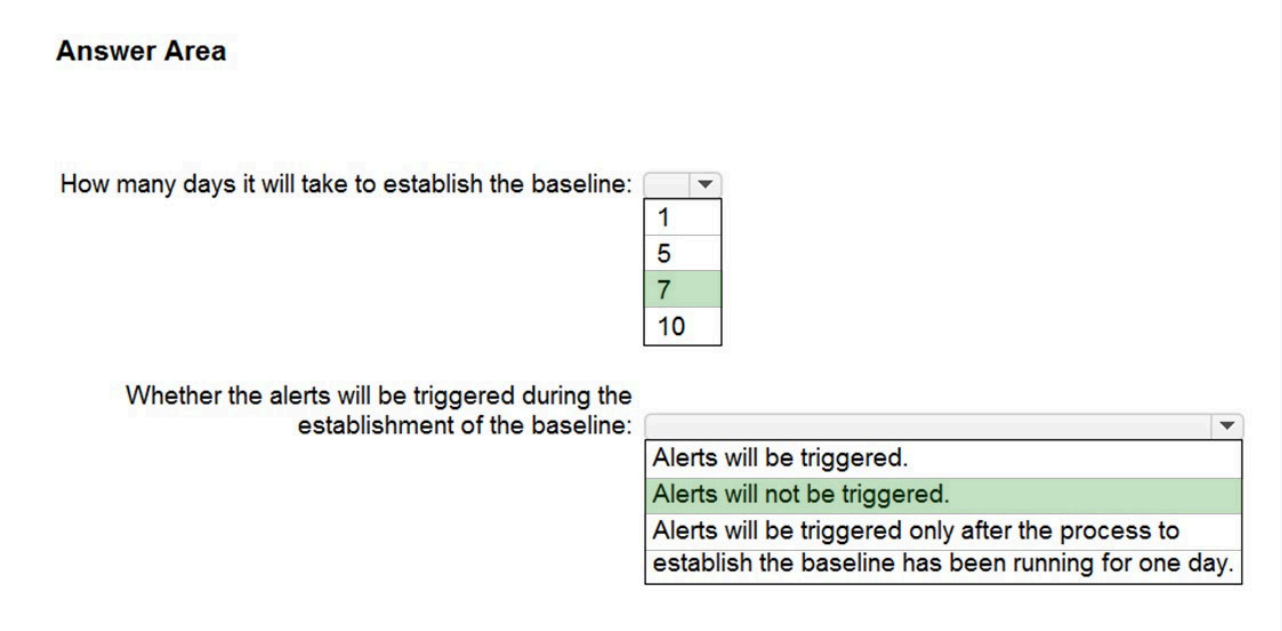
How many days it will take to establish the baseline:

- 1
- 5
- 7
- 10

Whether the alerts will be triggered during the establishment of the baseline:

- Alerts will be triggered.
- Alerts will not be triggered.
- Alerts will be triggered only after the process to establish the baseline has been running for one day.

Suggested Answer:



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

Creature Highly Voted 2 years, 8 months ago

7 days to establish baseline and alerts will not be triggered during this time - https://docs.microsoft.com/en-us/microsoft-365/compliance/alert-policies?view=o365-worldwide - Applicable section starts with " When the alert is triggered "

upvoted 8 times

Amir1909 Most Recent 11 months ago

Correct

upvoted 1 times

QuanN7 1 year, 11 months ago

If you select the setting based on unusual activity, Microsoft establishes a baseline value that defines the normal frequency for the selected activity. It takes up to seven days to establish this baseline, during which alerts won't be generated. After the baseline is established, an alert is triggered when the frequency of the activity tracked by the alert policy greatly exceeds the baseline value

https://learn.microsoft.com/en-us/microsoft-365/compliance/alert-policies?view=o365-worldwide&viewFallbackFrom=o365-worldwide%20-%20Applicable%20section%20starts%20with%20%22%20When%20the%20alert%20is%20triggered%20%22

upvoted 1 times

rnd3131 2 years, 4 months ago

Note: it may take up to a week for the baseline to be established for anomaly alerts. Until then this alert will not be triggered.

upvoted 3 times

Question #98 *Topic 2*

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

Platform	Count
Windows 10	50
Android	50
Linux	50

You need to configure an incident email notification rule that will be triggered when an alert occurs only on a Windows 10 device. The solution must minimize administrative effort.
What should you do first?

