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

Custom View Settings

Topic 1 - Question Set 1

Question #1 *Topic 1*

Note: The question is included in a number of questions that depicts the identical set-up. However, every question has a distinctive result.
Establish if the solution satisfies the requirements.
Your company Windows 10 computers that are enrolled in Microsoft Intune. You make use of Intune to manage the servicing channel settings of all company computers.
You receive an enquiry regarding the servicing status of a specific computer.
You need to review the necessary policy report.
Solution: You navigate to device status via Device configuration.
Does the solution meet the goal?

A. Yes

B. No

Correct Answer: *B*
Note 1: Intune offers integrated report views for the Windows update ring policies you deploy. These views display details about the update ring deployment and status:
1. Sign in to Microsoft Endpoint Manager admin center.
2. Select Devices > Monitor. Then under Software updates select Per update ring deployment state and choose the deployment ring to review.
Note 2: Use the Windows 10 and later feature updates (Organizational) report
To open the Windows 10 and later feature updates report and view device details for a specific feature updates profile:
In the admin center, go to Reports > Windows updates > select the Reports tab > select Windows Feature Update Report.
Note 3: To help you monitor and troubleshoot update deployments, Intune supports the following reporting options:
Reports in Intune:
Windows 10 and later update rings ↄ€" Use a built-in report that's ready by default when you deploy update rings to your devices.
Windows 10 and later feature updates In public preview ↄ€" Use two built-in reports that work together to gain a deep picture of update status and issues.
Reference:
https://docs.microsoft.com/en-us/intune/windows-update-compliance-reports

Community vote distribution
A (50%) B (50%)

b3arb0yb1m Highly Voted 9 months, 2 weeks ago
Intune offers integrated report views for the Windows update ring policies you deploy. These views display details about the update ring deployment and status:

Sign in to Microsoft Endpoint Manager admin center.

Select Devices > Monitor. Then under Software updates select Per update ring deployment state and choose the deployment ring to review.
upvoted 9 times

RodrigoT 6 months ago
I guess nobody here understood the question: "You need to review the necessary policy report". Review the policy. To do that you need to know what is the error. Go to Endpoint > Devices > Monitor > Noncompliant policies (preview) then you click on the policy that have a number on the "Noncompliant devices" column, then you click on the device with an Error on the "Deployment status" column and you will see clearly the error on the "Setting status" column.
upvoted 1 times

AVR31 5 months, 1 week ago
No, the question says: "Does the solution meet the goal?"
The proposed solution, in the question, is:
"Solution: You navigate to device status via Device configuration."

So, if you apply the solution, does THAT take you to a place where you can review the policy report. That is the question.
And the answer is NO. Going to Device configuration, as suggested in the question does NOT take you to "Device Status". There is no "Device Status" anywhere after clicking on "Device configuration".
The solution in the question clearly states that you get to "Device Status" VIA "Device Configuration". There is no such path.
upvoted 1 times

TonySuccess Most Recent 1 week, 3 days ago
Selected Answer: B
This is B, that path does not exist.

I did this wild thing and logged into endpoint.microsoft.com and selected Devices, what!, wait?! Where is the configuration button? I cried out.

So I clicked All Devices, still no button. So I clicked a device and there at last was the configuration button. But NO STATUS.

x
upvoted 1 times

AVR31 5 months, 1 week ago

Selected Answer: B

Question is not very clear.
If you search for a device in "all devices" and open it, you will have a "Device Configuration" item in the left menu but tha does NOT take you to a "Device Status" as suggested in the question solution: "You navigate to device status via Device configuration."

But, going to "Device Configuration" does show you the applied polices and you can review policy status from that menu.

So, if you want to be technically correct, the answer is B.

upvoted 2 times

ashriem 5 months, 2 weeks ago

Selected Answer: B

I'm going with B, only because the specific 'device status' tab does not appear to contain any policy reports according to this link.

https://docs.microsoft.com/en-us/mem/intune/configuration/device-profile-monitor#:~:text=View%20Details%20on%20A%20Profile

upvoted 1 times

MR_Eliot 6 months ago

Selected Answer: A

Just tested this in my test environment and I can confirm A is correct. In MDM > Monitor > Device Configuration you can see the applied policy.

upvoted 1 times

Vishbsoni 6 months, 3 weeks ago

Selected Answer: A

A is correct, you can check this in device configuration individual devices.

upvoted 3 times

FlitZ 11 months ago

B is correct

upvoted 3 times

Goofer 11 months ago

https://docs.microsoft.com/en-us/mem/intune/protect/windows-update-compliance-reports#reports-for-update-rings-for-windows-10-and-later-policy

upvoted 2 times

Question #2 *Topic 1*

Note: The question is included in a number of questions that depicts the identical set-up. However, every question has a distinctive result.
Establish if the solution satisfies the requirements.
Your company Windows 10 computers that are enrolled in Microsoft Intune. You make use of Intune to manage the servicing channel settings of all company computers.
You receive an enquiry regarding the servicing status of a specific computer.
You need to review the necessary policy report.
Solution: You navigate to the audit logs via Software updates.
Does the solution meet the goal?

A. Yes

B. No

Correct Answer: *B*
Note 1: Intune offers integrated report views for the Windows update ring policies you deploy. These views display details about the update ring deployment and status:
1. Sign in to Microsoft Endpoint Manager admin center.
2. Select Devices > Monitor. Then under Software updates select Per update ring deployment state and choose the deployment ring to review.
Note 2: Use the Windows 10 and later feature updates (Organizational) report
To open the Windows 10 and later feature updates report and view device details for a specific feature updates profile:
In the admin center, go to Reports > Windows updates > select the Reports tab > select Windows Feature Update Report.
Note 3: To help you monitor and troubleshoot update deployments, Intune supports the following reporting options:
Reports in Intune:
Windows 10 and later update rings ↨€" Use a built-in report that's ready by default when you deploy update rings to your devices.
Windows 10 and later feature updates In public preview ↨€" Use two built-in reports that work together to gain a deep picture of update status and issues.
Reference:
https://docs.microsoft.com/en-us/intune/windows-update-compliance-reports

Community vote distribution
B (100%)

b3arb0yb1m Highly Voted 9 months, 2 weeks ago
Intune offers integrated report views for the Windows update ring policies you deploy. These views display details about the update ring deployment and status:

Sign in to Microsoft Endpoint Manager admin center.

Select Devices > Monitor. Then under Software updates select Per update ring deployment state and choose the deployment ring to review.
upvoted 5 times

RodrigoT 6 months ago
None of this is necessary. You just need to review the policy for a specific device. To do that go to Endpoint > Devices > Monitor > Noncompliant policies (preview) then you click on the policy that have a number on the "Noncompliant devices" column, then you click on the device with an Error on the "Deployment status" column and you will see clearly the error on the "Setting status" column. Tested on my system and it even showed me that the error was "Minimum OS version".
upvoted 1 times

TonySuccess Most Recent 1 week, 3 days ago
Selected Answer: B
It is B.
upvoted 1 times

MR_Eliot 5 months, 4 weeks ago
Selected Answer: B
It's asking for a specific device. So I guess the answer is B. In Devices > Monitor > Software Updates you will get a report of how many devices succeeded or failed.
upvoted 2 times

AL99 6 months, 3 weeks ago
Agree B
upvoted 1 times

nmurthy 9 months, 1 week ago
looks correct
upvoted 2 times

FlitZ 11 months ago
Seems correct to me
upvoted 2 times

Question #3 *Topic 1*

You have been tasked with reusing a Windows 10 computer that was assigned to a user who is no longer with the company.
The computer will be assigned to a new user. You plan to make use of Windows AutoPilot to redeploy the computer.
Which of the following actions should you take FIRST?

A. Reset the computer.

B. Wipe the computer.

C. Create a HTML file containing the computer info.

D. Create a CSV file containing the computer info.

Correct Answer: *D*
You can perform Windows Autopilot device registration within your organization by manually collecting the hardware identity of devices (hardware hashes) and uploading this information in a comma-separated-values (CSV) file.
Reference:
https://docs.microsoft.com/en-us/mem/autopilot/add-devices

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

Bones69 Highly Voted 6 months, 3 weeks ago
If the device is already used by the company I would have assumed the device was already registered, so just needed resetting.
upvoted 6 times

BAbdalla Highly Voted 11 months, 2 weeks ago
It's Correct to me!
upvoted 5 times

TonySuccess Most Recent 3 weeks, 2 days ago
If the device was previously using Autopilot then the answer would be A, if the device is using Autopilot for the first time the answer is D.

The question does not clarify this, so its trash. Maybe the exam has updated?
upvoted 1 times

AVR31 5 months, 1 week ago
Selected Answer: D
D because of the "You plan to use AutoPilot", implying that it probably wasn't used before, the the device is not enrolled.
upvoted 1 times

Harold 5 months, 1 week ago
Selected Answer: D
The question doesn't mention whether the device was already enrolled for Windows Autopilot, in that case I'd assume it would still have to get enrolled and therefor I'd select D just to be sure.
upvoted 2 times

MarvinG2 5 months, 3 weeks ago
Windows Autopilot Reset takes the device back to a business-ready state, allowing the next user to sign in and get productive quickly and simply. Specifically, Windows Autopilot Reset:

Removes personal files, apps, and settings.
Reapplies a device's original settings.
Sets the region, language, and keyboard to the original values.
Maintains the device's identity connection to Azure AD.
Maintains the device's management connection to Intune.

Why is it not A?
upvoted 1 times

RodrigoT 5 months, 1 week ago
Because the question says: You "plan" to make use of Windows AutoPilot to redeploy the computer. Meaning you never did it before.
upvoted 1 times

MarvinG2 5 months, 3 weeks ago
If it's already enrolled why do I need the CSV file for computer info again?
upvoted 1 times

RodrigoT 5 months, 1 week ago
The question doesn't say that. Maybe the company was using just on-premises servers before. So, the FIRST thing is D.
upvoted 1 times

Adhikari123 5 months, 3 weeks ago
Selected Answer: D
Its correct
upvoted 2 times

OwerGame 6 months, 1 week ago

Selected Answer: A

Ok, so after 6 months of doing similar tasks in Intune, I would say reset the computer because the assumption is that if it was used by a previous colleague, it was already enrolled and its CSV was already uploaded.

upvoted 5 times

MR_Eliot 5 months, 4 weeks ago

I also think the same. When the device has been used by an other employee it should still be in Intune assuming the user connected his work account to the computer.

upvoted 1 times

ExamTaker1995 6 months, 2 weeks ago

Selected Answer: D

D is the first step you should take

upvoted 2 times

jaroti2116 9 months, 1 week ago

It's not mentioned HW Hash has already registered or not so D is correct.It doesn't matter device is intune register or not

upvoted 1 times

mikl 9 months, 2 weeks ago

Selected Answer: D

Sure D is correct in this sense, however no need for CSV files here - just use the -online parameter when running Get-WindowsAutoPilotInfo

https://oofhours.com/2020/03/25/importing-a-device-hash-directly-into-intune/

upvoted 3 times

b3arb0yb1m 9 months, 2 weeks ago

D. Create a CSV file containing the computer info.

upvoted 3 times

hawkens 11 months, 2 weeks ago

If the computer isn't already managed with Intune, the answer is correct

upvoted 1 times

[Removed] 6 months, 4 weeks ago

Just for clarification: Intune enrollment and autopilot registration are separate things. Devices can be enrolled in Intune without being assigned an autopilot profile. Registration for an autopilot group is what the hardware hash is for. So there are cases where you need that even if the device is already enrolled in Intune.
See https://docs.microsoft.com/en-us/mem/autopilot/enrollment-autopilot

upvoted 1 times

hawkens 11 months, 2 weeks ago

Doesn't this need to be wipe?

upvoted 1 times

FlitZ 11 months, 2 weeks ago

No, you need first de HW ID to enroll the device in intune, Autopilot reconfigures the operative system to your preferences.

upvoted 5 times

Question #4 *Topic 1*

DRAG DROP -

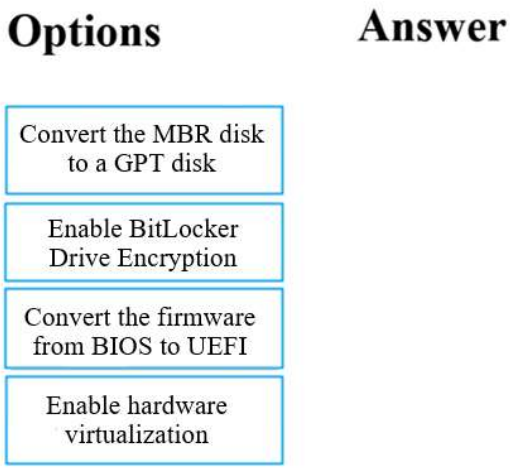
Your company has a number of Windows 7 computers that you want to upgrade to Windows 10.

The computers all have a single MBR disk, and a disabled TPM chip. Also, the computers have hardware virtualization disabled, Data Execution Prevention (DEP) enabled, and UEFI firmware running in BIOS mode.

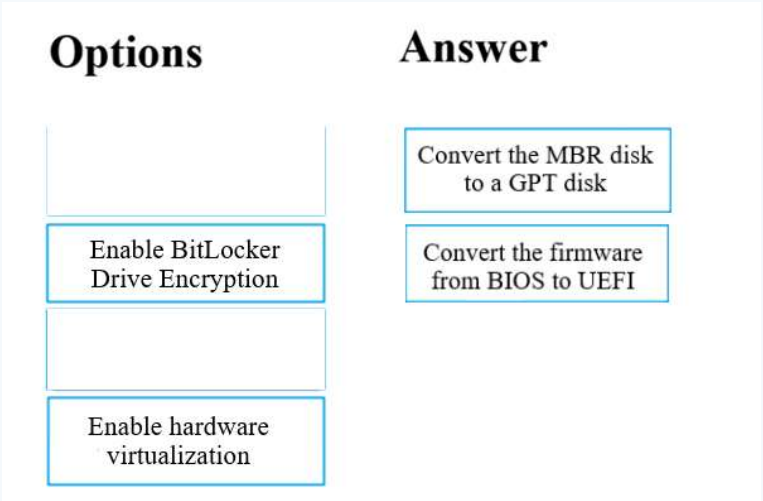
You have been tasked with making sure that Secure Boot can be used by the computers.

Which of the following actions should you take? Answer by dragging the correct options from the list to the answer area. Choose two.

Select and Place:



Correct Answer:



Step 1: Convert the MBR disk to a GPT disk

If you want to ensure that your drive boots into a certain mode, use drives that you've preformatted with the GPT file format for UEFI mode, or the MBR file format for BIOS mode. When the installation starts, if the PC is booted to the wrong mode, Windows installation will fail. To fix this, restart the PC in the correct firmware mode.

Step 2: Convert the firmware from BIOS to UEFI

Reference:

https://docs.microsoft.com/en-us/windows-hardware/manufacture/desktop/boot-to-uefi-mode-or-legacy-bios-mode

AVP_Riga Highly Voted 1 year ago

Seems good

upvoted 7 times

RodrigoT 6 months ago

Same as Question #10 page 6
https://www.examtopics.com/exams/microsoft/md-101/view/6/

upvoted 1 times

BAbdalla Highly Voted 11 months, 2 weeks ago

It's Correct!

upvoted 5 times

MR_Eliot Most Recent 5 months, 4 weeks ago

I agree with the solution.

upvoted 1 times

AL99 6 months, 3 weeks ago

Agree the answwer

upvoted 1 times

Vishbsoni 6 months, 3 weeks ago

MBR > GPT
BIOS > UEFI

UEFI was available in the Windows 7 timeframe. However, Windows 7 systems typically used UEFI in BIOS-Compatibility mode and MBR disks. This means, that to migrate a Windows 7 system to Windows 10 and take advantage of the new security features, the disk must be repartitioned using the GPT format. The system firmware will also have to be configured to use UEFI mode.

https://docs.microsoft.com/en-au/archive/blogs/deploymentguys/security-implications-of-upgrading-to-windows-10#migrating-from-windows-7

upvoted 1 times

mikl 9 months, 2 weeks ago

Correct.

https://docs.microsoft.com/en-us/windows-hardware/manufacture/desktop/windows-setup-installing-using-the-mbr-or-gpt-partition-style?view=windows-11

upvoted 3 times

b3arb0yb1m 9 months, 2 weeks ago

MBR > GPT
BIOS > UEFI

upvoted 3 times

Question #5 *Topic 1*

Your company has an Active Directory domain that includes a large number of Windows 10 computers.
You have recently configured hybrid Microsoft Azure Active Directory (Azure AD) and Microsoft Intune in the environment.
You want to make sure that all the current computers are automatically registered to Azure AD, as well as enrolled in Intune. The strategy that you employ should reduce the administrative effort required to achieve your goal.
Which of the following actions should you take?

A. You should make use of Windows Reset.

B. You should make use of a Windows AutoPilot deployment profile.

C. You should make use of a n Autodiscover service connection point (SCP).

D. You should make use of a device configuration profile.

Correct Answer: *B*
When will Windows Autopilot support on-premises Active Directory enrollment for Windows 10 devices?
Hybrid Azure AD join.
Today [November 2018], we are excited to introduce support for Hybrid Azure AD join (on-premises AD) using Windows Autopilot user-driven mode. This capability is now available with Windows 10, version 1809 (or later).
In this mode, you can use Windows Autopilot to join a device to an on-premises Active Directory domain. Configuring this feature is very similar to the Windows
Autopilot user-driven mode process today:
1. Register the device with Windows Autopilot.
2. Create an Autopilot deployment profile specifying Hybrid Azure AD as the method in which you would like to join devices to Azure AD.
3. Install the Intune Connector for Active Directory on a computer running Windows Server 2016 (or later).
Reference:
https://techcommunity.microsoft.com/t5/Windows-IT-Pro-Blog/Windows-Autopilot-Hybrid-Azure-AD-join-and-automatic/ba-p/286126

Community vote distribution
C (100%)

Haso Highly Voted 12 months ago
B is correct. You have to create an Autopilot deployment profile.
Service Connection Points (SCPs) are objects in Active Directory that hold information about services. Client applications use this information to find and connect to instances of the service.
upvoted 12 times

mikl 9 months, 2 weeks ago
You're statement about SCP is wrong.

https://docs.microsoft.com/en-us/azure/active-directory/devices/hybrid-azuread-join-managed-domains

I know deploying all devices with Autopilot through the Autopilot Deployment Profile could make sure devices are co-managed, however that would require us to re-configure all devices - not sure that's the best solution though.
upvoted 5 times

Fuzzy43 Highly Voted 9 months, 2 weeks ago
C. Is the correct answer. The question is asking "You want to make sure that all the current computers are automatically registered" Keyword all current computers are auto-registered. B, will not give us the solution. When you create an autopilot profile that's purely for newly auto piloted devices. The devices would need to already be registered for us to even click the autopilot option within azure. It will do nothing for existing devices.

https://docs.microsoft.com/en-us/azure/active-directory/devices/hybrid-azuread-join-control
upvoted 11 times

RodrigoT 5 months, 2 weeks ago
You are wrong, read my comments and the link provided. Answer is B.
upvoted 1 times

Harold Most Recent 5 months, 1 week ago
Selected Answer: C
I'd vote for C too, since this is a step you'd have to take before any of the other three options.
upvoted 1 times

MR_Eliot 5 months, 2 weeks ago
Selected Answer: C
In order for your Windows 10 devices to know to join Azure AD and which Azure AD tenant to join, Azure AD Connect populates Active Directory with a service connection point (SCP), configured on the SCP configuration page.
upvoted 1 times

RodrigoT 5 months, 2 weeks ago
Wrong again.
upvoted 1 times

MarvinG2 5 months, 3 weeks ago

Selected Answer: C

https://petri.com/how-to-automatically-hybrid-azure-ad-join-and-intune-enroll-pcs/
in order for your Windows 10 devices to know to join Azure AD and which Azure AD tenant to join, Azure AD Connect populates Active Directory with a service connection point (SCP), configured on the SCP configuration page

upvoted 2 times

PChi 6 months, 1 week ago

I would go with B. You would have to go to each computer and configure hybrid join when using SCP. Whereas, with Intune MDM, you can configure profiles to join Azure AD as hybrid... this profile can be deployed to a group.

upvoted 3 times

ExamTaker1995 6 months, 2 weeks ago

Selected Answer: C

C https://docs.microsoft.com/en-us/azure/active-directory/devices/howto-hybrid-azure-ad-join

upvoted 2 times

RodrigoT 5 months, 2 weeks ago

Another wrong.

upvoted 2 times

RodrigoT 7 months ago

The link provided says: "new Microsoft Intune capability that will make it easier for you to use Windows Autopilot with EXISTING devices by allowing you to automatically register all targeted devices with Windows Autopilot. Available as part of the Windows Autopilot deployment profile creation page in Intune, you will now be able to create a Windows Autopilot deployment profile and flag that profile so that it will automatically register any devices targeted by that profile into Windows Autopilot.
With this feature, you simply enable automatic Windows Autopilot registration in a deployment profile and target that profile to all devices in the organization. The next time a targeted device checks into Intune, it will be automatically registered into Windows Autopilot and show up in your list of registered devices.

upvoted 3 times

RodrigoT 5 months, 2 weeks ago

FINAL ANSWER: B is correct. I just got this question on a KAPLAN exam practice. You can use an Autopilot Deployment Profile for joining computers to your on-premisses AD domain, and the steps are:
1-Register the device with Windows Autopilot
2-Create an Autopilot deployment profile
3-Specify Hybrid Azure AD as the method
4-Install the Intune Connector for Active Directory on a computer running Windows Server 2016
https://techcommunity.microsoft.com/t5/windows-it-pro-blog/windows-autopilot-hybrid-azure-ad-join-and-automatic/ba-p/286126

upvoted 3 times

RodrigoT 5 months, 1 week ago

This question will repeat on Page 6 Question #11 and the answer is always B. Autopilot Deployment Profile.

upvoted 2 times

IcemanJim 7 months, 2 weeks ago

"All the current computers are automatically registered to Azure AD" Autopilot won't do this. A CSP is required for Hybrid AAD join. C is the correct answer.

upvoted 1 times

IcemanJim 7 months, 2 weeks ago

But that wouldn't enrol them into Intune, I'm confused. Resetting a bunch of devices to take advantage of Autopilot doesn't sound like less admin. This question is awful.

upvoted 2 times

forummj 8 months, 1 week ago

I think I see it now. The two questions from Topic 1 & 2 that are similar.

This question states you recently configured hybrid AAD, so you haven't implemented it yet, thus you can still use the SCP setup from this link,
https://docs.microsoft.com/en-us/azure/active-directory/devices/hybrid-azuread-join-managed-domains

Whereby the second question states that you have implemented hybrid AAD, that means the SCP portion can't be rerun, so the easier way of doing it would be to use GPO.

Autopilot, resets devices, this is not something you will be wanting for all your devices.

upvoted 2 times

RodrigoT 5 months, 2 weeks ago

Check the link provided. Answer is B.

upvoted 2 times

rovert94 8 months, 1 week ago

Selected Answer: C

I beleive C is correct. With Autopilot, you would have to basically reset the machine. WIth SCP it uses the existing AD domain to send AD tenant information to the endpoints.

"Configure a service connection point: Your devices use a service connection point (SCP) object during the registration to discover Azure AD tenant information."

See this: https://docs.microsoft.com/en-us/azure/active-directory/devices/hybrid-azuread-join-manual

upvoted 3 times

lucadp010 8 months, 2 weeks ago

Selected Answer: C

C. is correct
https://blog.alschneiter.com/2018/08/16/configure-device-registration-with-azure-ad-connect/

upvoted 3 times

Solaris2002 8 months, 3 weeks ago

The problem with B, Autopilot Deployment Profile, is that only applies if you re-register a device using Autopilot. Meaning you are configuring a machine from scratch. That is not "least administrative effort" the answer should be C and then use GPO to enroll since its a hybrid environment

upvoted 2 times

nmurthy 9 months, 1 week ago

Answer c is correct

upvoted 2 times

b3arb0yb1m 9 months, 2 weeks ago

B. You should make use of a Windows AutoPilot deployment profile.

upvoted 1 times

hawkens 11 months, 2 weeks ago

Answer should be C and then create a GPO for auto register client machines.

upvoted 4 times

FlitZ 11 months, 2 weeks ago

B is correct because is the one that takes less administrative effort. With one task you distribute to the pc's

upvoted 2 times

Trifoks 11 months, 3 weeks ago

B is correct, taken from the provided website:

“... use Windows Autopilot with existing devices by allowing you to automatically register all targeted devices with Windows Autopilot. Available as part of the Windows Autopilot deployment profile creation page in Intune, you will now be able to create a Windows Autopilot deployment profile and flag that profile so that it will automatically register any devices targeted by that profile into Windows Autopilot.”

upvoted 3 times

ercluff 10 months ago

Your quoted web-page from techcommunity.microsoft.com describes a process by which Azure tenant computers can be added to an on-premise AD domain through Autopilot and Intune features. Here is a passage near the top of that page: 'In this mode, you can use Windows Autopilot to join a device to an on-premises Active Directory domain. Configuring this feature is very similar to the Windows Autopilot user-driven mode process today:

Register the device with Windows Autopilot.
Create an Autopilot deployment profile specifying Hybrid Azure AD as the method in which you would like to join devices to Azure AD.
Install the Intune Connector for Active Directory on a computer running Windows Server 2016 (or later)."
The passage you quoted is near the bottom of that page and is referring to steps in loading web-tenant devices into the AutoPilot process to then add to the on-premises AD domain. Since this test question comes from the on-premises AD domain insuring all systems get registered in the AAD and enrolled in Intune, the Service Connection Point autodiscover and Group Policy steps are the only path to achieve complete hybrid status. Answer should be C.

upvoted 2 times

Question #6 *Topic 1*

You need to consider the underlined segment to establish whether it is accurate.

You have recently created a provisioning package that uses Comp%RAND:1% as the device name.

You will be able to successfully run the package on as much as 5 devices.

Select `No adjustment required` if the underlined segment is accurate. If the underlined segment is inaccurate, select the accurate option.

A. No adjustment required

B. 10

C. 15

D. 20

Correct Answer: *B*

The device name uses a single random number (applied by %RAND:1%). This allows for 10 unique values (0 9 "€ƛ).

Community vote distribution

B (100%)

Davidchercm Highly Voted 1 year, 2 months ago

i think the answer is wrong , it should be no change needed . %Rand:1% means that it will only randomize one number, from 0-9. That means a total of 10 computers.

upvoted 8 times

anzer123 1 year ago

I agree on this too. the 1 represent a single value which can be any of this 0-9. hence no adjustment required

upvoted 1 times

anzer123 1 year ago

on a second thought, i think 10 should be the right answer. The question says for as much as meaning maximum. %rand:1% will generate random digits from 0-9 hence You will be able to successfully run the package on as much as 10 devices not 5

upvoted 2 times

Solaris2002 6 months, 3 weeks ago

If the Answer is B then what is stopping the other answers from also being right? You could also have %RAND:15% and that would also be right, you can run it on 5 or more devices you just get more integers.

upvoted 1 times

daonga 1 year, 2 months ago

I agree on this. Unless I'm missing something (which is likely), there's not need to change the config.

upvoted 3 times

IcemanJim 10 months, 3 weeks ago

And 10 is more than 5. So the statement is incorrect meaning "B" is the correct answer.
They don't word this question very well, which adds confusion.

upvoted 2 times

FlitZ 11 months, 2 weeks ago

You are missing the focus of the underlined segment that says: "You will be able to successfully run the package on as much as 5 devices."
%RAND:1% means from 0-9 like you said.
Therefore, the statement in the question is incorrect. Opcion B is the correct answer.

upvoted 5 times

Harold Most Recent 5 months, 1 week ago

Selected Answer: B

Rand:1 = 10 combinations, so B

upvoted 1 times

MR_Eliot 5 months, 2 weeks ago

Selected Answer: B

I mean, how is this even a question :)

upvoted 1 times

AL99 6 months, 3 weeks ago

Answer B

upvoted 1 times

RodrigoT 7 months, 1 week ago

Explaining the question: It says that if you use "%RAND:1%" then "You will be able to successfully run the package on on as much as 5 devices". That's wrong. You need to adjust it to: "on as much as 10 devices". So the answer B is correct. The expression: "underlined segment" is confusing because there is nothing really "underlined" there, maybe there is in a real exam. Here it's more like if a "condition" is true or not, and what's the right answer.

upvoted 1 times

RodrigoT 7 months, 1 week ago

https://docs.microsoft.com/en-us/windows/configuration/wcd/wcd-accounts#computeraccount

Check the part: ComputerName.
upvoted 1 times

forummj 8 months, 3 weeks ago
This took me a while, but I think I see it now, so for those still struggling with the wording. The portion you need to look at is;

"You will be able to successfully run the package on as much as 5 devices." - Yes, this is technically correct, however, you are being asked if this exactly correct, which it isn't. The line should read.

"You will be able to successfully run the package on as much as 10 devices." - Hence why the answer is B: 10
upvoted 4 times

b3arb0yb1m 9 months, 2 weeks ago
B. 10 is correct.
upvoted 1 times

ElFrijole 9 months, 3 weeks ago
maybe someone can help me make sense of the mob discussion, the underlined can run up to 5 machines, the random generator will give us results for 10 machines, (0-9) so the answer would be A. No adjustment right? the way I see it, is that yes, the randomizer will give us 10, but doesn't the question state, leave it be if no change? or we CAN leave it if needed?
upvoted 1 times

FrancisLai 11 months, 1 week ago
I agree with FlitZ. The answer B is correct because the underlined segment says that: "You will be able to successfully run the package on as much as 5 devices." However the %RAND:1% can be applied as much as 10 devices.
upvoted 1 times

tf444 11 months, 3 weeks ago
You will be able to successfully run the package on as many as 10 devices.
upvoted 2 times

BAbdalla 1 year ago
The answer is wrong in my understanding. The description of the answer even informs that it is wrong:

Correct answer: B
The device name uses a single random number (applied by %RAND:1%). This allows for 10 unique values (0 9 "€λ).

Therefore, I believe the correct option is alternative A, No adjustment required, as %RAND:1% is enough to deploy up to 10 devices, and in the description it is saying that only 5. will be deployed.
upvoted 2 times

FlitZ 11 months, 2 weeks ago
The answer B is correct because the segment says that: You will be able to successfully run the package on as much as 5 devices. And the random applied can be aplied only to 10 devices.
upvoted 2 times

Jeff8989 1 year ago
Use %RAND:x% to generate x number of random digits in the name, where x must be a number less than 63. In this case, %RAND:1% means only 1 computer.
upvoted 1 times

Sironin 1 year ago
A number of digits specifies the length rather than the contents. So 1 digit is any number 0-9. 2 digits is 00-99. 3 digits is 000-999 and so on.
Comp%RAND:8% might produce Comp12345678, Comp09523216, Comp13200077, etc

Answer B. 10 is correct.
upvoted 3 times

Question #7 *Topic 1*

Your company has an Active Directory domain, named weylandindustries.com. The domain is synced to Microsoft Azure Active Directory (Azure AD) and all company computers have been enrolled in Microsoft Intune.
You are preparing to perform a Wipe action on certain company devices.
Which of the following operating systems support the Wipe action? Choose all that apply.

A. Windows Vista

B. Windows 8.1

C. Windows 10

D. iOS

Correct Answer: *CD*
The iOS/iPadOS, Android, and Windows 10 platforms are the only platforms currently supported for wiping corporate data from Intune managed apps.
Reference:
https://docs.microsoft.com/en-us/mem/intune/apps/apps-selective-wipe

Angarali 5 months, 2 weeks ago
BCD.
IOS devices can also be wiped
https://docs.microsoft.com/en-us/mem/intune/remote-actions/devices-wipe
upvoted 1 times

Deric 2 weeks, 5 days ago
It clearly states that it is NOT available for iOS in the link.
upvoted 1 times

MR_Eliot 5 months, 4 weeks ago
I'm going with BCD. I think the question is more likely asking which operating systems are capable of wipe function. How can we assume the company has Windows 8.1 devices when the questions don't mention that and yet it is one of the options.
upvoted 1 times

AL99 6 months, 3 weeks ago
Shall be BCD, as the question just ask about "the following operating systems support the Wipe action".
upvoted 1 times

PiPe 8 months ago
The default enrollment of an IOS mobile device is device-based instead of user-based. So device-based enrolled IOS devices CAN be wiped.
You can set up user-based enrollment however to disable the wipe functionality but it requires 'a bit more' configuration:
https://docs.microsoft.com/en-us/mem/intune/enrollment/ios-user-enrollment
So the answer is BCD
upvoted 3 times

Mun11 8 months, 1 week ago
It says "The Wipe action is not available for iOS/iPadOS devices enrolled with User Enrollment. To create a User Enrollment profile: Set up iOS/iPadOS and iPadOS User Enrollment
upvoted 2 times

Z33di 8 months, 2 weeks ago
Its B and C. They are talking about Active Directory as well. Only Windows Devices have been discussed. iOS doesn't need AD. 8.1 and 10 is the answer.
upvoted 3 times

Angarali 5 months, 2 weeks ago
"all company computers have been enrolled in Microsoft Intune"

You can't wipe from AD in the first place, so I trust that's just to confuse us.
upvoted 1 times

manwithplan 8 months, 2 weeks ago
The question states "company computers" and not "company devices" so it should only be the windows versions by that logic.
upvoted 4 times

b3arb0yb1m 9 months, 2 weeks ago
B. Windows 8.1
C. Windows 10
upvoted 3 times

CaloyB_IT 10 months, 1 week ago
According to the supporting article you can wipe IOS devices as well so the answer is BCD
https://docs.microsoft.com/en-us/mem/intune/remote-actions/devices-wipe#wipe
upvoted 4 times

IcemanJim 10 months, 3 weeks ago
Likely to be B and C, but not D as it doesn't mention mobile devices being enrolled into Intune.

upvoted 3 times

Fuzzy43 9 months, 2 weeks ago

iOS devices have the wipe option when they are enrolled as corporate devices

upvoted 3 times

fatape 10 months, 3 weeks ago

I'm pretty sure it's either BCD or a trick question. You can wipe iOS with MMD and intune.
https://docs.microsoft.com/en-us/mem/intune/remote-actions/devices-wipe

upvoted 3 times

Malinaa 11 months, 2 weeks ago

BCD is correct answer:
https://docs.microsoft.com/en-us/mem/intune/remote-actions/devices-wipe

upvoted 3 times

hawkens 11 months, 2 weeks ago

BCD is correct

upvoted 3 times

[Removed] 1 year ago

You can wipe an iPhone/iPad as well.

upvoted 4 times

Sironin 1 year ago

Yup, answer should be BCD, Windows 8.1 and on as well as iOS.

upvoted 3 times

FlitZ 11 months, 2 weeks ago

Incorrect, you can't wipe iOS /iPadOS devices enrolled with intune.
See the note here: https://docs.microsoft.com/en-us/mem/intune/remote-actions/devices-wipe

upvoted 3 times

HellRaver80 10 months, 2 weeks ago

If you're using bulk actions to wipe several iOS/iPadOS devices at once, the data plan is not preserved by default. thats the note later on

upvoted 1 times

nanerforever 1 year, 2 months ago

Wipe is available from Windows 8.1 and later

upvoted 4 times

Question #8 *Topic 1*

Your company has an Active Directory domain, named weylandindustries.com. The domain is synced to Microsoft Azure Active Directory (Azure AD) and all company computers have been enrolled in Microsoft Intune.
You are preparing to perform a Fresh Start action on certain company devices.
Which of the following operating systems support the Fresh Start action? Choose all that apply.

A. Windows Vista

B. Windows 8.1

C. Windows 10

D. iOS

Correct Answer: *C*
The Fresh Start device action removes any apps that are installed on a PC running Windows 10, version 1709 or later.
Reference:
https://docs.microsoft.com/en-us/intune/device-fresh-start

Community vote distribution
C (100%)

Davidchercm Highly Voted 1 year, 2 months ago
The Fresh Start device action removes any apps that are installed on a PC running Windows 10, version 1709 or later.
upvoted 10 times

anzer123 Highly Voted 1 year ago
fresh starts works on W10 only. the answer is correct
upvoted 5 times

Angarali Most Recent 5 months, 2 weeks ago
Selected Answer: C
Only available on Win 10
upvoted 1 times

MR_Eliot 5 months, 4 weeks ago
Selected Answer: C
The Fresh Start device action removes any apps that are installed on a PC running Windows 10, version 1709 or later. Fresh Start helps remove pre-installed (OEM) apps that are typically installed with a new PC.
upvoted 1 times

PiPe 8 months ago
The default enrollment of an IOS mobile device is device-based instead of user-based. So device-based enrolled IOS devices CAN be wiped. You can set up user-based enrollment however to disable the wipe functionality but it requires 'a bit more' configuration:
https://docs.microsoft.com/en-us/mem/intune/enrollment/ios-user-enrollment
So the answer is BCD
upvoted 1 times

PiPe 8 months ago
Ignore my previous comment. Was supposed to be for the previous question regarding wipe functionality.

The answer to this fresh start question is obviously C. Windows 10
https://docs.microsoft.com/en-us/mem/intune/remote-actions/device-fresh-start
upvoted 2 times

mikl 9 months, 2 weeks ago
Selected Answer: C
The Fresh Start device action removes any apps that are installed on a PC running Windows 10, version 1709 or later. Fresh Start helps remove pre-installed (OEM) apps that are typically installed with a new PC.
upvoted 2 times

b3arb0yb1m 9 months, 2 weeks ago
C. Windows 10
upvoted 1 times

waseemsmr 10 months ago
Selected Answer: C
Correct
upvoted 2 times

Question #9 *Topic 1*

Your company has a number of Windows 10 Microsoft Azure Active Directory (Azure AD) joined workstations. These workstations have been enrolled in Microsoft
Intune.
You have been tasked with making sure that the has self-service password reset enabled on the logon screen. You have navigated to the Microsoft Intune blade.
Which of the following is the setting you should configure?

A. The Device configuration settings.

B. The Device compliance settings

C. The Windows AutoPilot deployment settings

D. The App protection settings

Correct Answer: *A*
Create a device configuration policy in Intune
1. Sign in to the Azure portal and select Intune.
2. Create a new device configuration profile by going to Device configuration > Profiles, then select + Create Profile
3. Etc.
Reference:
https://docs.microsoft.com/en-us/azure/active-directory/authentication/tutorial-sspr-windows

Community vote distribution
A (100%)

MR_Eliot 5 months, 4 weeks ago
Selected Answer: A
I agree with the answer.
upvoted 1 times

RodrigoT 5 months, 1 week ago
And the same question will repeat on Page 7 Question #17.
upvoted 1 times

mikl 9 months, 2 weeks ago
A is correct.
https://docs.microsoft.com/en-us/azure/active-directory/authentication/howto-sspr-windows
upvoted 2 times

RodrigoT 7 months ago
This information is outdated. When you try to access Intune from Azure Portal there is a message: "Microsoft Intune has moved! Our new home is the Microsoft Endpoint Manager admin center."
upvoted 2 times

b3arb0yb1m 9 months, 2 weeks ago
A. The Device configuration settings.
upvoted 1 times

Malinaa 11 months, 2 weeks ago
The default answer is correct
https://docs.microsoft.com/en-us/azure/active-directory/authentication/howto-sspr-windows
upvoted 2 times

tf444 11 months, 2 weeks ago
In AAD \password rest \SSPR.
upvoted 2 times

badguytoo 1 year, 1 month ago
none of these are correct, as self-password reset done in Azure Portal not in Intune.
upvoted 2 times

[Removed] 1 year ago
Your are wrong. You can use a OMA-URI. There's a graphical way to to this in Intune as well, a new way.
upvoted 8 times

mikl 9 months, 2 weeks ago
Wrong : https://docs.microsoft.com/en-us/azure/active-directory/authentication/howto-sspr-windows
upvoted 1 times

petersnet 9 months, 2 weeks ago
Remember: You have navigated to the Microsoft Intune blade, answer is correct
upvoted 2 times

Question #10 *Topic 1*

You need to consider the underlined segment to establish whether it is accurate.
Your company's Microsoft Azure subscription includes an Azure Log Analytics workspace.
After deploying a new Windows 10 computer, which belongs to a workgroup, you are tasked with making sure that you are able to utilize Log Analytics to query events from the new computer.
You configure the new computer's commercial ID.
Select `No adjustment required` if the underlined segment is accurate. If the underlined segment is inaccurate, select the accurate option.
What should you do on Computer1?

A. No adjustment required.

B. install the Azure Diagnostic extension on the new computer

C. install the Dependency agent on the new computer

D. install the Microsoft Monitoring Agent on the new computer

Correct Answer: *D*
The Azure Monitor agent (AMA) collects monitoring data from the guest operating system of Azure and hybrid virtual machines and delivers it to Azure Monitor where it can be used by different features, insights, and other services such as Microsoft Sentinel and Microsoft Defender for Cloud.
Reference:
https://docs.microsoft.com/en-us/azure/azure-monitor/agents/azure-monitor-agent-migration

Community vote distribution
D (100%)

BAbdalla Highly Voted 1 year ago
It's Correct.

Another question about this theme:
You have a Microsoft Azure subscription that contains an Azure Log Analytics workspace.
You deploy a new computer named Computer1 that runs Windows 10. Computer1 is in a workgroup.
You need to ensure that you can use Log Analytics to query events from Computer1.
What should you do on Computer1?
Answer: D. Install the Microsoft Monitoring Agent
upvoted 20 times

RodrigoT 5 months, 1 week ago
And this question will repeat on Page 7 Question #24. Same answer, install MMA.
upvoted 1 times

ADHDave Highly Voted 1 year ago
Seems correct.
https://docs.microsoft.com/en-us/services-hub/premier/health/mma-setup

"On the Agent Setup Options page, choose the Connect the agent to Azure Log Analytics (OMS) option."
upvoted 6 times

MR_Eliot Most Recent 5 months, 4 weeks ago
Selected Answer: D
I agree with the answer.
upvoted 1 times

mikl 9 months, 2 weeks ago
Selected Answer: D
D is correct.

The Log Analytics agent for Windows is often referred to as Microsoft Monitoring Agent (MMA). The Log Analytics agent for Linux is often referred to as OMS agent.

https://docs.microsoft.com/en-us/azure/azure-monitor/agents/agents-overview#supported-operating-systems
upvoted 1 times

b3arb0yb1m 9 months, 2 weeks ago
D. install the Microsoft Monitoring Agent on the new computer
upvoted 1 times

Question #11 *Topic 1*

You need to consider the underlined segment to establish whether it is accurate.
After installing a feature update on a Windows 10 computer, you have 7 days to roll back the update
Select `No adjustment required` if the underlined segment is accurate. If the underlined segment is inaccurate, select the accurate option.

A. No adjustment required.

B. 10

C. 90

D. 30

Correct Answer: *B*
By default settings, Windows 10 allows you to go back to the previous version of Windows in the first 10 days. And after that system Automatically delete this old windows folder, and can't go back to the previous build windows 10.
Reference:
https://howtofixwindows.com/roll-back-windows-10-upgrade-after-10-days-limit/

Community vote distribution
B (100%)

4Shawsy Highly Voted 8 months ago
This style of question is horrendous
upvoted 7 times

ADHDave Highly Voted 1 year ago
Correct.

There's one catch: you can only uninstall a major update within 10 days after installing it, so act fast if you think the update may have borked your system. After 10 days, Microsoft removes the old files to free up space on your hard drive, and you can no longer roll back.
upvoted 7 times

MR_Eliot Most Recent 5 months, 4 weeks ago
Selected Answer: B
B is indeed correct.
upvoted 1 times

MR_Eliot 5 months, 2 weeks ago
Default is 10 days, however, you can change the uninstall period up to 60 days with policies.
upvoted 1 times

Ivandro 8 months, 4 weeks ago
Correct
upvoted 1 times

mikl 9 months, 2 weeks ago
Selected Answer: B
https://support.microsoft.com/en-us/windows/go-back-to-windows-8-1-40e2d7dc-f640-b0e5-56e1-b41a27e28533
upvoted 1 times

mikl 9 months, 2 weeks ago
Selected Answer: B
B. 10 days.

https://www.bleepingcomputer.com/news/microsoft/how-to-get-more-time-to-uninstall-windows-10-feature-updates/
upvoted 1 times

b3arb0yb1m 9 months, 2 weeks ago
B. 10 is correct.
upvoted 1 times

BAbdalla 1 year ago
seems correct to me
upvoted 4 times

Question #12 *Topic 1*

Your company has a Microsoft 365 subscription configured for their environment. All devices in the environment have Windows 10 installed.
You have been instructed to make sure that users are not allowed to enroll devices in the Windows Insider Program.
To achieve your goal, you access Microsoft 365 Device Management.
Which of the following actions should you take?

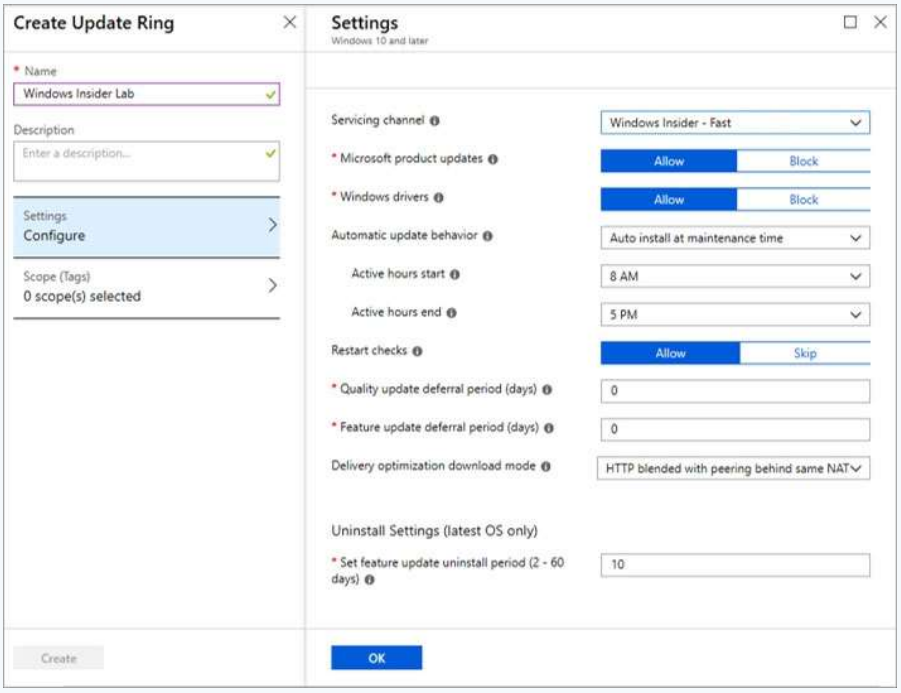
A. You should configure a Windows 10 security baseline.

B. You should configure an app protection policy.

C. You should configure device restriction policy.

D. You should configure a Windows 10 update ring.

Correct Answer: *D*
Set up Insider Preview builds using Intune
1. Log in to the Azure portal and select Intune.
2. Go to Software Updates > Windows 10 Update Rings and select + Create to make an Update Ring policy.
Add a name and select the Settings section to configure its settings.



3. Etc.
Reference:
https://docs.microsoft.com/en-us/windows-insider/business/manage-builds

Question #13 *Topic 1*

Note: The question is included in a number of questions that depicts the identical set-up. However, every question has a distinctive result. Establish if the solution satisfies the requirements.
Your company has a hybrid configuration of Microsoft Azure Active Directory (Azure AD). Your company also has a Microsoft 365 subscription.
After creating a conditional access policy for Microsoft Exchange Online, you are tasked with configuring the policy to block access to Exchange Online. However, the policy should allow access for hybrid Azure AD-joined devices
Solution: You should configure the Device platforms settings.
Does the solution meet the goal?

A. Yes

B. No

Correct Answer: *B*
Within a Conditional Access policy, an administrator can make use of signals from conditions like risk, device platform, or location to enhance their policy decisions.

Client apps -
By default, all newly created Conditional Access policies will apply to all client app types even if the client apps condition isn't configured. These conditions are commonly used when requiring a managed device, blocking legacy authentication, and blocking web applications but allowing mobile or desktop apps.
Reference:
https://docs.microsoft.com/en-us/azure/active-directory/conditional-access/conditions#device-state

MR_Eliot 5 months, 4 weeks ago

Selected Answer: B

The answer is correct. You can change the setting in "AAD > Security > Conditional Access > [your policy] > Access Controls > Grant" and then chose "Require Hybrid Azure AD joined device".

upvoted 2 times

Cisco 6 months ago

When I inspect the options I can use, I cant see an option here for a platform of Hybrid Azure AD Joined when I check the options in the drop down list for platforms. Has anyone visually verified this is an option?
I only have the options of: Android, IOS, Windows Phone, Windows, Mac OS or Linux.

upvoted 1 times

Anker 8 months, 1 week ago

Just as an FYI, device state is being deprecated so eventually Filters will take the place of Device State so that would be the correct answer going forward.:)

upvoted 4 times

syougun200x 3 weeks, 6 days ago

I see. In conditinal access
conditions -> filter for devices -> exclude filtered devices.

upvoted 1 times

Harisasikumar92 11 months, 2 weeks ago

B is correct. You need to include the device state to include the Azure AD Hybrid Joined option.

upvoted 4 times

Harisasikumar92 11 months, 2 weeks ago

Edit: Create a new conditional access policy and configure the device state to EXCLUDE Hybrid Azure AD Joined devices

upvoted 7 times

Question #14 *Topic 1*

Note: The question is included in a number of questions that depicts the identical set-up. However, every question has a distinctive result. Establish if the solution satisfies the requirements.
Your company has a hybrid configuration of Microsoft Azure Active Directory (Azure AD). Your company also has a Microsoft 365 subscription.
After creating a conditional access policy for Microsoft Exchange Online, you are tasked with configuring the policy to block access to Exchange Online. However, the policy should allow access for hybrid Azure AD-joined devices
Solution: You should configure the Client apps settings.
Does the solution meet the goal?

A. Yes

B. No

Correct Answer: *B*
Within a Conditional Access policy, an administrator can make use of signals from conditions like risk, device platform, or location to enhance their policy decisions.

Client apps -
By default, all newly created Conditional Access policies will apply to all client app types even if the client apps condition isn't configured. These conditions are commonly used when requiring a managed device, blocking legacy authentication, and blocking web applications but allowing mobile or desktop apps.
Reference:
https://docs.microsoft.com/en-us/azure/active-directory/conditional-access/conditions#device-state

AVP_Riga Highly Voted 11 months, 1 week ago
Create a new conditional access policy and configure the device state to EXCLUDE Hybrid Azure AD Joined devices
upvoted 8 times

ashriem Most Recent 5 months, 2 weeks ago
Selected Answer: A
https://www.enowsoftware.com/solutions-engine/conditional-access-to-exchange-online-and-office-365
upvoted 1 times

ashriem 5 months, 1 week ago
Sorry, meant to select B
upvoted 1 times

MR_Eliot 5 months, 2 weeks ago
Selected Answer: B
Changing my answer to B. The policy is already there, so I assume it's only configured for Exchange Online, therefore Cloud Apps has been already configured. To meet the requirement you will need to change the access controls or create a new policy.
upvoted 1 times

MR_Eliot 5 months, 4 weeks ago
Selected Answer: A
I think the answer is Yes from my own research. They want to only apply the policy for the Exchange Online.
upvoted 1 times

MR_Eliot 5 months, 2 weeks ago
Changed my Answer to B
upvoted 1 times

Question #15 *Topic 1*

Note: The question is included in a number of questions that depicts the identical set-up. However, every question has a distinctive result. Establish if the solution satisfies the requirements.
Your company has a hybrid configuration of Microsoft Azure Active Directory (Azure AD). Your company also has a Microsoft 365 subscription.
After creating a conditional access policy for Microsoft Exchange Online, you are tasked with configuring the policy to block access to Exchange Online. However, the policy should allow access for hybrid Azure AD-joined devices
Solution: You should configure the Device state settings.
Does the solution meet the goal?

A. Yes

B. No

Correct Answer: *A*
Within a Conditional Access policy, an administrator can make use of signals from conditions like risk, device platform, or location to enhance their policy decisions.

Client apps -
By default, all newly created Conditional Access policies will apply to all client app types even if the client apps condition isn't configured. These conditions are commonly used when requiring a managed device, blocking legacy authentication, and blocking web applications but allowing mobile or desktop apps.
Reference:
https://docs.microsoft.com/en-us/azure/active-directory/conditional-access/conditions#device-state

anzer123 Highly Voted 1 year ago
The device state condition can be used to exclude devices that are hybrid Azure AD joined and/or devices marked as compliant with a Microsoft Intune compliance policy from an organization's Conditional Access policies.
upvoted 8 times

JGN Highly Voted 10 months ago
Device state (preview)
Caution

This preview feature is being deprecated. Customers should use Filter for devices condition in Conditional Access to satisfy scenarios, previously achieved using device state (preview) condition.
upvoted 7 times

TonySuccess 3 weeks, 2 days ago
Word. This is right.
upvoted 1 times

MR_Eliot Most Recent 5 months, 4 weeks ago
Selected Answer: B
[Device State] This preview feature has been deprecated. Customers should use Filter for devices condition in Conditional Access to satisfy scenarios, previously achieved using device state (preview) condition.
This preview feature has been deprecated. Customers should use Filter for devices condition in Conditional Access to satisfy scenarios, previously achieved using device state (preview) condition.
https://docs.microsoft.com/en-us/azure/active-directory/conditional-access/concept-conditional-access-conditions#device-state-preview
upvoted 2 times

RodrigoT 5 months, 2 weeks ago
Thank you for your link. Even though the answer provided (A) is correct for this outdated question.
upvoted 1 times

mikeliny228 6 months, 3 weeks ago
Selected Answer: B
Device state was preview feature and for now it is deprecated.
For me, answer is no.
upvoted 4 times

ExamTaker1995 6 months, 2 weeks ago
answer is yes. the question is just old. the new question will refer to filters instead.
upvoted 8 times

ADHDave 1 year ago
Correct.

The device state condition can be used to exclude devices that are hybrid Azure AD joined and/or devices marked as compliant with a Microsoft Intune compliance policy from an organization's Conditional Access policies.
upvoted 7 times

Question #16 *Topic 1*

Your company makes use of Microsoft Intune to manage computers.
You have been tasked with configuring Windows Hello for Business. You are preparing to create an Intune profile to achieve your goal.
Which of the following is an operating system that supports Windows Hello for Business?

A. Windows Vista

B. Windows 8.1

C. Windows 10

D. macOS

Correct Answer: *C*
You can configure Windows Hello for Business settings in an Identity protection profile. Identity protection profiles are part of device configuration policy in
Microsoft Intune. With an Identity protection profile, you can configure settings on discrete groups of Windows 10/11 devices.
Reference:
https://docs.microsoft.com/en-us/intune/protect/identity-protection-windows-settings

badguytoo Highly Voted 1 year, 1 month ago
That one is easy... Not sure whether it will show up in the really world.
upvoted 9 times

MR_Eliot Most Recent 5 months, 4 weeks ago
Selected Answer: C
Is this even a question? Easiest answer of my life!
upvoted 1 times

mikl 9 months, 2 weeks ago
C. Windows 10
upvoted 1 times

b3arb0yb1m 9 months, 2 weeks ago
C. Windows 10.
upvoted 1 times

sbmkhize 12 months ago
i dought it will
upvoted 3 times

Question #17 *Topic 1*

Your company has a large number of Android and iOS devices, which are enrolled in Intune.
You are preparing to deploy new Intune policies will apply to devices, based on the version of Android or iOS that is being run.
You are required to make sure that the policies are able to target the devices according to your plan.
Which of the following actions should you take?

A. You should start by accessing Intune and configuring corporate device identifiers.

B. You should start by accessing Microsoft Azure Active Directory (Azure AD) and configuring Device settings.

C. You should start by accessing Microsoft Azure Active Directory (Azure AD) and configuring Application settings.

D. You should start by creating a distribution group.

Correct Answer: *B*
Device Properties -

Operating System Version -

Minimum OS version -
When a device doesn't meet the minimum OS version requirement, it's reported as noncompliant. A link with information about how to upgrade is shown. The end user can choose to upgrade their device, and then get access to company resources.
By default, no version is configured.

Maximum OS version -
When a device is using an OS version later than the version specified in the rule, access to company resources is blocked. The user is asked to contact their IT admin. Until a rule is changed to allow the OS version, this device can't access company resources.
Reference:
https://docs.microsoft.com/en-us/intune/compliance-policy-create-android https://docs.microsoft.com/en-us/intune/compliance-policy-create-ios

Jeff8989 Highly Voted 1 year ago
Correct answer is to create a dynamic membership groups so none of the anwsers are correct.
upvoted 14 times

AVP_Riga 11 months, 1 week ago
Yes, correct!
upvoted 1 times

mikl 9 months, 2 weeks ago
I agree.

https://social.technet.microsoft.com/Forums/windows/en-US/f0b7451f-7663-4420-989b-7721f9ecc2ec/creating-dynamic-group-for-android-corporateowned-fully-managed-user-devicespreview?forum=microsoftintuneprod

However - I would go with the answer provided here - since no other options are feasible.
upvoted 1 times

RodrigoT 5 months, 2 weeks ago
You are right but it's not what they're asking. I guess I understand now the question:
B. You should "start" by Azure AD > Device settings. There you need to enable "Users may register their devices with Azure AD". The link bellow explains that if you want to manage device identities by using the Azure portal, the devices need to be either registered or joined to Azure AD. In this case (Android and IOS) registered. This is just the start, of course. If don't do this, how can you apply the policies.

https://docs.microsoft.com/en-us/azure/active-directory/devices/device-management-azure-portal#configure-device-settings
upvoted 1 times

RodrigoT 5 months, 1 week ago
The worst part is that this question will repeat at Page 15 Question #10 and there the answer is: you configure "first" dynamic membership groups, even if another option available is the device settings. Crazy, crazy, crazy.
upvoted 1 times

Toaster Most Recent 7 months, 1 week ago
The best answer would be to create a filter that allows to define the desired OS version for Android, iOS & Windows 10/11. It could look like "Apply to Android 9 and above" and exclude all devices that don't meet this criteria.

https://docs.microsoft.com/en-us/mem/intune/fundamentals/filters
upvoted 3 times

Mun11 8 months ago
distribution group is nothing but device collection for a specific model
upvoted 1 times

badguytoo 1 year, 1 month ago

none of these are correct. :(
upvoted 4 times

RodrigoT 7 months ago
You're right! From the links provided the answer should be: "You should start by accessing Microsoft Azure Active Directory (Azure AD) and configuring Device COMPLIANCE settings."
upvoted 1 times

Alfred666 1 year, 2 months ago
One can change device settings in Android and IOS via Intune.
upvoted 1 times

nanerforever 1 year, 2 months ago
At the previously similar question, the answer is: D. Groups that have dynamic membership rules in Microsoft Azure Active Directory (Azure AD)
upvoted 4 times

ExamStudy101 1 year, 2 months ago
A distribution group is for email
upvoted 8 times

maciak 9 months, 1 week ago
distribution list is for email not group.
upvoted 2 times

Bouncy 5 months, 3 weeks ago
There is no such thing as "distribution group", it's clearly distribution list they mean and it cannot contain machine accounts
upvoted 1 times

Question #18 *Topic 1*

You need to consider the underlined segment to establish whether it is accurate.
Your company has Microsoft Azure Active Directory (Azure AD) joined Windows 10 Pro computers that have been enrolled in Microsoft Intune.
You have been tasked with making sure that the computers are upgraded to Windows 10 Enterprise.
You start by configuring a device enrollment policy in Intune.
Select `No adjustment required` if the underlined segment is accurate. If the underlined segment is inaccurate, select the accurate option.
What should you configure in Intune?

A. No adjustment required

B. an app protection policy

C. a Windows AutoPilot deployment profile

D. A device configuration profile

Correct Answer: *D*
Do you have a bunch of Windows 10 Pro devices and would like upgrade them to Windows 10 Enterprise? Microsoft 365 (specifically Microsoft Intune) can help you!
First, create a Microsoft Intune configuration policy. In the Azure Portal navigate to Microsoft Intune -> Device Configuration -> Profiles. Click Create Profile
Reference:
https://blogs.technet.microsoft.com/skypehybridguy/2018/09/21/intune-upgrade-windows-from-pro-to-enterprise-automatically/

Malinaa Highly Voted 11 months, 2 weeks ago
Correct: https://docs.microsoft.com/nl-nl/archive/blogs/skypehybridguy/intune-upgrade-windows-from-pro-to-enterprise-automatically
upvoted 9 times

MR_Eliot Most Recent 5 months, 4 weeks ago
Selected Answer: D
The answer is correct.
upvoted 2 times

lucadp010 8 months, 2 weeks ago
Selected Answer: D
D is correct
upvoted 4 times

RodrigoT 5 months, 1 week ago
Of course, they are already enrolled in Microsoft Intune. Why enroll them again?
upvoted 1 times

mikl 9 months, 2 weeks ago
D is correct.

https://docs.microsoft.com/en-us/mem/intune/configuration/edition-upgrade-configure-windows-10
upvoted 3 times

b3arb0yb1m 9 months, 2 weeks ago
D. A device configuration profile
upvoted 2 times

Question #19 *Topic 1*

Your company has a Microsoft 365 subscription.
You have enrolled all the company computers in Microsoft Intune.
You have been tasked with making sure that Microsoft Exchange Online is only accessible from known locations.
Which of the following actions should you take?

A. You should create a device configuration profile.

B. You should create a device compliance policy.

C. You should create a Windows AutoPilot deployment profile.

D. You should create a conditional access policy.

Correct Answer: *D*
Within a Conditional Access policy, an administrator can make use of signals from conditions like risk, device platform, or location to enhance their policy decisions.

Locations -
When configuring location as a condition, organizations can choose to include or exclude locations. These named locations may include the public IPv4 network information, country or region, or even unknown areas that don't map to specific countries or regions. Only IP ranges can be marked as a trusted location.
Reference:
https://docs.microsoft.com/en-us/azure/active-directory/conditional-access/conditions

Cabanna94 Highly Voted 1 year, 2 months ago
I agree with the answer. Known locations can be configured under “conditions”.
upvoted 9 times

Angarali Most Recent 5 months, 2 weeks ago
Selected Answer: D
Correct
upvoted 1 times

MR_Eliot 5 months, 4 weeks ago
Selected Answer: D
The answer is indeed correct.
upvoted 1 times

fmodel 7 months, 2 weeks ago
Selected Answer: D
D is correct answer https://docs.microsoft.com/en-us/mem/intune/protect/conditional-access
upvoted 3 times

DDHP7 7 months, 3 weeks ago
Selected Answer: D
D is correct answer
upvoted 1 times

mikl 9 months, 2 weeks ago
D. You should create a conditional access policy.

Conditions - Locations
upvoted 1 times

b3arb0yb1m 9 months, 2 weeks ago
D. You should create a conditional access policy.
upvoted 1 times

sbmkhize 12 months ago
Seems true,,
upvoted 2 times

Question #20 *Topic 1*

Your company has a Microsoft 365 subscription.
You have enrolled all the company computers in Microsoft Intune.
You have been tasked with making sure that devices with a high Windows Defender Advanced Threat Protection (Windows Defender ATP) risk score are locked.
Which of the following actions should you take?

A. You should create a device configuration profile.

B. You should create a device compliance policy.

C. You should create a Windows AutoPilot deployment profile.

D. You should create a conditional access policy.

Correct Answer: *ABD*
You can integrate Microsoft Defender for Endpoint with Microsoft Intune as a Mobile Threat Defense solution. Integration can help you prevent security breaches and limit the impact of breaches within an organization.
To be successful, you'll use the following configurations in concert:
* Establish a service-to-service connection between Intune and Microsoft Defender for Endpoint.
* 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.
Reference:
https://docs.microsoft.com/en-us/mem/intune/protect/advanced-threat-protection

MR_Eliot 5 months, 4 weeks ago
Selected Answer: B
I agree.
upvoted 1 times

PChi 6 months, 1 week ago
Answer B. Compliance and Conditional Policies are dependent on each other ("To use device compliance policies to block devices from corporate resources, Azure AD Conditional Access must be set up."- see link below) but you use compliance policy to retire noncompliant devices.
https://docs.microsoft.com/en-us/mem/intune/protect/actions-for-noncompliance#:~:text=1%20Send%20email%20to%20end%20users%3A%20When%20the,device%20and%20remove%20the%20device%20from%20Intune%20management.
CONTIDITONAL ACCESS:
https://docs.microsoft.com/en-us/mem/intune/protect/conditional-access-intune-common-ways-use
upvoted 1 times

Anker 8 months, 1 week ago
Tested this, can confirm it is B. You create the compliance policy in the compliance settings you specify the risk level and in the next step (Actions for noncompliance) you can select remotely lock the noncompliant device.
upvoted 3 times

mikl 9 months, 2 weeks ago
Its surely B.

https://docs.microsoft.com/en-us/mem/intune/protect/actions-for-noncompliance

By default, each compliance policy includes the action for noncompliance of Mark device noncompliant with a schedule of zero days (0). The result of this default is when Intune detects a device isn't compliant, Intune immediately marks the device as noncompliant. After a device is marked as noncompliance, Azure Active Directory (AD) Conditional Access can block the device.
upvoted 2 times

mikl 9 months, 2 weeks ago
B. You should create a device compliance policy.
upvoted 1 times

velosiraptor 10 months, 1 week ago
B is the only close enough as an answer. Remote Lock option is only present in Device Compliance. Although W 10 do not support Remote lock if the question is not worded differently its the only option to fulfil the question requirement.
upvoted 3 times

Malinaa 11 months, 2 weeks ago
I would say that B and D are both correct. In my opinion you have to create a device compliance policy first and then you enforce your compliance policy with a conditional access policy.
Also the questions remains: Which of the following actionS (multiple) should you take?

B:
Require the device to be at or under the machine risk score:

Use this setting to take the risk assessment from your defense threat services as a condition for compliance. Choose the maximum allowed threat level.
https://docs.microsoft.com/en-us/mem/intune/protect/compliance-policy-create-windows#microsoft-defender-for-endpoint-rules

D: https://docs.microsoft.com/en-us/mem/intune/protect/advanced-threat-protection
upvoted 1 times

Nuru_ 11 months ago
Answer B is insuficiant. In a compliance policy the only action possibles are sending a notification or retire the device which are not whas is asked : block the device.

So to do it boss a compliance policy and a conditional access are required.

First a compliance to mark all device that do not meet the required and then block the devices with a conditional access using the "grant access" option with the "Require device to be marked as compliant".
upvoted 1 times

Solaris2002 7 months, 1 week ago
This is correct. Compliance alone only marks a device as non-compliant you need to then set a conditional access to block the device based on that non-compliance.

Microsoft states the same below:

https://docs.microsoft.com/en-us/mem/intune/protect/advanced-threat-protection

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 2 times

HellRaver80 12 months ago
The implementation of Conditional Access in Defender for Endpoint is based on Microsoft Intune (Intune) device compliance policies and Azure Active Directory (Azure AD) conditional access policies.

The compliance policy is used with Conditional Access to allow only devices that fulfill one or more device compliance policy rules to access applications.
upvoted 2 times

blueninja 12 months ago
Answer is D
upvoted 1 times

mikl 9 months, 2 weeks ago
Why not B?
upvoted 1 times

badguytoo 1 year, 1 month ago
To use device compliance policies to block devices from corporate resources, Azure AD Conditional Access must be set up.
upvoted 1 times

forummj 8 months, 2 weeks ago
You need AAD Premium licencing for Conditional Access. Compliance Policies can be applied WITHOUT Conditional Access.

https://docs.microsoft.com/en-us/mem/intune/protect/create-compliance-policy
upvoted 2 times

ashriem 5 months, 2 weeks ago
I would like to add a link that specifically addresses the ability to remotely lock the device based on compliance policy.

https://docs.microsoft.com/en-us/mem/intune/protect/device-compliance-get-started
upvoted 1 times

ifxsvprdzixekrgivt 1 year, 2 months ago
From: https://docs.microsoft.com/en-us/mem/intune/protect/advanced-threat-protection

Because you have an Intune device compliance policy to classify devices with a Medium or High level of risk as noncompliant, the compromised device is classified as noncompliant. This classification allows your conditional access policy to kick in and block access from that device to your corporate resources.

Conditions under a Conditional Access Policy are only user and sign-in risk and then Device Platforms
upvoted 2 times

nyashac 1 year, 2 months ago
B. https://docs.microsoft.com/en-us/mem/intune/protect/actions-for-noncompliance
upvoted 4 times

FrancisLai 11 months, 2 weeks ago
Answer B is correct. I support your answer. We can setup conditions under device compliance policy and when if it's noncompliance, we can set action to remotely lock the device.
upvoted 3 times

Jana08 1 year, 2 months ago
- 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.

Answer is D - Conditional Access Policy

https://docs.microsoft.com/en-us/mem/intune/protect/advanced-threat-protection

upvoted 2 times

ExamStudy101 1 year, 2 months ago

You can set a device compliancy policy to take certain actions if their health score doesn't meet your requirements, like locking them out.

upvoted 1 times

Prianishnikov 1 year, 1 month ago

Remotely lock the noncompliant device: Use this action to issue a remote lock of a device. The user is then prompted for a PIN or password to unlock the device. More on the Remote Lock feature.

The following platforms support this action:

Android device administrator
Android Enterprise:
Fully Managed
Dedicated
Corporate-Owned Work Profile
Personally-Owned Work Profile
Android Enterprise kiosk devices
iOS/iPadOS
macOS

I cant find any Windows OS in this reequipment's. I think, the correct answer will Conditional Access Policy

upvoted 1 times

captainspork 9 months, 3 weeks ago

I've worked for multiple very established international companies. In reality and in practice B is the right answer, Compliance policy is basically the front door, where you can only pass if are considered not a threat to company data. To put in perspective its often "windows defender" not being updated for over 10 day for example. Someone who is a high risk should not even come as far. B comes first, but D is the security guy managing the door with a button from inside. Microsoft tends to ask you questions in a very trick way.

upvoted 2 times

Trifoks 11 months, 3 weeks ago

I think you are wrong and the answer is B.

Conditional access policy only acts on device that are marked as noncompliant. The question is what needs to be done to make sure the devices with a high score are locked (read: marked as noncompliant). To have them marked, you need to set up a device compliance policy. You said yourself: “Devices that exceed the allowed risk level are identified as noncompliant.“

upvoted 2 times

Question #21 *Topic 1*

Your company plans to deploy tablets to 50 meeting rooms.
The tablets run Windows 10 and are managed by using Microsoft Intune. The tablets have an application named App1.
You need to configure the tablets so that any user can use App1 without having to sign in. Users must be prevented from using other applications on the tablets.
Which device configuration profile type should you use?

A. Kiosk

B. Endpoint protection

C. Identity protection

D. Device restrictions

Correct Answer: *A*
A single-app kiosk uses the Assigned Access feature to run a single app above the lock screen. When the kiosk account signs in, the app is launched automatically. The person using the kiosk cannot do anything on the device outside of the kiosk app.
Reference:
https://docs.microsoft.com/en-us/windows/configuration/kiosk-single-app

MikeMatt2020 Highly Voted 1 year, 4 months ago
We have suffered through countless convoluted questions. Let us rejoice for such an easy question. Rejoice, my brothers.
upvoted 48 times

jh999 1 year, 2 months ago
and sisters. :)
upvoted 16 times

AVP_Riga 10 months, 4 weeks ago
and other's (:
upvoted 4 times

forExamCert2023 6 months, 3 weeks ago
Are you sure the answer is correct?

I am kidding, I am trying to stir it up like some comments that I see and make me think that there is no solid solution.
upvoted 1 times

Moderator Most Recent 8 months, 3 weeks ago
Incredibly tough question but I heard through the grapevine that this probably should be answer A indeed! Very uncertain though ;-)
upvoted 2 times

Perycles 1 year, 3 months ago
A for sure
upvoted 2 times

reyco 1 year, 4 months ago
If only they could all be this simple ..
upvoted 3 times

AzZnLuVaBol 1 year, 7 months ago
A. is correct.
upvoted 4 times

Question #22 *Topic 1*

All of your company's devices are managed via Microsoft Intune.
Conditional access is used to prevent devices that are not compliant with company security policies, from accessing Microsoft 365 services.
You need to access Device compliance to view the non-compliant devices.
Where should you access Device compliance from?

A. System Center Configuration Manager

B. Windows Defender Security Center.

C. The Intune admin center.

D. The Azure Active Directory admin center.

Correct Answer: *C*
Open the Intune Device compliance dashboard:
1. Sign in to the Microsoft Endpoint Manager admin center.
2. Select Devices > Overview > Compliance status tab.
Important: Devices must be enrolled into Intune to receive device compliance policies.
Note 1: Intune Admin portal URL, Microsoft Endpoint Manager admin center: https://endpoint.microsoft.com
Microsoft Intune, which is a part of Microsoft Endpoint Manager, provides the cloud infrastructure, the cloud-based mobile device management (MDM), cloud- based mobile application management (MAM), and cloud-based PC management for your organization.
Note 2: Compliance reports help you review device compliance and troubleshoot compliance-related issues in your organization. Using these reports, you can view information on:
The overall compliance states of devices
The compliance status for an individual setting
The compliance status for an individual policy
Drill down into individual devices to view specific settings and policies that affect the device
Reference:
https://docs.microsoft.com/en-us/mem/intune/protect/compliance-policy-monitor https://docs.microsoft.com/en-us/mem/intune/fundamentals/account-sign-up

Jana08 Highly Voted 1 year, 2 months ago
Correct - Microsoft Endpoint Manager Admin Center - Formerly known as intune.

Home > Endpoint Security > Device Compliance
upvoted 16 times

AVP_Riga 11 months, 1 week ago
Thanks
upvoted 3 times

RodrigoT 7 months ago
The answer is correct but your path is not, because Device Compliance is now the place where you create and edit compliance policies. The path now is: Home > Endpoint Security > All devices. There you can sort them using the column Compliant or creating a filter.
upvoted 1 times

RodrigoT 7 months ago
Or also: Home > Devices > Monitor > Noncompliant devices
upvoted 2 times

MR_Eliot Most Recent 5 months, 2 weeks ago
Selected Answer: C
C, But keep in mind that the name is changed to MDM or Microsoft Endpoint Manager.
upvoted 1 times

mikl 9 months, 2 weeks ago
C. The Intune admin center.
upvoted 1 times

b3arb0yb1m 9 months, 2 weeks ago
C. The Intune admin center.
upvoted 1 times

sbmkhize 12 months ago
the answer is correct
upvoted 2 times

Question #23 *Topic 1*

You manage a large number of Windows 10 computers.
You have been tasked with creating a provisioning package that will allow you to remove the Microsoft News and the Xbox Microsoft Store apps, as well as add a
VPN connection to the company network.
Which of the following are the customization settings you should configure?

A. Connections and Personalization

B. ConnectivityProfiles and Policies

C. Connections and Policies

D. ConnectivityProfiles and Personalization

Correct Answer: *B*
The Policy configuration service provider enables the enterprise to configure policies on Windows 10
ConnectivityProfiles is uses to configure profiles that a user will connect with, such as an email account or VPN profile.
Reference:
https://docs.microsoft.com/en-us/windows/configuration/wcd/wcd-connectivityprofiles https://docs.microsoft.com/en-us/windows/client-management/mdm/policy-configuration-service-provider#applicationmanagement-applicationrestrictions https://docs.microsoft.com/en-us/windows/configuration/wcd/wcd-policies

Jeff8989 Highly Voted 1 year ago
UniversalAppUninstall
ConnectivityProfiles
upvoted 14 times

PiPe 8 months ago
Agreed. None of the given answers are correct. Should be UniversalAppUninstall:
https://docs.microsoft.com/en-us/windows/configuration/wcd/wcd-universalappuninstall

ConnectivityProfiles:
https://docs.microsoft.com/en-us/windows/configuration/wcd/wcd-connectivityprofiles
upvoted 6 times

RodrigoT 6 months, 1 week ago
But if you don't have this option on your real exam, you will have to choose B. This question will repeat at:
https://www.examtopics.com/exams/microsoft/md-101/view/17/
Question #27 and still wouldn't have a UniversalAppUninstall option.
upvoted 4 times

Mikey82 Highly Voted 1 year, 1 month ago
It took a lot of searching, but I found that allowing or disallowing certain apps would be a policy enabled by ADMX. Although the question doesn't mention Intune, this was the only link I could find to control apps with policy or personalization. Badly worded / vague question. But the answer does appear to be B.
upvoted 9 times

b3arb0yb1m Most Recent 9 months, 2 weeks ago
B. ConnectivityProfiles and Policies
upvoted 6 times

young_snoop 11 months, 1 week ago
I believe B is correct. There are 3 separate links provided but they are jumbled together.
upvoted 2 times

daonga 1 year, 1 month ago
Anyone able to confirm if B? The link they provided does not work
upvoted 1 times

RodrigoT 7 months ago
B is the "best" answer because you have to eliminate the answers with "Personalization" and "Connections". So, B is the only one left.
upvoted 1 times

Question #24 *Topic 1*

All users at your company have Azure AD joined Windows 10 workstations that are managed via Microsoft Intune.
You have been tasked with making sure that Windows Analytics is used to monitor the workstations centrally.
Which of the following actions should you take?

A. You should create a device configuration profile via Intune.

B. You should create a device compliance policy via Intune.

C. You should create a Windows AutoPilot deployment profile via Intune.

D. You should create an app configuration policy via Intune.

Correct Answer: *A*
To configure the setting go to Device configuration ג€" Profiles > Device Restriction ג€" Properties > Device restrictions > Reporting and Telemetry

Reference:
https://www.scconfigmgr.com/2019/03/27/windows-analytics-onboarding-with-intune/

daye 1 week, 6 days ago

Selected Answer: A

Windows analytics was deprecated 2 years ago... and desktop analytcs is going to be depecrated as well. In any case I think A is correct.

upvoted 2 times

Question #25 *Topic 1*

Your company has a number of Windows 10 Microsoft Azure Active Directory (Azure AD) joined workstations. These workstations have been enrolled in Microsoft
Intune.
You are creating a device configuration profile for the workstations. You have been informed that a custom image should be displayed on the sign-in screen.
Which of the following is a Device restriction setting that should be configured?

A. Locked screen experience

B. Personalization

C. Display

D. General

Correct Answer: *A*
Sign-in screen, or Locked screen, image is set under Locked screen experience
Reference:
https://docs.microsoft.com/en-us/intune/device-restrictions-windows-10

TonySuccess 1 month ago
Configuration Profiles - Device Restrictions - Lock Screen Experience x
upvoted 2 times

MR_Eliot 5 months, 1 week ago
Selected Answer: A
100% A
upvoted 1 times

ashriem 5 months, 2 weeks ago
Selected Answer: A
https://www.imab.dk/moving-away-from-group-policy-and-set-wallpaper-and-lock-screen-images-with-local-source-files-with-microsoft-endpoint-manager-intune/
upvoted 1 times

jage01 7 months, 3 weeks ago
Selected Answer: A
A - Device restrictions > Locked Screen Experience
upvoted 3 times

Dane12421 8 months, 2 weeks ago
Selected Answer: A
A obviously for sign in screen
upvoted 3 times

mikl 9 months, 2 weeks ago
Selected Answer: A
Locked screen picture URL (desktop only): Enter the URL to a picture in JPG, JPEG, or PNG format that's used as the Windows lock screen wallpaper. For example, enter https://contoso.com/image.png. This setting locks the image, and can't be changed afterwards.

https://docs.microsoft.com/en-us/mem/intune/configuration/device-restrictions-windows-10
upvoted 4 times

RodrigoT 7 months ago
https://docs.microsoft.com/en-us/mem/intune/configuration/device-restrictions-windows-10#locked-screen-experience
upvoted 1 times

b3arb0yb1m 9 months, 2 weeks ago
A. Locked screen experience
upvoted 2 times

Ferrix 10 months ago
A is the Correct one. On personalization you can only set a Desktop background picture URL
upvoted 4 times

Rick11221 10 months ago
Selected Answer: A
Gonna go with A on this one.
upvoted 3 times

Duyons 10 months, 1 week ago
A is correct - https://docs.microsoft.com/en-us/mem/intune/configuration/device-restrictions-windows-10#locked-screen-experience
upvoted 4 times

Duyons 10 months, 1 week ago

Selected Answer: B

B is correct - https://docs.microsoft.com/en-us/mem/intune/configuration/device-restrictions-windows-10#locked-screen-experience

upvoted 2 times

forummj 8 months, 3 weeks ago

Under the Device Restriction Settings, Personalization only allows you to set the desktop wallpaper. It is the Locked Screen Experience settings that allow you to control the Lock Screen. It is confusing, because under the Lock Screen Experience settings, it says "Personalization/LockScreenImageUrl CSP" however, this is not the overriding setting.

https://docs.microsoft.com/en-us/mem/intune/configuration/device-restrictions-windows-10#locked-screen-experience

https://docs.microsoft.com/en-us/mem/intune/configuration/device-restrictions-windows-10#personalization

upvoted 2 times

encxorblood 10 months, 4 weeks ago

Correct B - LockScreenImageUrl in Personalization

upvoted 2 times

forummj 8 months, 3 weeks ago

Under the Device Restriction Settings, Personalization only allows you to set the desktop wallpaper. It is the Locked Screen Experience settings that allow you to control the Lock Screen. It is confusing, because under the Lock Screen Experience settings, it says "Personalization/LockScreenImageUrl CSP" however, this is not the overriding setting.

https://docs.microsoft.com/en-us/mem/intune/configuration/device-restrictions-windows-10#locked-screen-experience

https://docs.microsoft.com/en-us/mem/intune/configuration/device-restrictions-windows-10#personalization

upvoted 2 times

ADHDave 1 year ago

Correct. A custom image can be set under locked screen experience.

Locked screen picture URL (desktop only): Enter the URL to a picture in JPG, JPEG, or PNG format that's used as the Windows lock screen wallpaper.

upvoted 3 times

Question #26 *Topic 1*

Your company has a number of Windows 10 Microsoft Azure Active Directory (Azure AD) joined workstations. These workstations have been enrolled in Microsoft
Intune.
You are creating a device configuration profile for the workstations. You have been informed that a custom image should be displayed as the Desktop background picture.
Which of the following is a Device restriction setting that should be configured?

A. Locked screen experience

B. Personalization

C. Display

D. General

Correct Answer: *B*
Wallpaper image, or Desktop background picture, URL is set under Personalization.
Reference:
https://docs.microsoft.com/en-us/intune/device-restrictions-windows-10

blueninja Highly Voted 12 months ago
Answer is correct (B).
https://docs.microsoft.com/en-us/mem/intune/configuration/device-restrictions-windows-10#personalization
upvoted 8 times

TonySuccess Most Recent 1 month ago
Configuration Profiles - Device Restrictions - Personalisation x
upvoted 1 times

MR_Eliot 5 months, 2 weeks ago
Selected Answer: B
Correct.
upvoted 1 times

b3arb0yb1m 9 months, 2 weeks ago
B. Personalization
upvoted 2 times

ADHDave 1 year ago
Incorrect. Answer should be A

Locked screen picture URL (desktop only): Enter the URL to a picture in JPG, JPEG, or PNG format that's used as the Windows lock screen wallpaper.
upvoted 1 times

BieLey 1 year ago
It's about the Desktop background, not the locked screen. Given answer is correct.
upvoted 10 times

Duyons 10 months, 1 week ago
Correct
upvoted 2 times

ADHDave 11 months, 3 weeks ago
You are right, i misread the question. B is the correct answer
upvoted 9 times

Question #27 *Topic 1*

Your company has a large number of Windows 10 workstations that are managed via Microsoft Intune.
Delivery Optimization is not being used for Windows updates at present.
You want to make sure that Delivery Optimization is configured for all of the workstations.
Which of the following actions should you take?

A. You should create a device configuration profile via Intune.

B. You should create a device compliance policy via Intune.

C. You should create a Windows AutoPilot deployment profile via Intune.

D. You should create a conditional access policy via Intune.

Correct Answer: *A*
With Intune, use Delivery Optimization settings for your Windows devices to reduce bandwidth consumption when those devices download applications and updates. Configure Delivery Optimization as part of your device configuration profiles.
Reference:
https://docs.microsoft.com/en-us/intune/delivery-optimization-windows

Jana08 Highly Voted 1 year, 2 months ago
With Intune, use Delivery Optimization settings for your Windows 10 devices to reduce bandwidth consumption when those devices download applications and updates. Configure Delivery Optimization as part of your device configuration profiles.
upvoted 13 times

Jana08 1 year, 2 months ago
^ From the provided article
upvoted 1 times

TonySuccess Most Recent 1 month ago
Configuration Profiles - Delivery Optimization x
upvoted 1 times

MR_Eliot 5 months, 2 weeks ago
Selected Answer: A
Answer is correct.
upvoted 1 times

mikl 9 months, 2 weeks ago
A. You should create a device configuration profile via Intune.

Totally agree!
upvoted 1 times

b3arb0yb1m 9 months, 2 weeks ago
A. You should create a device configuration profile via Intune.
upvoted 1 times

Question #28 *Topic 1*

Your company's environment includes the following:
⇨ Microsoft Azure Active Directory (Azure AD)
⇨ Microsoft 365
⇨ Microsoft Intune
⇨ Azure Information Protection.
A new security policy declares that enrollment for private devices in Intune is not required. However, to access corporate email information, users have to make use of a PIN for authentication purposes. Also, users are able to access corporate cloud services from their private iOS and Android devices. Furthermore, the copying corporate email information to a cloud storage service should not be allowed, unless users are copying the information to Microsoft OneDrive for
Business.
You have to make sure that security policy is enforced.
Which of the following actions should you take?

A. You should create a data loss prevention (DLP) policy.

B. You should create a device enrollment policy.

C. You should create an app protection policy.

D. You should create a Windows AutoPilot deployment profile.

Correct Answer: *C*
App protection policies (APP) are rules that ensure an organization's data remains safe or contained in a managed app. A policy can be a rule that is enforced when the user attempts to access or move "corporate" data, or a set of actions that are prohibited or monitored when the user is inside the app. A managed app is an app that has app protection policies applied to it, and can be managed by Intune.
Reference:
https://docs.microsoft.com/en-us/intune/app-protection-policy

CaloyB_IT Highly Voted 10 months, 1 week ago
Selected Answer: C
https://docs.microsoft.com/en-us/intune/app-protection-policy

App protection policies (APP) are rules that ensure an organization's data remains safe or contained in a managed app. A policy can be a rule that is enforced when the user attempts to access or move "corporate" data, or a set of actions that are prohibited or monitored when the user is inside the app. A managed app is an app that has app protection policies applied to it, and can be managed by Intune.
upvoted 8 times

DDHP7 Most Recent 7 months, 3 weeks ago
C is correct
upvoted 3 times

Moderator 9 months ago
Selected Answer: C
Yes, an app protection policy is the best option here.
upvoted 3 times

mikl 9 months, 1 week ago
Selected Answer: C
C. You should create an app protection policy.
upvoted 2 times

b3arb0yb1m 9 months, 2 weeks ago
C. You should create an app protection policy.
upvoted 2 times

Question #29 *Topic 1*

Note: The question is included in a number of questions that depicts the identical set-up. However, every question has a distinctive result. Establish if the solution satisfies the requirements.
Your company has a number of Windows 10 Microsoft Azure Active Directory (Azure AD) joined workstations. These workstations have been enrolled in Microsoft
Intune.
You have been tasked with making sure that the workstations are only able to run applications that you have explicitly permitted.
Solution: You make use of Windows Defender Antivirus.
Does the solution meet the goal?

A. Yes

B. No

Correct Answer: *B*
Instead use Windows Defender Application Control (WDAC).
Windows Defender Application Control and virtualization-based protection of code integrity.
Using WDAC to restrict devices to only authorized apps has these advantages over other solutions:
1. WDAC lets you set application control policy for code that runs in user mode, kernel mode hardware and software drivers, and even code that runs as part of
Windows.
2. WDAC policy is enforced by the Windows kernel itself, and the policy takes effect early in the boot sequence before nearly all other OS code and before traditional antivirus solutions run.
3. Etc.
Reference:
https://docs.microsoft.com/en-us/windows/security/threat-protection/device-guard/introduction-to-device-guard-virtualization-based-security-and-windows- defender-application-control

MR_Eliot 5 months, 1 week ago
Selected Answer: B
B should be right
upvoted 1 times

b3arb0yb1m 9 months, 2 weeks ago
B. No is correct.
upvoted 3 times

ercluff 1 year, 1 month ago
I believe mobile application management app protection is what the organization is needing. https://docs.microsoft.com/en-us/mem/intune/apps/mam-faq
upvoted 4 times

ercluff 9 months, 4 weeks ago
I'll update my answer. It still is B. NO but not MAM App Protection. It is Windows Defender Application Control. Comments from Q. 31 by Angelize and Andrevox are especially well done: ""Angelize' comment concisely states: "Application Guard only affects Edge (and Office if you have a plugin - the correct answer should be Windows Defender Application Control." Andrevox' explanation is the best: "Application Guard, a hardware-based endpoint defense, is a security tool that is built into Microsoft Edge. Application Guard isolates enterprise-defined untrusted sites from the desktop (host) in a virtual machine (VM) to prevent malicious activity from reaching the desktop. For Microsoft Office, Application Guard helps prevents untrusted Word, PowerPoint and Excel files from accessing trusted resources. ... This container isolation means that if the untrusted site or file turns out to be malicious, the host device is protected, and the attacker can't get to your enterprise data. "
upvoted 2 times

ercluff 1 year, 1 month ago
B. No on this question
upvoted 7 times

Question #30 *Topic 1*

Note: The question is included in a number of questions that depicts the identical set-up. However, every question has a distinctive result. Establish if the solution satisfies the requirements.
Your company has a number of Windows 10 Microsoft Azure Active Directory (Azure AD) joined workstations. These workstations have been enrolled in Microsoft
Intune.
You have been tasked with making sure that the workstations are only able to run applications that you have explicitly permitted.
Solution: You make use of Windows Defender SmartScreen.
Does the solution meet the goal?

A. Yes

B. No

Correct Answer: *B*
Instead use Windows Defender Application Control (WDAC).
Windows Defender Application Control and virtualization-based protection of code integrity.
Using WDAC to restrict devices to only authorized apps has these advantages over other solutions:
1. WDAC lets you set application control policy for code that runs in user mode, kernel mode hardware and software drivers, and even code that runs as part of
Windows.
2. WDAC policy is enforced by the Windows kernel itself, and the policy takes effect early in the boot sequence before nearly all other OS code and before traditional antivirus solutions run.
3. Etc.
Reference:
https://docs.microsoft.com/en-us/windows/security/threat-protection/device-guard/introduction-to-device-guard-virtualization-based-security-and-windows- defender-application-control

ercluff Highly Voted 1 year, 1 month ago
B. NO - Mobile Application Management App Protection is what is needed.
upvoted 5 times

ercluff 9 months, 4 weeks ago
I'll update my answer. It still is B. NO but not MAM App Protection. It is Windows Defender Application Control. Comments from Q. 31 by Angelize and Andrevox are especially well done: ""Angelize' comment concisely states: "Application Guard only affects Edge (and Office if you have a plugin - the correct answer should be Windows Defender Application Control." Andrevox' explanation is the best: "Application Guard, a hardware-based endpoint defense, is a security tool that is built into Microsoft Edge. Application Guard isolates enterprise-defined untrusted sites from the desktop (host) in a virtual machine (VM) to prevent malicious activity from reaching the desktop. For Microsoft Office, Application Guard helps prevents untrusted Word, PowerPoint and Excel files from accessing trusted resources. ... This container isolation means that if the untrusted site or file turns out to be malicious, the host device is protected, and the attacker can't get to your enterprise data. "
upvoted 2 times

RodrigoT 7 months ago
You're right, Windows Defender Application CONTROL, don't confuse this with Windows Defender Application Guard (that is for Edge).
upvoted 3 times

MR_Eliot Most Recent 5 months, 1 week ago
Selected Answer: B
B, smart screen is just protection and nothing more.
upvoted 1 times

b3arb0yb1m 9 months, 2 weeks ago
B. No is correct.
upvoted 3 times

CaloyB_IT 10 months, 1 week ago
B - MAM is what is needed
https://docs.microsoft.com/en-us/mem/intune/apps/mam-faq
upvoted 2 times

RodrigoT 7 months ago
Sorry dude but you're wrong. This is the right answer:
https://docs.microsoft.com/en-us/windows/security/threat-protection/windows-defender-application-control/select-types-of-rules-to-create
Windows Defender Application Control (WDAC) is used to restrict devices to run only approved apps.
upvoted 1 times

Webleyboy 10 months, 3 weeks ago
Windows Defender Application Guard is needed for this.
Next question on this website is also saying: Windows Defender Application Guard.
upvoted 1 times

RodrigoT 7 months ago

And the next question is also NO. The right option is: Windows Defender Application CONTROL.
https://docs.microsoft.com/en-us/windows/security/threat-protection/windows-defender-application-control/select-types-of-rules-to-create
Windows Defender Application Control (WDAC) is used to restrict devices to run only approved apps.

upvoted 2 times

Question #31 *Topic 1*

Note: The question is included in a number of questions that depicts the identical set-up. However, every question has a distinctive result. Establish if the solution satisfies the requirements.
Your company has a number of Windows 10 Microsoft Azure Active Directory (Azure AD) joined workstations. These workstations have been enrolled in Microsoft
Intune.
You have been tasked with making sure that the workstations are only able to run applications that you have explicitly permitted.
Solution: You make use of Windows Defender Application Guard.
Does the solution meet the goal?

A. Yes

B. No

Correct Answer: *B*
Instead use Windows Defender Application Control (WDAC).
Windows Defender Application Control and virtualization-based protection of code integrity.
Using WDAC to restrict devices to only authorized apps has these advantages over other solutions:
1. WDAC lets you set application control policy for code that runs in user mode, kernel mode hardware and software drivers, and even code that runs as part of
Windows.
2. WDAC policy is enforced by the Windows kernel itself, and the policy takes effect early in the boot sequence before nearly all other OS code and before traditional antivirus solutions run.
3. Etc.
Note: Application Guard helps to isolate enterprise-defined untrusted sites, protecting your company while your employees browse the Internet. As an enterprise administrator, you define what is among trusted web sites, cloud resources, and internal networks. Everything not on your list is considered untrusted. If an employee goes to an untrusted site through either Microsoft Edge or Internet Explorer, Microsoft Edge opens the site in an isolated Hyper-V-enabled container.
For Microsoft Office, Application Guard helps prevents untrusted Word, PowerPoint and Excel files from accessing trusted resources.
Reference:
https://docs.microsoft.com/en-us/windows/security/threat-protection/device-guard/introduction-to-device-guard-virtualization-based-security-and-windows- defender-application-control https://docs.microsoft.com/en-us/windows/security/threat-protection/device-guard/introduction-to-device-guard-virtualization-based-security-and-windows- defender-application-control

nyashac Highly Voted 1 year, 2 months ago
wrong answer windows defender application control
https://docs.microsoft.com/en-us/mem/configmgr/protect/deploy-use/use-device-guard-with-configuration-manager#:~:text=Windows%20Defender%20Application%20Control%20is,malware%20and%20other%20untrusted%20software.&text=Windows%20Defender%20Application%20Control%20is%20a%20software%2Dbased%20security%20layer,to%20run%20on%20a%20PC.
upvoted 22 times

RodrigoT 7 months ago
And the link provided is also broken (must remove an space character). This is the right one: https://docs.microsoft.com/en-us/windows/security/threat-protection/device-guard/introduction-to-device-guard-virtualization-based-security-and-windows-defender-application-control
that says: "we no longer use the Device Guard brand". So it used to be the right answer, but the test was updated on November 24, so beware. Now it's: Windows Defender Application CONTROL. Check for yourself:
https://docs.microsoft.com/en-us/windows/security/threat-protection/windows-defender-application-control/select-types-of-rules-to-create
Windows Defender Application Control (WDAC) is used to restrict devices to run only approved apps.
upvoted 1 times

RodrigoT 5 months, 1 week ago
Nowadays Windows Defender Application Guard is only for Edge and Office. It opens untrusted sites and files in an isolated Hyper-V-enabled container. This container isolation means that if the untrusted site or file turns out to be malicious, the host device is protected, and the attacker can't get to your enterprise data.

https://docs.microsoft.com/en-us/windows/security/threat-protection/microsoft-defender-application-guard/md-app-guard-overview
upvoted 1 times

justabasicuser Highly Voted 1 year, 2 months ago
Its no as it should be Windows Defender Application Control.
upvoted 11 times

MR_Eliot Most Recent 5 months, 1 week ago
Selected Answer: B
B is correct.
upvoted 1 times

AL99 6 months, 2 weeks ago
Agree B "No"

upvoted 1 times

Garito 7 months, 1 week ago

Selected Answer: B

Application Control and not Application Guard

upvoted 4 times

ameli8222 8 months, 3 weeks ago

Selected Answer: B

Its B. App control would be the right answer

upvoted 3 times

b3arb0yb1m 9 months, 2 weeks ago

B - Windows Defender Application Control.

upvoted 2 times

GLL 10 months ago

It should be Application Control?

upvoted 3 times

Duyons 10 months, 1 week ago

Selected Answer: B

Correct Answer is B - Windows Defender Application Control is designed to protect PCs against malware and other untrusted software. It prevents malicious code from running by ensuring that only approved code, that you know, can be run.