A. From the Microsoft 365 admin center, create a mail-enabled security group.

B. From the Microsoft 365 Defender portal, create a device group.

C. From the Microsoft Endpoint Manager admin center, create a device category.

D. From the Azure Active Directory admin center, create a dynamic device group.

Suggested Answer: *B*
Reference:
https://docs.microsoft.com/en-us/microsoft-365/security/defender-endpoint/machine-groups?view=o365-worldwide
https://docs.microsoft.com/en-us/microsoft-365/security/defender-endpoint/configure-email-notifications?view=o365-worldwide

Community vote distribution
B (50%) D (45%) 5%

agnesmandriva 1 year, 9 months ago

Selected Answer: D

"The solution must minimize administrative effort" so D I think.
upvoted 3 times

RiTh73 1 year, 9 months ago

Selected Answer: D

D is Correct. Create a dynamic group to query all those devices with Windows 10 first.
upvoted 2 times

Meebler 1 year, 10 months ago

B is a more specific solution for this particular use case. The Microsoft 365 Defender portal is specifically designed for threat protection, and creating a device group in this portal allows you to better focus on security and threat management. On the other hand, creating a dynamic device group in the Azure Active Directory admin center is a more general solution that could be used for a wider range of scenarios.

B is also easier to use for this specific scenario. Creating a device group in the Microsoft 365 Defender portal is a simple and straightforward process, and you can quickly filter devices based on specific criteria such as operating system version, device type, etc. This can help you create a more targeted device group that meets your needs.

Overall, while D is also a valid choice for creating a device group, B is a better option for this specific scenario because it is a more specific and easier-to-use solution that is designed specifically for threat protection.
upvoted 2 times

Y2 1 year, 11 months ago

Selected Answer: D

The solution must minimize administrative effort!!
upvoted 1 times

bac0n 2 years ago

Selected Answer: B

I know the dynamic device group sounds like the best answer, but this is asking about Defender for Endpoint and Device Groups are king. In Defender for Endpoint you can configure device groups to contain only PCs of a certain OS, IE Windows 10, like the question asks, and Email notifications are configured directly in Defender for Endpoint; this is not asking about an alert policy. The answer is 100% B.

upvoted 4 times

Fala_Fel 1 year, 12 months ago

Agree Ans is B - device groups in 365 Defender by Win OS already have a setting there to select, and you would create the email notification rule in 365 Defender as well. So B minimises admin effort.

upvoted 1 times

DaDaDave 2 years, 2 months ago

Selected Answer: D

D is correct since it will only be needed to be configured once, minimizing administrative effort, dynamic groups can be generated from either endpoint manager or azure AD portal

pyramidhead further explains

upvoted 2 times

Mayank71291 2 years, 2 months ago

Selected Answer: B

In the navigation pane, select Settings > Endpoints > Permissions > Device groups.

Click Add device group.

Enter the group name and automation settings and specify the matching rule that determines which devices belong to the group.

upvoted 3 times

pyramidhead 2 years, 3 months ago

Answer is D. Key is "The solution must minimize administrative effort".

https://learn.microsoft.com/en-us/mem/intune/enrollment/device-group-mapping

"To enable automatic grouping, you must create a dynamic group using attribute-based rules in Azure AD. For instructions, see Using attributes to create advanced rules in the Azure AD documentation. Create an advanced rule for your group using the deviceCategory attribute and the category name you created in Step 1 of this article.

For example, to create a rule that automatically groups devices belonging in the HR category, use the following rule syntax:
device.deviceCategory -eq "HR"

upvoted 3 times

rolia 2 years, 3 months ago

Selected Answer: C

Endpoint.microsoft.com -> Groups -> Dynamic Device Group

Answer seems to be C

upvoted 1 times

RenegadeOrange 2 years, 3 months ago

Selected Answer: B

Correct.
You create an rule for alert notifications and in that you select the device group so you have to create the device group first.