Windows Defender Application Control is a software-based security layer that enforces an explicit list of software that is allowed to run on a PC. On its own, Application Control does not have any hardware or firmware prerequisites. Application Control policies deployed with Configuration Manager enable a policy on PCs in targeted collections that meet the minimum Windows version and SKU requirements outlined in this article. Optionally, hypervisor-based protection of Application Control policies deployed through Configuration Manager can be enabled through Group Policy on capable hardware.

upvoted 3 times

handsofthelp 10 months, 1 week ago

Wrong. Should be Microsoft Defender Application Control.

upvoted 3 times

Nen0 11 months ago

Right answer is 'No'. Solution requires Application Control, not Application Guard.

upvoted 4 times

ANDREVOX 11 months ago

Answer is B.
Application control is a security approach designed to protect against malicious code (also known as malware) executing on systems. While application control is primarily designed to prevent the execution and spread of malicious code, it can also prevent the installation or use of unapproved applications.

Application Guard, a hardware-based endpoint defense, is a security tool that is built into Microsoft Edge. Application Guard isolates enterprise-defined untrusted sites from the desktop (host) in a virtual machine (VM) to prevent malicious activity from reaching the desktop.
For Microsoft Office, Application Guard helps prevents untrusted Word, PowerPoint and Excel files from accessing trusted resources. ... This container isolation means that if the untrusted site or file turns out to be malicious, the host device is protected, and the attacker can't get to your enterprise data.

upvoted 3 times

DLSN 1 year ago

https://docs.microsoft.com/en-us/windows/security/threat-protection/windows-defender-application-control/windows-defender-application-control

upvoted 3 times

angelize 1 year, 3 months ago

the answe is NO. Application Guard only affects Edge (and Office if you have a plugin= the correct anser should be App protection

upvoted 4 times

Question #32 *Topic 1*

You are currently making use of the Antimalware Assessment solution in Microsoft Azure Log Analytics.
You have accessed the Protection Status dashboard and find that there is a device that has no real time protection.
Which of the following could be a reason for this occurring?

A. Windows Defender has been disabled.

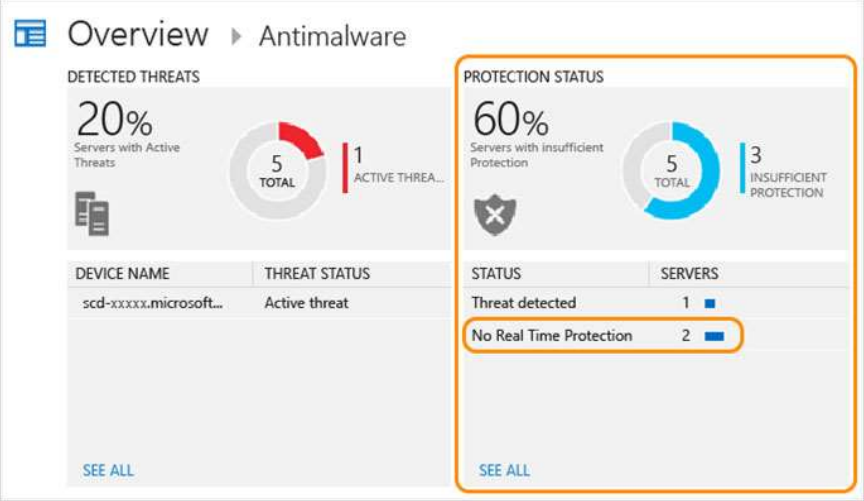
B. You need to install the Azure Diagnostic extension.

C. Windows Defender Credential Guard is incorrectly configured.

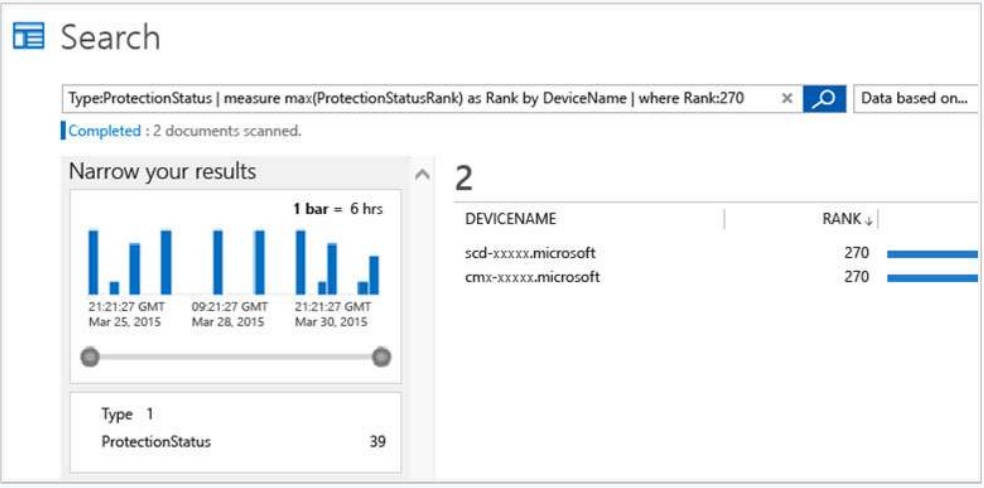
D. Windows Defender System Guard is incorrectly configured.

Correct Answer: *A*
Microsoft Defender Antivirus is usually the primary antivirus/antimalware product on your device.

To review protection status -
1. On the Antimalware dashboard, you will review the Protection Status blade and click no real time protection.



2. Search shows a list of servers without protection.



3. At this point you now know what servers do not have realtime protection.
Computers that do not have System Center Endpoint Protection installed (or if SCEP is not detected) will be reported as no real time protection.
Reference:
https://docs.microsoft.com/ga-ie/azure/security-center/security-center-install-endpoint-protection

Question #33 *Topic 1*

You are currently making use of the Antimalware Assessment solution in Microsoft Azure Log Analytics.
You have accessed the Protection Status dashboard and find that there is a device that is not reporting.
Which of the following could be a reason for this occurring?

A. Windows Defender System Guard is incorrectly configured.

B. You need to install the Azure Diagnostic extension.

C. Windows Defender Application Guard is incorrectly configured.

D. The Microsoft Malicious Software Removal tool is installed.

Correct Answer: *B*
Azure Diagnostics extension is an agent in Azure Monitor that collects monitoring data from the guest operating system of Azure compute resources including virtual machines.
Note: As the Azure Diagnostic extension can only be used for Virtual Machines a better answer would be that the Microsoft Monitoring Agent (MMA) is missing.
Incorrect:
Not A: Windows Defender System Guard reorganizes the existing Windows 10 system integrity features under one roof and sets up the next set of investments in
Windows security. It's designed to make these security guarantees:
Protect and maintain the integrity of the system as it starts up
Validate that system integrity has truly been maintained through local and remote attestation
Not C: For Microsoft Edge, Application Guard helps to isolate enterprise-defined untrusted sites, protecting your company while your employees browse the
Internet. As an enterprise administrator, you define what is among trusted web sites, cloud resources, and internal networks. Everything not on your list is considered untrusted. If an employee goes to an untrusted site through either Microsoft Edge or Internet Explorer, Microsoft Edge opens the site in an isolated
Hyper-V-enabled container.
Reference:
https://docs.microsoft.com/en-us/azure/azure-monitor/agents/diagnostics-extension-overview https://docs.microsoft.com/en-us/azure/azure-monitor/visualize/tutorial-logs-dashboards

Ka1Nn Highly Voted 1 year, 2 months ago
The answer is not present :
The Microsoft Monitoring Agent is uninstalled.
upvoted 21 times

mikl 9 months, 2 weeks ago
Agree.

You may also see the Log Analytics agent referred to as the Microsoft Monitoring Agent (MMA).

https://docs.microsoft.com/en-us/azure/azure-monitor/agents/log-analytics-agent
upvoted 2 times

RodrigoT 7 months ago
The Microsoft Monitoring Agent (MMA) is not something that you install on every computer, but mainly on a data collection machine, or a server or on the gateway.
https://docs.microsoft.com/en-us/services-hub/health/mma-setup
The question says that there is one device that is not reporting, not all of them.
So, if just one device is not reporting, it could be a misconfiguration, not that the Agent is not installed.
upvoted 3 times

RodrigoT 5 months ago
Anyway, I found this:
A yellow warning icon means the agent is having issues. One common reason is the Microsoft Monitoring Agent service has stopped. Use service control manager to restart the service.

https://docs.microsoft.com/en-us/azure/azure-monitor/faq#how-can-i-confirm-that-the-log-analytics-agent-is-able-to-communicate-with-azure-monitor-
upvoted 1 times

angelize Highly Voted 1 year, 3 months ago
I would say B. https://docs.microsoft.com/en-us/azure/azure-monitor/agents/diagnostics-extension-overview
upvoted 6 times

HellRaver80 10 months, 1 week ago
in my eyes that is active on the server not on clients
upvoted 1 times

RodrigoT 7 months ago

Azure Diagnostics Extension can be used only with Azure virtual machines:
https://docs.microsoft.com/en-us/azure/azure-monitor/agents/diagnostics-extension-overview
upvoted 1 times

RodrigoT Most Recent 7 months ago
A.Windows Defender System Guard is for hardware.
B.Azure Diagnostic extension is for Azure virtual machines.
C.Windows Defender Application Guard is for browsing (Edge) and Office.
D.Microsoft Malicious Software Removal tool is that update package that used to scan your computer every month.
So, none of the above.
Azure Log Analytics is on a deprecation path and you should migrate to the new Azure Monitor agent (AMA):
https://docs.microsoft.com/en-us/azure/azure-monitor/agents/azure-monitor-agent-migration
Meaning that this question is so outdated.
upvoted 5 times

RodrigoT 7 months ago
Anyway, if we are talking about malware protection and a device that is not reporting the new tool is Microsoft Defender for Endpoint:
https://docs.microsoft.com/en-us/microsoft-365/security/defender-endpoint/microsoft-defender-endpoint?view=o365-worldwide
One of the reasons that one device is not reporting could be found here:
https://docs.microsoft.com/en-us/microsoft-365/security/defender-endpoint/troubleshoot-onboarding?view=o365-worldwide#confirming-onboarding-of-newly-built-devices
And one of the ways to solve this could be:
https://docs.microsoft.com/en-us/microsoft-365/security/defender-endpoint/run-detection-test?view=o365-worldwide
upvoted 2 times

Garito 7 months, 1 week ago
Assuming it is Microsoft Azure Log Analytics and from this article:

https://docs.microsoft.com/en-us/azure/azure-monitor/visualize/tutorial-logs-dashboards

Best answer available is B
upvoted 1 times

RodrigoT 7 months ago
Azure Diagnostics Extension can be used only with Azure virtual machines.
https://docs.microsoft.com/en-us/azure/azure-monitor/agents/diagnostics-extension-overview
upvoted 1 times

Juun 7 months, 1 week ago
Where do the questions come from exactly?
None of the options make much sense
upvoted 2 times

Bettito 8 months, 1 week ago
ninguna ya que no esta presente MMA
upvoted 1 times

AK311 10 months, 3 weeks ago
I dont think any of the options present here are correct?
upvoted 4 times

amarro 11 months ago
Is the answer correct because I have a doubt with the option B
upvoted 1 times

Ka1Nn 1 year, 2 months ago
Azure Diagnostics Extension can be used only with Azure virtual machines
upvoted 2 times

Question #34 *Topic 1*

You need to consider the underlined segment to establish whether it is accurate.
To enable Windows Defender Credential Guard on Windows 10 computers, the computers must have Hyper-V installed.
Select `No adjustment required` if the underlined segment is accurate. If the underlined segment is inaccurate, select the accurate option.
What should you install on the computers?

A. No adjustment required.

B. Windows Defender Smartscreen

C. a virtual machine

D. a container cluster

Correct Answer: *A*
Credential Guard can protect secrets in a Hyper-V virtual machine, just as it would on a physical machine. When Credential Guard is deployed on a VM, secrets are protected from attacks inside the VM. Credential Guard does not provide additional protection from privileged system attacks originating from the host.
Note: Hardware and software requirements
To provide basic protections against OS level attempts to read Credential Manager domain credentials, NTLM and Kerberos derived credentials, Windows
Defender Credential Guard uses:
Support for Virtualization-based security (required)
Secure boot (required)
Trusted Platform Module (TPM, preferred - provides binding to hardware) versions 1.2 and 2.0 are supported, either discrete or firmware
UEFI lock (preferred - prevents attacker from disabling with a simple registry key change)
The Virtualization-based security requires:
64-bit CPU
CPU virtualization extensions plus extended page tables
Windows hypervisor (does not require Hyper-V Windows Feature to be installed)
Reference:
https://docs.microsoft.com/en-us/windows/security/identity-protection/credential-guard/credential-guard-requirements

Jana08 Highly Voted 1 year, 2 months ago
The link provided states that Hyper-V is not required...

Hardware and software requirements
To provide basic protections against OS level attempts to read Credential Manager domain credentials, NTLM and Kerberos derived credentials, Windows Defender Credential Guard uses:

Support for Virtualization-based security (required)
Secure boot (required)
Trusted Platform Module (TPM, preferred - provides binding to hardware) versions 1.2 and 2.0 are supported, either discrete or firmware
UEFI lock (preferred - prevents attacker from disabling with a simple registry key change)
The Virtualization-based security requires:

64-bit CPU
CPU virtualization extensions plus extended page tables
Windows hypervisor (does not require Hyper-V Windows Feature to be installed)
upvoted 9 times

Angarali 5 months, 2 weeks ago
https://docs.microsoft.com/en-us/windows/security/identity-protection/credential-guard/credential-guard-manage
upvoted 1 times

RodrigoT 7 months ago
You HAVE to at least select the Hyper-V Hypervisor check box on Windows Features. Check for yourself:
https://docs.microsoft.com/en-us/windows/security/identity-protection/credential-guard/credential-guard-manage
upvoted 6 times

lucadp010 Highly Voted 8 months, 2 weeks ago
Selected Answer: C
C. a virtual machine
Hyper-V is not required. You can use also VMware for virtualization.
upvoted 6 times

RodrigoT 7 months ago
The question is not about using virtualization but "to enable Windows Defender Credential Guard" on a device. To do this you don't need all the components of Hyper-V like Management Tools or Services Platform, but you HAVE to at least select the Hyper-V Hypervisor check box on Windows Features. That means that at least one component of Hyper-V must be installed. Check for yourself:
https://docs.microsoft.com/en-us/windows/security/identity-protection/credential-guard/credential-guard-manage
under the subtitle: Add the virtualization-based security features by using Programs and Features.
So, for me the answer is correct, A.
upvoted 5 times

TonySuccess Most Recent 1 week ago

Selected Answer: A

A Fo Sho

upvoted 1 times

asturmark 3 weeks, 6 days ago

Selected Answer: A

I will choose A. It is necessary to enable Hyper-V in the Windows features but it is not necessary to create a VM (this is done automatically by the service itself)

upvoted 1 times

cdhoesje 5 months, 1 week ago

Hyper-v is used and windows 10 is using it to create a container (vm) for the passwords etc. It is a automatic proces so you dont have to make a VM. I have roll out thise to many customers. Answer is A.

upvoted 1 times

MR_Eliot 5 months, 1 week ago

Selected Answer: A

I'm going with A. Other answers don't make any sense regarding the question.

upvoted 1 times

Angarali 5 months, 2 weeks ago

Selected Answer: A

A is correct as the others make no sense

https://docs.microsoft.com/en-us/windows/security/identity-protection/credential-guard/credential-guard-manage

upvoted 2 times

Moderator 6 months ago

Selected Answer: A

A makes the most sense, since the other answers make no sense at all.

upvoted 2 times

PChi 6 months, 1 week ago

The question is worder poorly but essentially, it's saying hyper v is enabled meaning the systems support virtualization. I am certain it isn't talking about the hyper-v server being installed (that is where you create vms). With that being said, nothing else needs to be done. It honestly does not make any sense for you to go around installing vms on every workstation... Answer A seems to be the correct answer.

upvoted 2 times

b3arb0yb1m 9 months, 2 weeks ago

A. No adjustment is required.

upvoted 2 times

vinodhg 9 months, 1 week ago

Select `No adjustment required` if the underlined segment is accurate - According to underlined segment Hyper-V is mandatory which is not true so Option A is wrong

upvoted 2 times

RodrigoT 7 months ago

Not all the components but the Hyper-V Hypervisor feature is mandatory. Check my links.

upvoted 1 times

ritte1337 1 year ago

"What should you install on the computers?"
The answer to that is nothing = A
Method of elimination, none of the other choices is correct.

Anyhow, as stated by "Jana08" before, Hyper-V doesn't need to be enabled. Seems like a silly question and is probably worded differently on the actual exam.

upvoted 4 times

vinodhg 9 months, 1 week ago

Select `No adjustment required` if the underlined segment is accurate - According to underlined segment Hyper-V is mandatory which is not true so Option A is wrong

upvoted 2 times

RodrigoT 7 months ago

You HAVE to at least select the Hyper-V Hypervisor check box on Windows Features. Check for yourself:
https://docs.microsoft.com/en-us/windows/security/identity-protection/credential-guard/credential-guard-manage

upvoted 1 times

Ka1Nn 1 year, 2 months ago

C
Windows Defender Credential Guard deployment in virtual machines
Credential Guard can protect secrets in a Hyper-V virtual machine, just as it would on a physical machine. When Credential Guard is deployed on a VM, secrets are protected from attacks inside the VM. Credential Guard does not provide additional protection from privileged system attacks originating from the host.

upvoted 4 times

RodrigoT 7 months ago

You're very confused dude. There are websites saying that VMware and Device Credential Guard are not Compatible. You have to enable at least the Hyper-V Hypervisor feature to enable Credential Guard.

upvoted 2 times

Angarali 5 months, 2 weeks ago

Feel sorry for the ones who follows his answer

upvoted 1 times

Question #35 *Topic 1*

You manage one hundred Microsoft Azure Active Directory (Azure AD) joined Windows 10 devices.
You want to make sure that users are unable to join their home PC's to Azure AD.
Which of the following actions should you take?

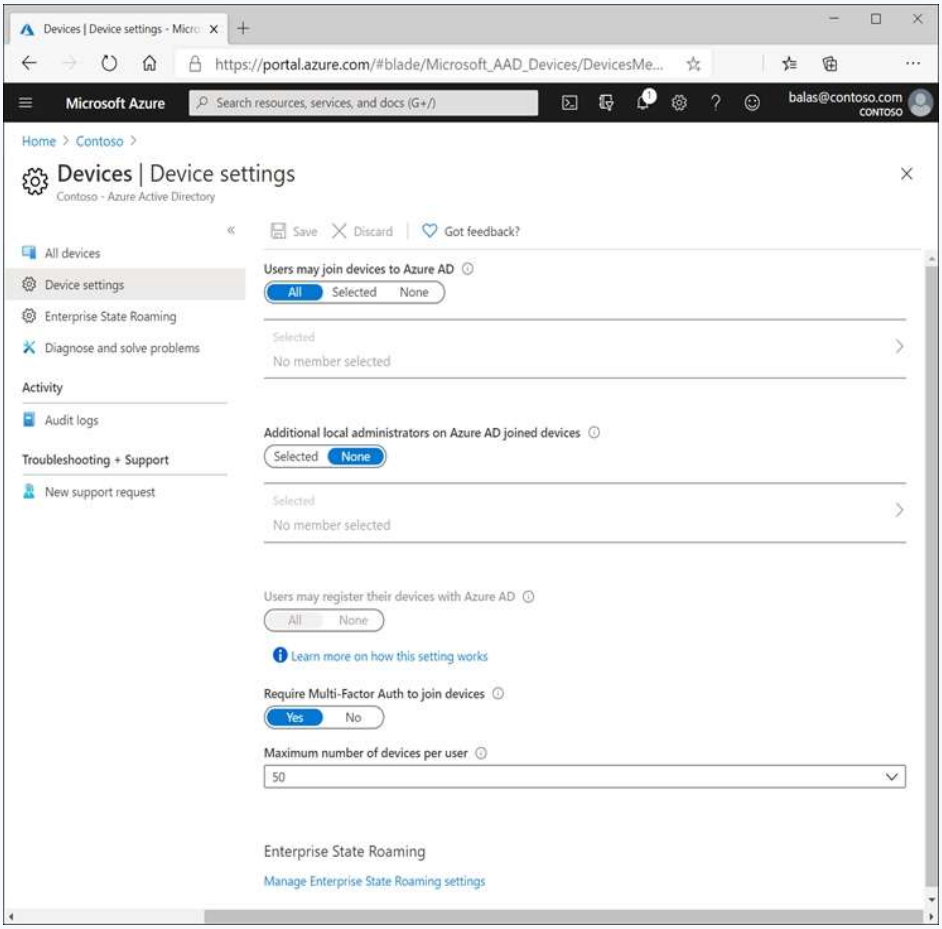
A. You should configure the Enrollment restriction settings via the Device enrollment blade in the Intune admin center.

B. You should configure the Enrollment restriction settings via the Security & Compliance admin center.

C. You should configure the Enrollment restriction settings via the Azure Active Directory admin center.

D. You should configure the Enrollment restriction settings via the Windows Defender Security Center.

Correct Answer: *C*
Azure Active Directory (Azure AD) provides a central place to manage device identities and monitor related event information.
Configure device settings.



* Users may join devices to Azure AD: This setting enables you to select the users who can register their devices as Azure AD joined devices.
The default is All.
Reference:
https://docs.microsoft.com/en-us/azure/active-directory/devices/device-management-azure-portal

BRoald Highly Voted 2 weeks, 4 days ago

Selected Answer: A

Its A; Open Intune / Endpoint admin center > Devices > Enrollment Device Platform Restriction > All Users > Here you can block personally owned devices, such as a home PC. Answer A

upvoted 5 times

daye 1 week, 6 days ago

this will block Intune Enrollment, the Question is related with Azure, so C is the correct one IMHO

upvoted 2 times

TonySuccess 1 week ago

I agree with you, I will be careful to read the wording of the question in the Exam.

upvoted 1 times

Zarkata Most Recent 1 week, 6 days ago

Selected Answer: A

BRoald is correct indeed.

upvoted 1 times

RickyBee 2 weeks, 3 days ago

Selected Answer: A

Broald is correct

upvoted 1 times

Question #36 *Topic 1*

You need to consider the underlined segment to establish whether it is accurate.
To enable sideloading in Windows 10, you should navigate to the For developers setting via Update & Security in the Settings app.
Select `No adjustment required` if the underlined segment is accurate. If the underlined segment is inaccurate, select the accurate option.

A. No adjustment required.

B. Widows Insider

C. Delivery Optimization

D. Activation

Correct Answer: *A*
How to allow Windows 10 to sideload apps on your computer
1. Open Settings.
2. Click on Update & security.
3. Click on For developers.
4. Under "Use developer features," select the Sideload apps option.
Reference:
https://www.windowscentral.com/how-enable-windows-10-sideload-apps-outside-store https://docs.microsoft.com/en-us/windows/application-management/sideload-apps-in-windows-10

Deric 1 week, 5 days ago

Selected Answer: A

Agreed, the answer is A.

upvoted 1 times

MR_Eliot 5 months, 1 week ago

Selected Answer: A

I'm going with A. No Adjustment is required.

upvoted 1 times

AL99 6 months, 2 weeks ago

B, C, D are incorrect. So remaining is A

upvoted 1 times

mikl 9 months, 2 weeks ago

Selected Answer: A

A. No adjustment required.

upvoted 2 times

b3arb0yb1m 9 months, 2 weeks ago

A. No adjustment is required.

upvoted 1 times

CaloyB_IT 10 months, 1 week ago

Selected Answer: A

correct answer
https://www.windowscentral.com/how-enable-windows-10-sideload-apps-outside-store

upvoted 2 times

Question #37 *Topic 1*

You need to consider the underlined segment to establish whether it is accurate.
To enable sideload a LOB application in Windows 10, you should run the Install-Package cmdlet.
Select `No adjustment required` if the underlined segment is accurate. If the underlined segment is inaccurate, select the accurate option.

A. No adjustment required.

B. Install-PackageProvider

C. Save-Package

D. Add-AppxPackage

Correct Answer: *D*
Install the app -
From the folder with the .msix package, run the Windows PowerShell Add-AppxPackage command to install the .msix package.
Reference:
https://docs.microsoft.com/en-us/windows/application-management/sideload-apps-in-windows-10

MR_Eliot 5 months, 1 week ago

Selected Answer: D

D is correct.

upvoted 3 times

mikl 9 months, 2 weeks ago

D. Add-AppxPackage

https://docs.microsoft.com/en-us/windows/application-management/sideload-apps-in-windows-10#step-3-install-the-app

upvoted 2 times

b3arb0yb1m 9 months, 2 weeks ago

D. Add-AppxPackage

upvoted 1 times

ercluff 9 months, 4 weeks ago

D. Add-AppxPackage
See Reference: https://docs.microsoft.com/en-us/windows/application-management/sideload-apps-in-windows-10
Step 1 - Turn on Sideloading,
Step 2 - Import the security certificate
Step 3 – Install the app;
From the folder with the .msix package,
run the Windows PowerShell Add-AppxPackage command to install the .msix package.
Commandline sytax for the PowerShell Add-AppxPackage is found here:
https://docs.microsoft.com/en-us/powershell/module/appx/add-appxpackage?view=windowsserver2019-ps

upvoted 3 times

Cezt 11 months, 1 week ago

To install an app on Windows client, you can:

Install Windows apps from a web page.
Users can double-click any .msix or .appx package.
https://docs.microsoft.com/en-us/windows/application-management/sideload-apps-in-windows-10

upvoted 3 times

ercluff 9 months, 4 weeks ago

This is mentioned in step 1 of the cited reference. The question is asking about step3, running the PowerShell Add-AppxPackage.

upvoted 1 times

john909 11 months, 3 weeks ago

I couldn't find anything about the "Install-package " cmdlet enabling sideloading of LOB apps.

This article mentions only 2 ways of enabling sideloading:
This article shows you how to:

Turn on sideloading: You can deploy using Group Policy or a mobile device management (MDM) provider. Or, you can use the Settings app to turn on sideloading.

https://docs.microsoft.com/en-us/windows/application-management/sideload-apps-in-windows-10

upvoted 3 times

Question #38 *Topic 1*

Note: The question is included in a number of questions that depicts the identical set-up. However, every question has a distinctive result.
Establish if the solution satisfies the requirements.
Your company's environment includes a Microsoft 365 subscription.
Users in the company's sales division have personal iOS or Android devices that are enrolled in Microsoft Intune. New users are added to the sales division on a monthly basis.
After a mobile application is created for users in the sales division, you are instructed to make sure that the application can only be downloaded by the sales division users
Solution: You start by adding the application to Microsoft Store for Business.
Does the solution meet the goal?

A. Yes

B. No

Correct Answer: *B*
Before you can configure, assign, protect, or monitor apps, you must add them to Microsoft Intune.
Reference:
https://docs.microsoft.com/en-us/intune/apps-add

ercluff Highly Voted 1 year, 1 month ago
Answer is no. "Apps purchased from the Store for Business and Education only work on Windows 10 devices."
https://docs.microsoft.com/en-us/microsoft-store/microsoft-store-for-business-overview
upvoted 8 times

MR_Eliot Most Recent 5 months, 1 week ago
Selected Answer: B
B is correct. Microsoft Store for Business is for Windows devices & it's being deprecated soon.
upvoted 2 times

b3arb0yb1m 9 months, 2 weeks ago
B. No is correct. Add the app to Intune first.
upvoted 2 times

Alfred666 1 year, 2 months ago
why is there no article backing up answer?
upvoted 2 times

Davidchercm 1 year, 2 months ago
similar to topic 4 , add to app to intunes
upvoted 1 times

Question #39 *Topic 1*

Note: The question is included in a number of questions that depicts the identical set-up. However, every question has a distinctive result.
Establish if the solution satisfies the requirements.
Your company's environment includes a Microsoft 365 subscription.
Users in the company's sales division have personal iOS or Android devices that are enrolled in Microsoft Intune. New users are added to the sales division on a monthly basis.
After a mobile application is created for users in the sales division, you are instructed to make sure that the application can only be downloaded by the sales division users
Solution: You start by assigning the application to a group.
Does the solution meet the goal?

A. Yes

B. No

Correct Answer: *B*
Before you can configure, assign, protect, or monitor apps, you must add them to Microsoft Intune.
Reference:
https://docs.microsoft.com/en-us/intune/apps-add

Ka1Nn Highly Voted 1 year, 1 month ago
Yes, but you need FIRST to create the App in intune before assign to a group
upvoted 10 times

MR_Eliot Most Recent 5 months, 1 week ago
Selected Answer: A
"you are instructed to make sure that the application can only be downloaded by the sales division users". Your only job is to make sure that the application can only be installed by the sales department. I'm going with A.
upvoted 1 times

MR_Eliot 5 months, 1 week ago
Changed my mind to B. See Topic 1, Question #40.
upvoted 2 times

maggie_petrova 6 months, 2 weeks ago
Selected Answer: A
The question states that the application is already created "After a mobile application...".
So the answer is YES.
upvoted 4 times

Moderator 9 months, 2 weeks ago
Selected Answer: B
And B is correct. The app should be added to Intune first and since there is also a question on here (Q40) that has the solution "You start by adding the app to Intune" I'm sure this is correct.
upvoted 4 times

b3arb0yb1m 9 months, 2 weeks ago
B. No is correct. Add the app to Intune first.
upvoted 1 times

john909 11 months, 3 weeks ago
I think the catch is in the wording "you _start_ by...". You should start by adding the app to Intune (As Daonga has mentioned)
upvoted 3 times

tf444 11 months, 3 weeks ago
Yes! Create /add the app in Intune, select the platform, include /exclude the group.
upvoted 2 times

ExamStudy101 1 year, 2 months ago
Wouldn't this be correct? You can assign apps to ios and android devices through a group
upvoted 2 times

daonga 1 year, 1 month ago
You need to first create the app in Intune. Only then you can assign it.
upvoted 3 times

auton 11 months, 2 weeks ago
"After a mobile application is created for users in the sales division, you are instructed to make sure that the application can only be downloaded by the sales division users"

The mobile app has been created (= Created in Intune) and now we're deploying it.

Now we're at the assign part where we determine the users / devices who receives the app.

So either this question is flawed or the answer is wrong.

upvoted 2 times

Glorence 10 months, 1 week ago
I agree, the app is already been created and the next step is on the assign part.
upvoted 2 times

Question #40 *Topic 1*

Note: The question is included in a number of questions that depicts the identical set-up. However, every question has a distinctive result.
Establish if the solution satisfies the requirements.
Your company's environment includes a Microsoft 365 subscription.
Users in the company's sales division have personal iOS or Android devices that are enrolled in Microsoft Intune. New users are added to the sales division on a monthly basis.
After a mobile application is created for users in the sales division, you are instructed to make sure that the application can only be downloaded by the sales division users.
Solution: You start by adding the application to Intune.
Does the solution meet the goal?

A. Yes

B. No

Correct Answer: *A*
Before you can configure, assign, protect, or monitor apps, you must add them to Microsoft Intune.
Reference:
https://docs.microsoft.com/en-us/intune/apps-add

TonySuccess 6 days, 4 hours ago
Selected Answer: A
AAAAAAAAAAAA
upvoted 1 times

Solaris2002 7 months, 1 week ago
The only thing confusing about this is, it isn't clear if it's a win32 app or a Windows Store App. Technically if its a business store app, you can add it via businessstore.microsoft.com, search for the app, then click "Get the app". You can then add the app to your company store by clicking "Add Collection". After that, sync your Intune tenant and it will appear.
upvoted 1 times

mikl 9 months, 2 weeks ago
Solution: You start by adding the application to Intune.

A is ok.
upvoted 1 times

b3arb0yb1m 9 months, 2 weeks ago
A. Yes is correct. Add the app to Intune first.
upvoted 1 times

Nicholas 10 months ago
A is correct answer
upvoted 1 times

AVP_Riga 1 year ago
Seems correct!
upvoted 4 times

Question #41 *Topic 1*

You company has a Microsoft Azure Active Directory (Azure AD) tenant that includes Microsoft Intune. All of the Windows 10 devices are enrolled in Intune.
You are preparing to configure a Windows Information Protection (WIP) policy:
You need to make sure that the policy is configured to allow for the logging of unacceptable data sharing, but not blocking the action.
Which of the following is the WIP protection mode that you should use?

A. Block

B. Silent

C. Off

D. Allow Overrides

Correct Answer: *B*
Silent: WIP runs silently, logging inappropriate data sharing, without blocking anything that would have been prompted for employee interaction while in Allow
Override mode. Unallowed actions, like apps inappropriately trying to access a network resource or WIP-protected data, are still stopped.
Reference:
https://docs.microsoft.com/en-us/windows/security/information-protection/windows-information-protection/create-wip-policy-using-intune

AVP_Riga Highly Voted 12 months ago
Seems good 😊
upvoted 6 times

TonySuccess Most Recent 6 days, 4 hours ago
Selected Answer: B
BBBBBBBBB
upvoted 1 times

AL99 6 months, 2 weeks ago
Answer B: Silent
upvoted 1 times

mikl 9 months, 2 weeks ago
B. Silent is correct.

https://docs.microsoft.com/en-us/mem/intune/apps/windows-information-protection-policy-create
upvoted 1 times

Moderator 9 months, 2 weeks ago
Selected Answer: B
Allow Overrides: WIP looks for inappropriate data sharing, warning employees if they do something deemed potentially unsafe. However, this management mode lets the employee override the policy and share the data, logging the action to your audit log.

Silet: WIP runs silently, logging inappropriate data sharing, without blocking anything that would've been prompted for employee interaction while in Allow Override mode. Unallowed actions, like apps inappropriately trying to access a network resource or WIP-protected data, are still stopped.

Both are kinda right, but Silent does seem like the best option here since it doesn't prompt or block the action (but does block certain unallowed actions).
upvoted 1 times

b3arb0yb1m 9 months, 2 weeks ago
B. Silent
upvoted 1 times

Question #42 *Topic 1*

Your company has an Active Directory domain, named weylandindustries.com, and a Microsoft Office 365 subscription. The domain is also synced to Microsoft
Azure Active Directory (Azure AD).
All company computers are domain-joined, and are running the most recent Microsoft OneDrive sync client.
You are currently configuring OneDrive group policy settings.
Which of the following is the setting that will minimize the disk space consumed by a user profile, when enabled?

A. OneDrive Files On-Demand

B. Silently move known folders to OneDrive

C. Prompt users to move Windows known folders to OneDrive

D. Silently configure OneDrive using the primary Windows account

Correct Answer: *A*
OneDrive Files On-Demand enables users to view, search for, and interact with files stored in OneDrive from within File Explorer without downloading them and taking up space on the local hard drive.
Reference:
https://docs.microsoft.com/en-us/onedrive/plan-onedrive-enterprise

AVP_Riga Highly Voted 12 months ago
Seems correct 😊. A.
upvoted 6 times

TonySuccess Most Recent 6 days, 4 hours ago
Selected Answer: A
A A A A A A
upvoted 1 times

MR_Eliot 5 months, 1 week ago
Selected Answer: A
A is correct.
upvoted 1 times

distortion 8 months ago
Depending on what they want to hear it could also be B. Moving the known folders to onedrive moves them out of the profile to onedrive. You will still need the files on demand setting to free up diskspace on the client.
upvoted 1 times

mikl 9 months, 2 weeks ago
Selected Answer: A
A is correct.

https://support.microsoft.com/en-us/office/save-disk-space-with-onedrive-files-on-demand-for-windows-10-0e6860d3-d9f3-4971-b321-7092438fb38e
upvoted 1 times

b3arb0yb1m 9 months, 2 weeks ago
A. OneDrive Files On-Demand
upvoted 1 times

CaloyB_IT 10 months, 1 week ago
Correct answer is A
upvoted 2 times

Question #43 *Topic 1*

You manage your company's Microsoft 365 subscription.
You are tasked with creating an app protection policy for the Microsoft Outlook app on iOS devices that are not enrolled in Microsoft 365 Device Management.
You have to make sure that the policy is configured to prohibit the users from using the Outlook app if the operating system version is less than 12.0.0. You also have to make sure that an alphanumeric passcode is required for users to access the Outlook app.
Which of the following is policy settings that you should configure? (Choose two.)

A. Conditional launch

B. Data transfer exemptions

C. Data protection

D. Access requirements

Correct Answer: *AD*
Conditional launch -
Configure conditional launch settings to set sign-in security requirements for your access protection policy.
By default, several settings are provided with pre-configured values and actions. You can delete some of these, like the Min OS version. You can also select additional settings from the Select one dropdown.

Access requirements -
PIN for access Select Require to require a PIN to use this app. The user is prompted to set up this PIN the first time they run the app in a work or school context.
The PIN is applied when working either online or offline.
Reference:
https://docs.microsoft.com/en-us/intune/app-protection-policy-settings-ios

Jana08 Highly Voted 1 year, 2 months ago
Answer is correct
upvoted 9 times

TonySuccess Most Recent 6 days, 4 hours ago
Selected Answer: AD
AD, thnks
upvoted 1 times

MR_Eliot 5 months, 1 week ago
Selected Answer: AD
answer is correct.
upvoted 1 times

mikl 9 months, 2 weeks ago
Seems right.
upvoted 2 times

Moderator 9 months, 2 weeks ago
Yes, correct answer given.
upvoted 2 times

b3arb0yb1m 9 months, 2 weeks ago
A. Conditional launch
D. Access requirements
upvoted 2 times

Question #44 *Topic 1*

You are responsible for your company's Microsoft 365 environment, with co-management enabled.
All company computers have been deployed via Microsoft Deployment Toolkit (MDT), and have Windows 10 installed.
You have been tasked devising a strategy for deploying Microsoft Office 365 ProPlus to new computers. You have to make sure that most recent version is installed at all times, while also reducing the effort required to meet the prerequisites.
Which of the following actions should you take?

A. You should make use of Windows Deployment Services (WDS).

B. You should make use of the Microsoft Deployment Toolkit

C. You should make use of the Office Deployment Tool (ODT).

D. You should make use of a Windows Configuration Designer provisioning package

Correct Answer: *C*
The Office Deployment Tool (ODT) is a command-line tool that you can use to download and deploy Microsoft 365 Apps to your client computers. The ODT gives you more control over an Office installation: you can define which products and languages are installed, how those products should be updated, and whether or not to display the install experience to your users.
Reference:
https://docs.microsoft.com/en-us/deployoffice/overview-of-the-office-2016-deployment-tool

Davidchercm Highly Voted 1 year, 2 months ago
https://docs.microsoft.com/en-us/deployoffice/plan-office-365-proplus
upvoted 6 times

TonySuccess Most Recent 6 days, 4 hours ago
Selected Answer: C
I see that it is C
upvoted 1 times

MR_Eliot 5 months, 1 week ago
Selected Answer: C
Answer seems to be correct. ODT in combination with a fileserver to host the offline installation / configuration file should reduce the network traffic as well.
upvoted 1 times

mikl 9 months, 2 weeks ago
Agree - ODT.
upvoted 1 times

b3arb0yb1m 9 months, 2 weeks ago
C. You should make use of the Office Deployment Tool (ODT).
upvoted 2 times

Rick11221 11 months, 3 weeks ago
Office Deployment Tool (ODT)
upvoted 2 times

Topic 2 - Question Set 2

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.
Your company uses Windows Autopilot to configure the computer settings of computers issued to users.
A user named User1 has a computer named Computer1 that runs Windows 10. User1 leaves the company.
You plan to transfer the computer to a user named User2.
You need to ensure that when User2 first starts the computer, User2 is prompted to select the language setting and to agree to the license agreement.
Solution: You create a new Windows Autopilot self-deploying deployment profile.
Does this meet the goal?

A. Yes

B. No

Correct Answer: *B*
Instead:
Windows Autopilot user-driven mode lets you configure new Windows devices to automatically transform them from their factory state to a ready-to-use state. This process doesn't require that IT personnel touch the device.
The process is very simple. Devices can be shipped or distributed to the end user directly with the following instructions:
Unbox the device, plug it in, and turn it on.
Choose a language (only required when multiple languages are installed), locale, and keyboard.
Connect it to a wireless or wired network with internet access. If using wireless, the user must establish the Wi-Fi link.
Specify your e-mail address and password for your organization account.
The rest of the process is automated. The device will:
Join the organization.
Enroll in Intune (or another MDM service)
Get configured as defined by the organization.

Wilf32 Highly Voted 1 year, 5 months ago
I believe this to be NO. i have Intune open right now i create a new profile select Self-Driven and the option to show or hide the EULA is greyed out and set to HIDE. The user can still set the keyboard but cannot accept the EULA so in my mind "does not meet the goal"
upvoted 8 times

marz Highly Voted 1 year, 7 months ago
Just checked this myself. On a self-deploying profile the option for the license is greyed out and set to "Hide" and there is no "user select" option for the language. So I believe "NO" is correct.
upvoted 5 times

MR_Eliot Most Recent 5 months, 1 week ago
Selected Answer: B
B is correct. You should first reset the device from the endpoint manager.
upvoted 1 times

Moderator 9 months, 2 weeks ago
Correct answer is No (B). When selecting 'Self-deploying' you can't select or change options like Language and or Microsoft Software License Terms etc.
upvoted 1 times

hawkens 9 months, 4 weeks ago
Answer is correct, no option for user select (language) using self-deploying
upvoted 1 times

Goofer 11 months ago
Answer is No, Under 'Windows Autopilot deployment profiles' you cannot set the option 'language (Region)' to 'User select' if the Deployment mode is Self-Deploying.
upvoted 3 times

j0eyv 1 year, 10 months ago
Devices without a LAN connection are using WIFI. The WIFI connected devices show language/locale/keyboard because a user has to fill in a WIFI password which is easy to do with the correct keyboard. This is a personal thing for everyone and the Admin has no clue what kind of keyboard is in the device (azerty/qwerty).. In fact, no one knows if the device is connected to LAN or WIFI so the answer is not clear at all. So i should say NO (B) cause with a LAN the user will never see the locale/keyboard settings.
upvoted 1 times

blablablax 1 year, 11 months ago
link you all refer says:
Windows Autopilot self-deploying mode lets you deploy a device with little to no user interaction.
For devices with an Ethernet connection, no user interaction is required.
For devices connected via Wi-fi, the user must only:
Choose the language, locale, and keyboard.
upvoted 1 times

loganharris 2 years ago

I am leaning towards yes with this one. Same as with the user driven, you can set what you want the user to set/accept with the new profile that you create.

upvoted 1 times

Saldi 2 years, 5 months ago

"If the Autopilot profile has been configured to automatically configure the language, locale, and keyboard layout, these OOBE screens should be skipped as long as Ethernet connectivity is available. Otherwise, manual steps are required:
**If multiple languages are preinstalled in Windows 10, the user must pick a language.
The user must pick a locale and a keyboard layout, and optionally a second keyboard layout."

The IT admin can configure the device so as the user choose a language of preference. The answer is (A) YES.

upvoted 1 times

Saldi 2 years, 5 months ago

Sorry Guys ...Discard that. The Answer is (B) NO
Windows Autopilot self-deploying mode enables a device to be deployed with little to no user interaction. For devices with an Ethernet connection, no user interaction is required; for devices connected via Wi-fi, no interaction is required after making the Wi-fi connection (choosing the language, locale, and keyboard, then making a network connection).

https://docs.microsoft.com/en-us/windows/deployment/windows-autopilot/self-deploying

upvoted 9 times

GSBXL 2 years, 5 months ago

well then it is half true, if by wifi you need to make wifi connection by first making the previous steps...

upvoted 1 times

loganharris 2 years ago

However, you create a new deployment profile and configure the settings you want to include if you want them to agree to the license agreement.

upvoted 1 times

Question #2 *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 need to ensure that feature and quality updates install automatically on a Windows 10 computer during a maintenance window.
Solution: In Group policy, from the Maintenance Scheduler settings, you configure Automatic Maintenance Random Delay.
Does this meet the goal?

A. Yes

B. No

Correct Answer: *B*
This just changes the random delay of the Maintenance window.
Instead. In Group policy, from the Windows Update settings, you enable Configure Automatic Updates, select 4-Auto download and schedule the install, and then enter a time.
Note: In Group Policy, within Configure Automatic Updates, you can configure a forced restart after a specified installation time.
To set the time, you need to go to Configure Automatic Updates, select option 4 - Auto download and schedule the install, and then enter a time in the Scheduled install time dropdown. Alternatively, you can specify that installation will occur during the automatic maintenance time.
Note 2: Automatic Maintenance Random Delay.
This policy setting allows you to configure Automatic Maintenance activation random delay. The maintenance random delay is the amount of time up to which
Automatic Maintenance will delay starting from its Activation Boundary. If you enable this policy setting Automatic Maintenance will delay starting from its
Activation Boundary by upto this time. If you do not configure this policy setting 4 hour random delay will be applied to Automatic Maintenance. If you disable this policy setting no random delay will be applied to Automatic Maintenance.
Reference:
https://docs.microsoft.com/en-us/windows/deployment/update/waas-restart https://www.windows-security.org/4e3326cbf573247dc63f65d3e2627d75/automatic-maintenance-random-delay

MikeMatt2020 Highly Voted 1 year, 4 months ago
I believe the answer is *FALSE*
I don't understand how setting a random delay on our install time has ANYTHING to do with our objective of automatically installing updates during a maintenance windows. What does setting a delay have to do with this?
upvoted 10 times

Wilf32 1 year, 4 months ago
Setting a delay will cause the update to run automaticcally after a random delay during the maintenance window....

So yes it will automaticially run insdie the windows which is what the question is asking.
upvoted 7 times

ExamStudy101 Highly Voted 1 year, 2 months ago
I think the answer is no. Looking at: https://docs.microsoft.com/en-us/windows-server/administration/windows-server-update-services/deploy/4-configure-group-policy-settings-for-automatic-updates#automatic-maintenance-random-delay

It states that "This setting(Automatic Maintenance Random Delay) is related to option 4(Autodownload and schedule) in Configure Automatic Updates. If you did not select option 4 in Configure Automatic Updates, it is not necessary to configure this setting.

So option "4. Autodownload and schedule" NEEDS to be selected for this to do anything. Therefore this answer is incorrect.
upvoted 8 times

syougun200x 1 month ago
Among all the comments here, your observation goes the deepest and seems right. Thank you.
upvoted 1 times

RodrigoT 6 months, 3 weeks ago
Since option 4 is usually "Not Configured" and the automatic updates run anyway, this "random-delay" is enough to reach the goal. So the answer is A.YES.
upvoted 4 times

ShanePh Most Recent 3 months ago
Selected Answer: B
Setting a delay will cause the update to run automatically after a random delay during the maintenance window....
upvoted 1 times

nipsey 6 months, 3 weeks ago
In Group Policy, within Configure Automatic Updates, you can configure a forced restart after a specified installation time.

To set the time, you need to go to Configure Automatic Updates, select option 4 - Auto download and schedule the install, and then enter a time in the Scheduled install time dropdown. Alternatively, you can specify that installation will occur during the automatic maintenance time (configured using Computer Configuration\Administrative Templates\Windows Components\Maintenance Scheduler).
upvoted 1 times

rovert94 8 months, 1 week ago

Selected Answer: B

I believe the answer is FALSE. Random delay does not specify a time in which updates will occur, it just allows for a delay once a maintenance window is started. Without setting the time, this will not complete the goal.

upvoted 3 times

Solaris2002 8 months, 2 weeks ago

The answer is correct. It's a complicated GPO, but this link gives a good description of what it does
https://admx.help/?Category=Windows_10_2016&Policy=Microsoft.Policies.MaintenanceScheduler::RandomDelayPolicy#:~:text=The%20maintenance%20random%20delay%20is%20the%20amount%20of,from%20its%20Activation%20Boundary%2C%20by%20upto%20this%20time.
The maintenance random delay is the amount of time up to which Automatic Maintenance will delay starting from its Activation Boundary.

If you enable this policy setting, Automatic Maintenance will delay starting from its Activation Boundary, by upto this time.

If you do not configure this policy setting, 4 hour random delay will be applied to Automatic Maintenance.

upvoted 7 times

Goofer 11 months ago

Automatic Maintenance Random delay
This policy setting allows you to configure the random delay for Automatic Maintenance activation.

The maintenance random delay is the amount of time up to which Automatic Maintenance will delay starting from its activation boundary. This setting is useful for virtual machines where random maintenance might be a performance requirement.

This setting is related to option 4 in Configure Automatic Updates. If you did not select option 4 in Configure Automatic Updates, you don't need to configure this setting.

Not Configured - A four-hour random delay is applied to Automatic.
Enabled - Automatic Maintenance will delay starting from its activation boundary by up to the specified amount of time.
Disabled - No random delay is applied to Automatic Maintenance.

upvoted 2 times

tf444 1 year ago

This policy setting allows you to configure Automatic Maintenance activation random delay. The maintenance random delay is the amount of time up to which Automatic Maintenance will delay starting from its Activation Boundary. If you enable this policy setting Automatic Maintenance will delay starting from its Activation Boundary by upto this time. If you do not configure this policy setting 4 hour random delay will be applied to Automatic Maintenance. If you disable this policy setting no random delay will be applied to Automatic Maintenance.

Policy path:
Windows Components\Maintenance Scheduler

upvoted 1 times

Tomtom11 1 year, 4 months ago

activation boundary
Enabling this policy setting overrides any default or modified settings configured on client computers in Control Panel > Action Center > Automatic Maintenance (or in some client versions, Maintenance).

upvoted 1 times

Tomtom11 1 year, 4 months ago

Does Automatic Maintenance Random Delay not mean that activation boundary GPO has be set?
The maintenance random delay is the amount of time up to which Automatic Maintenance will delay starting from its activation boundary. This setting is useful for virtual machines where random maintenance might be a performance requirement.

upvoted 1 times

J4ck13 1 year, 4 months ago

Answer appears to be correct.

To clarify on Mayurmak's statement, this policy is valid for windows 10:

"Supported On: At least Windows Server 2012, Windows 8 or Windows RT"

Reference: https://gpsearch.azurewebsites.net/#7817

upvoted 2 times

Wilf32 1 year, 5 months ago

It is valid for Windows 10. This link has some info.

My understanding is that the update will run within the maintenance window but at a random time.

https://docs.microsoft.com/en-us/windows-server/administration/windows-server-update-services/deploy/4-configure-group-policy-settings-for-automatic-updates#automatic-maintenance-random-delay

upvoted 2 times

mayurmak 1 year, 5 months ago

The Answer should be NO as this feature is not Supported for Windwos 10. The GPO says "Windows XP Professional Service Pack 1 or At least Windows 2000 Service Pack 3"

upvoted 2 times

MR_Eliot 5 months, 1 week ago

Requirements: At least Windows Server 2012, Windows 8 or Windows RT

upvoted 1 times

Question #3 *Topic 2*

Note: This question is part of a series of questions that present the same scenario. Each question in the series contains a unique solution that might meet the stated goals. Some question sets might have more than one correct solution, while others might not have a correct solution.
After you answer a question in this section, you will NOT be able to return to it. As a result, these questions will not appear in the review screen.
You need to ensure that feature and quality updates install automatically on a Windows 10 computer during a maintenance window.
Solution: In Group policy, from the Windows Update settings, you enable Configure Automatic Updates, select 4-Auto download and schedule the install, and then enter a time.
Does this meet the goal?

A. Yes

B. No

Correct Answer: *A*
In Group Policy, within Configure Automatic Updates, you can configure a forced restart after a specified installation time.
To set the time, you need to go to Configure Automatic Updates, select option 4 - Auto download and schedule the install, and then enter a time in the Scheduled install time dropdown. Alternatively, you can specify that installation will occur during the automatic maintenance time.
Reference:
https://docs.microsoft.com/en-us/windows/deployment/update/waas-restart

MikeMatt2020 Highly Voted 1 year, 4 months ago
I spent quite a lot of time researching the 3 possible solutions and decided to place my bets on this being the CORRECT answer.
1) Automatic Maintenance Random Delay has NOTHING to do with us achieving our goal of automatically installing updates during a maintenance window
2) Automatic Maintenance Activation Boundary made me take a deeper dive into these specific GPOs. From my understanding, configuring Activation Boundary will install updates on devices that are not in use. If a user is currently signed in, the updates will not install.
3) "Auto download and schedule the install" does what our question asks. We can decide NOT to check the option for "Automatic Maintenance", which includes Activation Boundary and Random Delay. This question is once again quite non-specific. Activation Boundary seems to do more than what the question is asking. If we just need to auto install updates during a maintenance window, I believe this answer achieves that goal.
upvoted 21 times

Pleebb 1 year, 3 months ago
I agree
https://docs.microsoft.com/en-us/windows/deployment/update/waas-restart
upvoted 1 times

ClaudioItCosta 1 year, 3 months ago
I think if your maintenance Windows is from 1:00 AM to 3:AM, the Random Delay can help you achieve the goal of update inside this maintenance window, since Random Delay put a max delay for the maintenance to start. Without this setting, the schedule will randomize the start to up to 4 hours, by default.
upvoted 4 times

letters1234 7 months, 2 weeks ago
You are assuming the maintenance window size and time, there is no mention in the question. It's a situational requirement not catered for in the exam.
upvoted 1 times

ExamStudy101 1 year, 2 months ago
Reread the beginning of these questions folks. Some situations have MULTIPLE SOLUTIONS, some situations have NO SOLUTIONS. It also is not asking for what is he 'correct method', it's only asking if the job gets done.
upvoted 5 times

RodrigoT 6 months, 3 weeks ago
Since option 4 is usually "Not Configured" and the automatic updates run anyway, this "random-delay" is enough to reach the goal. But, anyway in this question I think the answer is A.YES.
upvoted 1 times

RodrigoT 5 months ago
I'm changing my answer to NO, because if you set a FIXED time, and the maintenance window is changed by an admin decision, then the updates won't be "during a maintenance window" anymore.
upvoted 1 times

badguytoo Highly Voted 1 year, 1 month ago
I think this should be A. See below:
- 4 - Auto download and schedule the install
You can specify the schedule by using the options in this Group Policy setting. If no schedule is specified, the default schedule for all installations will be every day at 3:00 A.M. If any updates require a restart to complete the installation, Windows will restart the computer automatically. (if a user is signed in to the computer when Windows is ready to restart, the user will be notified and given the option to delay the restart.) Note: starting Windows 8, you can set updates to install during automatic maintenance instead of using a specific schedule tied to Windows Update. Automatic maintenance will install updates when the computer is not in use, and avoid installing updates when the computer is running on battery power. If automatic maintenance is unable to install updates within days, Windows Update will install updates right away. Users will then be notified about a pending restart. A pending restart will only take place if there is no potential for accidental data loss.
upvoted 5 times

coelho4cc Most Recent 3 months, 2 weeks ago

Selected Answer: B

B) The solution asks to specify a "time", which is not the same as my "maintenance window". The correct one is "checkbox" Install during automatic maintenance.

upvoted 1 times

RodrigoT 5 months, 1 week ago

Selected Answer: B

I guess the point is to "ensure" install during a maintenance window you can't enter a time. Because if the maintenance window changes, our time is still fixed and it could be out of the new maintenance window. So, I change my vote to B. No.

upvoted 3 times

MR_Eliot 5 months ago

I agree with you.

upvoted 1 times

Cisco 5 months, 3 weeks ago

Answer is A, it DOES meet the goal, see this video to show how its done: https://www.youtube.com/watch?v=AUn4KGGV2kI

upvoted 1 times

nipsey 6 months, 3 weeks ago

https://docs.microsoft.com/en-us/windows/deployment/update/waas-restart
In Group Policy, within Configure Automatic Updates, you can configure a forced restart after a specified installation time.

To set the time, you need to go to Configure Automatic Updates, select option 4 - Auto download and schedule the install, and then enter a time in the Scheduled install time dropdown. Alternatively, you can specify that installation will occur during the automatic maintenance time (configured using Computer Configuration\Administrative Templates\Windows Components\Maintenance Scheduler).

upvoted 1 times

rovert94 8 months, 1 week ago

Selected Answer: A

I agree with everything MikeMatt2020 said

upvoted 2 times

defrey 9 months ago

Hola, can someone explains why the answer is B? Thank you

upvoted 1 times

forummj 1 year, 2 months ago

From my understanding, if you want to configure automatic updates, you must select the option, 4-Auto download and schedule the install in the Configure Automatic Updates GPO. When enabled, and this option chosen, you can set the schedule, and this will install all updates available.

The other options simply appear to relate to scheduling behaviour.

Automatic Maintenance Activation Boundary is a schedule for when automatic maintenance starts, if not configured, the option 4-Auto download and schedule the install schedule you set will simply run.

The Automatic Maintenance Random Delay simply tells automatic maintenance to start after X-Minutes or X-Seconds after the Automatic Maintenance Activation Boundary is reached.

upvoted 2 times

RodrigoT 6 months, 3 weeks ago

Since option 4 is usually "Not Configured" and the automatic updates run anyway, this "random-delay" is enough to reach the goal.

upvoted 1 times

Perycles 1 year, 4 months ago

No : nothing about "maintenance" inside this GPO.

upvoted 1 times

ExamStudy101 1 year, 2 months ago

You're able to select the time at which the update installs, so within your maintenance window

upvoted 2 times

Wilf32 1 year, 5 months ago

The answer is no, you can set it to be within the maintenance windows, but if you then change the mainenance windows in the future this setting may fall outside of that window. It will not auto change this setting.

I agree with NO

upvoted 5 times

ExamStudy101 1 year, 2 months ago

In the given scenario at that given moment the solution works. These tests are only asking about the present moment, not some bs of what 'could' happen in the future.

upvoted 2 times

MikeMatt2020 1 year, 4 months ago

So...if my maintenance window changed in the future, my couldn't I just change this setting to adhere to the new maintenance window?

upvoted 3 times

Question #4 *Topic 2*

Note: This question is part of a series of questions that present the same scenario. Each question in the series contains a unique solution that might meet the stated goals. Some question sets might have more than one correct solution, while others might not have a correct solution.
After you answer a question in this section, you will NOT be able to return to it. As a result, these questions will not appear in the review screen.
You need to ensure that feature and quality updates install automatically on a Windows 10 computer during a maintenance window.
Solution: In Group policy, from the Maintenance Scheduler settings, you configure Automatic Maintenance Activation Boundary.
Does this meet the goal?

A. Yes

B. No

Correct Answer: *B*
Instead. In Group policy, from the Windows Update settings, you enable Configure Automatic Updates, select 4-Auto download and schedule the install, and then enter a time.
Note: In Group Policy, within Configure Automatic Updates, you can configure a forced restart after a specified installation time.
To set the time, you need to go to Configure Automatic Updates, select option 4 - Auto download and schedule the install, and then enter a time in the Scheduled install time dropdown. Alternatively, you can specify that installation will occur during the automatic maintenance time.
Reference:
https://docs.microsoft.com/en-us/windows/deployment/update/waas-restart

Mujja Highly Voted 1 year, 3 months ago
Answer should be Yes.
The setting changes the maintenance window. The updates still get installed, but at your defined maintenance window.
upvoted 9 times

Deric Most Recent 1 week, 5 days ago
Selected Answer: A
The answer is A. https://learn.microsoft.com/en-us/windows-server/administration/windows-server-update-services/deploy/4-configure-group-policy-settings-for-automatic-updates#computer-configuration--maintenance-scheduler-policy-settings
upvoted 1 times

veteran_tech 2 months, 2 weeks ago
I don't see setting a "window" of time in Group Policy. The closest is randomization. But the language "maintenance window" seems to apply to Configuration Manager, not GP.
upvoted 1 times

RodrigoT 5 months, 1 week ago
Selected Answer: B
Again here I guess the point is to "ensure" install during a maintenance window you can't enter a time. Because if the maintenance window changes, our time is still fixed and it could be out of the new maintenance window. So, my vote is B. No.
upvoted 1 times

RodrigoT 5 months, 1 week ago
And if you enable this policy it will override the maintenance window setting.
upvoted 2 times

nipsey 6 months, 3 weeks ago
https://docs.microsoft.com/en-us/windows-server/administration/windows-server-update-services/deploy/4-configure-group-policy-settings-for-automatic-updates#computer-configuration--maintenance-scheduler-policy-settings
Automatic Maintenance Activation Boundary
This policy enables you to configure the Automatic Maintenance activation boundary.

The activation boundary is the daily scheduled time at which Automatic Maintenance starts.
upvoted 1 times

nipsey 6 months, 3 weeks ago
https://docs.microsoft.com/en-us/windows/deployment/update/waas-restart
In Group Policy, within Configure Automatic Updates, you can configure a forced restart after a specified installation time.

To set the time, you need to go to Configure Automatic Updates, select option 4 - Auto download and schedule the install, and then enter a time in the Scheduled install time dropdown. Alternatively, you can specify that installation will occur during the automatic maintenance time (configured using Computer Configuration\Administrative Templates\Windows Components\Maintenance Scheduler).
upvoted 1 times

rj_client 6 months, 3 weeks ago
Yes I agree it is A.

If you disable or do not configure this policy setting, the daily scheduled time as specified in Security and Maintenance/Automatic Maintenance Control Panel will apply.

The “Automatic Maintenance Activation Boundary” policy description mentions the following:
“If you enable this policy setting, this will override the default daily scheduled time as specified in Security and Maintenance/Automatic Maintenance Control Panel.”
upvoted 1 times

RodrigoT 5 months ago

I vote NO, because if you set a FIXED time, and the maintenance window is changed by an admin decision, then the updates won't be "during a maintenance window" anymore.

upvoted 1 times

Mun11 8 months, 1 week ago

Maintenance Scheduler settings are located in the path: PolicyName > Computer Configuration > Policies > Administrative Templates > Windows Components > Maintenance Scheduler. The Maintenance Scheduler extension of Group Policy contains the following settings:

Automatic Maintenance Activation Boundary

Automatic Maintenance Random Delay

upvoted 1 times

IykeP 8 months, 2 weeks ago

Selected Answer: A

The maintenance activation boundary is the daily scheduled time at which Automatic Maintenance starts.

upvoted 3 times

tf444 11 months, 2 weeks ago

This policy setting allows you to configure the Automatic Maintenance activation boundary.

The maintenance activation boundary is the daily schduled time at which Automatic Maintenance starts

If you enable this policy setting, this will override the default daily scheduled time as specified in Security and Maintenance/Automatic Maintenance Control Panel.

If you disable or do not configure this policy setting, the daily scheduled time as specified in Security and Maintenance/Automatic Maintenance Control Panel will appl

upvoted 1 times

ExamStudy101 1 year, 2 months ago

I think it's no but only because the option for "Automatic Download and schedule" option from a previous questions NEEDS to be enabled for this setting to do anything.

upvoted 3 times

ExamStudy101 1 year, 2 months ago

Actually I'd change my answer to A

upvoted 3 times

Tomtom11 1 year, 4 months ago

The maintenance activation boundary is the daily schduled time at which Automatic Maintenance starts

If you enable this policy setting, this will override the default daily scheduled time as specified in Security and Maintenance/Automatic Maintenance Control Panel.

upvoted 1 times

Wilf32 1 year, 5 months ago

This will overide the maintenance window setting.

https://www.windows-security.org/070988756d95e4fc3ebfe6be6cc1094b/automatic-maintenance-activation-boundary

upvoted 3 times

Wilf32 1 year, 5 months ago

I agree with answer is NO

upvoted 1 times

Question #5 *Topic 2*

DRAG DROP -

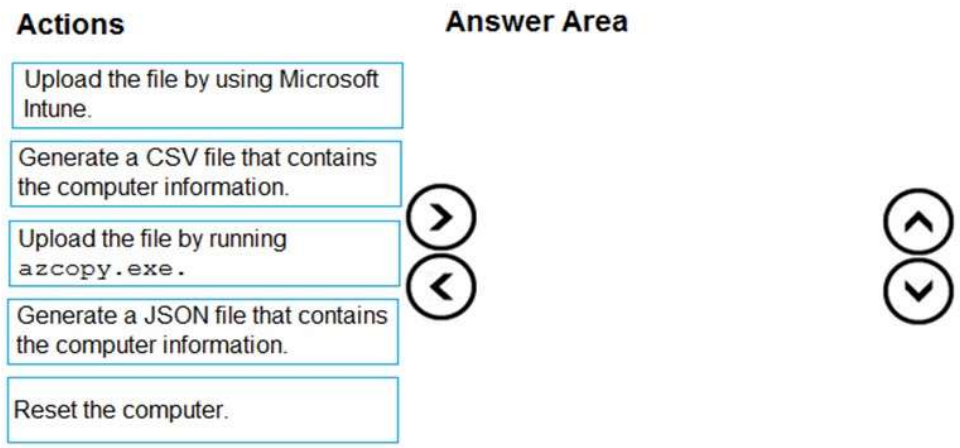
Your company has a computer named Computer1 that runs Windows 10.

Computer1 was used by a user who left the company.

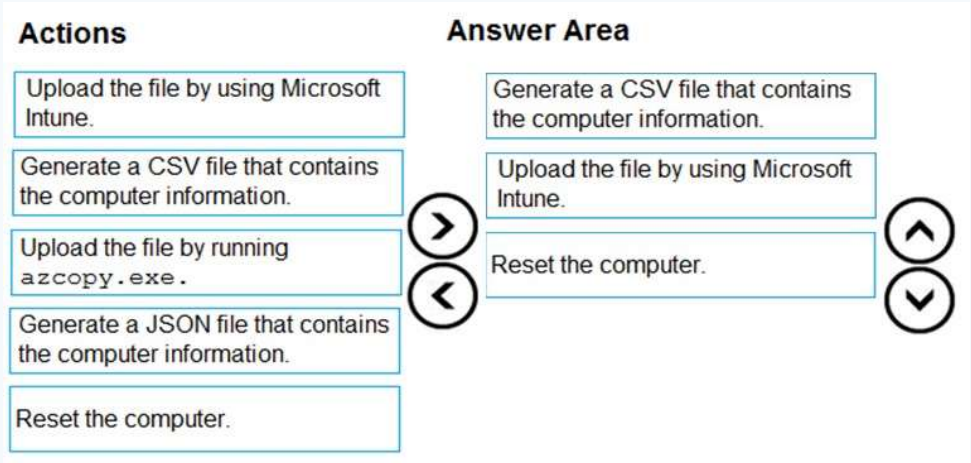
You plan to repurpose Computer1 and assign the computer to a new user. You need to redeploy Computer1 by using Windows AutoPilot.

Which three actions should you perform in sequence? To answer, move the appropriate actions from the list of actions to the answer area and arrange them in the correct order.

Select and Place:



Correct Answer:



Step 1: Generate a CSV file that contains the computer information

You can perform Windows Autopilot device registration within your organization by manually collecting the hardware identity of devices (hardware hashes) and uploading this information in a comma-separated-values (CSV) file.

Step 2: Upload the file by using Microsoft Intune

By default, Intune only applies this profile to Windows Autopilot devices. Yes, to convert all targeted, non-auto pilot devices to Autopilot so that they can receive the profile the next time they perform a factory reset.

Step 3: Reset the computer -

Windows Autopilot Reset takes the device back to a business-ready state, allowing the next user to sign in and get productive quickly and simply. Specifically,

Windows Autopilot Reset:

Removes personal files, apps, and settings.

Reapplies a device's original settings.

Sets the region, language, and keyboard to the original values.

Maintains the device's identity connection to Azure AD.

Maintains the device's management connection to Intune.

Reference:

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

https://docs.microsoft.com/en-us/windows/deployment/windows-autopilot/windows-autopilot-reset

Wilf32 Highly Voted 1 year, 5 months ago

I agree with the Answer.

Generate CSV
Upload to intune
Reset PC

upvoted 20 times

Lodan Most Recent 5 months, 3 weeks ago

Correct answer BUT: you may reset the device first; and have a USB which carries the scripts to get the CSV file. When the device is in Language select mode, you can hit Shift-F10 to get a CMD prompt to start Powershell in -bypass mode to generate the CSV.

Especially if the users has left the company, the account should be disabled by this time. Personally I find it's way easier to do it this way instead.

upvoted 1 times

RodrigoT 5 months ago

If you are and Associate Administrator in the company, you have administrative right on the computer. You just have to:
-Using PS admin:
Install-Script -Name Get-Windowsautopilotinfo
Y and Y
Get-ExecutionPolicy
Set-ExecutionPolicy Unrestricted
Y
Get-WindowsAutoPilotInfo.ps1 -outputfile c:\temp\deviceid.csv
Then go to endpoint.microsoft.com > Devices > Enroll devices > Devices > Import > point to the csv file.

Then you'll be able to use Autopilot reset.

upvoted 2 times

mikl 9 months, 2 weeks ago

Correct.

Generate CSV
Upload
Reset

upvoted 1 times

Perycles 1 year, 4 months ago

correct answer : for more information,Json file is used to upgrade windows 7 to Windows 10 using SCCM and then automatically start autopilot after OOBE.

upvoted 4 times

MikeMatt2020 1 year, 4 months ago

Correct

upvoted 2 times

Question #6 *Topic 2*

HOTSPOT -

Your company has an infrastructure that has the following:

⇨ A Microsoft 365 tenant

⇨ An Active Directory forest

⇨ Microsoft Intune

⇨ A Key Management Service (KMS) server

⇨ A Windows Deployment Services (WDS) server

⇨ A Microsoft Azure Active Directory (Azure AD) Premium tenant

The company purchases 100 new computers that run Windows 10.

You need to ensure that the new computers are joined automatically to Azure AD by using Windows Autopilot.

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

NOTE: Each correct selection is worth one point.

Hot Area:

Answer Area

Management tool:
- Azure Active Directory admin center
- Microsoft Endpoint Manager admin center
- Volume Activation Management Tool console
- Windows Deployment Services console

Required information from each computer:
- Device serial number and hardware hash
- MAC address and computer name
- Volume License Key and computer name

Correct Answer:

Answer Area

Management tool:
- Azure Active Directory admin center
- **Microsoft Endpoint Manager admin center**
- Volume Activation Management Tool console
- Windows Deployment Services console

Required information from each computer:
- **Device serial number and hardware hash**
- MAC address and computer name
- Volume License Key and computer name

Box 1: Microsoft Endpoint Manager admin center

Create an Autopilot device group using Intune

1. In the Microsoft Endpoint Manager admin center, select Groups > New group.

2. Etc.

Box 2: Device serial number and hardware hash

Ensure that the CSV file meets requirements.

Device information in the CSV file where you capture hardware hashes should include:

Serial number -

Windows product ID -

Hardware hash -

Optional group tag -

Optional assigned user -

Reference:

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

https://docs.microsoft.com/en-us/mem/autopilot/add-devices

RodrigoT 5 months ago

Answer is correct.

upvoted 4 times

Question #7 *Topic 2*

Your company purchases new computers that run Windows 10. The computers have cameras that support Windows Hello for Business.
You configure the Windows Hello for Business Group Policy settings as shown in the following exhibit.

Setting	State	Comment
Phone Sign-in		
Allow enumeration of emulated smart card for all users	Not configured	No
Turn off smart card emulation	Not configured	No
Use PIN Recovery	Not configured	No
Use a hardware security device	Not configured	No
Use biometrics	Enabled	No
Configure device unlock factors	Not configured	No
Configure dynamic lock factors	Enabled	No
Use Windows Hello for Business	Enabled	No
Use certificate on-premises authentication	Not configured	No

What are two valid methods a user can use to sign in? Each correct answer presents part of the solution.
NOTE: Each correct selection is worth one point.

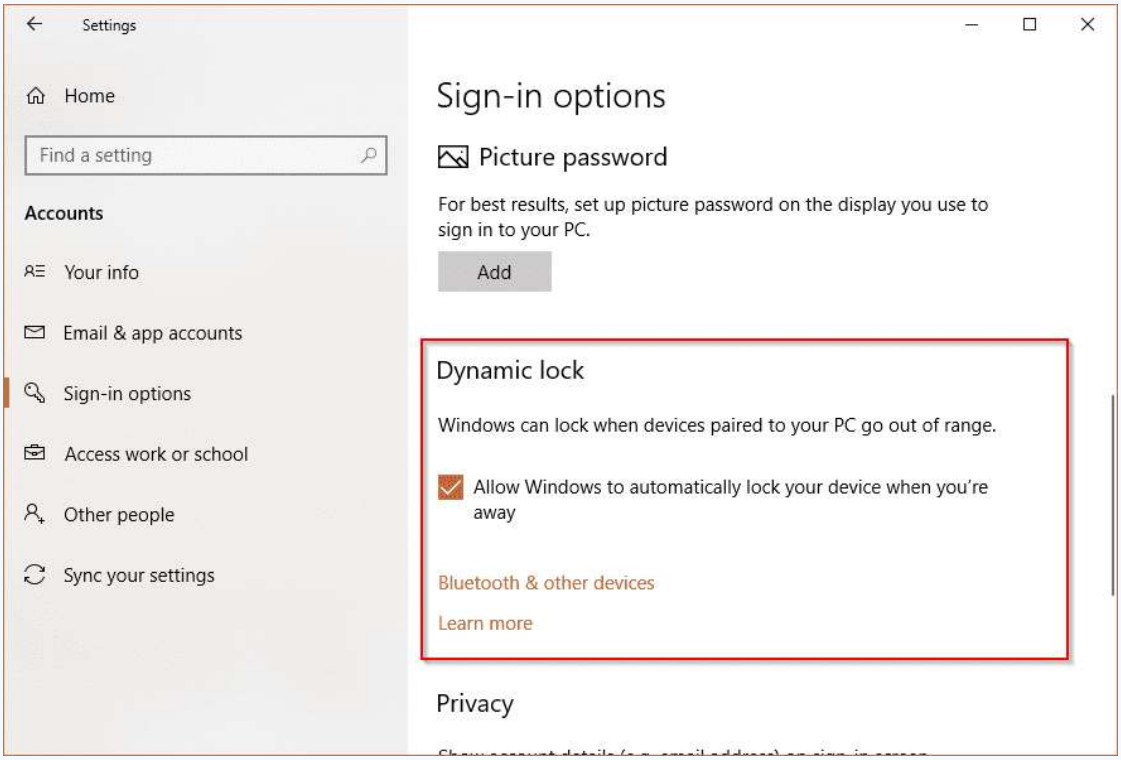
A. Facial recognition

B. A smartwatch that is Bluetooth-enabled

C. A PIN

D. A USB key

Correct Answer: *AB*
A: The default Windows Hello for Business enables users to enroll and use biometrics. However, some organization may want more time before using biometrics and want to disable their use until they are ready. To not allow users to use biometrics, configure the Use biometrics Group Policy setting to disabled and apply it to your computers.
B: Dynamic Lock is another feature introduced in 2018.
The setting is disabled by default. To enable it, go to Settings app, Accounts, and Sign-in options. Then check the option ג€Allow Windows to automatically lock your device when you are awayג€ in the Dynamic Lock section.



The system will scan and check to see if any paired devices that can be used to determine your presence. Once enabled, Dynamic Lock locks your PC automatically when it detects that you are not around. To me, it works the best when you pair your smartphone with your Windows 10 computer.
Click the Bluetooth & other devices link to go to the Bluetooth pairing page, and click the ג€Add Bluetooth or other devicesג€ button to start the pairing process.

Reference:

https://docs.microsoft.com/en-us/windows/security/identity-protection/hello-for-business/hello-cert-trust-policy-settings

https://www.nextofwindows.com/windows-10-what-is-dynamic-lock-and-how-to-turn-it-on

Derrickdrx Highly Voted 4 weeks ago

I will choose A and C. Question states "What are two valid methods can be use to sign in? Each correct answer presents part of the solution". Facial recognition and pin are the only choices to be able to sign in. A smartwatch that is Bluetooth-enabled has to do with locking the Windows device.

upvoted 9 times

FlailingLimbs 2 weeks ago

Agreed.

upvoted 1 times

cbjorn8931 Most Recent 4 days, 21 hours ago

https://windows.do/lock-your-pc-with-smartphone-or-watch/
Truthfully, A,B,C but since it asking for two I'm going with A,B because dynamic lock configure is enabled for smart devices. When you walk away the pc scans paired devices such as cell phones and smartwatches and if you are away a certain feet the desktop locks screen appears

upvoted 1 times

cbjorn8931 4 days, 21 hours ago

Never mind, question states sign in not logging out so I'm going with AC

upvoted 1 times

RickyBee 2 weeks, 3 days ago

Selected Answer: AC

Agree i

upvoted 1 times

thuba_TD 2 weeks, 5 days ago

Selected Answer: AC

i agree

upvoted 1 times

Question #8 *Topic 2*

You have 10 computers that run Windows 8.1 and have the following configurations:
⇨ A single MBR disk
⇨ A disabled TPM chip
⇨ Disabled hardware virtualization
⇨ UEFI firmware running in BIOS mode
Enabled Data Execution Prevention (DEP)
▪
You plan to upgrade the computers to Windows 10.
You need to ensure that the computers can use Secure Boot.
Which two actions should you perform? Each correct answer presents part of the solution.
NOTE: Each correct selection is worth one point.

A. Convert the MBR disk to a GPT disk

B. Enable the TPM chip.

C. Disable DEP

D. Enable hardware virtualization

E. Convert the firmware from BIOS to UEFI.

Correct Answer: *AE*
E: Need to use the UEFI mode to get the UEFI Security features.
A: If you want to ensure that your drive boots into a certain mode, use drives that you've preformatted with the GPT file format for UEFI mode, or the MBR file format for BIOS mode. When the installation starts, if the PC is booted to the wrong mode, Windows installation will fail. To fix this, restart the PC in the correct firmware mode.
Reference:
https://docs.microsoft.com/en-us/windows-hardware/manufacture/desktop/boot-to-uefi-mode-or-legacy-bios-mode

Question #9 *Topic 2*

Your network contains an Active Directory domain. The domain contains 2,000 computers that run Windows 10.
You implement hybrid Microsoft Azure Active Directory (Azure AD) and Microsoft Intune.
You need to automatically register all the existing computers to Azure AD and enroll the computers in Intune. The solution must minimize administrative effort.
What should you use?

A. An Autodiscover address record.

B. A Windows AutoPilot deployment profile.

C. An Autodiscover service connection point (SCP).

D. A Group Policy object (GPO).

Correct Answer: *B*
Hybrid Azure AD join.
Support for Hybrid Azure AD join (on-premises AD) using Windows Autopilot user-driven mode is available with Windows 10, version 1809 (or later).
Note: In this mode, you can use Windows Autopilot to join a device to an on-premises Active Directory domain. Configuring this feature is very similar to the
Windows Autopilot user-driven mode process today:
1. Register the device with Windows Autopilot.
2. Create an Autopilot deployment profile specifying Hybrid Azure AD as the method in which you would like to join devices to Azure AD.
3. Install the Intune Connector for Active Directory on a computer running Windows Server 2016 (or later).
Reference:
https://techcommunity.microsoft.com/t5/Windows-IT-Pro-Blog/Windows-Autopilot-Hybrid-Azure-AD-join-and-automatic/ba-p/286126

Mendel Highly Voted 3 years ago
D should be correct.
https://docs.microsoft.com/en-us/windows/client-management/mdm/enroll-a-windows-10-device-automatically-using-group-policy
upvoted 31 times

Sortjuh 2 years, 11 months ago
From the url you provided:
"Auto-enrollment into Intune via Group Policy is valid only for devices which are hybrid Azure AD joined. This means that the device must be joined into both local Active Directory and Azure Active Directory."

The question leads me to believe these devices aren't joined to Azure AD yet, and therefore the group policy wouldn't work. Correct me if I'm wrong.
upvoted 7 times

CvdK 1 year, 10 months ago
Yes, it will work. From https://docs.microsoft.com/en-us/windows/client-management/mdm/enroll-a-windows-10-device-automatically-using-group-policy :

The enrollment into Intune is triggered by a group policy created on your local AD and happens without any user interaction.
And
Starting in Windows 10, version 1607, once the enterprise has registered its AD with Azure AD, a Windows PC that is domain joined is automatically Azure AD–registered.
upvoted 2 times

CvdK 1 year, 10 months ago
So D is the correct answer!
upvoted 9 times

MZONDERL 8 months, 3 weeks ago
Azure AD–registered is not the same as Azure AD Joined...
upvoted 1 times

PESK 2 years, 11 months ago
Answer should be B: You're right. You can use GPO to register devices into Intune, but they must be AzureAD joined as a pre-req.
upvoted 9 times

Nemo19 2 years, 8 months ago
Correct answer is D!
In Fact the question says: "You implement hybrid Microsoft Azure Active Directory (Azure AD) and Microsoft Intune."
upvoted 7 times

cantCme 2 years, 1 month ago
"You need to automatically register all the existing computers to Azure AD"
So they aren't enrolled just yet.
upvoted 7 times

egdeeptha 1 year, 3 months ago

Yes, This GPO can enroll On premises AD joined devices to Intune Automatically. The answer is D.

Requirements:

Active Directory-joined PC running Windows 10, version 1709 or later
The enterprise has configured a mobile device management (MDM) service
The on-premises Active Directory must be integrated with Azure AD (via Azure AD Connect)
The device should not already be enrolled in Intune using the classic agents (devices managed using agents will fail enrollment with error 0x80180026)
The minimum Windows Server version requirement is based on the Hybrid Azure AD join requirement. See How to plan your hybrid Azure Active Directory join implementation for more information.

upvoted 1 times

RodrigoT 5 months, 1 week ago

You are right. If you use GPO you can only enroll the devices in MDM, not join them to Azure AD. This question will repeat on Page 1 Question #5 and the answer is always B. Autopilot Deployment Profile. I got this same question in a KAPLAN practice test and the answer is also B.

upvoted 1 times

jojolababu Highly Voted 1 year, 11 months ago

I think B is correct
To join the domain to AAD you would use AAD Connect
Then you would use a GPO to enroll in Intune
But we want to do both at the same time, Autopilot is supposed to do that

upvoted 13 times

RodrigoT 6 months ago

The link provided is for using Autopilot to join a device to an on-premises Active Directory domain. The question is exactly the opposite, to join and enroll EXISTING on-premises devices to AzureAD. To achieve this you use Group Policy. End of story.
https://docs.microsoft.com/en-us/windows/client-management/mdm/enroll-a-windows-10-device-automatically-using-group-policy#configure-the-auto-enrollment-for-a-group-of-devices

upvoted 2 times

RodrigoT 5 months, 1 week ago

FINAL ANSWER: B is correct. I just got this question on a KAPLAN practice test. You can use an Autopilot Deployment Profile for joining computers to your on-premisses AD domain, and the steps are:
1-Register the device with Windows Autopilot
2-Create an Autopilot deployment profile
3-Specify Hybrid Azure AD as the method
4-Install the Intune Connector for Active Directory on a computer running Windows Server 2016
https://techcommunity.microsoft.com/t5/windows-it-pro-blog/windows-autopilot-hybrid-azure-ad-join-and-automatic/ba-p/286126

upvoted 4 times

mikl 9 months, 2 weeks ago

Thats not how you minimize administrative effort - answer is D.

upvoted 1 times

Deric Most Recent 1 month ago

Lots of opinions here, but after doing some research I found this link, which as I understand it, points to B as the solution:
https://docs.microsoft.com/en-us/mem/intune/configuration/domain-join-configure?source=recommendations

upvoted 1 times

raduM 2 months ago

B shopuld be correct

upvoted 1 times

Harold 5 months ago

Selected Answer: B

In the official MCA MD101 practice tests from Wiley, the answer to this question is B - Windows Autopilot. I tend to agree with it, because it's not stated whether the existing devices are already even hybrid-joined, only that they want to. So yes, I'd say it's B.

upvoted 1 times

MR_Eliot 5 months ago

Selected Answer: C

C. You need to configure SCP records. You can do this by using Azure Connect tool.

upvoted 1 times

Cisco 5 months, 3 weeks ago

My Vote is B as selected, Autopilot can auto register all devices into Azure and then in turn enrol in intune. In this article refer to Phase A for how it works: https://docs.microsoft.com/en-us/azure/active-directory/devices/device-registration-how-it-works

And in this Article it shows that you can also use Autopilot to enrol in Intune:
https://docs.microsoft.com/en-us/mem/intune/enrollment/tutorial-use-autopilot-enroll-devices

upvoted 1 times

rajpatel007 6 months ago

so is it D or B?

upvoted 4 times

PChi 6 months, 1 week ago

In regard to PESK's comment... B is correct. If I am missing something here, lmk. Especially to those who are experienced or have done tests! I am seeing a lot of shaky answers on most of these posts so far.
https://docs.microsoft.com/en-us/mem/autopilot/windows-autopilot-hybrid

upvoted 1 times

PChi 6 months, 1 week ago

You cannot use GPO to enroll/join hybrid devices. I dunno why this has turned into a debate... but again, if I am missing something please let me know with hard facts please c:

upvoted 1 times

Garito 7 months, 1 week ago

Selected Answer: D

Minimal Effort

upvoted 2 times

forummj 8 months, 1 week ago

I think I see it now. The two questions from Topic 1 & 2 are similar.

The previous question states you recently configured hybrid AAD, so you haven't implemented it yet, thus you can still use the SCP setup from this link,
https://docs.microsoft.com/en-us/azure/active-directory/devices/hybrid-azuread-join-managed-domains

Whereby this question states that you have implemented hybrid AAD, which means the SCP portion can't be rerun, so the easier way of doing it would be to use GPO.

Autopilot, resets devices, this is not something you will be wanting for all your devices.

upvoted 3 times

Solaris2002 8 months, 1 week ago

We had this exact project at my org, we did this by implementing a GPO to register the devices in MDM. An Autopilot profile can only be deployed if you re-set the device, which does NOT minimize administrative effort!

upvoted 4 times

jenraed 6 months ago

We used a GPO in my organization as well!

upvoted 1 times

pogap64757 8 months, 2 weeks ago

This a repeat of question 5 from part 1
C. SCP connection point
https://docs.microsoft.com/en-us/azure/active-directory/devices/hybrid-azuread-join-managed-domains

upvoted 3 times

a92876 8 months, 2 weeks ago

Selected Answer: D

B will not work unless you want to reset and re-provision ALL the existing devices.
So D.

upvoted 2 times

b3arb0yb1m 9 months, 2 weeks ago

B. A Windows AutoPilot deployment profile.

upvoted 1 times

mikl 9 months, 2 weeks ago

Thats not really the way to accomplish : The solution must minimize administrative effort.

upvoted 1 times

NKG123 9 months, 3 weeks ago

If you think the right answer is B, go back to Ms documentation to study the question!
We will not reset 2000 devices to enroll them in Intune.
Right answer is D.

upvoted 6 times

sbmkhize 12 months ago

The correct answer is B.

upvoted 1 times

HOTSPOT -

Your network contains an Active Directory domain. The domain contains computers that run Windows 10 and are enrolled in Microsoft Intune.

Updates are deployed by using Windows Update for Business.

Users in a group named Group1 must meet the following requirements:

- Update installations must occur any day only between 00:00 and 05:00.
- Updates must be downloaded from Microsoft and from other company computers that already downloaded the updates.

You need to configure the Windows 10 Update Rings settings in Intune to meet the requirements.

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

NOTE: Each correct selection is worth one point.

Hot Area:

Update settings

Servicing channel	Semi-Annual Channel (Targeted)	
*Microsoft product updates	Allow	Block
*Windows drivers	Allow	Block
*Quality update deferral period (days)	0	
*Feature update deferral period (days)	0	
*Set feature update uninstall period (2-60 days)	10	

User experience settings

Automatic update behavior	Notify download	
Restart checks	Allow	Skip
Delivery optimization download mode	Not configured	

Correct Answer:

Update settings

Servicing channel	Semi-Annual Channel (Targeted)	
*Microsoft product updates	Allow	Block
*Windows drivers	Allow	Block
*Quality update deferral period (days)	0	
*Feature update deferral period (days)	0	
*Set feature update uninstall period (2-60 days)	10	

User experience settings

Automatic update behavior	Notify download	
Restart checks	Allow	Skip
Delivery optimization download mode	Not configured	

Box 1: Notify download -
Here's what Automatic update behavior means:
* Notify download â€" Notify the user before downloading the update. Users choose to download and install updates.
* Auto install at maintenance time â€" Updates download automatically and then install during Automatic Maintenance when the device isn't in use or running on battery power.
* Auto install and restart at maintenance time â€" Updates download automatically and then install during Automatic Maintenance when the device isn't in use or running on battery power.

Box 2: Not configured -
With Intune, use Delivery Optimization settings for your Windows devices to reduce bandwidth consumption when those devices download applications and updates. Configure Delivery Optimization as part of your device configuration profiles.
Reference:
https://deviceadvice.io/2020/01/27/windows-10-update-rings-the-best-user-experience/ https://docs.microsoft.com/en-us/intune/delivery-optimization-windows#move-from-existing-update-rings-to-delivery-optimization

VCE_player Highly Voted 1 year, 9 months ago
Answer is correct. Though today The Delivery Optimization settings reside in a specific Windows 10 configuration profile called "Delivery Optimization". They don't seem to show up in the Update Ring settings anymore...
upvoted 12 times

RodrigoT 6 months ago
And you should change also the Automatic update behavior, because when it's set to "Notify download" you won't be even able to choose a scheduled time.
upvoted 1 times

PESK Highly Voted 2 years, 11 months ago
Answer is incorrect.
Automatic update behaviour should be set to "Auto install and restart at scheduled time". This setting allows you to specify an installation day and time. If "Scheduled install time" is unspecified, installation runs at 3am daily by default.

Delivery optimization download mode should be set to "HTTP blended with peering behind the same NAT" which allows computer to get updates from the internet and from other computers on your network.
upvoted 8 times

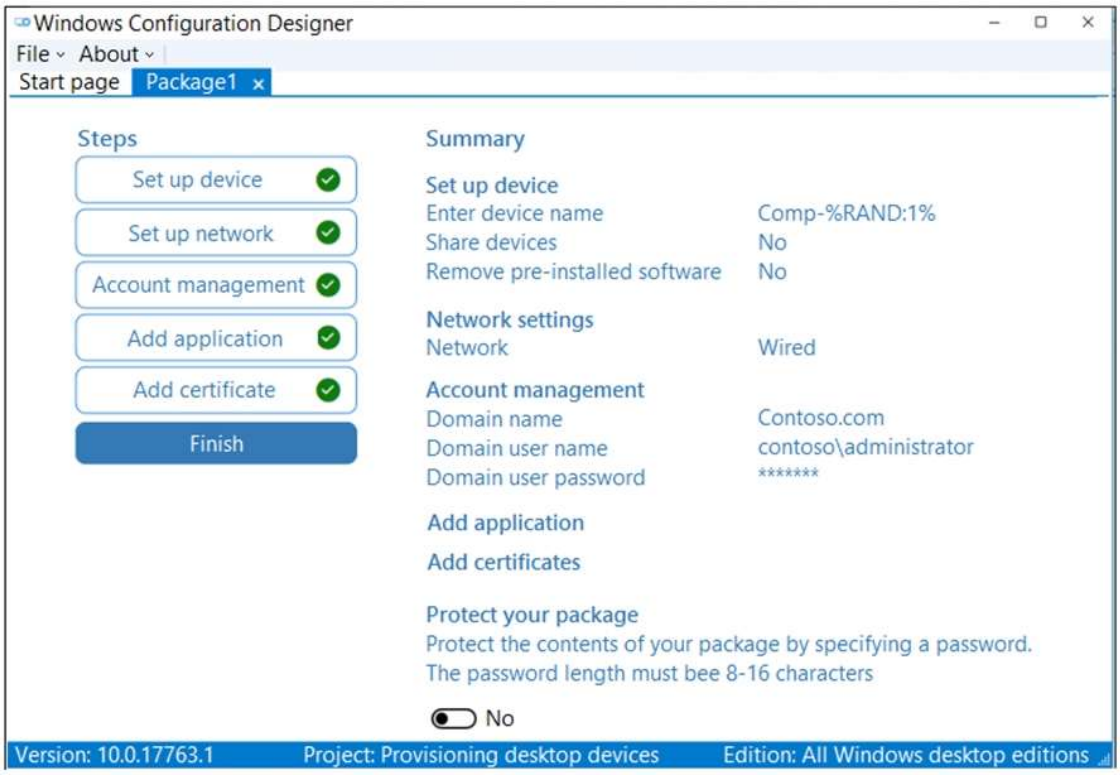
Sortjuh 2 years, 11 months ago
Automatic update behaviour and Delivery optimization download mode are the settings that need to be changed, it doesn't ask for which options to select there. The highlighted settings are the ones that need to be changed and are therefore the correct answer.
upvoted 29 times

PESK 2 years, 11 months ago
Thanks for the clarification. I'm over-thinking it as usual.
upvoted 8 times

Question #11 *Topic 2*

Your network contains an Active Directory domain named contoso.com.

You create a provisioning package named Package1 as shown in the following exhibit.



What is the maximum number of devices on which you can run Package1 successfully?

A. 1

B. 10

C. 25

D. unlimited

Correct Answer: *B*

The device name uses a single random number (applied by %RAND:1%). This allows for 10 unique values (0 9 "€ƛ).

Merma Highly Voted 1 year, 4 months ago

Answer is correct as shown in the example in link provided. "%RAND:<# of digits> Generates the specified number of random digits. Test%RAND:6% Test123456" In this case %RAND:<# of digits> Generates the specified number of random digits. Comp %RAND:1%. The computer name can be Comp0 - Comp9 = 10 as a maximum number of computers.
"%SERIAL% Generates the serial number derived from the device. If the serial number causes the new name to exceed the 15 character limit, the serial number will be truncated from the beginning of the sequence."

upvoted 16 times

MaxMink Most Recent 2 months, 2 weeks ago

Selected Answer: B

Right!

upvoted 1 times

AL99 6 months, 2 weeks ago

Answer : B : 10 device

upvoted 1 times

Hulisanimellla 6 months, 2 weeks ago

Selected Answer: B

ANSWER IS CORRECT

upvoted 1 times

PersoDaniels 1 year, 3 months ago

Answer B. is correct.
0-9 = 10

https://docs.microsoft.com/en-us/windows/configuration/provisioning-packages/provision-pcs-for-initial-deployment#configure-settings

upvoted 3 times

Alphurs 1 year, 3 months ago

Answer is D

upvoted 2 times

Mujja 1 year, 3 months ago

I can see Merma's explanation, and at first it's what I thought. But it's a random number, not sequential. The same number could repeat for the 2nd, 3rd or 4th device. The PPKG has no history of which number has already been used, it's random. All devices will process the PPKG regardless. and you will end up with duplicate hostnames in AD.

upvoted 1 times

justabasicuser 1 year, 2 months ago

The PPKG package in this instance has to join it to the active directory domain which would not allow duplicates... I'd presume it would have issues then and fail to deploy

upvoted 2 times

AVR31 5 months, 1 week ago

You cannot have duplicate names in AD. If the computer name already exists in AD, the package will fail.

upvoted 1 times

Perycles 1 year, 4 months ago

i'm agree with the answer - pc number depend on RAND capacity.

upvoted 2 times

HOTSPOT -

You have computers that run Windows 10 and are configured by using Windows Autopilot.