Settings > Endpoints > General > Email notifications.
https://learn.microsoft.com/en-us/microsoft-365/security/defender-endpoint/configure-email-notifications?view=o365-worldwide

Settings > Endpoints > Permissions > Device groups
https://learn.microsoft.com/en-us/microsoft-365/security/defender-endpoint/machine-groups?view=o365-worldwide

upvoted 3 times

Gloomer 2 years, 3 months ago

Selected Answer: D

To minimize the effort required, a dynamic device group is the correct choice. The easiest way to target windows 10.

upvoted 1 times

reastman66 2 years, 4 months ago

I guess it could be B but when creating the Incident notification it only asks for the basic information and then an email address. I think the correct answer is A.

upvoted 1 times

rjoihsoh 2 years, 6 months ago

seems correct - https://docs.microsoft.com/en-us/microsoft-365/security/defender-endpoint/configure-email-notifications?view=o365-worldwide

upvoted 1 times

Question #99 *Topic 2*

Note: This question is part of a series of questions that present the same scenario. Each question in the series contains a unique solution that might meet the stated goals. Some question sets might have more than one correct solution, while others might not have a correct solution.
After you answer a question in this section, you will NOT be able to return to it. As a result, these questions will not appear in the review screen.
You have a Microsoft 365 E5 subscription.
You create an account for a new security administrator named SecAdmin1.
You need to ensure that SecAdmin1 can manage Microsoft Defender for Office 365 settings and policies for Microsoft Teams, SharePoint, and OneDrive.
Solution: From the Microsoft 365 admin center, you assign SecAdmin1 the Exchange admin role.
Does this meet the goal?

A. Yes

B. No

Suggested Answer: *B*
You need to assign the Security Administrator role.
Reference:
https://docs.microsoft.com/en-us/microsoft-365/security/office-365-security/office-365-atp?view=o365-worldwide

RenegadeOrange 2 years, 3 months ago
Exchange Admin is part of Organization Management which can manage the Microsoft 365 Defender portal (security.microsoft.com) but it can't manage Teams, SharePoint & OneDrive so I'd say the answer is correct.
upvoted 1 times

k9_bern_001 2 years, 4 months ago
Correct
upvoted 1 times

Question #100 *Topic 2*

You have a Microsoft 365 tenant.
You plan to implement Endpoint Protection device configuration profiles.
Which platform can you manage by using the profiles?

A. macOS

B. Windows 8.1

C. iOS

D. Android Enterprise

Suggested Answer: *A*
Create a device profile containing Endpoint protection settings
1. Sign in to the Microsoft Endpoint Manager admin center.
2. Select Devices > Configuration profiles > Create profile.
3. Enter the following properties:
4. Platform: Choose the platform of your devices. Your options: macOS

Windows 10 and later -
Profile: Select Templates > Endpoint protection.
5. Select Create.
6. Etc.
Reference:
https://docs.microsoft.com/en-us/mem/intune/protect/endpoint-protection-configure

Community vote distribution

Fala_Fel 1 year, 12 months ago

Selected Answer: A

Ans A - Only macOS has Endpoint Protection available as a Template when creating a configuration profile in Endpoint Manager.

upvoted 2 times

FiberMonkey 2 years, 2 months ago

Answer 'A. macOS' is correct.

upvoted 1 times

Question #101 *Topic 2*

HOTSPOT -

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

Name	Group
Device1	DeviceGroup1
Device2	DeviceGroup2

At 08:00, you create an incident notification rule that has the following configurations:

✑ Name: Notification1

✑ Notification settings

- Notify on alert severity: Low
- Device group scope: All (3)
- Details: First notification per incident

✑ Recipients: User1@contoso.com, User2@contoso.com

At 08:02, you create an incident notification rule that has the following configurations:

✑ Name: Notification2

✑ Notification settings

- Notify on alert severity: Low, Medium
- Device group scope: DeviceGroup1, DeviceGroup2

✑ Recipients: User1@contoso.com

In Microsoft 365 Defender, alerts are logged as shown in the following table.

Time	Alert name	Severity	Impacted assets
08:05	Activity1	Low	Device1
08:07	Activity1	Low	Device1
08:08	Activity1	Medium	Device1
08:15	Activity2	Medium	Device2
08:16	Activity2	Medium	Device2
08:20	Activity1	High	Device1
08:30	Activity3	Medium	Device2
08:35	Activity2	High	Device2

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@contoso.com will receive two incident notification emails for the alert at 08:05.	○	○
User2@contoso.com will receive an incident notification email for the alert at 08:07.	○	○
User1@contoso.com will receive an incident notification email for the alert at 08:20.	○	○

Suggested Answer:

Statements	Yes	No
User1@contoso.com will receive two incident notification emails for the alert at 08:05.	○	●
User2@contoso.com will receive an incident notification email for the alert at 08:07.	●	○
User1@contoso.com will receive an incident notification email for the alert at 08:20.	○	●

Box 1: No -

Notification it has: First notification per incident
Only notify on first occurrence per incident - Select if you want a notification only on the first alert that matches your other selections. Later updates or alerts related to the incident won't send additional notifications.