A user performs the following tasks on a computer named Computer1:

- Creates a VPN connection to the corporate network
- Installs a Microsoft Store app named App1
- Connects to a Wi-Fi network

You perform a Windows Autopilot Reset on Computer1.

What will be the state of the computer when the user signs in? To answer, select the appropriate options in the answer area.

NOTE: Each correct selection is worth one point.

Hot Area:

Answer Area

The Wi-Fi connection will be:

- Removed
- Retained and the passphrase will be retained
- Retained but the passphrase will be reset

App1 will be:

- Reinstalled at sign-in
- Removed
- Retained

The VPN connection will be:

- Removed
- Retained and the credentials will be cached
- Retained but the credentials will be reset

Correct Answer:

Answer Area

The Wi-Fi connection will be:

- Removed
- **Retained and the passphrase will be retained**
- Retained but the passphrase will be reset

App1 will be:

- Reinstalled at sign-in
- **Removed**
- Retained

The VPN connection will be:

- **Removed**
- Retained and the credentials will be cached
- Retained but the credentials will be reset

Box 1: Retained and the passphrase will be retained

The Windows Autopilot Reset process automatically keeps information from the existing device:

* Wi-Fi connection details.

Box 2: Removed -

Windows Autopilot Reset:

* Removes personal files, apps, and settings.

Box 3: Removed -

Windows Autopilot Reset:

Removes personal files, apps, and settings.
Reapplies a device's original settings.
Sets the region, language, and keyboard to the original values.
Maintains the device's identity connection to Azure AD.
Maintains the device's management connection to Intune.
The Windows Autopilot Reset process automatically keeps information from the existing device:
Wi-Fi connection details.
Provisioning packages previously applied to the device.
A provisioning package present on a USB drive when the reset process is started.
Azure Active Directory device membership and MDM enrollment information.
Reference:
https://docs.microsoft.com/en-us/windows/deployment/windows-autopilot/windows-autopilot-reset

j0eyv Highly Voted 1 year, 10 months ago
Tested this today. Answer is ok:
- Wifi password remain
- App1 removed
- VPN removed
upvoted 55 times

RodrigoT 5 months, 1 week ago
Thank you for really testing.
upvoted 3 times

Lomak Highly Voted 2 years, 1 month ago
The Windows Autopilot Reset process automatically retains information from the existing device:

Set the region, language, and keyboard to the originally-configured values.
Wi-Fi connection details.
Provisioning packages previously applied to the device, as well as a provisioning package present on a USB drive when the reset process is initiated.
Azure Active Directory device membership and MDM enrollment information.
upvoted 15 times

NKG123 Most Recent 10 months, 1 week ago
Shut your mouth instead of saying wrong statements
upvoted 4 times

sbmkhize 12 months ago
The answer does not look to be right BUT it is right....
upvoted 2 times

uns_uns 1 year, 6 months ago
I agree with the answers. For users who question why the WIFI information will be retained, think of it from the device's standpoint/Autopilot, "How will the device communicate with Autopilot if there is no internet connection?"
upvoted 11 times

forExamCert2023 7 months ago
Well, we, actually, used LAN cable drop. That should not be surprised to any IT person. Just a bit of more info, better use power cable instead of relying on the laptop battery, if the computer is a laptop. Just FYI from an old dog.
upvoted 2 times

RodrigoT 6 months ago
Even so, the "new dog" uns_uns is right.
https://docs.microsoft.com/en-us/mem/autopilot/windows-autopilot-reset
Autopilot is designed to deploy, reset, reuse, etc. devices remotely around the world. Even in a hotel room. Welcome to the "new dog modern desktop" world.
upvoted 1 times

67_sbc 1 year, 10 months ago
"Wi-fi, VPN profile, certificates, e-mail accounts, the Azure AD join record, and apps will all be removed." - https://deviceadvice.io/2019/08/09/autopilot-reset-what-does-it-do-how-is-it-different/
upvoted 2 times

RodrigoT 6 months ago
Wrong source, try the official one:
https://docs.microsoft.com/en-us/mem/autopilot/windows-autopilot-reset
"Autopilot Reset process automatically keeps information from the existing device:
Wi-Fi connection details"
upvoted 3 times

MaxMink 2 months, 2 weeks ago
From the website you shared: "Autopilot Reset also maintains the region/language/keyboard, any provisioning packages applied, and Wi-Fi connections." - https://deviceadvice.io/2019/08/09/autopilot-reset-what-does-it-do-how-is-it-different/
upvoted 1 times

Jammer 1 year, 11 months ago
I believe the answer provided is correct. Since it was a user that set up the vpn connection. If it been done through a different way it wouldn't be removed.
upvoted 2 times

RGM 1 year, 11 months ago

https://docs.microsoft.com/en-us/mem/autopilot/windows-autopilot-reset
wifi details will remain.
app1 will be removed
vpn will be removed

upvoted 4 times

Justin0020 1 year, 12 months ago

This question answer is correct: https://docs.microsoft.com/en-us/mem/autopilot/windows-autopilot-reset

upvoted 2 times

MD0000 1 year, 11 months ago

there is no specific mention of VPN status after reset on the referenced link

upvoted 1 times

loganharris 2 years ago

VPN connection will be retained and the credentials will be cached rest is correct

upvoted 1 times

MD0000 1 year, 11 months ago

source please

upvoted 2 times

Mujja 1 year, 3 months ago

VPN uses personal credentials, usually the same as AD credentials. Would be a security risk to leave these on the device, you don't want an unknown user access the company network remotely.

upvoted 1 times

aronutics 2 years, 1 month ago

Why Wi-Fi connection will not removed?

upvoted 3 times

Mujja 1 year, 3 months ago

Wifi is usually a connection to a user's private home network. Not much of a risk if the device remembers the WiFi passphrase for a private network.

upvoted 1 times

Duyons 1 year, 6 months ago

https://docs.microsoft.com/en-us/mem/autopilot/windows-autopilot-reset

upvoted 2 times

Question #13 *Topic 2*

HOTSPOT -

Your network contains an Active Directory domain named constoso.com that is synced to Microsoft Azure Active Directory (Azure AD). All computers are enrolled in Microsoft Intune.

The domain contains the computers shown in the following table.

Name	Operating system
Computer1	Windows 8.1 Enterprise
Computer2	Windows 10 Enterprise without the latest feature update
Computer3	Windows 10 Enterprise with the latest feature update

You are evaluating which Intune actions you can use to reset the computers to run Windows 10 Enterprise with the latest update.

Which computers can you reset by using each action? To answer, select the appropriate options in the answer area.

NOTE: Each correct selection is worth one point.

Hot Area:

Answer Area

Fresh Start action:

- Computer1 only
- Computer2 only
- Computer3 only
- Computer2 and Computer3 only
- Computer1, Computer2, and Computer3

Wipe action:

- Computer1 only
- Computer2 only
- Computer3 only
- Computer2 and Computer3 only
- Computer1, Computer2, and Computer3

Correct Answer:

Answer Area

Fresh Start action:

- Computer1 only
- Computer2 only
- Computer3 only
- **Computer2 and Computer3 only**
- Computer1, Computer2, and Computer3

Wipe action:

- Computer1 only
- Computer2 only
- Computer3 only
- Computer2 and Computer3 only
- **Computer1, Computer2, and Computer3**

Box 1: Computer 2 and Computer 3 only

The Fresh Start device action removes any apps that are installed on a PC running Windows 10, version 1709 or later.

Box 2: Computer1, Computer2, and Computer3

Windows Wipe:

Data type	Windows 8.1 (MDM) and Windows RT 8.1	Windows RT	Windows 10
Company apps and associated data installed by Intune	Keys are revoked for files that are protected by EFS. The user can't open the files.	Company apps aren't removed.	Apps are uninstalled. Sideloading keys are removed. For Windows 10 version 1709 (Creators Update) and later, Microsoft 365 Apps aren't removed. Intune management extension installed Win32 apps will not be uninstalled on unenrolled devices. Admins can leverage assignment exclusion to not offer Win32 apps to BYOD Devices.

Reference:
https://docs.microsoft.com/en-us/intune/device-fresh-start
https://docs.microsoft.com/en-us/intune/devices-wipe

Deric 1 week, 5 days ago
The answer is correct.
upvoted 3 times

Question #14 *Topic 2*

You have the 64-bit computers shown in the following table.

Name	Operating system	Memory	BitLocker Drive Encryption (BitLocker)
Computer1	32-bit version of Windows 7 Service Pack 1 (SP1)	1 GB	Enabled
Computer2	64-bit version of Windows 7 Service Pack 1 (SP1)	4 GB	Enabled
Computer3	32- bit version of Windows 8.1	2 GB	Enabled
Computer4	64-bit version of Windows 8.1	4 GB	Disabled

You plan to perform an in-place upgrade to the 64-bit version of Windows 10.

Which computers can you upgrade to the 64-bit version of Windows 10 in their current state?

A. Computer2 and Computer4 only

B. Computer4 only

C. Computer3 and Computer4 only

D. Computer1, Computer2, Computer3 and Computer4

E. Computer2, Computer3, and Computer4 only

Correct Answer: *A*

Note: Once the Windows 10 upgrade is complete the key in plain text is removed, and then BitLocker will enable again automatically. This means that the

Windows 10 upgrade process on a device using BitLocker is the same to a device without using the security feature

Incorrect:

Not Computer1 or Computer3:

Changing from Windows 7, Windows 8, or Windows 8.1 x86 to Windows 10 x64. The upgrade process cannot change from a 32-bit operating system to a 64-bit operating system, because of possible complications with installed applications and drivers.

Reference:

https://docs.microsoft.com/en-us/windows/deployment/windows-10-deployment-scenarios https://pureinfotech.com/upgrade-windows-10-bitlocker-enabled/

Santosh4u Highly Voted 2 years, 8 months ago

Answer A is correct. You can upgrade to Windows 10 even if the Bitlocker is enabled. Check this: https://docs.microsoft.com/en-us/windows/security/information-protection/bitlocker/bitlocker-upgrading-faq#can-i-upgrade-to-windows10-with-bitlocker-enabled

Also, the question is targeting whether it can be be done or not and the answer is yes.

upvoted 28 times

Dave4187 Highly Voted 2 years, 4 months ago

A is correct You cannot in place upgrade Windows when you are changing from 32bit to 64bit architecture. A wipe and load would have to be done in this case. Bitlocker will be suspended during inplace upgrade so that is a non issue

upvoted 18 times

MCSA11 Most Recent 8 months, 1 week ago

A. Computer2 and Computer4 only

upvoted 2 times

washandr 8 months, 1 week ago

Wrong
Only computer 4.
Question says "in their current state"
Device 2 cannot go from current state directly to windows 10. Therefore only device 4 is the correct answer.

upvoted 1 times

washandr 8 months, 1 week ago

Ignore the above. Apparently you can update w7 directly to w10

upvoted 2 times

mikl 9 months, 2 weeks ago

A. Computer2 and Computer4 only

Due to the fact that you cant do upgrade from 32-bit to 64-bit.

upvoted 3 times

Moderator 9 months, 2 weeks ago

Selected Answer: A

Answer A is correct.
If you're using BitLocker Disk Encryption, then by default Windows Setup automatically suspends it during upgrade. Starting in Windows 10 version 1803, Windows Setup includes the /BitLocker command-line parameter to control this behavior.

upvoted 1 times

b3arb0yb1m 9 months, 2 weeks ago

A. Computer2 and Computer4 only

upvoted 1 times

3citech 10 months, 2 weeks ago

You cannot changing from Windows 7, Windows 8, or Windows 8.1 x86 to Windows 10 x64. The upgrade process cannot change from a 32-bit operating system to a 64-bit operating system, because of possible complications with installed applications and drivers.
2 and 4 only

upvoted 1 times

encxorblood 10 months, 2 weeks ago

A is correct. x64 need 2GB of memory. And you can not upgrade a 32 bit system to 64 bit.

upvoted 2 times

imtiazL 1 year ago

correct option is computer 2 & 4
the reason is the memory
you can upgrade from 32bit to 64bit (as we did it in my environment) but wont on computer 1 & 3 because of the minimum requirements (even though you can its not recommended my Microsoft)

upvoted 2 times

Lodan 5 months, 3 weeks ago

Partially correct; it certainly is not possible to do an in-place upgrade from 32-bit to 64-bit. If it was possible, it should be E in your case, as 64-bit requires at least 2GB, which computer3 has.

upvoted 1 times

Danohav 1 year, 4 months ago

On the link provided (https://docs.microsoft.com/en-us/windows/deployment/windows-10-deployment-scenarios) with the solution you have all the answers:
- ... While devices encrypted with BitLocker can easily be upgraded....
- The upgrade process cannot change from a 32-bit operating system to a 64-bit operating system, because of possible complications with installed applications and drivers.

Therefore A (Cumputer 2 and Computer 4 only) is correct

upvoted 3 times

tezawynn 1 year, 9 months ago

you cannot do in place upgrade from 32 to 64bits OS.
Reference below.

If you have a desktop or laptop running the 32-bit version, you can upgrade to the 64-bit version without acquiring a new license. The only caveat is that there is no in-place upgrade path to make the switch, making a clean installation of Windows 10 the only viable option.https://www.google.com/url?sa=t&rct=j&q=&esrc=s&source=web&cd=&cad=rja&uact=8&ved=2ahUKEwjVrra95-DtAhWR7XMBHcM_CEQQFjABegQIBhAC&url=https%3A%2F%2Fwww.windowscentral.com%2Fhow-upgrade-32-bit-64-bit-version-windows-10&usg=AOvVaw1ZaGYzaOlYJqIKssyvm_T4

upvoted 5 times

hawkens 1 year, 9 months ago

In the current state bitlocker is enabled on comp 2, so cannot upgrade. To upgrade a machine from W7 and W10 with bitlocker enabled, you need to suspend bitlocker.

So the correct answer should be B if you aks me.

upvoted 1 times

ercluff 1 year, 1 month ago

Dave4187 and Santosh4u are correct. Bitlocker is disabled by the inplace upgrade process and restored when it is finished. see: https://superuser.com/questions/942969/can-i-upgrade-to-windows-10-with-bitlocker-enabled

upvoted 1 times

BLYBOI 1 year, 10 months ago

I think answer is correct.
Changing from Windows 7, Windows 8, or Windows 8.1 x86 to Windows 10 x64. The upgrade process cannot change from a 32-bit operating system to a 64-bit operating system, because of possible complications with installed applications and drivers.

upvoted 2 times

Samoanhulk 1 year, 10 months ago

Comp 2 and Comp 4

upvoted 2 times

Jammer 1 year, 11 months ago

Dave4187 got it right. Bit locker will just be suspended during the upgrade. A is correct.

upvoted 2 times

RobbieH 2 years ago

I go with A - however the question actually says which can you "upgrade". Not Inplace upgrade.... they are so picky on other questions - why not this one?

upvoted 1 times

Question #15 *Topic 2*

You have 200 computers that run Windows 10. The computers are joined to Microsoft Azure Active Directory (AD) and enrolled in Microsoft Intune.

You need to enable self-service password reset on the sign-in screen.

Which settings should you configure from the Microsoft Endpoint Manager admin center?

A. Device configuration

B. Device compliance

C. Device enrollment

D. Conditional access

Correct Answer: *A*

To enable the self service password reset option with Intune.

Use the Azure portal to create a new configuration policy. Open Microsoft Intune, choose Device Configuration, Profiles and Create profile.

Reference:

https://www.inthecloud247.com/enable-self-service-password-reset-feature-on-the-windows-logon-screen/

Perycles Highly Voted 1 year, 4 months ago

Answer is correct : we need to create a custom OMA-URI profil (so under DEVICE CONFIGURATION) to apply this parameters.
See the good link for more informations.
https://docs.microsoft.com/fr-fr/azure/active-directory/authentication/howto-sspr-windows

upvoted 11 times

RodrigoT 5 months, 1 week ago

The same question appeared on Page 1 Question #9.

upvoted 1 times

mikl Most Recent 9 months, 2 weeks ago

Selected Answer: A

A. Device configuration

Agree!

upvoted 4 times

b3arb0yb1m 9 months, 2 weeks ago

A. Device configuration

upvoted 2 times

Harisasikumar92 11 months, 2 weeks ago

This has changed. Now you can go to endpoint manager->Users->Password reset and you can enable sspr straight from there.

upvoted 3 times

asturmark 3 weeks, 5 days ago

You are talking about enabling self-password reset from the web. If you want to do enable it on windows log-on you need to do it from intune - device configuration - custom policy - OMA-URI

upvoted 1 times

tf444 11 months, 2 weeks ago

It is not in intune, it is in Azure !
Sign in to the Azure portal , then select Intune .

Create a device configuration profile by going to Device configuration > Profiles , then select + Create profile

For Platform , choose Windows 10 and later
For Profile type , choose Custom
Select Create , then provide a meaningful profile name, such as Windows 10 Login Screen for SSPR

Optionally, specify a meaningful description of the profile, and then select Next .

Under Configuration Settings , select Add , and then provide the following OMA-URI setting to enable the reset password link:

Provide a meaningful name to describe the action of the parameter, for example Add SSPR Link .
Optionally, specify an explicit description of the parameter.
OMA-URI parameter set to./Vendor/MSFT/Policy/Config/Authentication/AllowAadPasswordReset
Parameter Data type set to the value Integer
Parameter Value set to 1

upvoted 2 times

RodrigoT 6 months ago

Dude, if you open Intune from the Azure portal you'll be redirected to Endpoint. You are overthinking, relax man.

upvoted 5 times

Jvp21 1 year, 3 months ago

https://docs.microsoft.com/en-us/azure/active-directory/authentication/howto-sspr-windows

upvoted 4 times

Question #16 *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.
Your company uses Windows Update for Business.
The research department has several computers that have specialized hardware and software installed.
You need to prevent the video drivers from being updated automatically by using Windows Update.
Solution: From the Device Installation and Restrictions settings in a Group Policy object (GPO), you enable Prevent installation of devices using drivers that match these device setup classes, and then you enter the device GUID.
Does this meet the goal?

A. Yes

B. No

Correct Answer: *B*
Prevent installation of devices using drivers that match these device setup classes.
This policy setting allows you to specify a list of device setup class globally unique identifiers (GUIDs) for driver packages that Windows is prevented from installing. By default, this policy setting takes precedence over any other policy setting that allows Windows to install a device.
Reference:
https://admx.help/?Category=Windows_10_2016&Policy=Microsoft.Policies.DeviceInstallation::DeviceInstall_Classes_Deny

jairojunior_br Highly Voted 2 years, 7 months ago
The domain GPO exists, but would not be considered as correct, because it dont specify that drivers could not be installed via Windows Update. It prevents that drivers can be installed in every way possible.
Maybe this is why it's not the best option.

The Domain GPO can be found in: Group Policy Management Editor > Default Domain Policy>Computer Configuration>Policies>Administrative Templates>System>Device Installation Restrictions
upvoted 17 times

Morwen 6 days, 7 hours ago
The question isn't to block installation of drivers, but to prevent updates. Per docs article, it's B- NO, because proposed solution only blocks installation (it doesn't say anything about updates), while "Prevent installation of devices using drivers that match these device setup classes" says " can't install or update"
upvoted 1 times

Syed7 1 year, 4 months ago
so your answer is A -> Yes ???
upvoted 4 times

Anthony_2770 1 year, 7 months ago
Yes the question should have indicated if it was a workgroup or a domain as there are differences between the domain GPO and a local GPO
upvoted 3 times

Anthony_2770 1 year, 7 months ago
Also Local GPO does exist. It exists in a different place.
Computer Configuration > Administrative Templates > System > Device Installation> Device Installaton Restrictions > Prevent installation of devices using drivers that match these device setup classes
upvoted 1 times

Anthony_2770 1 year, 7 months ago
So the question is not questioning the user as regards whether the issue at hand relates to a domain gpo or simply does not exist in a local gpo
upvoted 1 times

snabelkabel Highly Voted 2 years, 8 months ago
I think this should be A: Yes, it is possible to do it this way, and the referenced url only states another way to achive the same goal, not that it is incorrect
upvoted 13 times

Dedutch Most Recent 2 months, 1 week ago
I've done this before for network drivers that have caused issues.
upvoted 1 times

MitchF 2 months, 2 weeks ago
Source: https://docs.microsoft.com/en-us/windows/client-management/manage-device-installation-with-group-policy

"When you use device Classes to allow or prevent users from installing drivers, you must specify the GUIDs for all of the device's device setup classes, or you might not achieve the results you want. The installation might fail (if you want it to succeed) or it might succeed (if you want it to fail)."

This means you should use GUIDs if you want to "prevent users from installing drivers"...I pick "A) Yes" as correct answer
upvoted 1 times

Whatsamattr81 3 months, 2 weeks ago

The question is 'updated automatically' not 'installed'. That GPO would prevent any installation, even manual.

upvoted 1 times

MR_Eliot 5 months ago

Selected Answer: A

Prevent installation of devices that match these device IDs
This policy setting specifies a list of Plug and Play hardware IDs and compatible IDs for devices that users cannot install. If you enable this policy setting, users cannot install or update the driver for a device if its hardware ID or compatible ID matches one in this list. If you disable or do not configure this policy setting, users can install devices and update their drivers, as permitted by other policy settings for device installation. Note: This policy setting takes precedence over any other policy settings that allow users to install a device. This policy setting prevents users from installing a device even if it matches another policy setting that would allow installation of that device.

upvoted 1 times

Moderator 6 months ago

Selected Answer: A

It does fulfill it's purpose, although it's a bit extreme to do it this way.

upvoted 2 times

PChi 6 months, 1 week ago

The GPO that the provided solution is referring to:
https://docs.microsoft.com/en-us/windows/client-management/manage-device-installation-with-group-policy
VS
The correct resolve:
https://docs.microsoft.com/en-us/windows/deployment/update/waas-wu-settings

upvoted 2 times

AL99 6 months, 2 weeks ago

Answer A:Yes

upvoted 1 times

PiPe 8 months ago

Selected Answer: B

"Prevent installation of devices using drivers that match these device setup classes" is different from "Prevent installation of devices that match any of these device IDs".
The first only accepts ClassGUIDs (f.e. ALL graphics cards), while the latter only accepts DeviceGUIDs (f.e. specific graphics card). Dropping a device GUID in the GPO for device setup classes will not work imho. So the answer is no for me.
https://admx.help/?Category=Windows_10_2016&Policy=Microsoft.Policies.DeviceInstallation::DeviceInstall_Classes_Deny

https://admx.help/?Category=Windows_10_2016&Policy=Microsoft.Policies.DeviceInstallation::DeviceInstall_IDs_Deny

https://docs.microsoft.com/en-us/windows-hardware/drivers/install/system-defined-device-setup-classes-available-to-vendors

upvoted 7 times

Santeria 8 months, 1 week ago

Selected Answer: A

If you specify the GUID, it's correct!

upvoted 1 times

tf444 1 year ago

The answer is YES!
This policy setting allows you to specify a list of device setup class globally unique identifiers (GUIDs) for device drivers that Windows is prevented from installing. This policy setting takes precedence over any other policy setting that allows Windows to install a device.

If you enable this policy setting, Windows is prevented from installing or updating device drivers whose device setup class GUIDs appear in the list you create. If you enable this policy setting on a remote desktop server, the policy setting affects redirection of the specified devices from a remote desktop client to the remote desktop server.

If you disable or do not configure this policy setting, Windows can install and update devices as allowed or prevented by other policy settings.

upvoted 2 times

auton 11 months, 2 weeks ago

You are correct, but the question is only asking for Windows update. What if we want to install drivers through a OEM installer?

The question is a bit flawed. If we're asking only for Windows update to be excluded from driver installations, then the answer is NO.

upvoted 2 times

badguytoo 1 year, 1 month ago

This should A. Checked from the MS doc: This policy setting allows you to specify a list of device setup class globally unique identifiers (GUIDs) for driver packages that Windows is prevented from installing. By default, this policy setting takes precedence over any other policy setting that allows Windows to install a device.

upvoted 1 times

Sironin 1 year, 2 months ago

Yes this obviously meets the goal. It is also the only way to specifically limit installation of specific types of drivers (such as video drivers) vs just setting windows update to not update any drivers (which would also meet the goal, but not update any other drivers). This is an important distinction in that one might want windows update to update other drivers. This is the only way to do that.

upvoted 1 times

Mujja 1 year, 3 months ago

The device is already installed, configuring device installation restrictions won't make a difference. We need to stop driver updates from Windows Update.

upvoted 2 times

Perycles 1 year, 4 months ago

Yes, no, yes, no, ...blablabla... Read the question : "BY USING Windows Udapte" : implied we have to installed it manually or by another method to hav more control. By using this GPO, we will block all methods and can never install drivers . Here, we want to keep control on video drivers by disabling windows Update , not to block installations. Sio for me answer IS NO.

upvoted 7 times

Tomtom11 1 year, 4 months ago

If you enable this policy setting, Windows is allowed to install or update device drivers whose device setup class GUIDs appear in the list you create

upvoted 3 times

Question #17 *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.

Your company uses Windows Update for Business.

The research department has several computers that have specialized hardware and software installed.

You need to prevent the video drivers from being updated automatically by using Windows Update.

Solution: From the Settings app, you clear the Give me updates for other Microsoft products when I update Windows check box.

Does this meet the goal?

A. Yes

B. No

Correct Answer: *B*

Reference:

https://www.stigviewer.com/stig/microsoft_windows_server_2012_member_server/2013-07-25/finding/WN12-CC-000024

Perycles Highly Voted 1 year, 4 months ago

Drivers are not part as "Microsoft Other Product" but included inside quality update, so uncheck this option has no effect. Answer is NO.

upvoted 9 times

daye Most Recent 1 week, 3 days ago

Currently you can select it when you are creating a profile within Intune so I guess this one is getting old

upvoted 1 times

daye 1 week, 3 days ago

nevermind I was thinking in a WUFB GPO rather than a W10 setting

upvoted 1 times

MR_Eliot 5 months ago

Selected Answer: B

It's B

upvoted 2 times

mclovin 1 year, 1 month ago

duh! ofc it's NO

upvoted 3 times

dinjo 2 years, 6 months ago

b - correct

upvoted 4 times

Question #18 *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.
Your company uses Windows Update for Business.
The research department has several computers that have specialized hardware and software installed.
You need to prevent the video drivers from being updated automatically by using Windows Update.
Solution: From the Device Installation settings in a Group Policy object (GPO), you enable Specify search order for device driver source locations, and then you select Do not search Windows Update.
Does this meet the goal?

A. Yes

B. No

Correct Answer: *A*
Device driver searches using Windows Update must be prevented.
Configure the policy value for Computer Configuration -> Administrative Templates -> System -> Device Installation -> "Specify search order for device driver source locations" to "Enabled: Do not search Windows Update".
Reference:
https://www.stigviewer.com/stig/microsoft_windows_server_2012_member_server/2013-07-25/finding/WN12-CC-000024

riel_gesh Highly Voted 2 years, 7 months ago
Answer is A.
You can open create the GPO as follow:
Configure the policy value for Computer Configuration -> Administrative Templates -> System -> Device Installation -> "Specify search order for device driver source locations" to "Enabled: Do not search Windows Update".
upvoted 20 times

muzzag Highly Voted 2 years, 7 months ago
Shouldn't this be B (False) This setting relates to manually updating and where to search for updates.

There is separate GPO to control whether to automatically update drivers during windows Update. "Do Not include drivers in Windows Updates" ... Enable this policy to not include drivers with Windows quality updates.

If you disable or do not configure this policy, Windows Update will include updates that have a Driver classification.
upvoted 11 times

MR_Eliot Most Recent 5 months ago
Selected Answer: A
A = correct
upvoted 1 times

Moderator 6 months ago
Selected Answer: A
And again, a bit overdone but it does do it's job:
https://gpsearch.azurewebsites.net/#183
upvoted 2 times

franto 7 months, 3 weeks ago
This policy setting allows you to specify the order in which Windows searches source locations for device drivers.
If you enable this policy setting, you can select whether Windows searches for drivers on Windows Update unconditionally, only if necessary, or not at all.
Answer is A.
upvoted 1 times

Perycles 1 year, 4 months ago
this GPO is only for NEW device , when is detected for the first time. Windows tries to install it by using local Drivers and then Windows Update Drivers. This GPo doesn't prevent windows updates (included Drivers) to be downloaded and installed. so answer is B.
upvoted 4 times

AnoniMouse 1 year, 4 months ago
I was about to say NO, but apparently there are two different methods to block device driver installation via GPO. I have just checked and they give the same results

Option 1:
Computer Configuration > Administrative Templates > Windows Components > Windows Update. On the right side, double-click the [Do not include drivers with Windows Update], select ENABLED

Option 2:
Computer Configuration > Administrative Templates > System > Device Installation. On the right side, double click [Specify search order for device driver source locations], select ENABLED and select [Do not search Windows Update]

Hence answer A is correct
upvoted 8 times

RodrigoT 6 months, 3 weeks ago

Apparently it works.

upvoted 2 times

GohanF2 1 year, 5 months ago

the answer to this question will be "no" due that we are cutting the tree of the windows updates . if we want to just cut the drivers updates then the solution must be like: Computer Configuration > Administrative Templates > Windows Components > Windows Update and select : do not include drivers with windows updates

upvoted 1 times

Merma 1 year, 5 months ago

A. Yes is correct.
To disable automatic searching of Windows Update by using Group Policy
Open Group Policy Management Editor.
In the navigation pane, open Computer Configuration\Administrative Templates\System\Internet Communication Management\Internet Communication settings.
In the details pane, double-click Turn off Windows Update device driver searching.
To turn off searching Windows Update, click Enabled
Click OK to save your settings.
https://support.displaylink.com/knowledgebase/articles/543895-how-to-prevent-windows-checking-or-upgrading-from#:~:text=In%20the%20navigation%20pane%2C%20open,Windows%20Update%20device%20driver%20searching.

upvoted 1 times

slaoui 1 year, 5 months ago

Another ambiguous question!
If you select do not search windows update for device drivers, you're not getting ANY device drivers from Windows Update.
The question asks you need to prevent video drivers (not all drivers)
Does it meet the goal? Yes but, you're cutting out all other device drivers.
The answer should be A if we are asked if the action meets the goal.
The answer should be B if the question was worded "prevent ONLY video drivers"

upvoted 4 times

TrustMebro 9 months, 2 weeks ago

I think you are thinking too much. All they ask if it meets the goal. So does the GPO prevent the video drivers, the answer is it does. the answer on this question is A.Yes. Please do not add complicated things outside of the question, you are making the other learners too complicated.

upvoted 1 times

Balena 1 year, 7 months ago

Its YES, but not only for those video drivers but for all drivers.
So yes, you cut the tree but in fact you cut the whole forest. Did you cut the tree? Yes.
These kind of questions go along with a new style of mind set. New generation...

upvoted 3 times

lucidgreen 1 year, 7 months ago

This is exactly what the question is looking for: How to keep getting driver updates from Windows Update.

upvoted 1 times

vinnyct 1 year, 10 months ago

it's A

http://woshub.com/how-to-turn-off-automatic-driver-updates-in-windows-10/

upvoted 5 times

hawkens 1 year, 10 months ago

The most logical answer (we also use this option in our Citrix environments, because we do not want the XenServer drivers to be updatet) is from muzzag if you aks me.

upvoted 2 times

Question #19 *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 need to ensure that feature and quality updates install automatically during a maintenance window.
Solution: In Group policy, from the Windows Update settings, you enable Configure Automatic Updates, select 3 `" Auto download and notify for Install, and then enter a time.
Does this meet the goal?

A. Yes

B. No

Correct Answer: *B*
Instead: In Group policy, from the Windows Update settings, you enable Configure Automatic Updates, select 4-Auto download and schedule the install, and then enter a time.
Reference:
https://docs.microsoft.com/en-us/sccm/sum/deploy-use/automatically-deploy-software-updates

Perycles Highly Voted 1 year, 4 months ago
B seems to be correct : "NOTIFY FOR Install" doesn't match with the question "Automatically installed".
upvoted 7 times

franto Most Recent 7 months, 3 weeks ago
3 = (Default setting) Download the updates automatically and notify when they are ready to be installed
Windows finds updates that apply to the computer and downloads them in the background (the user is not notified or interrupted during this process). When the downloads are complete, users will be notified that they are ready to install. After going to Windows Update, users can install them.
B is the correct answer.
upvoted 2 times

Question #20 *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 have 20 computers that run Windows 10 and are joined to Microsoft Azure Active Directory (Azure AD).
You plan to replace the computers with new computers that run Windows 10. The new computers will be joined to Azure AD.
You need to ensure that the desktop background, the favorites, and the browsing history are available on the new computers.
Solution: You configure Enterprise State Roaming.
Does this meet the goal?

A. Yes

B. No

Correct Answer: *A*
Enterprise State Roaming provides users with a unified experience across their Windows devices and reduces the time needed for configuring a new device.
Reference:
https://docs.microsoft.com/en-us/azure/active-directory/devices/enterprise-state-roaming-enable

MidCities Highly Voted 2 years, 11 months ago
Retract the above. Yes, the answer should be A.
upvoted 14 times

GrayRant27 Most Recent 3 weeks, 2 days ago
Correct answer A!
upvoted 1 times

MitchF 2 months, 2 weeks ago
https://docs.microsoft.com/en-us/managed-desktop/get-started/enterprise-state-roaming

In the above source, they wrote: "Enterprise State Roaming lets users securely synchronize user and application settings data to the cloud...For example, if you replace one of their Microsoft Managed Desktop devices with a new device, it will look and behave exactly the same as the last one."

This is the answer to our question, so answer is A) Yes
upvoted 1 times

Hulisanimellla 6 months, 2 weeks ago
Selected Answer: A
AGREE ON A
upvoted 1 times

mikl 9 months, 2 weeks ago
Agree on A.
upvoted 1 times

Perycles 1 year, 4 months ago
Agree for A.
upvoted 2 times

Merma 1 year, 4 months ago
"The following settings groups are available for end users to enable/disable settings sync on Windows 10 devices.
Theme: desktop background, user tile, taskbar position, etc.
Internet Explorer Settings: browsing history, typed URLs, favorites, etc.
Passwords: Windows credential manager, including Wi-Fi profiles
Language Preferences: spelling dictionary, system language settings
Ease of Access: narrator, on-screen keyboard, magnifier
Other Windows Settings: see Windows Settings details
Microsoft Edge browser setting: Microsoft Edge favorites, reading list, and other settings."
https://docs.microsoft.com/en-us/azure/active-directory/devices/enterprise-state-roaming-windows-settings-reference
upvoted 3 times

dinjo 2 years, 6 months ago
yep its a
upvoted 3 times

riel_gesh 2 years, 7 months ago
Yeap, it is A. You can configure Enterprise state roaming GPO settings to get all the computers to sync the desire settings
upvoted 3 times

MidCities 2 years, 11 months ago
I disagree with A as the answer, I think it should be B.
Enterprise State Roaming (ESR) is to allow the user to have the same settings on multiple devices.

"Enterprise state roaming allows to sync user settings and application settings securely across corporate azure domain joined devices. "
http://www.rebeladmin.com/2017/12/step-step-guide-enable-enterprise-state-roaming-azure-active-directory/

upvoted 1 times

Mujja 1 year, 3 months ago

https://docs.microsoft.com/en-us/azure/active-directory/devices/enterprise-state-roaming-faqs#what-data-roams-

Correct answer is A

upvoted 2 times

RodrigoT 6 months ago

Your link is outdated. Try:
https://docs.microsoft.com/en-us/azure/active-directory/devices/enterprise-state-roaming-windows-settings-reference
https://docs.microsoft.com/en-us/azure/active-directory/devices/enterprise-state-roaming-group-policy-settings

upvoted 1 times

Question #21 *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 have 20 computers that run Windows 10 and are joined to Microsoft Azure Active Directory (Azure AD).
You plan to replace the computers with new computers that run Windows 10. The new computers will be joined to Azure AD.
You need to ensure that the desktop background, the favorites, and the browsing history are available on the new computers.
Solution: You configure roaming user profiles.
Does this meet the goal?

A. Yes

B. No

Correct Answer: *B*
Instead: Enterprise State Roaming provides users with a unified experience across their Windows devices and reduces the time needed for configuring a new device.
Reference:
https://docs.microsoft.com/en-us/azure/active-directory/devices/enterprise-state-roaming-enable

Cornflakez Highly Voted 2 years ago
Correct answer is B.
Answer would be A if it was about enabling "Enterprise State Roaming" which is an Azure AD feature.
"Roaming user profiles" requires onprem AD
upvoted 27 times

mikl 9 months, 2 weeks ago
Agree.
upvoted 1 times

MikeMatt2020 Highly Voted 1 year, 5 months ago
Roaming Profiles is a feature in an on-premise AD-DS environment. Enterprise State Roaming is the similar solution targeted at AAD-based environments.
upvoted 8 times

GrayRant27 Most Recent 3 weeks, 2 days ago
Answer B:
Roaming User Profiles redirects user profiles to a file share so that users receive the same operating system and application settings on multiple computers.
upvoted 1 times

pamirsiu 2 years, 5 months ago
Would it not be A, because https://docs.microsoft.com/en-us/azure/active-directory/devices/enterprise-state-roaming-windows-settings-reference speaks of AAD and https://docs.microsoft.com/en-us/azure/active-directory-domain-services/compare-identity-solutions lists 'roaming of user settings across devices'?
upvoted 1 times

hbabera 2 years, 6 months ago
Roaming profile needs machines to be joined to ADDS, in this case machines are just joined to Azure AD so it's B
upvoted 6 times

Balena 1 year, 7 months ago
Not so. Have a look into the properties of a local user on a workgroup computer. There is a "profile" tab where you can type the profile path. Any shared folder, even on a NAS is ok.
Concerning this question, there is no local user account to make the setting since the accounts are in AZAD. So, no.
upvoted 2 times

riel_gesh 2 years, 7 months ago
I lean toward B. Roaming profiles do not retain desktop background, favorites or browsing history.
upvoted 4 times

Davidf 2 years, 10 months ago
Is B, no local share to save the profiles too (and even if you do, not easy to set permissions for Azure AD users on it)
upvoted 1 times

nolancl 3 years ago
Should be A, source listed states "Roaming User Profiles redirects user profiles to a file share so that users receive the same operating system and application settings on multiple computers." OS and application settings would include the objectives stated.
upvoted 1 times

nickw 2 years, 12 months ago
I'm leaning towards B, there is no suggestion that there's a local server to store the roaming profiles in.
upvoted 2 times

Question #22 *Topic 2*

You have a Microsoft Azure subscription that contains an Azure Log Analytics workspace.
You deploy a new computer named Computer1 that runs Windows 10. Computer1 is in a workgroup.
You need to ensure that you can use Log Analytics to query events from Computer1.
What should you do on Computer1?

A. Configure the commercial ID

B. Join Azure Active Directory (Azure AD)

C. Create an event subscription

D. Install the Microsoft Monitoring Agent

Correct Answer: *D*
Verify agent connectivity to Azure Monitor.
From the computer in Control Panel, find the item Microsoft Monitoring Agent. Select it and on the Azure Log Analytics tab, the agent should display a message stating: The Microsoft Monitoring Agent has successfully connected to the Microsoft Operations Management Suite service.
Reference:
https://docs.microsoft.com/en-us/azure/azure-monitor/platform/agent-windows

Mike_Row Highly Voted 2 years, 6 months ago
My first choise was answer A, but after reading:

https://docs.microsoft.com/en-us/azure/azure-monitor/platform/agent-windows

The answer is D
upvoted 25 times

RodrigoT 5 months, 1 week ago
And this question appeared on Page 1 Question #10. Same answer, install MMA.
upvoted 1 times

RodrigoT 5 months, 1 week ago
Commercial ID is to monitor Windows Updates with Update Compliance. Another story.
upvoted 4 times

riel_gesh Highly Voted 2 years, 7 months ago
I think it should be B because the machine is in Workgroup. So, even if you install Microsoft Monitoring Agent (MMA) you would need to configure the machine to grants access to a remote service.
upvoted 7 times

N0peasaurus Most Recent 2 months, 4 weeks ago
D:
D
https://docs.microsoft.com/en-us/azure/azure-monitor/agents/log-analytics-agent
upvoted 1 times

MR_Eliot 5 months ago
Selected Answer: D
D = Correct
upvoted 1 times

Perycles 1 year, 4 months ago
Log analytics Agent only work on VM (cloud or local) . for me computer needs to join Azure Ad . answer B.
upvoted 5 times

RodrigoT 6 months, 3 weeks ago
Wrong. Read the article again, paragraph 3, first line:

https://docs.microsoft.com/en-us/azure/azure-monitor/agents/log-analytics-agent
upvoted 2 times

RodrigoT 5 months, 1 week ago
Paragraph 2, I mean.
upvoted 2 times

Balena 1 year, 7 months ago
From Loga Analytics Workspace, you download the appropiate Agent that must be installed. While installing the Agent, you must paste the Workspace ID and Primary key you copy from the same place.
So = D.
upvoted 5 times

aronutics 2 years, 1 month ago
Just to add - Not for making query
upvoted 1 times

aronutics 2 years, 1 month ago

it is Install the Microsoft Monitoring Agent, you need commercial ID to enrol computer in windows analytics

upvoted 6 times

AnoniMouse 1 year, 4 months ago

No, it isn't a commercial ID that you need. You need a Workspace ID and Workspace Key
https://docs.microsoft.com/en-us/azure/azure-monitor/agents/agent-windows#install-agent-using-setup-wizard

upvoted 3 times

Question #23 *Topic 2*

You plan to deploy Windows 10 Pro to 200 new computers by using the Microsoft Deployment Toolkit (MDT) and Windows Deployment Services (WDS).
The company has a Volume Licensing Agreement and uses a product key to activate Windows 10.
You need to ensure that the new computers will be configured to have the correct product key during the installation.
What should you configure?

A. a WDS boot image

B. an MDT task sequence

C. the Device settings in Azure AD

D. a Windows AutoPilot deployment profile

Correct Answer: *B*
Create the deployment task sequence.
The task sequence used to deploy your production Windows 10 reference image. You will then configure the task sequence to enable patching via a Windows
Server Update Services (WSUS) server.
This includes: Specify Product Key: Do not specify a product key at this time
Reference:
https://docs.microsoft.com/en-us/windows/deployment/deploy-windows-mdt/deploy-a-windows-10-image-using-mdt#a-href-idsec08astep-8-deploy-the-windows-
10-client-image

MR_Eliot 5 months ago

Selected Answer: B

B is indeed correct.

upvoted 1 times

Question #24 *Topic 2*

Your network contains an Active Directory domain that is synced to Microsoft Azure Active Directory (Azure AD). The domain contains 500 laptops that run
Windows 8.1 Professional. The users of the laptops work from home.
Your company uses Microsoft Intune, the Microsoft Deployment Toolkit (MDT), and Windows Configuration Designer to manage client computers.
The company purchases 500 licenses for Windows 10 Enterprise.
You verify that the hardware and applications on the laptops are compatible with Windows 10.
The users will bring their laptop to the office, where the IT department will deploy Windows 10 to the laptops while the users wait.
You need to recommend a deployment method for the laptops that will retain their installed applications. The solution must minimize how long it takes to perform the deployment.
What should you include in the recommendation?

A. an in-place upgrade

B. a clean installation by using a Windows Configuration Designer provisioning package

C. Windows AutoPilot

D. a clean installation and the User State Migration Tool (USMT)

Correct Answer: *A*
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. This requires the least IT effort, because there is no need for any complex deployment infrastructure.
Reference:
https://docs.microsoft.com/en-us/windows/deployment/windows-10-deployment-scenarios#in-place-upgrade

riel_gesh Highly Voted 2 years, 7 months ago
A is correct. Existing applications are preserved through the process while a clean install using USMT will only retain user settings/profile
upvoted 16 times

tf444 1 year ago
not true, with i: migApp you can keep user application.
upvoted 1 times

LauLauLauw Highly Voted 2 years, 6 months ago
A is correct indeed.
With Intune you can do an Edition Uprade from for example Pro to Enterprise but that is for Windows 10 and later.
A new Install removes the Apps so A i the only answer that remains possible.
upvoted 9 times

MR_Eliot Most Recent 5 months ago
Selected Answer: A
A is the fastest and easiest way to upgrade from Windows 8.1 to Windows 10.
upvoted 2 times

b3arb0yb1m 9 months, 2 weeks ago
A. an in-place upgrade
upvoted 1 times

Mujja 1 year, 3 months ago
https://docs.microsoft.com/en-us/windows/deployment/deploy-windows-mdt/upgrade-to-windows-10-with-the-microsoft-deployment-toolkit#create-a-task-sequence-to-upgrade-to-windows10-enterprise

Use MDT for an in-place upgrade, add the product key to change the W10 edition to Enterprise
upvoted 1 times

MikeMatt2020 1 year, 5 months ago
It seems that A might be correct...But wouldn't an in-place upgrade from 8.1Professional bump up the OS to Windows 10 Pro? Did the company just waste 500 Enterprise licenses then? Confused.
upvoted 2 times

Perycles 1 year, 4 months ago
Windows 10 pro could be updated to Win 10 ENT after the inplaceUpgrade (with intune for example).
upvoted 1 times

letters1234 7 months, 2 weeks ago
"minimize how long it takes to perform the deployment." The deployment time would be minimized and as Merma mentioned, it can be upgraded later with InTune.
upvoted 1 times

Merma 1 year, 4 months ago
You can upgrade from WIndows 8.1 Pro to Windows 10 Enterprise.
https://docs.microsoft.com/en-us/windows/deployment/upgrade/windows-10-upgrade-paths

upvoted 3 times

Question #25 *Topic 2*

You have a computer named Computer5 that has Windows 10 installed.

You create a Windows PowerShell script named config.ps1.

You need to ensure that config.ps1 runs after feature updates are installed on Computer5.

Which file should you modify on Computer5?

A. Unattend.xml

B. Unattend.bat

C. SetupConfig.ini

D. LiteTouch.wsf

Correct Answer: *C*

You can run a post script after a Windows 10 feature upgrade with SetupConfig.ini

Reference:

https://www.joseespitia.com/2017/06/01/how-to-run-a-post-script-after-a-windows-10-feature-upgrade/

riel_gesh Highly Voted 2 years, 7 months ago

IT pros can use the setupconfig file to add parameters to Windows Setup from Windows Update and Windows Server Update Services. If the update is delivered through Windows Update, Windows Setup searches in a default location for a setupconfig file. You can include the setupconfig file here:

"%systemdrive%\Users\Default\AppData\Local\Microsoft\Windows\WSUS\SetupConfig.ini"
https://docs.microsoft.com/en-us/windows-hardware/manufacture/desktop/windows-setup-automation-overview

upvoted 25 times

Perycles Highly Voted 1 year, 4 months ago

Answer is correct.

upvoted 7 times

MR_Eliot Most Recent 5 months ago

Selected Answer: C

C => Correct!

upvoted 1 times

b3arb0yb1m 9 months, 2 weeks ago

C. SetupConfig.ini

upvoted 2 times

HOTSPOT -

You use Microsoft Intune to manage Windows updates.

You have computers that run Windows 10. The computers are in a workgroup and are enrolled in Intune. The computers are configured as shown in the following table.

Name	Tag	Member of
Computer1	None	Group1
Computer2	Tag2	Group2
Computer3	Tag3	Group3

On each computer, the Select when Quality Updates are received Group Policy setting is configured as shown in the following table.

Name	State	Configuration
Computer1	Not configured	*Not applicable*
Computer2	Enabled	Deferral period of 5 days
Computer3	Disabled	*Not applicable*

You have Windows 10 update rings in Intune as shown in the following table.

Name	Quality update deferral period (days)	Scope (Tags)	Assignment
Ring1	2	Tag1	Group1
Ring2	7	Tag2	Group2
Ring3	14	Tag2	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
On Computer1, quality updates will be deferred for two days.	○	○
On Computer2, quality updates will be deferred for seven days.	○	○
On Computer3, qulity updates will be deferred for 14 days.	○	○

Correct Answer:

Answer Area

Statements	Yes	No
On Computer1, quality updates will be deferred for two days.	○	○
On Computer2, quality updates will be deferred for seven days.	○	○
On Computer3, qulity updates will be deferred for 14 days.	○	○

Reference:

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

Wilf32 Highly Voted 1 year, 5 months ago

I think the answer is YES, NO, YES

Computer1 = Group1 + GPO NOT configured = update ring is applied = 2 days = YES
Computer2 = Group2 + GPO IS configured = update ring NOT applied = 5 days = NO
Computer3 = Group3 + GPO disabled = update ring is applied = 14 days = YES

As i understand it GPO takes precedence over update rings.

upvoted 54 times

IrvSus 1 year, 4 months ago

this question feels like a trick because they say workgroup and then reference GPO - so do they mean Local GPO then, and I can't seem to find anything on CSP vs Local GPO (I would think CSP would win over local GPO)

upvoted 3 times

Wilf32 1 year, 4 months ago

The setting for local GPO is here

Computer Configuration > Administrative Templates > Windows Components > Windows Update > Windows Update for Business > Select when Quility Updates are received.

See this link https://docs.microsoft.com/en-us/windows/deployment/update/waas-configure-wufb

Also GPO settings always win unless "MDMWinsOverGP" is enabled - this is referenced in a similar question

https://docs.microsoft.com/en-us/windows/client-management/mdm/policy-csp-controlpolicyconflict
upvoted 4 times

letters1234 7 months, 2 weeks ago
"Also GPO settings always win unless "MDMWinsOverGP" is enabled - this is referenced in a similar question" But isn't referenced in this one, the default setting for MDMWins is for GPO to win.
upvoted 2 times

Slammer900 1 year, 4 months ago
I agree
upvoted 1 times

Layer8 1 year, 4 months ago
but wouldn't the GPO being set to "disabled" override the intune setting then?
upvoted 3 times

RodrigoT 6 months, 3 weeks ago
If you open the Local Group Policy Editor > Select when Quality Updates are received, you can read the Description that states: "If you disable or do not configure this policy, Windows Update will not alter its behavior", meaning "Not Configured" and "Disabled" are the same thing in this policy. Keep studying.
upvoted 4 times

Jimbob77 1 year, 4 months ago
YES
NO
YES (From the GPO being referenced for the 'Disabled' setting "If you disable or do not configure this policy, Windows Update will not alter its behavior." So the update Ring setting should apply.)
upvoted 4 times

Perycles Highly Voted 1 year, 4 months ago
after 2 hours Tests, my final answer is YES, NO , YES. easy for computer 1 and 3. For computer 2, intune settings for updates rights are never applied if GPO is active. TAGS have no impact here (used only to easy admin jobs).
upvoted 21 times

RodrigoT 5 months ago
Thank you for really testing.
upvoted 2 times

TonySuccess Most Recent 6 days, 4 hours ago
Feel like it should specify Local GPO, as that is misleading.
upvoted 1 times

coelho4cc 3 months, 2 weeks ago
Computer1 - NO. Not in "Scope (Tags)"
Computer2 - NO. MDM over GPO takes precedence over "Policy CSP - ControlPolicyConflict" for setting to 1, default is 0. As Wilf32 mentioned.
Computer3 - NO. This computer does not have a Tag2.
upvoted 1 times

Gulshan85 3 months, 2 weeks ago
No, Yes, No
The above is the correct answer.
https://docs.microsoft.com/en-us/mem/intune/fundamentals/scope-tags
upvoted 2 times

AVR31 5 months, 1 week ago
Answer should be corrected. It is YES-NO-YES. For reasons very well explained by other users.
upvoted 1 times

Dedutch 2 months ago
I don't think so.

Option 1 - No -

Option 2 - Yes - Devices aren't domain joined so the GPO must be a local GPO. Intune should override locally applied GPOs but not domain pushed GPOs (unless the flag to do such is checked).

Option 3- NO - Scope tags should apply so option 3 the policy applied in intune isn't going to apply to the machine since its not in scope.
upvoted 1 times

Dedutch 2 months ago
No. Scope tag not applied.
upvoted 1 times

Solaris2002 7 months, 1 week ago
Do people read these questions? Global Group Policy doesn't apply here. The devices are in a workgroup but managed by Intune, it says at the top:

The computers are in a workgroup and are enrolled in Intune.

I'm still confused by the given answers however. Intune policies should override local GPO unless I'm missing something.
upvoted 2 times

ChrisThrelfall 7 months, 3 weeks ago

I agree with YES, NO, YES:

Tags are disregarded & GPO Wins over MDM:

Computer 1 - No GPO configured (Bypass) > Update ring applies to Group 1 (2 Days): YES
Computer 2 - GPO Enabled (Ignore MDM) > Deferral period of 5 days applies: NO
Computer 3 - CONFIGURATION GPO disabled > Unknown state of other GPO's, the assumption is that updates are enabled (Bypass GPO) > Update ring applies to Group 3 (14 Days): YES

upvoted 2 times

b3arb0yb1m 9 months, 2 weeks ago

Yes
No
Yes

upvoted 1 times

encxorblood 10 months, 2 weeks ago

Answer is correct. GPO in a workgroup? Only intune is the solution and the scope tag ist important.

upvoted 2 times

letters1234 7 months, 2 weeks ago

"Local" Group Policy Object - still accessed by GPedit.msc where it shows both domain and local policies set.

upvoted 1 times

mikl 9 months, 2 weeks ago

I was wondering the exact same - GPO settings cant apply to devices in workgroup.

upvoted 2 times

ANDREVOX 10 months, 4 weeks ago

The Question does not say who wins in case of conflict. Default action is GPO always wins unless specified otherwise.
"In Windows 10, version 1709 or later, when the same policy is configured in GP and MDM, the GP policy wins (GP policy takes precedence over MDM). Since Windows 10, version 1803, a new setting allows you to change the policy conflict winner to MDM."

GPO's as follows:
Computer 1 - No GPO configured - (MDM will apply because there is no conflict) = YES
Computer 2 - GPO Enabled - (MDM will not apply because there is a conflict) = NO
Computer 3 - GPO Disable - (MDM will apply because there is no conflict) = YES

upvoted 2 times

AnoniMouse 1 year, 4 months ago

The answer provided is correct NO, YES, NO

Computer1 is in Group1. The Intune policy Ring1 applies to Group1 if the device has Tag1, which Computer1 doesn't, so this policy doesn't apply, neither the other policies because they are set to other groups which Computer1 isn't member of. So here the local GPO wins which is set to Not Configured. So the answer is NO

Computer2 is in Group2. The Intune policy Ring2 applies to Group2 if the device has Tag2, which Computer2 does have, so this policy applies. No other policy is applied. Computer2 has a local GPO to set the deferral, but this will get override by the Intune CSP which says 7 days. So the answer is YES

Computer3 is in Group3. The Intune policy Ring3 applies to Group3 if the device has Tag2, but Computer3 has Tag3 so this policy doesn't apply neither does other policies. Computer3 has a local GPO which disables the configuration of deferrals, which reverts to default, i.e, none. So the answer is NO

upvoted 12 times

camino 7 months, 2 weeks ago

Tags are just for RBAC and have nothing to do with assigning a policies

upvoted 3 times

[Removed] 6 months, 3 weeks ago

Correct: https://docs.microsoft.com/en-us/mem/intune/fundamentals/scope-tags

upvoted 2 times

ceskil 5 months, 3 weeks ago

Base on Ans 1 & 3, both not applicable as one not exist and one disabled, hence GPO doesn't apply and Intune Ring is bypassed. But in Ans 2, GPO enable and 5 days are applied and no other policy should apply, hence should be 5 days and Ans should be No too, but you applied Intune Ring 7 days as override, which make no sense.

upvoted 1 times

RomeIndian 1 year, 4 months ago

Computer1 = Group1 + GPO NOT configured = update ring is applied = 2 days = so since local GPO is not configured the intune policies should take affect and in that case it is -> YES
Computer2 = Group2 + GPO IS configured hence GPO will win because "MDMWinsOverGP" is not mentioned and it is off by default = 5 days -> NO
Computer3 = Group3 + GPO disabled = update ring is applied = 14 days = YES

upvoted 3 times

RomeIndian 1 year, 4 months ago

Computer1 = Group1 + GPO NOT configured = update ring is applied = 2 days = so since local GPO is not configured the intune policies should take affect and in that case it is -> YES
Computer2 = Group2 + GPO IS configured hence GPO will win because "MDMWinsOverGP" is not mentioned and it is off by default = 5 days -> NO
Computer3 = Group3 + GPO disabled = update ring is applied = 14 days = YES

I think it should be Yes -> NO -> Yes

upvoted 8 times

IrvSus 1 year, 4 months ago

I think the tags are a red herring - they don't control the application of policy, only who can administer those tagged objects.
upvoted 9 times

Mujja 1 year, 3 months ago
Correct, the W10 update profiles can only be assigned to Groups, there is no option to select Tags.
upvoted 2 times

Poncho25 1 year, 4 months ago
Correct, Scope Tags are just used to determine which admin accounts can control which groups. It doesn't have any affect on this particular question.
upvoted 3 times

Moorebid 1 year, 4 months ago
Exactly, it's the usual Microsoft's unnecessary information in an attempt to confuse you.
upvoted 5 times

Question #27 *Topic 2*

Your network contains an Active Directory forest. The forest contains a single domain and three sites named Site1, Site2, and Site3. Each site is associated to two subnets. Site1 contains two subnets named SubnetA and SubnetB.
All the client computers in the forest run Windows 10. Delivery Optimization is enabled.
You have a computer named Computer1 that is in SubnetA.
From which hosts will Computer1 download updates?

A. the computers in Site1 only

B. any computer in the domain

C. the computers in SubnetA only

D. any computer on the network

Correct Answer: *B*
Delivery Optimization limits sharing of content to only the devices that are members of the same Active Directory domain.
Note: How Microsoft uses Delivery Optimization.
At Microsoft, to help ensure that ongoing deployments weren't affecting our network and taking away bandwidth for other services, Microsoft IT used a couple of different bandwidth management strategies. Delivery Optimization, peer-to-peer caching enabled through Group Policy, was piloted and then deployed to all managed devices using Group Policy. Based on recommendations from the Delivery Optimization team, we used the "group" configuration to limit sharing of content to only the devices that are members of the same Active Directory domain. The content is cached for 24 hours. More than 76 percent of content came from peer devices versus the Internet.
Reference:
https://docs.microsoft.com/en-us/windows/deployment/update/waas-delivery-optimization

nolancl Highly Voted 3 years ago
Would assume that since it didn't state that Site 1 separates the two Subnets it has with different NATs that it is NATing for both with the same public address. So answer A would be the best answer as both Subnet A and B would be behind the same NAT.
upvoted 24 times

Layer8 1 year, 4 months ago
it's tough to make this determination based on the information given, but I would agree from a practical standpoint.
upvoted 2 times

distortion 8 months ago
It could also be answer D if all computers in the network are behind the same NAT. The question lacks information about the network. The question cannot be answered without doing assumptions.
upvoted 1 times

MZONDERL Highly Voted 8 months, 3 weeks ago
Selected Answer: C
Download mode option : LAN (1=Default)
This default operating mode for Delivery Optimization enables peer sharing on the same network. The Delivery Optimization cloud service finds other clients that connect to the Internet using the same public IP as the target client. These clients then try to connect to other peers on the same network by using their private subnet IP.

https://docs.microsoft.com/en-us/windows/deployment/update/waas-delivery-optimization-reference
upvoted 9 times

RodrigoT 5 months, 1 week ago
You got it my friend! Same subnet only, by default.
upvoted 3 times

Dedutch 2 months ago
I think yes for this question but thats poor. I have multiple subnets in many of my offices that communicate to the public with the same IP.
upvoted 1 times

Alejack Most Recent 3 months ago
It is D:
https://docs.microsoft.com/en-us/windows/deployment/do/waas-delivery-optimization-reference#download-mode
LAN Mode= Default
This default operating mode for Delivery Optimization enables peer sharing on the same network. The Delivery Optimization cloud service finds other clients that connect to the Internet using the same public IP as the target client. These clients then try to connect to other peers on the same network by using their private subnet IP.
upvoted 1 times

MR_Eliot 5 months ago
Selected Answer: C
C. See MZONDERL's answer. He's right.
https://docs.microsoft.com/en-us/windows/deployment/do/waas-delivery-optimization-reference#download-mode
https://techcommunity.microsoft.com/t5/windows-it-pro-blog/delivery-optimization-scenarios-and-configuration-options/ba-p/280195
upvoted 2 times

b3arb0yb1m 9 months, 2 weeks ago

A. the computers in Site1 only.
upvoted 1 times

Ka1Nn 1 year, 1 month ago
download mode for delivery optimization is not specify so :
LAN (1 – Default) This default operating mode for Delivery Optimization enables peer sharing on the same network. The Delivery Optimization cloud service finds other clients that connect to the Internet using the same public IP as the target client. These clients then try to connect to other peers on the same network by using their private subnet IP.
upvoted 2 times

mikl 9 months, 2 weeks ago
So ; A. the computers in Site1 only ?
upvoted 1 times

forummj 1 year, 2 months ago
https://support.microsoft.com/en-us/windows/windows-update-delivery-optimization-and-privacy-bf86a244-8f26-a3c7-a137-a43bfbe688e8

It's my thinking that because the question only states that Delivery Optimization is enabled, that would leave it in its default state. i.e. PCs on my local network. That would mean it can only download from it's own local subnet.
upvoted 1 times

RM21 1 year, 3 months ago
I think its A. They don't say anything about "Select a method to restrict peer selection" being configured. That's where the subnet restriction is.
upvoted 1 times

Tomtom11 1 year, 3 months ago
https://docs.microsoft.com/en-us/windows/deployment/update/waas-delivery-optimization-reference
upvoted 1 times

Perycles 1 year, 4 months ago
Microsoft official course : "...By default in Windows 10 Enterprise and Education editions, Delivery Optimization allows peer-to-peer sharing only on the organization's own network (specifically, all of the devices must be behind the same NAT). However, you can configure it differently in Group Policy and mobile device management (MDM) solutions such as Microsoft Intune." SO the answer is Correct (BY DEFAULT).
upvoted 3 times

Perycles 1 year, 4 months ago
sorry , answer NOT Correct ...
upvoted 2 times

mikl 9 months, 2 weeks ago
Why not?

Do you know for a fact that SubnetA & B are not behind the same NAT?

Please convince me :)
upvoted 4 times

Dedutch 2 months ago
I feel like thats probably more common for a single site. Kind of a bad question.

I have my wireless devices and wired devices in every office going through the same public IP despite being on different subnets. I can't speak to everyone but I reckon things like that are pretty common?
upvoted 1 times

GohanF2 1 year, 4 months ago
Here is another tricky question from Microsoft. In doesnt actually says that each subnet as a separate public IP to do natting . So , delivery optimization works under the say NAT rule . computers from the same subnet 1 must be able to retrieve this updates unless theres is specific traffic security rules that doesnt allow communications between the subnets " intrazone traffic" so , i stick with what it says and I choose " site 1"
this question appeared in the exam that i took on may first and i went for the subnet A .... because of presuming...
upvoted 1 times

MikeMatt2020 1 year, 5 months ago
I'm going with A but we're making a few assumptions:

- Default operating mode for D.O enables peer sharing for devices connecting to the internet using the same PUBLIC IP
- Assuming that SubnetA and SubnetB have a route configured (for inter-subnet communication), a device in SubnetA should be able to conduct peer-to-peer sharing to a device in SubnetB. If there's no route between A and B, then the answer is C
upvoted 6 times

Tomtom11 1 year, 6 months ago
From the Below the answer is Subnet A. As it does not say which setting in Delivery Optimization is selected so it must be the default mode
upvoted 5 times

mikl 9 months, 2 weeks ago
I agree.
upvoted 1 times

Tomtom11 1 year, 6 months ago
LAN (1 – Default) This default operating mode for Delivery Optimization enables peer sharing on the same network. The Delivery Optimization cloud service finds other clients that connect to the Internet using the same public IP as the target client. These clients then attempts to connect to other peers on the same network by using their private subnet IP.

upvoted 3 times

John555 1 year, 7 months ago

test one two three

upvoted 1 times

Balena 1 year, 7 months ago

A. Between subnet a and subnet b there is routing, not nat-ing. All subnets of site 1 access internet through same nat, same external public IP.

upvoted 3 times

Pointwood 1 year, 7 months ago

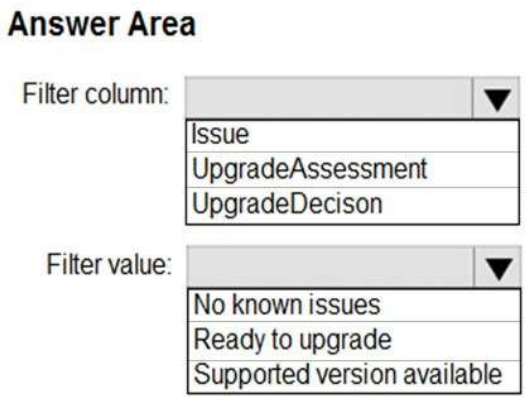
In Windows 10 Enterprise, Professional, and Education editions, Delivery Optimization is enabled by default for peer-to-peer sharing on the local network (NAT).

https://docs.microsoft.com/en-us/windows/deployment/update/waas-delivery-optimization

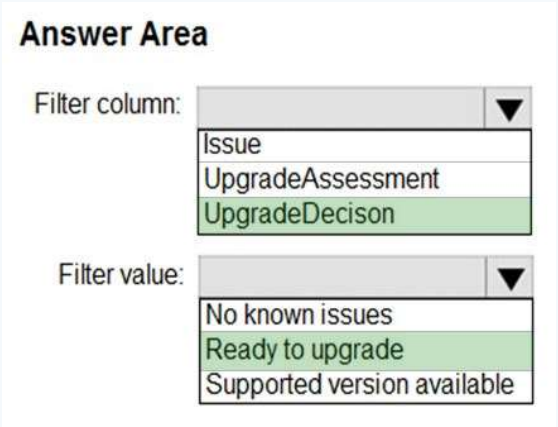
So I think its the Subnet.

upvoted 1 times

HOTSPOT -
Your network contains an Active Directory domain. The domain contains 1,200 computers that run Windows 8.1.
You deploy an Upgrade Readiness solution in Microsoft Azure and configure the computers to report to Upgrade Readiness.
From Upgrade Readiness, you open a table view of the applications.
You need to filter the view to show only applications that can run successfully on Windows 10.
How should you configure the filter in Upgrade Readiness? To answer, select the appropriate options in the answer area.
NOTE: Each correct selection is worth one point.
Hot Area:



Correct Answer:



Box 1: UpgradeDecision -
To approve an asset for upgrade, select the name in the list, and then select one of the following options from the Upgrade decision list:

Review in progress -

Ready -
Ready (with remediation)

Unable -

Not reviewed -

Box 2: Ready to upgrade -
Reference:
https://docs.microsoft.com/en-us/mem/configmgr/desktop-analytics/deploy-prod#

LordCaine Highly Voted 1 year ago
can't believe this is a question, how irrelevant.
upvoted 9 times

Perycles Highly Voted 1 year, 4 months ago
correct answer. Another good link : https://www.anoopcnair.com/windows-10-upgrade-readiness/
upvoted 7 times

RodrigoT Most Recent 6 months, 3 weeks ago
The link provided is broken. It immediately redirects to: https://docs.microsoft.com/en-us/mem/configmgr/desktop-analytics/overview
upvoted 1 times

daye 1 week, 3 days ago

Also it's deprecated
upvoted 1 times

Timmi 1 year, 8 months ago
https://cloudblogs.microsoft.com/industry-blog/en-gb/technetuk/2019/11/14/getting-more-of-what-you-need-from-upgrade-readiness/
upvoted 4 times

HOTSPOT -

You have two computers that run Windows 10. The computers are enrolled in Microsoft Intune as shown in the following table.

Name	Member of
Computer1	Group1
Computer2	Group1, Group2

Windows 10 update rings are defined in Intune as shown in the following table.

Name	Quality deferral (days)	Assigned
Ring1	3	Yes
Ring2	10	Yes

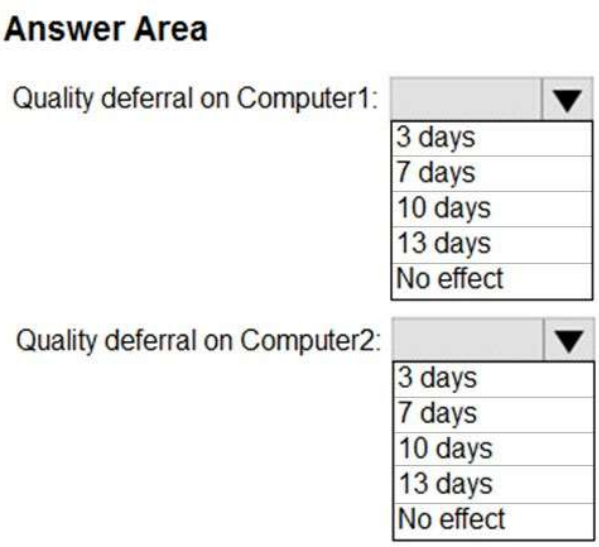
You assign the update rings as shown in the following table.

Name	Include	Exclude
Ring1	Group1	Group2
Ring2	Group2	Group1

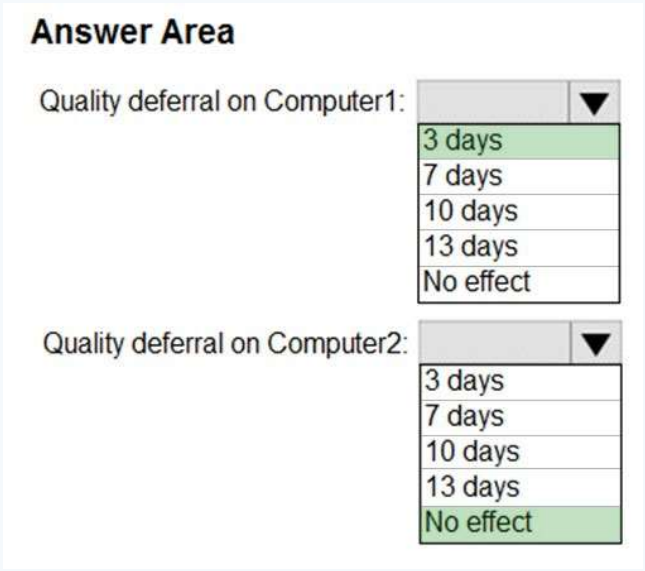
What is the effect of the configurations on Computer1 and Computer2? To answer, select the appropriate options in the answer area.

NOTE: Each correct selection is worth one point.

Hot Area:



Correct Answer:



Box 1: 3 days -

Box 2: No effect -

Since Computer2 is a member of a group that is excluded in both assignments, neither are applied to Computer2. So 'No effect' for Computer2.

Reference:

https://docs.microsoft.com/en-us/mem/intune/configuration/device-profile-assign#exclude-groups-from-a-profile-assignment

LauLauLauw Highly Voted 2 years, 6 months ago

Comp 1 - 3 Days
Comp 2 - No Effect

Policy Applies if you are in Group 1 excluding for members that are in Group 2

And the same for the other ring with Group 2 and Group 1.
So both rings will not apply on Comp 2.

Another way to set this up is to Include All devices and Exclude Group X, same result but maybe gives a better overview on how the include and exclude works.
upvoted 66 times

mikl 9 months, 2 weeks ago
Thanks for clarifying!
upvoted 1 times

RodrigoT 5 months ago
And the justification for the answer provided is absurd. They're saying that Computer2 is a member of Group1, then Ring1 is applied to Group1. Well Computer2 is ALSO a member of Group2. So, why he's not ALSO on Ring2?
I tested this in my tenant. And on the Assignments part there is a link about excluding groups from a profile assignment, and there is nothing there talking about "misleading exclude groups". They're just saying to not mix users and devices groups. The links provided on the answer doesn't help too.
So, I agree with you guys.
upvoted 1 times

nolancl Highly Voted 3 years ago
Computer 2 is No Effect. Both policies exclude the other group and Computer 2 belongs to both so it is excluded by both policies.
upvoted 26 times

Parzival 2 years, 10 months ago
True, Even through the basic group permissions.
upvoted 1 times

steven1 2 years, 7 months ago
That's not how policies work, one always take precedence over the other.
upvoted 2 times

DJM 1 year, 10 months ago
I tested this myself in a lab, this is the correct answer.
upvoted 8 times

Johan99 1 year, 10 months ago
So the the given answer is correct?
upvoted 1 times

DJM 1 year, 10 months ago
No, I meant nolancl's comment is correct, the answer is:

Computer 1: 3 Days
Computer 2: No Effect
upvoted 15 times

Altheus Most Recent 2 days, 12 hours ago
3 Days and no effect.

Exclude always beats include.
upvoted 1 times

moobdoob 8 months, 2 weeks ago
Comp 1 - 3 Days
Comp 2 - No Effect
upvoted 5 times

handsofthelp 10 months, 1 week ago
I Think it is correct. 3 days in both.
Computer 1 is 3 days - Group 1 - Ring 1.
Computer 2 is group 1 and group 2. Ring 2 no have effect but Ring 1 (group 1), yes.
upvoted 1 times

RodrigoT 5 months ago
Following your logic then Computer2 is ALSO a member of Group2. So, why he's not ALSO on Ring2? If Ring1 excludes Group2 so Ring2 excludes Group1.
upvoted 1 times

tf444 11 months, 2 weeks ago
1-Computer 2 is in Group1 and Group2.
2-Ring 2 applies in Group2(include) and Group1(exclude).
3-Exclusion overrides inclusion.
4 Group1 /3 days deferral.
upvoted 2 times

RodrigoT 5 months ago
But Ring1 applies in Group1(include) and Group2(exclude). So, if exclusion overrides inclusion then Computer2 is not in any ring.
upvoted 1 times

Ouianonymous 1 year, 4 months ago
I had this question recently on my exam and the right answer is 3 days -- No effect. For reference, see link; https://docs.microsoft.com/en-us/mem/intune/configuration/device-profile-assign#exclude-groups-from-a-profile-assignment

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

Including user groups and excluding user groups
Including device groups and excluding device group
For example, you assign a device profile to the All corporate users user group, but exclude members in the Senior Management Staff user group. Since both groups are user groups, All corporate users except the Senior Management staff get the profile."

upvoted 6 times

RodrigoT 5 months ago

I agree with you answer, but how do you know that this was right on you exam if they don't say if you answered correctly or not?

upvoted 2 times

MitchF 2 months, 2 weeks ago

1. Where did you find the info you reported in your reference? I don't see anything like it in your reference! Nothing at all!
2. Also, how do you know you got the correct answer on the exam when Microsoft doesn't report it?
Your post does haven't have any facts to support your story.

upvoted 1 times

MitchF 2 months, 2 weeks ago

This is the proper reference you may be talking about:
"Exclusion takes precedence over inclusion in the following same group type..."
https://docs.microsoft.com/en-us/mem/intune/apps/apps-inc-exl-assignments

upvoted 1 times

GohanF2 1 year, 4 months ago

Answer is : Computer 1 - 3 days and COmputer 2 no effecr. Exlcude for groups , apps and objects always takes precedence over include . because the computer belongs to 2 groups and each policy exclude one of them , then there is no effecrt for computer 2

upvoted 4 times

N0peasaurus 2 months, 4 weeks ago

This ^.
I had to look over it several times, to get it and come to the same conclusion.

upvoted 1 times

Koenvld 1 year, 6 months ago

Has this question changed? Seems like it's 1 - No effect 2 - 10 days.
Discussion talks about excluding group 2 twice, but I see group 1 being excluded twice

upvoted 1 times

CvdK 1 year, 10 months ago

3 days and No Effect.
If you click on 'more information about group exclusion' when configuring Ring assignment in Intune, it takes you to https://docs.microsoft.com/en-us/mem/intune/configuration/device-profile-assign#exclude-groups-from-a-profile-assignment
There it states that exclusion takes precedence over inclusion. Since Computer2 is a member of a group that is excluded in both assignments, neither are applied to Computer2. So 'No effect' for Computer2.

upvoted 7 times

Nail 1 year, 11 months ago

3 days, no effect. https://docs.microsoft.com/en-us/mem/intune/apps/apps-inc-exl-assignments Exclude, in my experience, always takes precedence over include.

upvoted 2 times

JackofIT 2 years, 1 month ago

Computer1 and Computer2 are members of Group1. Ring1 is applied to Group1.

The term "Exclude" is misleading. It means that the ring is not applied to that group, rather than that group being blocked.

upvoted 3 times

newark123 2 years, 1 month ago

I cant find anywhere in any documentation about conflict between include and exclude . It says here that being excluded will not block it but the sources it states don't have any info on that ? Very confused on this one .
Anyone got a legit source for this ?

upvoted 1 times

Davood 2 years, 2 months ago

Intune will check Exclude first, then Include. So answer will be 3 and 10.

upvoted 1 times

DJM 1 year, 10 months ago

I tested it, it is 3 days / No Effect

upvoted 3 times

gigimail3332 2 years, 5 months ago

I also believe Computer 2 is No Effect. That is the purpose of the exclusion. Apply updates to a big group then if needed exclude smaller groups or computers from it so they are not affected.

upvoted 3 times

Redders 2 years, 6 months ago

Correction - I agree with nolancl - Computer 2 is No Effect. Both policies exclude the other group and Computer 2 belongs to both so it is excluded by both policies.

upvoted 7 times

Redders 2 years, 6 months ago

Should be 3 and 10 as EXCLUSION takes priority over inclusion. Comp2 would be excluded from Grp1.

https://docs.microsoft.com/en-gb/mem/intune/apps/apps-inc-exl-assignments

(although this is for Application Deployments, I assume the same rule types apply here)

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

For example, if you assign a device group to the All corporate users user group, but exclude members in the Senior Management Staff user group, All corporate users except the Senior Management staff get the assignment, because both groups are user groups.

upvoted 2 times

Question #30 *Topic 2*

Your company standardizes on Windows 10 Enterprise for all users.
Some users purchase their own computer from a retail store. The computers run Windows 10 Pro.
You need to recommend a solution to upgrade the computers to Windows 10 Enterprise, join the computers to Microsoft Azure Active Directory (Azure AD), and install several Microsoft Store apps. The solution must meet the following requirements:
⇨ Ensure that any applications installed by the users are retained.
⇨ Minimize user intervention.
What is the best recommendation to achieve the goal? More than one answer choice may achieve the goal. Select the BEST answer.

A. Microsoft Deployment ToolKit (MDT)

B. Windows Deployment Services (WDS)

C. a Windows Configuration Designer provisioning package

D. Windows AutoPilot

Correct Answer: *C*
You use Windows Configuration Designer to create a provisioning package (.ppkg) that contains customization settings. You can apply the provisioning package to a device running Windows 10.
Incorrect Answers:
A: Microsoft Deployment Toolkit (MDT) allows you to automate the deployment of Windows operating systems in your organization. It is not used to upgrade to
Windows 10 Enterprise.
B: Windows Deployment Services (WDS) is the revised version of Remote Installation Services (RIS). WDS enables the deployment of Windows operating systems. You can use it to set up new computers using network-based installations. It is not used to upgrade to Windows 10 Enterprise.
D: Windows Autopilot is a user-driven mode designed to minimize intervention of the IT administrator.
Reference:
https://docs.microsoft.com/en-us/windows/deployment/upgrade/windows-10-edition-upgrades https://docs.microsoft.com/en-us/windows/configuration/provisioning-packages/provisioning-create-package

h3nk13 Highly Voted 2 years, 7 months ago
MDT can be used to inplace upgrade, but if would be a lot more work. So provisioning package is best.
upvoted 14 times

Mage10 Most Recent 2 weeks ago
Selected Answer: C
C since all users apps will be retained
upvoted 1 times

MR_Eliot 5 months ago
Selected Answer: C
C seems to be right.
upvoted 1 times

b3arb0yb1m 9 months, 2 weeks ago
C. a Windows Configuration Designer provisioning package
upvoted 3 times

justabasicuser 1 year, 2 months ago
"Some users purchase their own computer from a retail store." it sounds like the users do not have access to any enterprise network. PPKGs are designed for remote users to do everything that is required in the question including upgrade using license key
upvoted 2 times

AnoniMouse 1 year, 4 months ago
Hmmmm. I would say MDT because it does have the possibility to do an in-place upgrade of the OS but it will take too much time

Windows Configuration Designer, from Provision Desktop Devices, just on the first TAB [Set up device], there is a filed called ENTER PRODUCY KEY. So here if you enter your Enterprise MAK key or the Enterprise KMS key it should work! So the answer is correct! Windows Configuration Designer
upvoted 2 times

RodrigoT 6 months ago
MDT would not retain applications installed by the users. Answer is C.
upvoted 1 times

Nisaj 1 year, 7 months ago
if this answer is correct, can we use provisioning package to upgrade windows edition?
upvoted 1 times

vinnyct 1 year, 10 months ago
It's C

upvoted 3 times

goyelVishal 2 years, 5 months ago
Why not Autopilot?
upvoted 1 times

Perycles 1 year, 4 months ago
Autopilot (in Reset mode) could be used if we don't want to keep user's applications, because all these will be wiped.this mode reset users Settings, Apss and user's files.
upvoted 3 times

PrimeSki 2 years, 2 months ago
Autopilot on a device would wipe current apps the user wants to retain.
upvoted 11 times

mikl 9 months, 2 weeks ago
Ensure that any applications installed by the users are retained.
upvoted 2 times

Question #31 *Topic 2*

You install a feature update on a computer that runs Windows 10.

How many days do you have to roll back the update?

A. 5

B. 10

C. 14

D. 30

Correct Answer: *B*

Microsoft has changed the time period associated with operating system rollbacks with Windows 10 version 1607, decreasing it to 10 days.

Previously, Windows

10 had a 30-day rollback period.

Reference:

https://redmondmag.com/articles/2016/08/04/microsoft-shortens-windows-10-rollback-period.aspx

vinnyct Highly Voted 1 year, 10 months ago
It's B 10 days

https://howtofixwindows.com/roll-back-windows-10-upgrade-after-10-days-limit/#:~:text=By%20default%20settings%2C%20Windows%2010,in%20the%20first%2010%20days.
upvoted 6 times

Perycles Highly Voted 1 year, 4 months ago
10 by default with the availability to defer to 365 days max by GPO (windows update for business GPo).
upvoted 5 times

mikl Most Recent 9 months, 2 weeks ago
Selected Answer: B
B. 10 is correct.

Previous it was 30 days.
upvoted 4 times

Merma 1 year, 5 months ago
Go back to previous versions of Windows
For a limited time after upgrading to Windows 10, you'll be able to go back to your previous version of Windows by selecting the Start button, then select Settings > Update & Security > Recovery and then selecting Get started under Go back to the previous version of Windows 10. This will keep your personal files, but it'll remove apps and drivers installed after the upgrade, as well as any changes you made to settings. In most cases, you'll have 10 days to go back.
https://support.microsoft.com/en-us/windows/recovery-options-in-windows-10-31ce2444-7de3-818c-d626-e3b5a3024da5
upvoted 1 times

Question #32 *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.
Your company uses Windows Update for Business.
The research department has several computers that have specialized hardware and software installed.
You need to prevent the video drivers from being updated automatically by using Windows Update.
Solution: From the Windows Update settings in a Group Policy object (GPO), you enable Do not include drivers with Windows Updates.
Does this meet the goal?

A. Yes

B. No

Correct Answer: *A*
Do not include drivers with Windows Updates.
Allows admins to exclude Windows Update drivers during updates.
To configure this setting in Group Policy, use Computer Configuration\Administrative Templates\Windows Components\Windows update\Do not include drivers with Windows Updates. Enable this policy to not include drivers with Windows quality updates. If you disable or do not configure this policy, Windows Update will include updates that have a Driver classification.
Reference:
https://docs.microsoft.com/en-us/windows/deployment/update/waas-wu-settings

Santosh4u Highly Voted 2 years, 8 months ago
The link provided says that the answer is incorrect. This is the right link which shows the answer is correct:
https://docs.microsoft.com/en-us/windows/deployment/update/waas-configure-wufb#exclude-drivers-from-quality-updates
upvoted 17 times

espenm 2 years ago
Another similar question had this as the correct answer:
Device installation settings in GPO, enable specify search order, Do not search Windows update
upvoted 4 times

ExamStudy101 1 year, 2 months ago
Remember: Some question sets might have more than one correct solution, while others might not have a correct solution.
upvoted 1 times

morito Most Recent 7 months, 3 weeks ago
Selected Answer: A
Whilst this method is quite extreme, it does fulfill its purpose.
upvoted 4 times

lykeP 8 months, 2 weeks ago
Selected Answer: B
The Correct Answer is B.
If you enable this option "From the Windows Update settings in a Group Policy object (GPO), you enable Do not include drivers with Windows Updates.", this will stop all other drivers from installing.
upvoted 3 times

manwithplan 8 months, 1 week ago
The thing is, it doesn't matter if it stops all other drivers. That's not the question. The question is, will this excluse video drivers. And if that is the question, yes is the answer. Obviously not the best practice but it does do what it asks.
upvoted 13 times

TonySuccess 3 weeks, 2 days ago
Exactly, forget all logic. This is an MS Exam and they love to f with your head.
upvoted 2 times

mikl 9 months, 2 weeks ago
I would say A is correct.

https://docs.microsoft.com/en-us/windows/deployment/update/waas-wu-settings#do-not-include-drivers-with-windows-updates
upvoted 1 times

tf444 11 months, 2 weeks ago
Yes, enabling the policy result:
Enable this policy to not include drivers with Windows quality updates.
upvoted 1 times

tf444 1 year ago
Lol, the reference link is so unrelated to the question.
upvoted 1 times

Sironin 1 year, 2 months ago

While this does meet the goal, it also prevents other driver updates through windows update. GPO settings for restricting driver installation/update to specific GUIDs can be much more granular/permissive. See this for much more information: https://docs.microsoft.com/en-us/windows/client-management/manage-device-installation-with-group-policy

upvoted 1 times

ExamStudy101 1 year, 2 months ago

The question is just asking if it meets the goal. Not if it's the best practice

upvoted 1 times

Perycles 1 year, 4 months ago

Comparing with other previous questions for this scenario, this is the best answer. SO answer is correct.

upvoted 3 times

ExamStudy101 1 year, 2 months ago

"Some question sets might have more than one correct solution, while others might not have a correct solution."

upvoted 1 times

GohanF2 1 year, 5 months ago

this is the correct answer. The other solution that is similar where says" do not search on Windows Updates " is wrong

upvoted 1 times

vinnyct 1 year, 10 months ago

It's Yes

http://woshub.com/how-to-turn-off-automatic-driver-updates-in-windows-10/

upvoted 1 times

SaiVR 2 years, 3 months ago

"To configure this setting in Group Policy, use Computer Configuration\Administrative Templates\Windows Components\Windows update\Do not include drivers with Windows Updates. Enable this policy to not include drivers with Windows quality updates. If you disable or do not configure this policy, Windows Update will include updates that have a Driver classification."

From link below: able to disable all driver updates from WU (Y)

https://docs.microsoft.com/en-us/windows/deployment/update/waas-wu-settings#do-not-include-drivers-with-windows-updates

upvoted 2 times

DrDoom 2 years, 4 months ago

This does meet our goal, however, this will apply to all drivers, not only the video drivers.

upvoted 1 times

Question #33 *Topic 2*

HOTSPOT -

Your network contains an Active Directory domain named contoso.com. The domain contains 500 computers that run Windows 8.1. Some of the computers are used by multiple users.

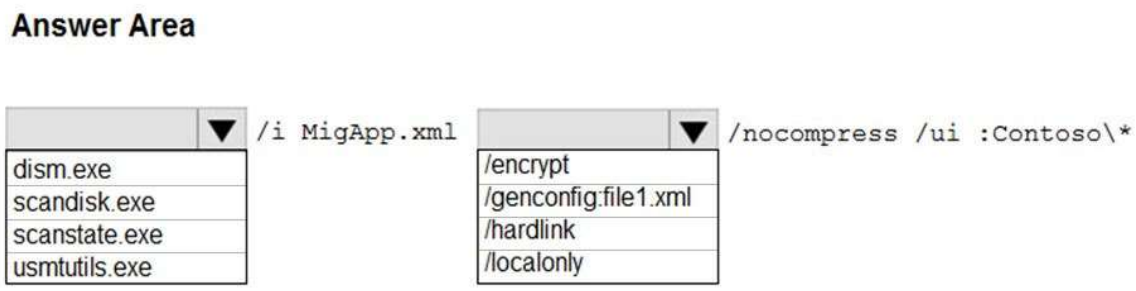
You plan to refresh the operating system of the computers to Windows 10.

You need to retain the personalization settings to applications before you refresh the computers. The solution must minimize network bandwidth and network storage space.

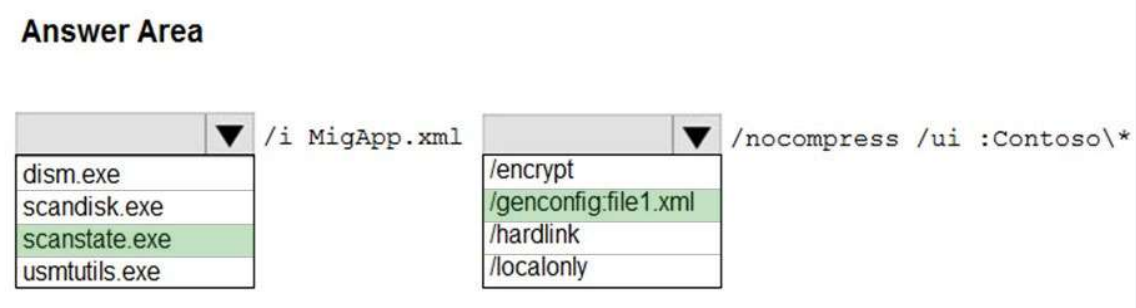
Which command should you run on the computers? To answer, select the appropriate options in the answer area.

NOTE: Each correct selection is worth one point.

Hot Area:



Correct Answer:



Box 1: scanstate.exe -

The ScanState command is used with the User State Migration Tool (USMT) 10.0 to scan the source computer, collect the files and settings, and create a store.

For example, to create a Config.xml file in the current directory, use: scanstate /i:migapp.xml /i:migdocs.xml /genconfig:config.xml /v:13

Box 2: genconfig:file.xml -

Reference:

https://docs.microsoft.com/en-us/windows/deployment/usmt/usmt-scanstate-syntax#how-to-use-ui-and-ue

Piscinita Highly Voted 3 years, 1 month ago

I would choose "Hardlink"

upvoted 24 times

PESK 2 years, 11 months ago

...and you would be wrong. The /hardlink option can only be used when a location is specified, as in this case, with the /genconfig option.

upvoted 7 times

bobboobsmith 2 years, 8 months ago

But /genconfig CAN'T be used when /nocompress is used as stated in the answer's documentation. Read the documentation:

/nocompress

Disables compression of data and saves the files to a hidden folder named "File" at StorePath\USMT. Compression is enabled by default. Combining the /nocompress option with the /hardlink option generates a hard-link migration store. You can use the uncompressed store to view what USMT stored, troubleshoot a problem, or run an antivirus utility against the files. You should use this option only in testing environments, because we recommend that you use a compressed store during your actual migration, unless you are combining the /nocompress option with the /hardlink option.

upvoted 5 times

Rammonon 1 year, 7 months ago

A: Scanstate.exe /iMigApp.xml
A: /Hardlink /nocompress /ui :Contoso*

Scannstate is used with the User State Migration Tool (USMT). It scans a source computer that collects files and settings.

The /Hardlink is used when refreshing computers on existing hardware, it increases performance, decreases disk utilization and other resources.When using hardlink you have to select /nocompress.

The /ui:Contoso\ is defining a Domain then Username to be entered. Hence you combine /Hardlink /nocompress /ui:Contoso\<Username> or </all>

upvoted 10 times

Moorebid 1 year, 4 months ago

I agree, hardlink is specifically used in an upgrade scenario and that is what the question is asking about; hardlink is also used with the /nocompress option as well..

upvoted 2 times

AnoniMouse Highly Voted 1 year, 4 months ago

I have been doing this for ages. It is SCANSTATE coming from the User State Migration Tool, with the option /HARDLINK to save the files locally on the device and not get wiped during the refresh

upvoted 11 times

RodrigoT 6 months ago

You're right, and here is the proof:
https://docs.microsoft.com/en-us/windows/deployment/usmt/usmt-hard-link-migration-store
The first paragraph says everything.

upvoted 5 times

rajpatel007 Most Recent 5 months ago

2nd answer is incorrect

upvoted 1 times

rajpatel007 5 months ago

Using a hard-link migration store saves network bandwidth and minimizes the server use needed to accomplish the migration

So Scanstate.exe and /hardlink

upvoted 3 times

anzer123 1 year ago

https://docs.microsoft.com/en-us/windows/deployment/usmt/usmt-scanstate-syntax

/hardlink

Enables the creation of a hard-link migration store at the specified location. The /nocompress option must be specified with the /hardlink option.

upvoted 1 times

BAbdalla 1 year ago

If /hardlink /nocompress command is used, where will we specify that we should copy the user's application settings, as requested in the question?
As such, I believe the /genconfig:file1.xml option is correct, as this way we specify that we want to copy the users' settings.

upvoted 1 times

Perycles 1 year, 4 months ago

hardlync is the answer ! this option is the best the minimize bandwith et storage usage. Settings are "hardlink" marked during the upgrade to Windows 10, and so don't deleted.

upvoted 3 times

Malfureeon 1 year, 4 months ago

I dont know if there was a change, but according to the Microsoft document, /genconfig and /nocompress can be used together. I personally believe that the given answers are correct on this question.
https://docs.microsoft.com/en-us/windows/deployment/usmt/usmt-scanstate-syntax

upvoted 1 times

slaoui 1 year, 5 months ago

You cannot use /nocompress with /encrypt or /localonly
(https://docs.microsoft.com/en-us/windows/deployment/usmt/usmt-scanstate-syntax#incompatible-command-line-options)

/genconfig generates the optional Config.xml file, but does not create a migration store
(https://docs.microsoft.com/en-us/windows/deployment/usmt/usmt-scanstate-syntax#migration-rule-options)

Answer is /scanstate and /hardlink

upvoted 6 times

Ste 1 year, 5 months ago

/genconfig generates a config file. Therefore doesn't do any migration of data. Further, /genconfig CANNOT be used with /UI. So the given answer is incorrect on 2 counts.

I would chose /Hardlink as this can be used with /nocompress.

/localonly is to be used when there are removeable drives, which can be discounted as the question doesn't mention these.

upvoted 3 times

Tomtom11 1 year, 6 months ago

A hard-link migration store functions as a map that defines how a collection of bits on the hard disk are “wired” into the file system. You use the new USMT hard-link migration store in the PC Refresh scenario only. This is because the hard-link migration store is maintained on the local computer while the old operating system is removed and the new operating system is installed. Using a hard-link migration store saves network bandwidth and minimizes the server use needed to accomplish the migration.

upvoted 4 times

fdiskolo 1 year, 6 months ago

The question is written in the worst possible way. In fact, if you test all possible cases by using the four options (hardlink, localonly, etc) you'll find that ALL of these options will cause a scanstate syntax error.
Genconfig options can't be used together with nocompress and/or ui.

On the other side, hardlink and/or encrypt require a store location, which is not provided in the command sample.
So...It's technically impossible to properly answer to this question.

upvoted 4 times

bastinez 1 year, 6 months ago

This is correct. All answers available are wrong.

I'm inclined to think that /HardLink is the answer they are looking for. Reviewing Hard-Link stores at the following address indicates that they are ideal for OS Refresh scenarios. https://docs.microsoft.com/en-us/windows/deployment/usmt/migration-store-types-overview

The other issue with /genconfig is that it does not preserve personalization settings; It creates a file that can be used in scanstate.exe with the /config switch. There's no real mention of a next step in the question implying to me that this is the final step in the objective. This is getting into the speculative but for what is happening in this question, /Hard-Link makes a lot more sense than /genconfig.

upvoted 2 times

hawkens 1 year, 7 months ago

/encrypt is for encrypting the migration store
/genconfig Generates the optional Config.xml file, but does not create a migration store. To ensure that this file contains every component, application and setting that can be migrated, you should create this file on a source computer that contains all the components, applications and settings that will be present on the destination computers.