Box 2: Yes -

Box 3: No -
Severity of the 8:20 incident is high, so neither of the notification rules will trigger.
Note: Alert severity - Choose the alert severities that will trigger an incident notification. For example, if you only want to be informed about high-severity incidents, select High.
Reference:
https://docs.microsoft.com/en-us/microsoft-365/security/defender/incidents-overview

RenegadeOrange Highly Voted 2 years, 3 months ago
N, N, N
One alert not 2.
Already got an alert at 805
Alert high so won't get it.
upvoted 14 times

pyramidhead Highly Voted 2 years, 3 months ago
Y, N, N

User1 will receive two incident notifications from "notification1" and "notification2"
User2 already received incident notification on device1 from the incident at 8:05
User1 will not receive at 8:20 as the severity is high and doesn'y apply
upvoted 8 times

pyramidhead 2 years, 3 months ago
On the first issue. "notification1" rule will send only the first notification per incident, but there is ANOTHER rule "notification2" where user1 is also a recipient and this rule will send a notification to user1 --> user1 will receive 2 incident notifications
upvoted 3 times

Amir1909 Most Recent 11 months, 2 weeks ago
Yes
No
No
upvoted 1 times

Learner2022 1 year, 11 months ago
Can anyone please explain why Activity 1 will have different level severity on the same device but different time frame?
upvoted 1 times

bac0n 2 years ago
I tested this. I made the alert trigger for adding someone to a sharepoint group. I tested it, and I got 2 emails. YNN.
upvoted 6 times

bac0n 2 years ago
I made the ALERTS* trigger I should say, I made TWO alerts with identical triggers and when doing the one action, I got two emails.
upvoted 2 times

bac0n 2 years ago
Triple comment; stand by; I tested with an Alert policy, not a Defender for Endpoint Email notification like the question is asking. I'll try and test and confirm soon.
upvoted 2 times

bac0n 2 years ago
Was able to get a test VM set up on my homelab and onboard it to Defender for Endpoint using script; set up two device groups and added the same machine to each and just made them check for All (I didn't want to do anything unsafe). Downloaded test EICAR_TEST_FILE virus (look it up, it's safe) and I got ONE notification, NOT TWO, for the alert. NNN.
upvoted 15 times

JackeD 1 year, 9 months ago

What a roller coaster! thanks for doing it for us!
upvoted 4 times

Gloomer 2 years, 3 months ago
Should be No/No/No. User 1 only gets a single copy, User 2 was already notified at 8:05 and per "First notification per incident" does not read the 8:07 because they were already sent one at 8:05. User 3 doesnt get a notification because they are not part of a alert that triggers off high.
upvoted 3 times

Gloomer 2 years, 3 months ago
User 1, not user 3.^^^^^
upvoted 1 times

lusis987 2 years, 3 months ago
Second answer is No
User2 got notification at 8:05, so at 8:07 he's not receiving message
upvoted 1 times

situa 2 years, 3 months ago
On the second issue, why is 08:07 the first notification for each incident?
Shouldn't it be 08:05?
upvoted 2 times

Question #102 *Topic 2*

Note: This question is part of a series of questions that present the same scenario. Each question in the series contains a unique solution that might meet the stated goals. Some question sets might have more than one correct solution, while others might not have a correct solution.
After you answer a question in this section, you will NOT be able to return to it. As a result, these questions will not appear in the review screen.
You have a Microsoft 365 subscription.
You discover that some external users accessed content on a Microsoft SharePoint site. You modify the SharePoint sharing policy to prevent sharing outside your organization.
You need to be notified if the SharePoint sharing policy is modified in the future.
Solution: From Microsoft 365 Defender, you create a Threat policy.
Does this meet the goal?

A. Yes

B. No

Suggested Answer: *B*
From the Security & Compliance admin center, Alerts, you create a new alert policy.
Reference:
https://docs.microsoft.com/en-us/microsoft-365/compliance/alert-policies

Community vote distribution
A (50%) B (50%)

Jo696 1 year, 7 months ago

Selected Answer: B

Needs to be an alert policy not threat

upvoted 1 times

boxojunk 1 year, 7 months ago

Selected Answer: A

Defender -> Policies & rules -> Alert Policy

upvoted 2 times

boxojunk 1 year, 7 months ago

Defender -> Policies & rules -> Alert Policy

upvoted 1 times

RenegadeOrange 2 years, 3 months ago

Selected Answer: B

B is correct, given explanation is right.

upvoted 1 times

Question #103 *Topic 2*

You have a Microsoft 365 E5 tenant.
You configure sensitivity labels.
Users report that the Sensitivity button is unavailable in Microsoft Word for the web. The Sensitivity button is available in Word for Microsoft 365.
You need to ensure that the users can apply the sensitivity labels when they use Word for the web.
What should you do?