/Localonly is used in case of removeable drives

/Hardlink seems to be the best answer (local storage on the samen machine). The question states the there should be used no network storage

upvoted 1 times

cubalondon 1 year, 7 months ago

This is the more logical explanation I have found about this scenario, and everything points to Hardlink.
https://docs.microsoft.com/en-us/windows/deployment/deploy-windows-mdt/refresh-a-windows-7-computer-with-windows-10

upvoted 1 times

hawkens 1 year, 8 months ago

It's hardlink! Nail his answer is correct, follow the link provided https://docs.microsoft.com/en-us/windows/deployment/usmt/usmt-hard-link-migration-store#bkmk-when

upvoted 3 times

Balena 1 year, 7 months ago

It's hardlink! Agreed. Not only it does preserve bandwidth by not using it at all, but also storage space because hardlink only records pointers on the local disk, to where the "to migrated" objects reside. So very little space and very fast.

upvoted 1 times

Nail 1 year, 11 months ago

scanstate.exe, hardlink. https://docs.microsoft.com/en-us/windows/deployment/usmt/usmt-hard-link-migration-store A hard-link migration store enables you to perform an in-place migration where all user state is maintained on the computer while the old operating system is removed and the new operating system is installed; this is why it is best suited for the computer-refresh scenario. Use of a hard-link migration store for a computer-refresh scenario drastically improves migration performance and significantly reduces hard-disk utilization, reduces deployment costs and enables entirely new migration scenarios.

upvoted 5 times

SaiVR 2 years, 3 months ago

Tricky thing is that it says, Reduce network bandwidth and storage space.

Hardlink and localonly would not work for this.

And from the table at https://docs.microsoft.com/en-us/windows/deployment/usmt/usmt-scanstate-syntax#incompatible-command-line-options

Looks like,

you can't do /nocompress /genconfig

But you can do /genconfig /nocompress. NOt sure if I am hella rigth or naw

upvoted 1 times

JeepScratch 2 years, 2 months ago

Like stated, /nocompress and /genconfig cannot be used together. We need hardlink. A hard-link migration store enables you to perform an in-place migration where all user state is maintained on the computer while the old operating system is removed and the new operating system is installed; this is why it is best suited for the computer-refresh scenario....

upvoted 3 times

Lomak 2 years ago

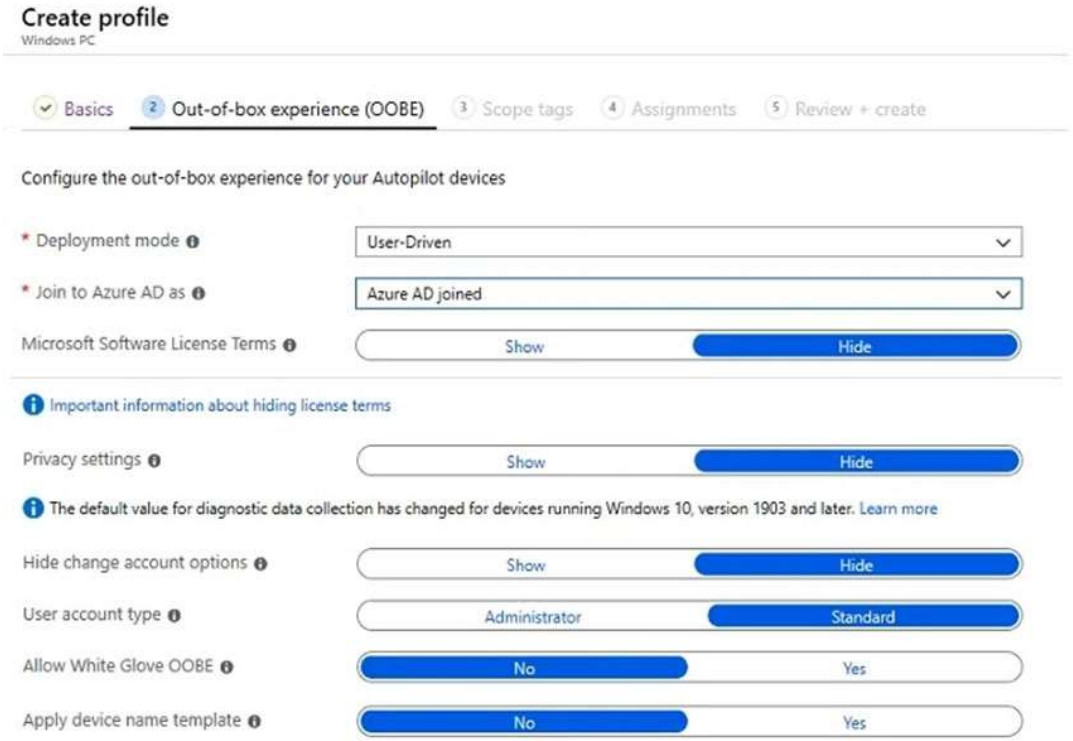
/Hardlink is not required with the Windows 10 USMT package, nor is given as an option in the syntax / example
https://docs.microsoft.com/en-us/windows/deployment/usmt/usmt-scanstate-syntax#syntax

upvoted 1 times

HOTSPOT -

You have a hybrid Microsoft Azure Active Directory (Azure AD) tenant.

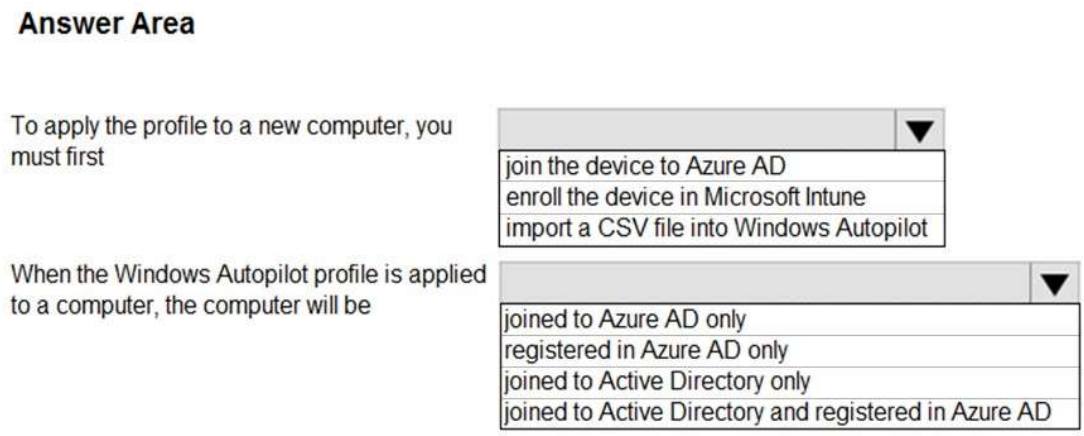
You configure a Windows Autopilot deployment profile as shown in the following exhibit.



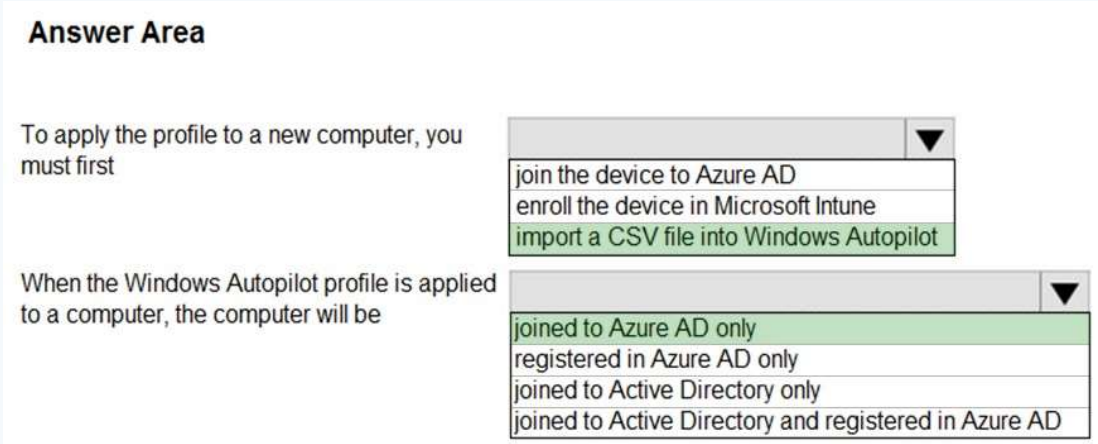
Use the drop-down menus to select the answer choice that completes each statement based on the information presented in the graphic.

NOTE: Each correct selection is worth one point.

Hot Area:



Correct Answer:



Box 1: import a CSV file into Windows Autopilot

You can perform Windows Autopilot device registration within your organization by manually collecting the hardware identity of devices (hardware hashes) and uploading this information in a comma-separated-values (CSV) file.

Box 2: joined to Azure AD only -
As per exhibit (Azure AD joined).
Reference:
https://docs.microsoft.com/en-us/mem/autopilot/add-devices
https://docs.microsoft.com/en-us/azure/active-directory/devices/concept-azure-ad-join-hybrid

jeroenski Highly Voted 1 year, 5 months ago
I would lean towards "CSV" and Azure Ad Joined Only.
upvoted 61 times

larry_cse20 1 year, 5 months ago
me too,
upvoted 6 times

Wilf32 1 year, 5 months ago
I also agree with this.
upvoted 6 times

mikl 9 months, 2 weeks ago
I agree.
upvoted 1 times

Solaris2002 8 months, 1 week ago
I have tested this in a production environment and this is correct. It doesn't matter if you are a hybrid environment. If a Autopilot profile is set to Azure-AD Join only, then the Device will be joined to Azure AD, not registered.
upvoted 6 times

RodrigoT 6 months ago
Tested creating an Autopilot deployment profile and when I hover the mouse pointer over the information symbol next to the line "Join to Azure Ad as" it shows: "Azure AD joined: Cloud-only without an on-premises Windows Server Active Directory".
So, for me is:
CSV
Join to Azure AD only
upvoted 3 times

MitchF 2 months, 2 weeks ago
This source also supports that "Azure AD joined only" is the answer for part 2.

And mid-page, you can read... "Azure AD join can be accomplished using self-service (e.g., "User Driven Mode" in our Question) options like the Out of Box Experience (OOBE), bulk enrollment, or Windows Autopilot (e.g. Autopilot was used in our Question)".

https://docs.microsoft.com/en-us/azure/active-directory/devices/concept-azure-ad-join
upvoted 1 times

JurFur Highly Voted 1 year, 5 months ago
What is the difference between Azure AD joined and registered?
Devices that are Azure AD registered are typically personally owned or mobile devices, and are signed in with a personal Microsoft account or another local account. Devices that are Azure AD joined are owned by an organization, and are signed in with an Azure AD account belonging to that organization.

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

Registered in Azure AD Only seems to be the correct answer
upvoted 8 times

Mujja 1 year, 3 months ago
A registered device is where a user signs in with a local or MS account and adds a work account.

In an Autopilot scenario, the user signs in to the device using a work account, which joins the device to Azure AD
upvoted 4 times

Danohav 1 year, 4 months ago
I guess you just answered your reasoning wrong.

Nowhere it write that the devices are user owned > only User Driven (but that is a different topic)
SO, I would also incline towards Azure AD Joined only
upvoted 3 times

Nen0 Most Recent 10 months, 3 weeks ago
The corret answer is: import CSV, and Azure AD Joined (as it states in the example screen - Azure AD joined).
upvoted 5 times

BAbdalla 11 months, 2 weeks ago
The correct anwser:
To apply the profile to a new computer, you must first: Import a CSV file into Windows Autopilot.

When the Windows Autopilot profile is applied to a computer, the computer will be: Registered in Azure AD only.

In all labs that I maked, after a new computer received a new profile of Autopilot, this PC has registered in Azure AD (not only joined).
upvoted 1 times

Bouncy 7 months, 2 weeks ago
"registered in Azure AD (not only joined)" <-- You might be confusing those terms - if there's something like a hierarchy in this case, "Joined" is more\higher than "Registered"

upvoted 3 times

Solaris2002 1 year ago

I have tested this multiple times and in a production environment. A hybrid AD environment doesn't matter unless the machine has some way of also joining on-prem AD using something like Intune Connector. If you use Autopilot to provision a machine, and select "Azure AD Join" the assumption is you are using a Azure AD email during setup. Therefore the answer is CSV and Azure AD Joined. No where in the question does it state that Intune Connector is installed, or that we are using a personal device/email. https://docs.microsoft.com/en-us/mem/autopilot/windows-autopilot-hybrid

upvoted 5 times

afhelton 1 year, 2 months ago

Directly from MS Docs as it pertains to a hybrid scenario:
A Windows Autopilot profile for user-driven mode must be created and Hybrid Azure AD joined must be specified as the selected option under Join to Azure AD as in the Autopilot profile.

Unfortunately, doesn't specify what happens when you select Azure AD joined instead of Hybrid Azure AD joined, but the use of the word "must" makes it sound like an imperative. As such, I also lean toward Azure AD only. Notice also that the first part of the questions says, "To apply the profile to a NEW computer.." This implies that this computer is neither currently joined to the on-prem domain nor Intune/MECM. At least that's how I read it, but this question is certainly vague...

upvoted 1 times

Perycles 1 year, 4 months ago

answers are "CSV file" for new devices.
Azure AD joined : Microsoft says "When applying Autopilot Profile, devices join Azure AD...".
for existing devices in Hybride AAD mode, this profile will change their connection status as "Azure AD joined" . If we want them to keep their "Hybrid AAD connection", we have to change the "join option" inside the autopilot profile from "Azure AD joined " to "Hybride Azure AD joined".

upvoted 3 times

Malfureeon 1 year, 4 months ago

CSV and Registered not joined. See below.

"If your environment has an on-premises AD footprint and you also want benefit from the capabilities provided by Azure Active Directory, you can implement hybrid Azure AD joined devices. These devices, are devices that are joined to your on-premises Active Directory and registered with your Azure Active Directory."

https://docs.microsoft.com/en-us/azure/active-directory/devices/concept-azure-ad-join-hybrid

upvoted 2 times

uns_uns 1 year, 3 months ago

Just a heads up, I also agreed with this at a point but changed my mind. Look at the screenshot once more and you'll see that: "Join to Azure AD as = Azure AD Join". If the other option had been chosen: "Hybrid Azure AD joined", then your note/answer would have applied and the answer would have been "joined to AD and registered in AAD". I believe that the correct answer for this would be: Box1 > CSV & Box2 > joined to Azure AD only

upvoted 2 times

FlailingLimbs 1 year, 4 months ago

This is correct. Key phrase "These devices, are devices that are joined to your on-premises Active Directory and registered with your Azure Active Directory."

upvoted 1 times

pogap64757 8 months, 1 week ago

https://docs.microsoft.com/en-us/azure/active-directory/devices/faq

"When your users add their accounts to apps on a domain-joined device, they might be prompted with Add account to Windows? If they enter Yes on the prompt, the device registers with Azure AD. The trust type is marked as Azure AD registered. After you enable hybrid Azure AD join in your organization, the device also gets hybrid Azure AD joined. Then two device states show up for the same device.

In most cases, Hybrid Azure AD join takes precedence over the Azure AD registered state, resulting in your device being considered hybrid Azure AD joined for any authentication and Conditional Access evaluation. However, sometimes, this dual state can result in a non-deterministic evaluation of the device and cause access issues. We strongly recommend upgrading to Windows 10 version 1803 and above where we automatically clean up the Azure AD registered state. Learn how to avoid or clean up this dual state on the Windows 10 machine."

upvoted 1 times

jcgm1990 3 months ago

You are wrong, the autopilot settings clearly show join as Azure AD joined, if this was set to join as hybrid Azure AD THEN at that point it will join machines to the domain and register with AD, look it up before providing misleading information.

upvoted 2 times

Technik 1 year, 4 months ago

Given aswer is correct. Question states: Hybrid AAD. This means the user is joined with AD and Registered with AAD.

upvoted 2 times

Perycles 1 year, 4 months ago

totaly wrong,

upvoted 2 times

densyo 1 year, 4 months ago

Agree with jeroenski.
box 1: import a CSV
box 2: joined to Azure AD only

Found it here: https://docs.microsoft.com/en-us/mem/autopilot/profiles

upvoted 4 times

DRAG DROP -

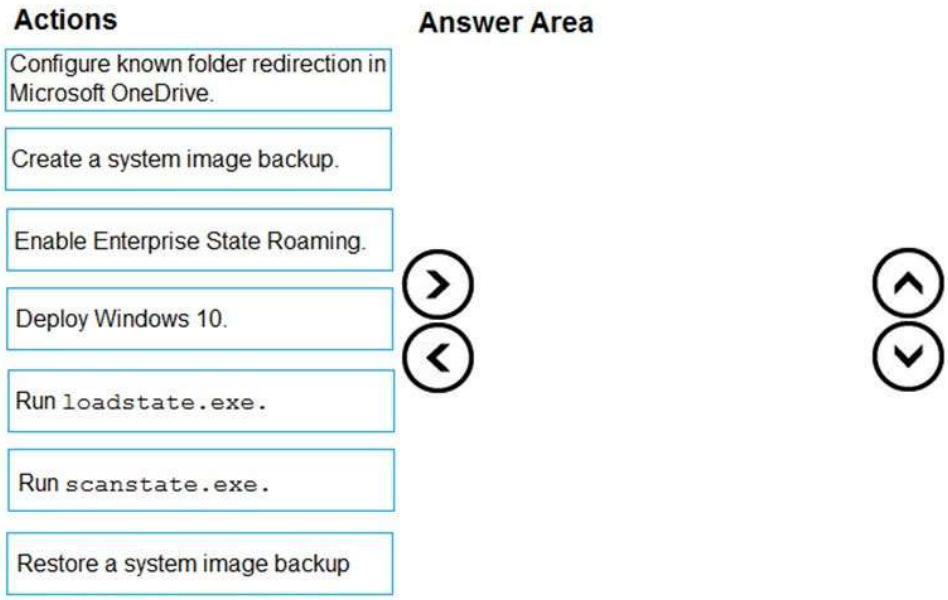
You have 100 computers that run Windows 8.1.

You plan to deploy Windows 10 to the computers by performing a wipe and load installation.

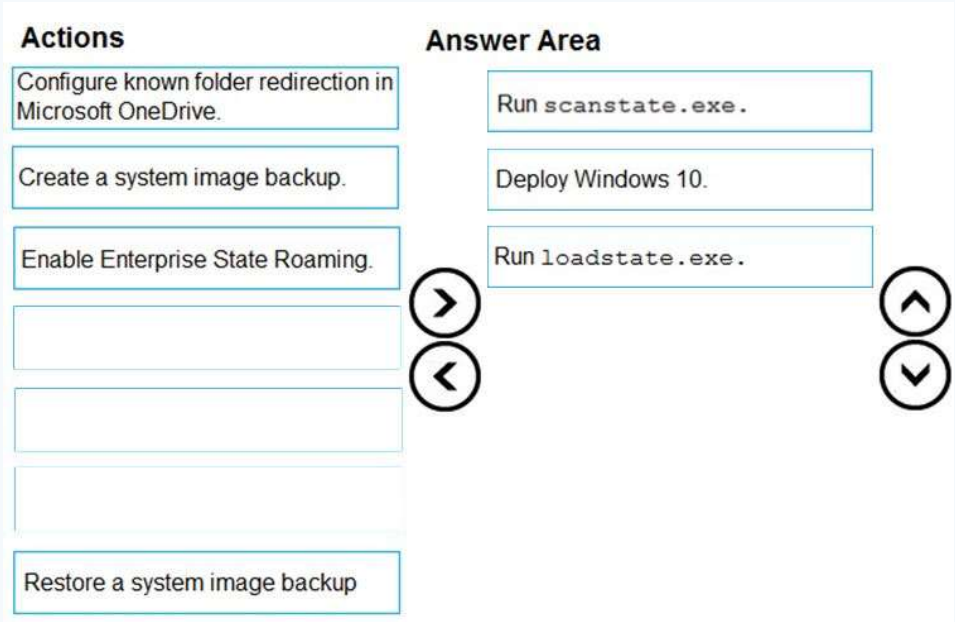
You need to recommend a method to retain the user settings and the user data.

Which three actions should you recommend be performed in sequence? To answer, move the appropriate actions from the list of actions to the answer area and arrange them in the correct order.

Select and Place:



Correct Answer:



Step 1: Run scanstate.exe -

1. Collect files and settings from the source computer.
2. Back up the source computer.
3. Close all applications.
4. Run the ScanState command on the source computer to collect files and settings.
5. Etc.

Step 2: Deploy Windows 10 -

Prepare the destination computer and restore files and settings.

Install the operating system on the destination computer.

Install all applications that were on the source computer. Although it is not always required, we recommend installing all applications on the destination computer before you restore the user state. This makes sure that migrated settings are preserved.

Step 3: Run loadstate.exe -

Run the LoadState command on the destination computer. Specify the same set of .xml files that you specified when you used the ScanState

command.
Reference:
https://docs.microsoft.com/en-us/windows/deployment/usmt/getting-started-with-the-user-state-migration-tool

Layer8 Highly Voted 1 year, 4 months ago
gotta love a straightforward question
upvoted 26 times

Perycles Highly Voted 1 year, 4 months ago
answers are correct.
upvoted 6 times

raduM Most Recent 2 months ago
correct
upvoted 1 times

BAbdalla 11 months, 2 weeks ago
It seems good
upvoted 1 times

Merma 1 year, 5 months ago
You can use User State Migration Tool (USMT) 10.0 to streamline and simplify user state migration during large deployments of Windows operating systems.
USMT provides the following sample scripts that can be easily modified for customization if needed:
MigApp.XML. Rules to migrate application settings.
MigDocs.XML. Rules that use the MigXmlHelper.GenerateDocPatterns helper function. MigUser.XML. Rules to migrate user profiles and user data.
Step 1: Download and Install USMT tools
Step 2: Gather (Backup) data using the USMT ScanState tool, Example:
scanstate /i:migapp.xml /i:migdocs.xml /genconfig:config.xml /v:13
Step 3: Install Windows 10
Step 4: Apply (Restore) data using the USMT LoadState tool, Example:
loadstate \\server\share\migration\mystore /i:migapp.xml /i:migdocs.xml /v:13 /decrypt /key:"mykey"
In addition to the reference links provided:
https://docs.microsoft.com/en-us/windows/deployment/usmt/usmt-scanstate-syntax
https://docs.microsoft.com/en-us/windows/deployment/usmt/usmt-loadstate-syntax
upvoted 6 times

goape 2 years, 1 month ago
I know this will work, but it's not the modern solution. Surely the better approach would be to configure known folders for data, enable enterprise state for settings and then deploy win 10?
upvoted 5 times

goape 2 years, 1 month ago
Actually, nevermind. Of course it's not avail in win 8.1
upvoted 7 times

Mujja 1 year, 3 months ago
It was a nice idea though.
upvoted 3 times

Jvp21 1 year, 4 months ago
I am really trying to search if the Azure AD Enterprise State Roaming is not available for Windows 8.1 and could find exact details. I would initially give same answer opting for a modern method: configure known folders for data, enable enterprise state for settings and then deploy win 10
upvoted 1 times

mikl 9 months, 2 weeks ago
I was thinking the exact same - but you got the point before me :)
upvoted 1 times

Question #36 *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.
Your company uses Windows Autopilot to configure the computer settings of computers issued to users.
A user named User1 has a computer named Computer1 that runs Windows 10.
User1 leaves the company.
You plan to transfer the computer to a user named User2.
You need to ensure that when User2 first starts the computer, User2 is prompted to select the language setting and to agree to the license agreement.
Solution: You perform a local Windows Autopilot Reset.
Does this meet the goal?

A. Yes

B. No

Correct Answer: *B*
Instead:
Windows Autopilot user-driven mode lets you configure new Windows devices to automatically transform them from their factory state to a ready-to-use state. This process doesn't require that IT personnel touch the device.
The process is very simple. Devices can be shipped or distributed to the end user directly with the following instructions:
Unbox the device, plug it in, and turn it on.
Choose a language (only required when multiple languages are installed), locale, and keyboard.
Connect it to a wireless or wired network with internet access. If using wireless, the user must establish the Wi-Fi link.
Specify your e-mail address and password for your organization account.
The rest of the process is automated. The device will:
Join the organization.
Enroll in Intune (or another MDM service)
Get configured as defined by the organization.
Reference:
https://docs.microsoft.com/en-us/windows/deployment/windows-autopilot/windows-autopilot-reset

Jonnaz Highly Voted 1 year, 3 months ago
The answer is correct, it's a No.
Reading the question is says:
"You need to ensure that when User2 first starts the computer, User2 is prompted to select the language setting and to agree to the license agreement."
Opening the link it clearly says:
he Windows Autopilot Reset process automatically keeps information from the existing device:

Set the region, language, and keyboard to the original values.
Wi-Fi connection details.
Provisioning packages previously applied to the device.

If it keeps the info of language and keyboard with will not prompt in the beginning for the language as clearly is requested.
upvoted 11 times

asturmark Most Recent 3 weeks, 5 days ago
Selected Answer: A
it is possible for the user to accept the software terms and language after an autopilot reset but this has to be configured in the autopilot deployment profile:
Software License Terms: Show
Language (region): User select
upvoted 2 times

TonySuccess 5 days, 2 hours ago
Yes, I tested this. But I think this will come down to wording of the question in the Exam x
upvoted 1 times

MitchF 2 months, 2 weeks ago
Ans is "No" – The local Windows Autopilot Reset does not “ensure” that user gets prompted for a language settings & lic. agreement. To “ensure” it, set the Autopilot Deployment Profile:
Set Language (region): "User select"
Microsoft Software License: "Show"
upvoted 2 times

ansilva 3 months, 1 week ago
the key here is local autopilot reset: I'm not sure why people are referencing the autopilot document and saying the answer is B when it clearly states it resets the values to the original: (I had just completed this from the admin console before running into this question)
Person had to select the language and keyboard then was presented by a login screen
Reapplies a device's original settings.
Sets the region, language, and keyboard to the original values.

The user agreement is irrelevant in this case because that's applied by whatever it was chosen in the profile

as MR_Eliot said, local autopilot reset presents no OOBE only way to know for sure its to test it then myself
upvoted 2 times

MR_Eliot 5 months ago

Selected Answer: B

When using Local AutoPilot Reset, after reset you will be presented with the login screen (no OOBE).
upvoted 2 times

Skorne 10 months, 3 weeks ago

The answer would be B:No

From this article: https://docs.microsoft.com/en-us/mem/autopilot/windows-autopilot-reset

Windows Autopilot Reset "Sets the region, language, and keyboard to the original values." Therefore as the questions asks for the User to be prompted Language the answer would be No.
upvoted 2 times

rovert94 10 months, 3 weeks ago

Answer is A: YES

From this article: https://docs.microsoft.com/en-us/mem/autopilot/windows-autopilot-reset

Windows Autopilot Reset:
Removes personal files, apps, and settings.
Reapplies a device's original settings.
Sets the region, language, and keyboard to the original values.
Maintains the device's identity connection to Azure AD.
Maintains the device's management connection to Intune.
upvoted 1 times

RodrigoT 6 months ago

But the user is NOT "prompted" to select the language setting and to agree to the license agreement. Everything is automatic. So, the answer is NO.
upvoted 1 times

daonga 1 year, 1 month ago

The people saying no - Did you test this? When I do an AutoPilot reset at work, it always prompts to select keyboard and accept EULA during OOBE, even if the AutoPilot profile policy is set to ignore these (which this question doesn't give info on) so I would assume answer is YES.

Can anyone else explain why no?
upvoted 3 times

RodrigoT 6 months, 3 weeks ago

Did it ask also to select the language? No. So, B.
upvoted 2 times

Angarali 1 year, 2 months ago

Answer is No
upvoted 1 times

justabasicuser 1 year, 2 months ago

"The Windows Autopilot Reset process automatically keeps information from the existing device:

Set the region, language, and keyboard to the original values."

Answer is No
upvoted 3 times

jibutoms 1 year, 3 months ago

"local" Windows Autopilot Reset prompts me to choose "Option B"
upvoted 1 times

Perycles 1 year, 4 months ago

after testing, autolpilot reset is the good way , so answer is A:YES
upvoted 2 times

Perycles 1 year, 4 months ago

"..It removes all personal files, apps, and settings,
and it resets a Windows 10 device to its initial state from the lock screen." answer is B
upvoted 2 times

Perycles 1 year, 4 months ago

after restart, user is prompted to select keyboard and language, then he has to clic on accept licence agreements.
upvoted 2 times

AnoniMouse 1 year, 4 months ago

The answer seems to be correct

Autopilot Reset maintains the region/language/keyboard which is not what the question wants

Autopilot Reset removes personal files, apps, and settings on a device but retains the connection to Azure AD and Intune (or 3rd party MDM). The key here is personal data; Autopilot Reset basically only removes the user profile instead of wiping the entire OS drive. This

makes Autopilot Reset a sort of middle-ground option, where you're wiping a device and maintaining the enrollment state but not maintaining the user data.

Autopilot Reset also maintains the region/language/keyboard, any provisioning packages applied, and Wi-Fi connections. Autopilot Reset is the best option for re-using a device within your organization. You're basically removing the last user from a device and (depending on your Intune deployment configuration) handing it right over to the next person with no extra work needed

upvoted 4 times

Testtest123 1 year, 5 months ago

Giving answer is correct

upvoted 4 times

Question #37 *Topic 2*

You have a Microsoft 365 subscription.

A remote user purchases a laptop from a retail store. The laptop is intended for company use and has Windows 10 Pro edition installed.

You need to configure the laptop to meet the following requirements:

- Modify the layout of the Start menu
- Upgrade Windows 10 to Windows 10 Enterprise
- Join the laptop to a Microsoft Azure Active Directory (Azure AD) domain named contoso.com

The solution must minimize how long it takes for the user to apply the configurations.

What should you do?

A. Create a custom Windows image (.wim) file that contains an image of Windows 10 Enterprise and upload the file to a Microsoft

B. Create a provisioning package (.ppkg) file and email the file to the user

C. Create a Windows To Go workspace and ship the workspace to the user

D. Create a Sysprep Unattend (.xml) file and email the file to the user

Correct Answer: *B*

A provisioning package (.ppkg) is a container for a collection of configuration settings. With Windows client, you can create provisioning packages that let you quickly and efficiently configure a device without having to install a new image.

Note: Windows provisioning makes it easy for IT administrators to configure end-user devices without imaging. Using Windows provisioning, an IT administrator can easily specify desired configuration and settings required to enroll the devices into management and then apply that configuration to target devices in a matter of minutes. It is best suited for small- to medium-sized businesses with deployments that range from tens to a few hundred computers.

Reference:

https://docs.microsoft.com/en-us/windows/configuration/provisioning-packages/provisioning-packages

Merma Highly Voted 1 year, 4 months ago

Correct B. Create a provisioning package (.ppkg) file and email the file to the user
"A provisioning package (.ppkg) is a container for a collection of configuration settings. With Windows 10, you can create provisioning packages that let you quickly and efficiently configure a device without having to install a new image.
Provisioning packages are simple enough that with a short set of written instructions, a student or non-technical employee can use them to configure their device. This can result in a significant reduction in the time required to configure multiple devices in your organization."
https://docs.microsoft.com/en-us/windows/configuration/provisioning-packages/provisioning-packages
https://docs.microsoft.com/en-us/windows/configuration/provisioning-packages/provisioning-create-package

upvoted 7 times

moobdoob Most Recent 8 months, 2 weeks ago

Selected Answer: B

Correct answer: B

upvoted 3 times

b3arb0yb1m 9 months, 2 weeks ago

B. Create a provisioning package (.ppkg) file and email the file to the user

upvoted 2 times

Perycles 1 year, 4 months ago

answer is correct.

upvoted 2 times

Question #38 *Topic 2*

You have a Microsoft 365 subscription. All devices run Windows 10.
You need to prevent users from enrolling the devices in the Windows Insider Program.
What two configurations should you perform from the Endpoint Management admin center? Each correct answer presents part of the solution.
NOTE: Each correct selection is worth one point.

A. a Windows 10 security baseline

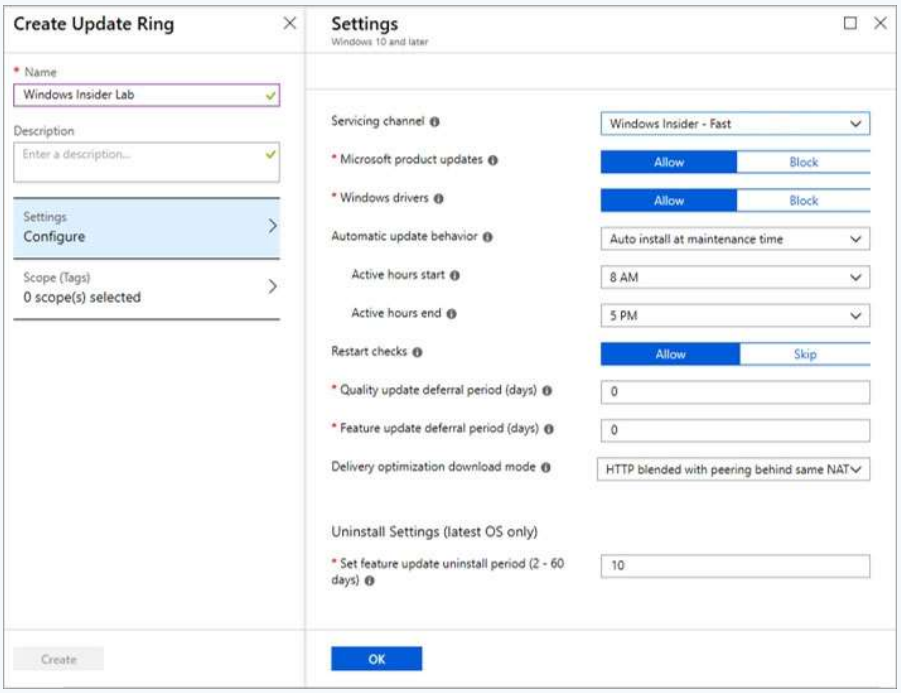
B. an app configuration policy

C. a custom device configuration profile

D. a Windows 10 update ring

E. a device restrictions device configuration profile

Correct Answer: *CD*
C: Microsoft Intune includes many built-in settings to control different features on a device. You can also create custom profiles, which are created similar to built- in profiles. Custom profiles are great when you want to use device settings and features that aren't built in to Intune. These profiles include features and settings for you to control on devices in your organization. For example, you can create a custom profile that sets the same feature for every Windows device.
D: Set up Insider Preview builds using Intune
1. Log in to the Azure portal and select Intune.
2. Go to Software Updates > Windows 10 Update Rings and select + Create to make an Update Ring policy.
Add a name and select the Settings section to configure its settings.



3. Etc.
Reference:
https://docs.microsoft.com/en-us/windows-insider/business/manage-builds

Question #39 *Topic 2*

Your network contains an Active Directory domain named contoso.com that syncs to Azure Active Directory (Azure AD).
Existing on-premises computers are managed by using Microsoft Endpoint Configuration Manager. You configure contoso.com for co-management.
You deploy 100 new devices that run Windows 10. The devices are joined to Azure AD and enrolled in Microsoft Intune.
You need to ensure that the devices are co-managed.
What should you create in Intune first?

A. a conditional access policy

B. a device compliance policy

C. an app for the Endpoint Configuration Manager client

D. a device configuration profile

E. an app configuration policy

Correct Answer: *C*
For new internet-based devices, you need to create an app in Intune. Deploy this app to Windows 10 devices that aren't already Configuration Manager clients.
This scenario is when 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.
Reference:
https://docs.microsoft.com/en-us/configmgr/comanage/how-to-prepare-win10

Anthony_2770 Highly Voted 1 year, 8 months ago
Answer is correct. Refer to the supplied link.
upvoted 21 times

MR_Eliot Most Recent 5 months ago
Selected Answer: C
C => Correct!
upvoted 1 times

ercluff 1 year, 1 month ago
Here is a nice overview reference showing installing the Configuration manager Client as the means of enabling the Co-management capability:
https://docs.microsoft.com/en-us/mem/configmgr/comanage/overview#configuration-manager-clients
upvoted 2 times

RodrigoT 6 months, 3 weeks ago
Excellent link. Check also this practical step-by-step:
https://docs.microsoft.com/en-us/mem/configmgr/comanage/how-to-prepare-Win10#install-the-configuration-manager-client
upvoted 2 times

RodrigoT 6 months, 3 weeks ago
https://docs.microsoft.com/en-us/mem/configmgr/comanage/tutorial-co-manage-new-devices#use-intune-to-deploy-the-configuration-manager-client
under the subtitle: Create an Intune app to install the Configuration Manager client
upvoted 1 times

Perycles 1 year, 4 months ago
yes it's correct .Configuration manager client program has to be add into intune and then deploy and devices.
upvoted 3 times

Question #40 *Topic 2*

Your network contains an Active Directory domain named contoso.com that syncs to Azure Active Directory (Azure AD).
The Active Directory domain contains 200 computers that run Windows 10. The computers are managed by using Microsoft System Center Configuration
Manager (Current Branch).
You need to pilot co-management for only five of the computers.
What should you create first?

A. a domain local distribution group in Active Directory

B. an Intune Connector for Active Directory

C. a device collection in Endpoint Configuration Manager

D. a dynamic device group in Azure AD

Correct Answer: *C*
The Pilot Intune setting switches the associated workload only for the devices in the pilot collection.
Note: 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.
Reference:
https://docs.microsoft.com/en-us/configmgr/comanage/tutorial-co-manage-new-devices

VCE_player Highly Voted 1 year, 9 months ago
Answer C seems correct, but has the wrong reference link.
According to the reference url: "This tutorial begins with the premise that your Windows 10 devices are already enrolled with Intune." -> this is not the case here

"If you have a hybrid Azure AD that joins your on-premises AD with Azure AD, we recommend following our companion tutorial, Enable co-management for Configuration Manager clients".
Correct ref url -> https://docs.microsoft.com/en-us/mem/configmgr/comanage/tutorial-co-manage-clients

It has this "Tip" mentioned throughout the tutorial:
"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.
Starting in Configuration Manager version 1906, you may need multiple collections since you can assign a different Pilot group for each workload."
upvoted 11 times

RodrigoT 6 months, 3 weeks ago
https://docs.microsoft.com/en-us/mem/configmgr/comanage/tutorial-co-manage-new-devices#enable-co-management-in-configuration-manager
And this link explains the pilot collection.
upvoted 1 times

b3arb0yb1m Most Recent 9 months, 2 weeks ago
C. a device collection in Endpoint Configuration Manager
upvoted 2 times

Perycles 1 year, 4 months ago
C of course, when configuring "intune pilot" under SCCM, we have to specific a collection.
upvoted 1 times

Anthony_2770 1 year, 8 months ago
Notes:
Collections are groupings of users or devices. Use collections for tasks like managing applications, deploying compliance settings, or installing software updates. ... A collection can contain users or devices, but not both.
upvoted 2 times

Anthony_2770 1 year, 8 months ago
Configuration Manager device collection
upvoted 8 times

HOTSPOT -

You network contains an Active Directory domain. The domain contains 200 computers that run Windows 8.1. You have a Microsoft Azure subscription.

You plan to upgrade the computers to Windows 10.

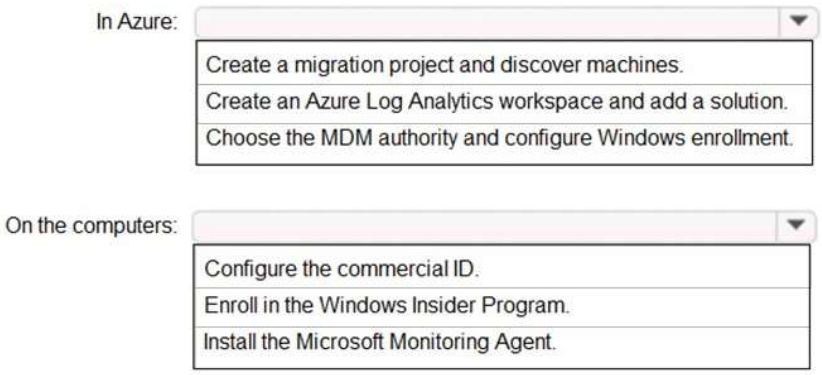
You need to generate an Upgrade Readiness report for the computers.

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

NOTE: Each correct selection is worth one point.

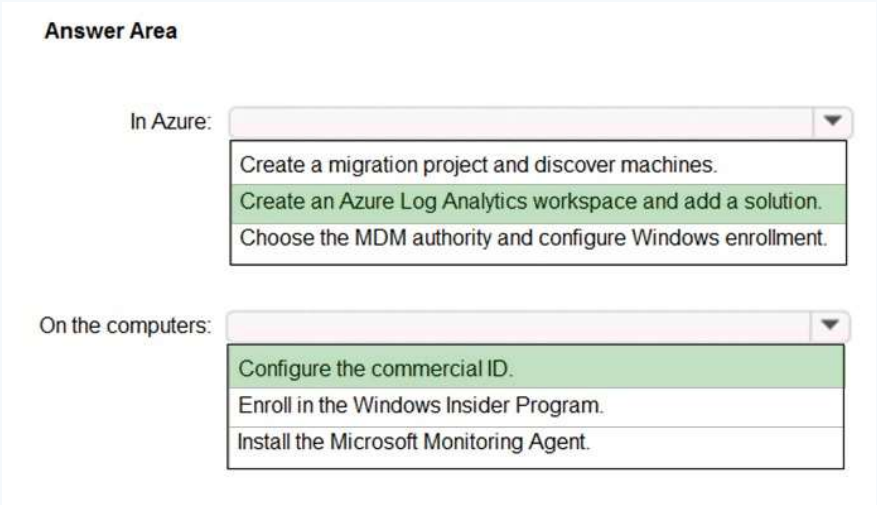
Hot Area:

Answer Area



Correct Answer:

Answer Area



Box 1: Create an Azure Log Analytics workspace and add a solution

Once you have an Azure subscription, follow the steps below to get stared with Upgrade Readiness.

Setup a subscription to Microsoft Operations Management Suite (OMS).

You will be prompted to link the OMS workspace to an Azure subscription.

Once the link with an Azure subscription is complete, your workspace should be ready and you will be redirected to your blank workspace.

Enable Upgrade Analytics. To do this, click on the Solutions Gallery In the Solutions Gallery page, scroll to the right to locate and select the Upgrade Analytics

(Preview) tile.

..

Now that your Upgrade Analytics subscription is ready, the last requirement is to configure Upgrade Analytics with the details of which version of Windows 10 you are targeting. To do this, click on the tile for Upgrade Analytics Preview . On the Upgrade Analytics Preview page, click on the gear icon labelled Solution Settings.

Box 2: Configure the Commercial ID

For the commercialIDValue variable, use the ג€Commercial IDג€ that was generated when you setup your Upgrade Readiness solution. If you don't have this, you can pull it out from your OMS workspace.

Reference:

https://techcommunity.microsoft.com/t5/core-infrastructure-and-security/getting-started-with-upgrade-readiness/ba-p/714705

https://docs.microsoft.com/sv-se/archive/blogs/ukplatforms/upgrade-readiness-client-configuration

Wilf32 Highly Voted 1 year, 5 months ago

From my understanding "in Azure" answer is correct but you need to install the Microsoft Monitoring Agent for Log analytics and the Commercial ID for Desktop Analytics.

I would Answer Microsoft Monitoring Agent on the computers.

Please comment if i am wrong, some info in link below

https://docs.microsoft.com/en-us/services-hub/health/mma-setup

upvoted 26 times

Moorebid 1 year, 4 months ago

I agree with you, it looks like you configure the MMA before you point to the commercial ID in Azure.

upvoted 4 times

mikl 9 months, 2 weeks ago

I agree.

upvoted 1 times

RodrigoT 5 months, 1 week ago

You would install MMA just to collect events. But the question is about update compliance. The answer provided is correct.

upvoted 5 times

AnoniMouse Highly Voted 1 year, 4 months ago

The answer provided is NOT correct:

1: You need a Log Analytics workspace, and you will get a Workspace ID and a Workspace Key
2: You need to install the Microsoft Monitoring Agent MMA and configure it with the above Workspace ID and Key which can be automated during setup or manually inserted (application is available from the classical Control Panel)

upvoted 15 times

Jimbob77 1 year, 4 months ago

Anonimouse has the best answer; question 2 for "on the computer" is install the MMA.
If the agent was already installed (for example, using SCOM) then you could configure the commercial ID so the agent is reporting back to the new and existing workspace. There's no reference to this in the Question so the agent needs to be installed.

upvoted 3 times

RodrigoT 5 months ago

Not this time. You would install MMA just to collect events. But the question is about update compliance. The answer provided is correct.

upvoted 2 times

Dedutch Most Recent 2 months ago

The thing to note here is that you don't need the full Desktop Analytics you just need telemetry data. That can be sent without installing the Microsoft Monitoring Agent.

upvoted 1 times

MR_Eliot 5 months ago

Answer is 100% as provided. Don't look at any other comments. MMA agent is for monitoring devices. I'm not gonna explain anything here, but just believe me and If you're not 100% sure, do your own research.

upvoted 2 times

lykeP 8 months, 3 weeks ago

The answer provided is CORRECT. Microsoft Monitoring Agent is incorrect, see the below link:
https://www.techtarget.com/searchwindowsserver/definition/Microsoft-Monitoring-Agent

upvoted 4 times

fatape 10 months, 2 weeks ago

The given answer looks correct. Looking at the step by step Config commercial ID comes right after create workspace and connect config man.
On the Diagnostic Data page, configure the following settings:

Commercial ID: this value should automatically populate with your organization's ID

https://docs.microsoft.com/en-us/mem/configmgr/desktop-analytics/tutorial-windows10

upvoted 2 times

NKG123 9 months, 3 weeks ago

You configure commercial ID on configuration manager and not on computers.

upvoted 2 times

RodrigoT 6 months ago

But the commercial ID is deployed to devices.
https://docs.microsoft.com/en-us/windows/deployment/update/update-compliance-get-started
Check the third blue box in the article.

upvoted 1 times

RodrigoT 5 months, 1 week ago

The answer provided is correct:
https://docs.microsoft.com/en-us/windows/deployment/update/update-compliance-using

upvoted 2 times

Sizz 1 year, 1 month ago

Given answer is correct. Upgrade Readiness is confusingly a blend of technologies to achieve the outcome. You're *not* using MMA here because you're not collecting diagnostics and events from endpoints to directly ingest into log analytics. Instead, the commercial ID is used so that the telemetry your W10 devices send to Microsoft can be segregated and copied from the central Microsoft Diagnostic Data Management service back to your nominated Log Analytics workspace where the readiness solution can be run in a distributed fashion.

upvoted 3 times

Percles 1 year, 4 months ago

another good link :https://systemcenterdudes.com/sccm-windows-analytics-log-analytics/
first we have to create a Workspace, then create a commercial ID on client. differents way possible for that (local script, OMA-URI in intune , GPO in ADDS, ccm client settings und SCCM...). SO answers are : create workspace + set ID on client.

upvoted 1 times

BLYBOI 1 year, 4 months ago

In Azure, you create an Azure Log Analytics workspace and add a solution.
In Computer, install MMA.

You configure Commercial ID in Azure, not computer

This is what I think.

upvoted 9 times

NKG123 9 months, 3 weeks ago

The best explanation I can see here

upvoted 1 times

MikeMatt2020 1 year, 4 months ago

I believe the given answer is correct, even though MMA makes sense as Merma said.

The following article mentions creating a workspace and immediately says to "Get your Commercial ID" https://docs.microsoft.com/en-us/windows/deployment/update/update-compliance-get-started

"A CommercialID is a globally unique identifier assigned to a specific Log Analytics workspace. The CommercialID is copied to an MDM or Group Policy and is used to identify devices in your environment.