A. Create an auto-labeling policy.

B. Enable sensitivity labels for files in Microsoft SharePoint Online and OneDrive.

C. Publish the sensitivity labels.

D. Copy policies from Azure Information Protection to the Microsoft 365 compliance center.

Suggested Answer: *C*
Sensitivity labels must be published from the Microsoft 365 compliance center or the Security & Compliance Center to be available in Office applications.
Reference:
https://support.microsoft.com/en-us/office/known-issues-with-sensitivity-labels-in-office-b169d687-2bbd-4e21-a440-7da1b2743edc

Community vote distribution

hcwelcomm Highly Voted 2 years, 3 months ago

Selected Answer: B

https://learn.microsoft.com/en-us/microsoft-365/compliance/sensitivity-labels-sharepoint-onedrive-files?view=o365-worldwide
upvoted 8 times

Amir1909 Most Recent 11 months ago

B is correct
upvoted 1 times

StudyBM 1 year, 9 months ago

Selected Answer: B

I had initially thought it was D, however, after reading the question carefully one can confirm lables are published and reading through MS link - https://learn.microsoft.com/en-us/microsoft-365/compliance/sensitivity-labels-sharepoint-onedrive-files?view=o365-worldwide

Answer has to be B
upvoted 2 times

psp65 1 year, 9 months ago

Selected Answer: B

https://learn.microsoft.com/en-us/microsoft-365/compliance/sensitivity-labels-sharepoint-onedrive-files?view=o365-worldwide
upvoted 2 times

Meebler 1 year, 10 months ago

To ensure that users can apply the sensitivity labels when they use Word for the web, you should publish the sensitivity labels.

When you publish sensitivity labels, they are made available to users in Microsoft 365 services and apps, including Word for the web. This allows users to apply the labels to documents and emails from within those apps.

Auto-labeling policies are used to automatically apply sensitivity labels to content based on predefined rules, and are not directly related to the availability of the Sensitivity button in Word for the web.

Enabling sensitivity labels for files in Microsoft SharePoint Online and OneDrive is also not directly related to the availability of the Sensitivity button in Word for the web, but it can help ensure that sensitive files are appropriately labeled and protected.

Copying policies from Azure Information Protection to the Microsoft 365 compliance center is also not directly related to the availability of the Sensitivity button in Word for the web.

upvoted 2 times

Meebler 1 year, 10 months ago

Enabling sensitivity labels for files in Microsoft SharePoint Online and OneDrive can help ensure that sensitive files are appropriately labeled and protected, but it does not directly address the issue of the Sensitivity button being unavailable in Word for the web.

Publishing the sensitivity labels, on the other hand, is the correct solution to ensure that the users can apply the sensitivity labels when they use Word for the web. When you publish sensitivity labels, they become available to users in Microsoft 365 services and apps, including Word for the web, and the Sensitivity button will become available in Word for the web as well.

Therefore, option C (Publish the sensitivity labels) is the correct answer to the question.

upvoted 2 times

EsamiTopici 1 year, 9 months ago

https://learn.microsoft.com/en-us/microsoft-365/compliance/sensitivity-labels-sharepoint-onedrive-files?view=o365-worldwide I think answer is B, first few lines as the answer

upvoted 1 times

den5_pepito83 1 year, 11 months ago

in exam 5.2.2023

upvoted 2 times

KennethYY 1 year, 11 months ago

the step need to publish label but the whole process is Enable Sensitive label...

upvoted 1 times

RenegadeOrange 2 years, 3 months ago

Selected Answer: B

Agree with comments below and article from hcwelcomm

upvoted 4 times

pyramidrising 2 years, 3 months ago

The link in the answer states that you need to publish the labels in order to view them in O365 Apps. But the question states that the labels are available in Word for O365 so they are published.

Correct answer is B as per the link from hcwelcomm

upvoted 3 times

Arlecchino 2 years, 3 months ago

Selected Answer: B

The link from hcwelcomm is sufficient, first few lines it has the answer.

upvoted 1 times