To find your CommercialID within Azure:
Navigate to the Solutions tab for your workspace, and then select the WaaSUpdateInsights solution. From there, select the Update Compliance Settings page on the navbar. Your CommercialID is available in the settings page."

upvoted 2 times

Merma 1 year, 4 months ago

MMA makes sense to me but when I look around I keep finding a reference to the Commercial ID. Even the Exam Ref MD-101 book says: "After you have created the workspace, you must enroll your devices. To do this, you need to know your Commercial ID. The Commercial ID is a unique reference number used to identify your tenant within the Log Analytics workspace, and it informs your devices where to send their telemetry data." I think the given answer is correct.

upvoted 6 times

Anna_Peters 1 year, 4 months ago

Wilf32 is correct.

upvoted 3 times

Question #42 *Topic 2*

You have a Microsoft 365 subscription.
You have 20 computers that run Windows 10 and are joined to Microsoft Azure Active Directory (Azure AD).
You plan to replace the computers with new computers that run Windows 10. The new computers will be joined to Azure AD.
You need to ensure that the desktop background, the favorites, and the browsing history are available on the new computers.
What should you use?

A. Folder Redirection

B. The Microsoft SharePoint Migration Tool

C. Enterprise State Roaming

D. Roaming user profiles

Correct Answer: *C*
Enterprise State Roaming provides users with a unified experience across their Windows devices and reduces the time needed for configuring a new device.
Reference:
https://docs.microsoft.com/en-us/azure/active-directory/devices/enterprise-state-roaming-enable

Justin0020 Highly Voted 1 year, 12 months ago
C is correct. D is not correct, because Roaming profiles does not work with Azure-AD only.
upvoted 15 times

raduM Most Recent 1 month ago
c is correct
upvoted 1 times

ZzeezZ 2 months, 1 week ago
Selected Answer: B
No, only applies to packages on removable media
upvoted 1 times

MR_Eliot 5 months ago
Selected Answer: C
C is Correct!
upvoted 1 times

mikl 9 months, 2 weeks ago
C. Enterprise State Roaming is correct!
upvoted 1 times

b3arb0yb1m 9 months, 2 weeks ago
C. Enterprise State Roaming
upvoted 1 times

Harrysa 1 year, 5 months ago
X-man - I guess because the setup is primarily Azure AD enterprise state roaming is a perfect fit
upvoted 1 times

Tomtom11 1 year, 5 months ago
https://docs.microsoft.com/en-us/azure/active-directory/devices/enterprise-state-roaming-faqs
upvoted 2 times

MD4439 1 year, 6 months ago
c is correct
upvoted 1 times

X_man 2 years ago
C is correct,
not enough detail to support option D
upvoted 4 times

Question #43 *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 computer named Computer1 that runs Windows 10.
You save a provisioning package named Package1 to a folder named C:\Folder1.
You need to apply Package1 to Computer1.
Solution: From the Settings app, you select Access work or school, and then you select Add or remove a provisioning package.
Does this meet the goal?

A. Yes

B. No

Correct Answer: *A*
To install a provisioning package, navigate to Settings > Accounts > Access work or school > Add or remove a provisioning package > Add a package, and select the package to install.
Reference:
https://docs.microsoft.com/en-us/windows/configuration/provisioning-packages/provisioning-apply-package

mlleremallqui Highly Voted 2 years, 1 month ago
No
https://docs.microsoft.com/es-es/windows/configuration/provisioning-packages/provisioning-how-it-works#:~:text=Los%20paquetes%20de%20aprovisionamiento%20de,settings%20to%20Windows%2010%20devices.
upvoted 25 times

jojolababu Highly Voted 2 years ago
No, this way off accessing the ppkg only applies to USB devices (easy to check on your Windows)
https://docs.microsoft.com/en-us/windows/configuration/provisioning-packages/provisioning-apply-package
Insert the USB drive to a desktop computer, navigate to Settings > Accounts > Access work or school > Add or remove a provisioning package > Add a package, and select the package to install. For a provisioning package stored on a network folder or on a SharePoint site, navigate to the provisioning package and double-click it to begin installation.
upvoted 19 times

geggio Most Recent 1 week, 1 day ago
y
https://learn.microsoft.com/en-us/windows/configuration/provisioning-packages/provisioning-apply-package
upvoted 1 times

Russ_A7x 2 months ago
Selected Answer: B
Knowing windows tests there's probably a folder on a USB named "C:/folder1". This option is for removable media only.
upvoted 3 times

bounce_united 3 months, 1 week ago
Selected Answer: B
In settings, needs removable media
upvoted 3 times

MR_Eliot 5 months ago
Selected Answer: B
Answer is B. You only can select *.ppkg files from removeable-devices.
upvoted 5 times

Angarali 5 months, 2 weeks ago
Selected Answer: B
NO WAY!
upvoted 1 times

PChi 5 months, 4 weeks ago
go to your settings... provided answer is correct
upvoted 1 times

PChi 5 months, 4 weeks ago
big oof. re-read the question. don't mind me peeps. Nothing to see here other than the correct answer is indeed B :p
package was only added to folder. you CAN go to settings> access work or school and add a provisioning package from there but a usb is indeed needed.
upvoted 3 times

Garito 7 months, 1 week ago
Selected Answer: B
documentation supported
upvoted 2 times

moobdoob 8 months, 2 weeks ago

Selected Answer: B

No is the correct answer, from settings you must add the provisioning package from removable media.

upvoted 2 times

mayleni 8 months, 3 weeks ago

Selected Answer: B

I tried in win 11 and win10. And it only allows from usb

upvoted 3 times

duure003 8 months, 3 weeks ago

The answer is NO !
If you select the described the solution you have to choose a method.
The only option that shows is: Add from: Removable Media.

upvoted 1 times

lykeP 8 months, 3 weeks ago

Selected Answer: B

B is the correct Answer. To apply a provisioning package, this can be done from a USB frive. not from settings!

upvoted 3 times

mikl 9 months, 2 weeks ago

Answer is no - since .ppkg is stored at C:\

For a provisioning package stored on a network folder or on a SharePoint site, navigate to the provisioning package and double-click it to begin installation.

https://docs.microsoft.com/en-us/windows/configuration/provisioning-packages/provisioning-apply-package

upvoted 1 times

handsofthelp 10 months, 1 week ago

Wrong. The answer is B. Add or remove provisioning package is only from removable devices.

upvoted 2 times

Johan_Dev 10 months, 1 week ago

Selected Answer: B

This way of adding provisioning package can only be done via removable media. B - NO

upvoted 4 times

encxorblood 10 months, 2 weeks ago

No - only from Medium or mouse click.

upvoted 1 times

Question #44 *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 computer named Computer1 that runs Windows 10.
You save a provisioning package named Package1 to a folder named C:\Folder1.
You need to apply Package1 to Computer1.
Solution: From File Explorer, you go to C:\Folder1, and then you double-click the Package1.ppkg file.
Does this meet the goal?

A. Yes

B. No

Correct Answer: *B*
Instead: From the Settings app, you select Access work or school, and then you select Add or remove a provisioning package.
To install a provisioning package, navigate to Settings > Accounts > Access work or school > Add or remove a provisioning package > Add a package, and select the package to install.
Reference:
https://docs.microsoft.com/en-us/windows/configuration/provisioning-packages/provisioning-apply-package

vnod007 Highly Voted 1 year, 10 months ago
Double clicking should work:
https://youtu.be/UU6l7-CMSRc
upvoted 23 times

RodrigoT 6 months ago
And if they can be attached to an email, an user for sure will download it to the local drive and double click it.
https://docs.microsoft.com/en-us/windows/configuration/provisioning-packages/provisioning-packages#benefits-of-provisioning-packages
upvoted 1 times

mlleremallqui Highly Voted 2 years, 1 month ago
Yes
Descargado de una conexión de red y copiado en una carpeta local Haz doble clic en el archivo de paquete.

https://docs.microsoft.com/es-es/windows/configuration/provisioning-packages/provisioning-how-it-works#:~:text=Los%20paquetes%20de%20aprovisionamiento%20de,settings%20to%20Windows%2010%20devices.
upvoted 11 times

zdiddy Most Recent 2 months ago
Selected Answer: A
Just try and import a provisioning package from the settings app and see what options you have available if you don't believe it.
upvoted 1 times

ZzeezZ 2 months, 1 week ago
Selected Answer: A
Yes, it will work
upvoted 2 times

MR_Eliot 5 months ago
Selected Answer: A
A is correct.
upvoted 2 times

Angarali 5 months, 2 weeks ago
Selected Answer: A
YES YES YES
upvoted 2 times

moobdoob 8 months, 2 weeks ago
Double clicking works, answer is YES.
upvoted 5 times

IykeP 8 months, 3 weeks ago
Selected Answer: A
A is the correct Answer, double clicking will work.
upvoted 3 times

Ferrix 9 months, 3 weeks ago
Tested in Lab, doble click is working! The Answer is YES
upvoted 2 times

TAndrasSF 10 months ago

Selected Answer: A

In fact, double click on .ppkg file works. I used it about 90 times in the last 2 months. :)

upvoted 7 times

encxorblood 10 months, 2 weeks ago

Yes . mouse click or add in account from medium

upvoted 1 times

BAbdalla 11 months, 2 weeks ago

Double click works! The Correct awnser is A.Yes

upvoted 2 times

encxorblood 1 year ago

Yes. Tested.

upvoted 3 times

jibutoms 1 year, 3 months ago

Answer should be Option A: Yes. Double-clicking ppkg will install.

upvoted 1 times

Perycles 1 year, 4 months ago

yes it's working fine.

upvoted 1 times

Tomtom11 1 year, 4 months ago

Yes I have try this and it works

upvoted 1 times

Tomtom11 1 year, 4 months ago

I have try this and this works

upvoted 1 times

Question #45 *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 computer named Computer1 that runs Windows 10.
You save a provisioning package named Package1 to a folder named C:\Folder1.
You need to apply Package1 to Computer1.
Solution: At a command prompt, you change the current folder to C:\Folder1, and then you run the RegSvr32.exe Package1.ppkg command.
Does this meet the goal?

A. Yes

B. No

Correct Answer: *B*
Instead: From the Settings app, you select Access work or school, and then you select Add or remove a provisioning package.
To install a provisioning package, navigate to Settings > Accounts > Access work or school > Add or remove a provisioning package > Add a package, and select the package to install.
Reference:
https://docs.microsoft.com/en-us/windows/configuration/provisioning-packages/provisioning-apply-package

jojolababu Highly Voted 2 years ago
Answer is No, but the explanation provided is incorrect
The command used here is wouldn't do but a Powershell Install-ProvisioningPackage would
And double-clicking on it too
upvoted 21 times

ZzeezZ Most Recent 2 months, 1 week ago
Selected Answer: B
Answer is No, but the explanation provided is incorrect
upvoted 1 times

moobdoob 8 months, 2 weeks ago
Answer is NO.
upvoted 2 times

Merma 1 year, 4 months ago
No is correct. Information about using PowerShell:
This cmdlet is used to install .ppkg files that are generated and exported by the Windows Configuration Designer tool.
You can use this cmdlet to install a .ppkg file interactively or silently by specifying the -QuietInstall switch parameter. Example:
Install-ProvisioningPackage -PackagePath C:\mypackage.ppkg -QuietInstall
Insert the USB drive to a desktop computer, navigate to Settings > Accounts > Access work or school > Add or remove a provisioning package > Add a package, and select the package to install.
https://docs.microsoft.com/en-us/powershell/module/provisioning/install-provisioningpackage?view=windowsserver2019-ps
https://docs.microsoft.com/en-us/windows/configuration/provisioning-packages/provisioning-apply-package
upvoted 4 times

Question #46 *Topic 2*

You manage 1,000 computers that run Windows 10. All the computers are enrolled in Microsoft Intune. You manage the servicing channel settings of the computers by using Intune.
You need to review the servicing status of a computer.
What should you do?

A. From Device configuration - Profiles, view the device status.

B. From Device compliance, view the device compliance.

C. From Software updates, view the audit logs.

D. From Software updates, view the Per update ring deployment state.

Correct Answer: *D*
Reports for Update rings for Windows 10 and later policy.
Intune offers integrated report views for the Windows update ring policies you deploy. These views display details about the update ring deployment and status:
1. Sign in to Microsoft Endpoint Manager admin center.
2. Select Devices > Monitor. Then under Software updates select Per update ring deployment state and choose the deployment ring to review.
Note: Windows 10 and later update rings â€" Use a built-in report that's ready by default when you deploy update rings to your devices.
Reference:
https://docs.microsoft.com/en-us/intune/windows-update-compliance-reports

Parzival Highly Voted 2 years, 10 months ago
Use Intune

To review a policy report on the deployment status for the Windows 10 update rings that you have configured:

Sign in to the Azure portal.

Choose All services, filter on Intune, and select Microsoft Intune.

Select Software updates > Overview. You can see general information about the status of any update rings you assigned.

Open one of the following reports:

For all deployment rings:
On the Software updates > Windows 10 Update Rings
In the Monitor section, choose Per update ring deployment state.

For specific deployment rings:
In Software updates > Windows 10 Update Rings, choose the deployment ring to review.
In the Monitor section, choose from the following reports to view more detailed information about the update ring:
Device status
User status
https://docs.microsoft.com/en-us/intune/protect/windows-update-compliance-reports
upvoted 19 times

Perycles Highly Voted 1 year, 3 months ago
path is a bit different today : from intune : "Reports > Windows update (preview) > Reports tab > Windows Feature updates report". So answer seems to be "D"
upvoted 8 times

Angarali Most Recent 5 months, 2 weeks ago
Selected Answer: D
D is the correct answer
upvoted 2 times

larteyotoo 9 months ago
D is correct
upvoted 3 times

mikl 9 months, 2 weeks ago
Selected Answer: D
Correct answer.

D. From Software updates, view the Per update ring deployment state.
upvoted 1 times

b3arb0yb1m 9 months, 2 weeks ago
D. From Software updates, view the Per update ring deployment state.
upvoted 1 times

encxorblood 1 year ago
D - a computer is the question
To view more details, select Monitor. Then below Software updates, select Per update ring deployment state and choose the deployment

ring to review.
upvoted 3 times

AnoniMouse 1 year, 4 months ago
A is the correct answer. I have just verified myself right now
upvoted 2 times

AnoniMouse 1 year, 4 months ago
Apparently I was wrong! The answer provided is correct
upvoted 6 times

Merma 1 year, 5 months ago
D. is correct. Another helpful link:
https://docs.microsoft.com/en-us/mem/intune/fundamentals/reports
upvoted 3 times

AzZnLuVaBol 1 year, 7 months ago
D. is correct.

Sign in to Microsoft Endpoint Manager admin center.

Select Devices > Overview > Software update status. You can see general information about the status of any update rings you assigned.
upvoted 3 times

BobF 1 year, 8 months ago
This practice questions is only 40% valid. I failed this exam earlier.
upvoted 3 times

cankayahmet 1 year, 8 months ago
Have you check discussions because some given answers are not correct.
upvoted 13 times

Question #47 *Topic 2*

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

You plan to use Windows Autopilot to configure the Windows 10 devices shown in the following table.

Name	Memory	TPM
Device1	16 GB	*None*
Device2	8 GB	Version 1.2
Device3	4 GB	Version 2.0

Which devices can be configured by using Windows Autopilot self-deploying mode?

A. Device2 and Device3 only

B. Device3 only

C. Device2 only

D. Device1, Device2, and Device3

Correct Answer: *B*

Self-deploying mode uses a device's TPM 2.0 hardware to authenticate the device into an organization's Azure AD tenant. Therefore, devices without TPM 2.0 can't be used with this mode.

Reference:

https://docs.microsoft.com/en-us/windows/deployment/windows-autopilot/self-deploying

Perycles Highly Voted 1 year, 3 months ago

answer is correct . physicalT PM2.0 is required for Autopilot self deployement. So trying this method on VM doesn't work :)

upvoted 9 times

Testtest123 Highly Voted 1 year, 5 months ago

Answer B is correct.
https://docs.microsoft.com/en-us/windows/deployment/windows-autopilot/self-deploying

upvoted 5 times

AnoniMouse 1 year, 4 months ago

You are correct
https://docs.microsoft.com/en-us/mem/autopilot/self-deploying#requirements

Requirements
Self-deploying mode uses a device's TPM 2.0 hardware to authenticate the device into an organization's Azure AD tenant. Therefore, devices without TPM 2.0 can't be used with this mode. Devices must also support TPM device attestation. All new Windows devices should meet these requirements. The TPM attestation process also requires access to a set of HTTPS URLs that are unique for each TPM provider. For more information, see the entry for Autopilot self-Deploying mode and Autopilot pre-provisioning in Networking requirements.

upvoted 2 times

MR_Eliot Most Recent 5 months ago

Selected Answer: B

Self-deploying mode uses a device's TPM 2.0 hardware to authenticate the device into an organization's Azure AD tenant. Therefore, devices without TPM 2.0 can't be used with this mode.

upvoted 2 times

mikl 9 months, 2 weeks ago

Self-deploying mode uses a device's TPM 2.0 hardware to authenticate the device into an organization's Azure AD tenant. Therefore, devices without TPM 2.0 can't be used with this mode.

upvoted 5 times

b3arb0yb1m 9 months, 2 weeks ago

B. Device3 only

upvoted 1 times

RamazanInce 1 year ago

elf-deploying mode uses a device's TPM 2.0 hardware to authenticate the device into an organization's Azure AD tenant. Therefore, devices without TPM 2.0 can't be used with this mode.

upvoted 4 times

Alexbz 1 year, 5 months ago

Answer is correct.
From the link: Self-deploying mode uses a device's TPM 2.0 hardware to authenticate the device into an organization's Azure AD tenant. Therefore, devices without TPM 2.0 can't be used with this mode.

upvoted 1 times

HOTSPOT -

Your network contains an on-premises Active Directory forest named contoso.com that syncs to Azure Active Directory (Azure AD). Azure AD contains the users shown in the following table.

Name	Source	Member of
User1	Azure AD	Group1
User2	Windows Active Directory	Group2

You assign Windows 10 Enterprise E5 licenses to Group1 and User2.

You add computers to the network as shown in the following table.

Name	Operating system	Joined to
Computer1	Windows 10 Pro	Azure AD
Computer2	Windows 10 Pro	Active Directory
Computer3	Windows 8.1	Active Directory

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 signs in to Computer1, Computer1 will be upgraded to Windows 10 Enterprise E5 automatically.	○	○
If User2 signs in to Computer2, Computer2 will be upgraded to Windows 10 Enterprise E5 automatically.	○	○
If User2 signs in to Computer3, Computer3 will be upgraded to Windows 10 Enterprise E5 automatically.	○	○

Correct Answer:

Answer Area

Statements	Yes	No
If User1 signs in to Computer1, Computer1 will be upgraded to Windows 10 Enterprise E5 automatically.	○	○
If User2 signs in to Computer2, Computer2 will be upgraded to Windows 10 Enterprise E5 automatically.	○	○
If User2 signs in to Computer3, Computer3 will be upgraded to Windows 10 Enterprise E5 automatically.	○	○

Box 1: Yes -

Computer 1 is directly connected to Azure AD.

Box 2: Yes -

Computer 2 is Hybrid Azure AD connected.

Box 3: No -

User2 is not in Azure Active Directory.

Reference:

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

Mosquat Highly Voted 1 year, 4 months ago

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

Organizations that have an Enterprise agreement can also benefit from the new service, using traditional Active Directory-joined devices. In this scenario, the Active Directory user that signs in on their device must be synchronized with Azure AD using Azure AD Connect Sync.

The question description states that the domain syncs with Azure AD - therefore the answer should be Y-Y-N

upvoted 26 times

Merma 1 year, 4 months ago

You're correct the answer should be YYN.

upvoted 3 times

Wilf32 1 year, 4 months ago

I agree, if i get this question on the exam i will answer YYN

upvoted 3 times

RodrigoT 6 months ago

Yes, and this will be confirmed on the page 11 Question #66 (The last question of the page):
https://www.examtopics.com/exams/microsoft/md-101/view/11/

upvoted 2 times

FleurJ 1 year, 2 months ago

https://docs.microsoft.com/en-us/windows/deployment/windows-10-subscription-activation
(No)
Devices must be Azure AD-joined or Hybrid Azure AD joined. Workgroup-joined or Azure AD registered devices are not supported.
(Yes)
Organizations that have an Enterprise agreement can also benefit from the new service, using traditional Active Directory-joined devices. In this scenario, the Active Directory user that signs in on their device must be synchronized with Azure AD using Azure AD Connect Sync.

=> In this case, it is not clear that the company has Enterprise Agreement. Basically the requirement is Azure AD-joined or Hybrid Azure AD joined. Since the Computer2 is Active Directory joined, it won't be automatically upgraded.

Licensing-Microsoft-365.pdf:
Microsoft 365 E3 and E5 is available through the Enterprise Agreement, Enterprise Agreement Subscription, Microsoft Products and Services Agreement (MPSA) for commercial and government customers, and in the Cloud Solution Provider (CSP) program for customers with cloud-only deployments.

I would vote for Yes-No-No.

upvoted 4 times

Solaris2002 1 year ago

This is correct the environment I work in the users are assigned a Win10 E5 license and the devices are joined to on-prem AD and *synced* to Azure AD and the license works fine. Therefore the answer is YYN

upvoted 7 times

N0peasaurus Most Recent 2 months, 4 weeks ago

Y, Y, N
Read the Scenarios
https://docs.microsoft.com/en-us/windows/deployment/windows-10-subscription-activation#how-it-works

upvoted 2 times

MR_Eliot 5 months ago

YES, YES, NO

Subscription Activation for Windows 10/11 Enterprise
Windows 10/11 Enterprise E3 and Windows 10/11 Enterprise E5 are available as online services via subscription. Deploying Windows 10 Enterprise or Windows 11 Enterprise in your organization can now be accomplished with no keys and no reboots.

If you are running Windows 10, version 1703 or later:

Devices with a current Windows 10 Pro license or Windows 11 Pro license can be seamlessly upgraded to Windows 10 Enterprise or Windows 11 Enterprise, respectively.
Product key-based Windows 10 Enterprise or Windows 11 Enterprise software licenses can be transitioned to Windows 10 Enterprise and Windows 11 Enterprise subscriptions.
Organizations that have an Enterprise agreement can also benefit from the new service, using traditional Active Directory-joined devices. In this scenario, the Active Directory user that signs in on their device must be synchronized with Azure AD using Azure AD Connect Sync.

upvoted 1 times

Angarali 5 months, 2 weeks ago

Yes
Yes
No

upvoted 1 times

erwiense 8 months ago

YES-YES-NO
All Windows 10 computers are synced to the Azure AD, Computer 1 is directly connected to Azure AD and Computer 2 is Hybrid Azure AD connected.

Windows 10/11 Enterprise E3 and Windows 10/11 Enterprise E5 are available as online services via subscription. Deploying Windows 10 Enterprise or Windows 11 Enterprise in your organization can now be accomplished with no keys and no reboots.

source :
https://docs.microsoft.com/en-us/windows/deployment/windows-10-subscription-activation#subscription-activation-for-windows-1011-enterprise

upvoted 3 times

moobdoob 8 months, 2 weeks ago

YES, YES, NO

upvoted 1 times

MZONDERL 8 months, 3 weeks ago

The anwer could be correct, when reading:

Your network contains an on-premises Active Directory forest named contoso.com that syncs to Azure Active Directory (Azure AD). Azure AD contains the users shown in the following table.

Yes, there is a sync, but it says Azure AD contains the following users in the table, so it is possible that User 2 is not synct to Azure AD. When not synct to Azure AD, the answer is correct.

upvoted 1 times

RodrigoT 6 months ago

But the license is applied directly to User2. So, for me Y Y N.

upvoted 1 times

IykeP 8 months, 3 weeks ago

Apologies. The Correct Answer is: YES, YES, NO.
Organizations that have an Enterprise agreement can also benefit from the new service, using traditional Active Directory-joined devices. In this scenario, the Active Directory user that signs in on their device must be synchronized with Azure AD using Azure AD Connect Sync.

upvoted 2 times

IykeP 8 months, 3 weeks ago

I stand by this Answer: YES, NO, NO. Even if a device syncs doesn't mean its going to upgrade. The device is on-premise and not in the cloud environment.

upvoted 1 times

IykeP 8 months, 3 weeks ago

Apologies. The Correct Answer is: YES, YES, NO.
Organizations that have an Enterprise agreement can also benefit from the new service, using traditional Active Directory-joined devices. In this scenario, the Active Directory user that signs in on their device must be synchronized with Azure AD using Azure AD Connect Sync.

upvoted 1 times

RodrigoT 6 months ago

But the license is applied directly to User2. So, for me Y Y N.

upvoted 1 times

b3arb0yb1m 9 months, 2 weeks ago

Yes
Yes - because there is Azure sync.
No

upvoted 2 times

handsofthelp 9 months, 3 weeks ago

After of thinking a lot, my answer is YES YES NO.
YES: User 1 is in Group 1 and Azure AD with E5 license, Computer 1 is Azure AD as well. So it is, Yes.
YES: User 2 have E5 license and is in AD. The syncing should work. Computer 2 is AD also but, if user logs in, it means Hybrid Azure AD Join is done. The upgrade does qualify.
NO: Computer 3 is Windows 8.1, the upgrade is only wipe-and-load.

upvoted 3 times

jorlloen 1 year, 1 month ago

I read requirements for Enterprise activation, (https://docs.microsoft.com/en-us/windows/deployment/windows-10-subscription-activation) and:
Devices must be Azure AD-joined or Hybrid Azure AD joined. Workgroup-joined or Azure AD registered devices are not supported.
I think that the correct answers ara YNN

upvoted 3 times

Perycles 1 year, 3 months ago

YES, NO ,NO. in "modern subscription activation", Enterprise licence E3/E5 or A3/5 should be assign to a AZURE AD user (not ADDS user). After that, to take effect, this user should log in a Azure AD joined or Hybrid Azure AD computer to transform Pro licence to Enterprise Licence. So login on ADDS computer takes no effect.

upvoted 3 times

Perycles 1 year, 3 months ago

after reading again, active directory is sync to azure ad. Si user 2 and computer 2 exist on azure AD; Adding a licence enterprise E5 to user2 should work. so for me it's YES YES NO

upvoted 7 times

Tomtom11 1 year, 4 months ago

Answers are correct as User 2 is not in Azure

upvoted 1 times

mikl 9 months, 2 weeks ago

But there are sync in place?

upvoted 1 times

Tomtom11 1 year, 4 months ago

Requirments:
Organizations that have an Enterprise agreement can also benefit from the new service, using traditional Active Directory-joined devices. In this scenario, the Active Directory user that signs in on their device must be synchronized with Azure AD
Windows 10 (Pro or Enterprise) version 1703 or later installed on the devices to be upgraded.
Azure Active Directory (Azure AD) available for identity management.
Devices must be Azure AD-joined or Hybrid Azure AD joined. Workgroup-joined or Azure AD registered devices are not supported.

upvoted 1 times

Tomtom11 1 year, 4 months ago

The device is AAD joined
When a licensed user signs in to a device that meets requirements using their Azure AD credentials, the operating system steps up from Windows 10 Pro to Windows 10 Enterprise (or Windows 10 Pro Education to Windows 10 Education) and all the appropriate Windows 10 Enterprise/Education features are unlocked. When a user's subscription expires or is transferred to another user, the device reverts seamlessly to Windows 10 Pro / Windows 10 Pro Education edition, once current subscription validity expires.

upvoted 1 times

Jvp21 1 year, 4 months ago

In order to upgrade a computer with Windows Pro to Windows Enterprise using E5 license, the license is assigned to the user and not to a group - N, N, N.
Please explain if there are other details I am not having attention, thanks.

upvoted 1 times

AnoniMouse 1 year, 4 months ago

You can assign a license to a group and this is supported. What isn't supported is a nested group. So if you assign the license to Group1 only direct users of group1 are licensed. If group1 contains other groups, say Group2 and user2 isn't a direct member of group1 he/she won't get the license

upvoted 2 times

Question #49 *Topic 2*

HOTSPOT -

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

Name	Role
User1	*None*
User2	Global administrator
User3	Cloud device administrator
User4	Intune administrator

You configure the following device settings for the tenant:

- Users may join devices to Azure AD: User1
- Additional local administrators on Azure AD joined devices: None

You install Windows 10 on a computer named Computer1.

You need to identify which users can join Computer1 to adatum.com, and which users will be added to the Administrators group after joining adatum.com.

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

Users who can join Computer1 to adatum.com:
- User1 only
- User1 and User2 only
- User1, User2, and User3 only
- User1, User3, and User 4 only
- User1, User2, User3, and User4

Users who will be added to the Administrators group after joining adatum.com:
- User1 only
- User2 only
- User1 and User2 only
- User3 and User4 only
- User2, User3, and User4 only

Correct Answer:

Answer Area

Users who can join Computer1 to adatum.com:
- User1 only
- User1 and User2 only
- User1, User2, and User3 only
- User1, User3, and User 4 only
- User1, User2, User3, and User4

Users who will be added to the Administrators group after joining adatum.com:
- User1 only
- User2 only
- User1 and User2 only
- User3 and User4 only
- User2, User3, and User4 only

Reference:

https://docs.microsoft.com/en-us/azure/active-directory/devices/assign-local-admin

Alexbz Highly Voted 1 year, 5 months ago

Correct
When you connect a Windows device with Azure AD using an Azure AD join, Azure AD adds the following security principals to the local administrators group on the device:
The Azure AD global administrator role
The Azure AD device administrator role
The user performing the Azure AD join

upvoted 19 times

Perycles Highly Voted 1 year, 3 months ago

Correct, after several tests, only user (without role) is able to join Azure AD. Using A global admin account display an error. After that, global admin account have local admin rights on this device. so answer are correct.

upvoted 12 times

RodrigoT 5 months, 1 week ago

Exactly, because the "Additional local administrators on Azure AD joined devices: None" setting excludes the global admin from joining devices. We need to pay attention. Thank you for your tests.

upvoted 2 times

moobdoob Most Recent 8 months, 2 weeks ago

Given answer is correct.

upvoted 3 times

angelize 1 year, 3 months ago

Correct:
The only one that can add deivce to intune is User1 because they have configured Device Settings "Users may join devices to Azure AD: User1"
Read more about it https://docs.microsoft.com/en-us/azure/active-directory/devices/device-management-azure-portal

upvoted 6 times

RodrigoT 5 months, 1 week ago

Thank you for the link. More specific go to the anchor:
https://docs.microsoft.com/en-us/azure/active-directory/devices/device-management-azure-portal#configure-device-settings
and read the two points after the picture.

upvoted 1 times

Question #50 *Topic 2*

You use Microsoft Intune to manage client computers. The computers run one of the following operating systems:

- Windows 8.1
- Windows 10 Pro
- Windows 10 Enterprise
- Windows 10 Enterprise LTSC

You plan to manage Windows updates on the computers by using update rings.

Which operating systems support update rings?

A. Windows 10 Pro, Windows 10 Enterprise, and Windows 10 Enterprise LTSC only

B. Windows 8.1, Windows 10 Pro, Windows 10 Enterprise, and Windows 10 Enterprise LTSC

C. Windows 10 Enterprise and Windows 10 Enterprise LTSC only

D. Windows 10 Pro and Windows 10 Enterprise only

Correct Answer: *D*

Update ring policies are supported for devices that run Windows 10 version 1607 or later, and Windows 11

Incorrect:

The Long-Term Servicing Channel (LTSC) is designed for Windows 10 devices and use cases where the key requirement is that functionality and features don't change over time. Examples include medical systems (such as those used for MRI and CAT scans), industrial process controllers, and air traffic control devices.

These devices share characteristics of embedded systems: they are typically designed for a specific purpose and are developed, tested, and certified before use.

They are treated as a whole system and are, therefore, commonly ג€upgradedג€ by building and validating a new system, turning off the old device, and replacing it with the new, certified device

Reference:

https://docs.microsoft.com/en-us/mem/intune/protect/windows-update-for-business-configure

https://techcommunity.microsoft.com/t5/windows-it-pro-blog/ltsc-what-is-it-and-when-should-it-be-used/ba-p/293181

BLYBOI Highly Voted 1 year, 10 months ago

Update rings are supported for the following Windows 10 editions:
Windows 10 Pro
Windows 10 Enterprise
Windows 10 Team - for Surface Hub devices
Windows Holographic for Business

https://docs.microsoft.com/en-us/mem/intune/protect/windows-10-update-rings

upvoted 20 times

skalolaz 2 months, 3 weeks ago

Update rings are supported for the following Windows editions:

Windows 10/11 Pro

Windows 10/11 Enterprise

Windows 10/11 Team - for Surface Hub devices

Windows Holographic for Business

Windows Holographic for Business supports a subset of settings for Windows updates, including:

Automatic update behavior
Microsoft product updates
Servicing channel: Any update build that is generally available.
For more information, see Manage Windows Holographic.

Windows 10/11 Enterprise LTSC - While LTSC is supported, the following ring controls are not supported for LTSC:

Pause of Feature updates
Feature Update Deferral period (days)
Set feature update uninstall period (2 - 60 days)
Enable pre-release builds, which includes the following build options:
Windows Insider – Release Preview
Beta Channel
Dev Channel
Use deadline settings for Feature updates.

upvoted 2 times

Perycles Highly Voted 1 year, 3 months ago

answers are correct

upvoted 5 times

neobahamutk Most Recent 2 months, 2 weeks ago

Selected Answer: A

Correct answer is A.
Update rings are supported for the following Windows editions:
Windows 10/11 Pro
Windows 10/11 Enterprise
Windows 10/11 Team - for Surface Hub devices
Windows Holographic for Business
Windows Holographic for Business supports a subset of settings for Windows updates, including:
Automatic update behavior
Microsoft product updates
Servicing channel: Any update build that is generally available.
For more information, see Manage Windows Holographic.
Windows 10/11 Enterprise LTSC - While LTSC is supported, the following ring controls are not supported for LTSC:
Pause of Feature updates
Feature Update Deferral period (days)
Set feature update uninstall period (2 - 60 days)
Enable pre-release builds, which includes the following build options:
Windows Insider – Release Preview
Beta Channel
Dev Channel
Use deadline settings for Feature updates.
https://docs.microsoft.com/en-us/mem/intune/protect/windows-10-update-rings

upvoted 4 times

Deric 1 week, 4 days ago

I agree with Neobahamutk. The article he mentions is currently dated 06/08/22 and does state that Windows 10/11 Enterprise LTSC is supported, and that some ring control options are not supported for LTSC.

upvoted 3 times

TonySuccess 1 month ago

Agreed, seems to have updated to the above since the question set was released so although some of the below people were correct at the time, they are no longer correct. Answer A x

upvoted 3 times

anu21 2 months, 4 weeks ago

Selected Answer: A

Looks like update ring is supported for all WIN 10 editions
https://docs.microsoft.com/en-us/mem/intune/protect/windows-10-update-rings

upvoted 2 times

MR_Eliot 5 months ago

Selected Answer: D

D is indeed correct.

upvoted 1 times

moobdoob 8 months, 2 weeks ago

My vote is D

upvoted 1 times

mikl 9 months, 2 weeks ago

Selected Answer: D

D. Windows 10 Pro and Windows 10 Enterprise only

Update rings are supported for the following Windows editions:

Windows 10/11 Pro

Windows 10/11 Enterprise

Windows 10/11 Team - for Surface Hub devices

Windows Holographic for Business

upvoted 3 times

neobahamutk 2 months, 2 weeks ago

Windows 10/11 Enterprise LTSC is suported too.
https://docs.microsoft.com/en-us/mem/intune/protect/windows-10-update-rings

upvoted 2 times

b3arb0yb1m 9 months, 2 weeks ago

D. Windows 10 Pro and Windows 10 Enterprise only

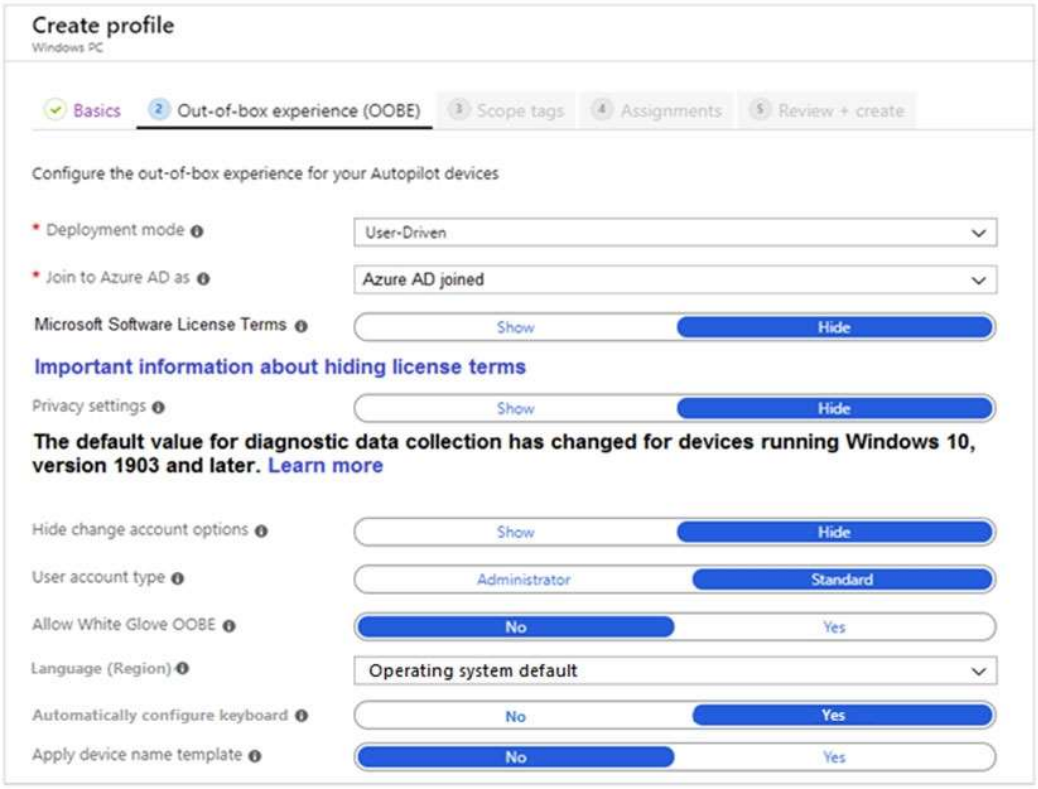
upvoted 1 times

Question #51 *Topic 2*

HOTSPOT -

You have a Microsoft Intune subscription.

You are creating a Windows Autopilot deployment profile named Profile1 as shown in the following exhibit. Profile1 will be deployed to Windows 10 devices.



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

Users who deploy a device by using Profile1 **[answer choice]**.

- are prevented from modifying any desktop settings
- can create additional local users on the device
- can modify the desktop settings for all device users
- can modify the desktop settings only for themselves

Users can configure the **[answer choice]** during the deployment.

- computer name
- Cortana settings
- keyboard layout

Correct Answer:

Answer Area

Users who deploy a device by using Profile1 **[answer choice]**.

- are prevented from modifying any desktop settings
- can create additional local users on the device
- can modify the desktop settings for all device users
- can modify the desktop settings only for themselves

Users can configure the **[answer choice]** during the deployment.

- computer name
- Cortana settings
- keyboard layout

Reference:

https://www.microsoftpressstore.com/articles/article.aspx?p=2453566

ANDREVOX Highly Voted 11 months, 3 weeks ago

Profile 1 wil create a Standard User on the device i.e. the user that Deploys the device via Profile 1 will have a Standard User Account created on the device, thus...
A Standard user account credentials allow a user to do things that affect only his or her account, including:
- Change or remove the password.
- Change the user account picture.
- Change the theme and desktop settings.
- View files stored in his or her personal folders and files in the Public folders.
Answer = Can modify the Desktop setting only for themselves.
And = Keyboard layout.

https://www.microsoftpressstore.com/articles/article.aspx?p=2453566

upvoted 17 times

[Removed] 6 months, 3 weeks ago

Are you sure? This is about customizations during the deployment process. Given the fact that the "Automatically configure keyboard" setting is configured as "Yes", the user wouldn't be able to make changes here (during deployment).
I would go for "Computer name" instead. The first part of the answer is clearly "Can modify the Desktop setting only for themselves."

upvoted 5 times

RodrigoT 6 months ago

In this link there is a LAB with the exact same scenario. There is also a demo video. It shows and says: "You should see the region selection screen, the keyboard selection screen, and the second keyboard selection screen".
https://docs.microsoft.com/en-us/windows/deployment/windows-autopilot/demonstrate-deployment-on-vm

upvoted 1 times

RodrigoT 5 months, 4 weeks ago

This question will repeat exactly the same on Page 17 Question #32 but the answers will be correct:
https://www.examtopics.com/exams/microsoft/md-101/view/17/
can modify desktop settings only for themselves
keyboard layout
This dump is full of erros, don't thrust the answers, study, study, study.

upvoted 1 times

mikl 9 months, 2 weeks ago

I totally agree.

upvoted 1 times

moobdoob Highly Voted 8 months, 2 weeks ago

My answer will be:
1. Can modify desktop settings only for themselves.
2. Computer name

upvoted 9 times

Angarali 5 months, 2 weeks ago

Get out of here. It will be keyboard layout instead for the second option.

Guys please don't make comments if you don't know and confuse everybody!

upvoted 3 times

NZS 5 months, 1 week ago

Alright, explain your reasoning. How would they change the keyboard settings if it's managed by the Autopilot profile?

upvoted 3 times

isatemelci Most Recent 1 week ago

The answer is:
-Can modify the Desktop setting only for themselves.
-computer name
because the keybord selection set to "Yes" and apply device name template is set to "NO", so you need to enter a computer name.

upvoted 2 times

MR_Eliot 5 months ago

Ready for the answer? See below:
1. Can modify the desktop settings only for themselves.
2. Cortana Settings

Why?
1. User is not administrator, but can still change his own desktop settings.
2. You need local administrator privileges to change the computer name. Since the computer name is not defined in Intune policy, the computer will get a random name.
Also after the first logon you will be prompted with Cortana settings.

upvoted 1 times

b3arb0yb1m 10 months, 3 weeks ago

Keyboard is set to automatic: Yes: It will not ask.
Apply device name template: No: It doesn't ask.
Cortana doesn't come up probably because of White Glove.

So~

upvoted 2 times

b3arb0yb1m 10 months, 3 weeks ago

Skip Cortana is on (and greyed) by default when creating a profile.

upvoted 1 times

RodrigoT 6 months ago

In this link there is a LAB with the exact same scenario. There is also a demo video. It shows and says: "You should see the region selection screen, the keyboard selection screen, and the second keyboard selection screen".
https://docs.microsoft.com/en-us/windows/deployment/windows-autopilot/demonstrate-deployment-on-vm

upvoted 1 times

FrancisLai 11 months, 1 week ago

I will go for answer below.

Can modify desktop settings only for themselves.
And = computer name (there has been a "no" for Apply device name template, so that means we do not specify a temperate to automatically register device name and users will be able to specify computer name themselves.)
Refer link https://docs.microsoft.com/en-us/mem/autopilot/profiles

upvoted 9 times

anzer123 11 months, 3 weeks ago

Or is it because of the standard account? Someone please help me with the correct answer

upvoted 1 times

anzer123 11 months, 3 weeks ago

Should be computer name

upvoted 2 times

mikl 9 months ago

You sure?

upvoted 1 times

Question #52 *Topic 2*

You have a computer named Computer1 that runs Windows 8.1.

You plan to perform an in-place upgrade of Computer1 to Windows 10 by using an answer file.

You need to identify which tool to use to create the answer file.

What should you identify?

A. System Configuration (Msconfig.exe)

B. Windows Configuration Designer

C. Windows System Image Manager (Windows SIM)

D. Windows Deployment Services (WDS)

Correct Answer: *C*

You can create Windows 10 Answer file using Windows System Image Manager (SIM).

Reference:

https://thesleepyadmins.com/2019/05/31/create-windows-10-answer-file/

Anthony_2770 Highly Voted 1 year, 8 months ago

Answer is Correct :
Windows System Image Manager (Windows SIM) is the tool that you use to create unattended Windows Setup answer files.
Windows SIM is included with the Windows ADK
You can create an answer file by using information from a Windows image (.wim) file and a catalog (.clg) file. Component settings are added to an appropriate configuration pass in the answer file. You can also add packages to be installed during Windows Setup.

upvoted 18 times

mikl 9 months, 2 weeks ago

Agree!

upvoted 1 times

MR_Eliot Most Recent 5 months ago

Selected Answer: C

C is correct.

upvoted 1 times

cor_ 6 months, 3 weeks ago

Selected Answer: C

C. Windows SIM can create unattended.xml, also known as 'answer file'

upvoted 1 times

RodrigoT 6 months ago

And by elimination since:
A. System Configuration (Msconfig.exe) has absolutely nothing to do with this
B. Windows Configuration Designer is for Provisioning Packages
C. Windows System Image Manager (Windows SIM) only option available
D. Windows Deployment Services (WDS) is for installing images.

upvoted 5 times

FlailingLimbs 1 week ago

Thanks for the breakdown with reasons why the others were not the right answer.

upvoted 1 times

moobdoob 8 months, 2 weeks ago

Given answer is correct.

upvoted 2 times

mikl 9 months, 2 weeks ago

Selected Answer: C

C. Windows System Image Manager (Windows SIM)

upvoted 3 times

mikl 9 months, 2 weeks ago

Windows System Image Manager (Windows SIM) is the tool that you use to create unattended Windows Setup answer files.

https://docs.microsoft.com/en-us/windows-hardware/customize/desktop/wsim/windows-system-image-manager-technical-reference

upvoted 1 times

b3arb0yb1m 9 months, 2 weeks ago

C. Windows System Image Manager (Windows SIM)

upvoted 1 times

Perycles 1 year, 3 months ago

Answer is C

upvoted 2 times

Timmi 1 year, 8 months ago

seems correct

https://docs.microsoft.com/en-us/windows-hardware/manufacture/desktop/update-windows-settings-and-scripts-create-your-own-answer-file-sxs

upvoted 4 times

Question #53 *Topic 2*

Your network contains an Active Directory domain. The domain contains 10 computers that run Windows 8.1 and use local user profiles.
You deploy 10 new computers that run Windows 10 and join the computers to the domain.
You need to migrate the user profiles from the Windows 8.1 computers to the Windows 10 computers.
What should you do?

A. From the Windows 8.1 computer of each user, run imagex.exe/capture, and then from the Windows 10 computer of each user, run imagex.exe/apply.

B. Configure roaming user profiles for the users. Instruct the users to first sign in to and out of their Windows 8.1 computer and then to sign in to their Windows 10 computer.

C. From the Windows 8.1 computer of each user, run scanstate.exe, and then from the Windows 10 computer of each user, run loadstate.exe.

D. Configure Folder Redirection for the users. Instruct the users to first sign in to and out of their Windows 8.1 computer, and then to sign in to their Windows 10 computer.

Correct Answer: *C*
The ScanState command is used with the User State Migration Tool (USMT) 10.0 to scan the source computer, collect the files and settings, and create a store.
Reference:
https://docs.microsoft.com/en-us/windows/deployment/usmt/usmt-scanstate-syntax https://docs.microsoft.com/en-us/windows/deployment/usmt/usmt-loadstate-syntax

vinnyct Highly Voted 1 year, 10 months ago
It's C
upvoted 12 times

pogap64757 Highly Voted 8 months ago
Reason why B is not the answer:

"Roaming user profiles in Windows 10, Windows Server 2016, and later versions are incompatible with roaming user profiles in earlier versions of Windows."

https://docs.microsoft.com/en-us/troubleshoot/windows-server/user-profiles-and-logon/roaming-user-profiles-versioning
upvoted 5 times

MR_Eliot Most Recent 5 months ago
Selected Answer: C
C is correct.
upvoted 1 times

moobdoob 8 months, 2 weeks ago
Correct answer is C.

scanstate.exe on each user
Upgrade OS
loadstate.exe on each user
upvoted 2 times

mikl 9 months, 2 weeks ago
C. From the Windows 8.1 computer of each user, run scanstate.exe, and then from the Windows 10 computer of each user, run loadstate.exe.
upvoted 1 times

b3arb0yb1m 9 months, 2 weeks ago
C. From the Windows 8.1 computer of each user, run scanstate.exe, and then from the Windows 10 computer of each user, run loadstate.exe.
upvoted 1 times

Perycles 1 year, 3 months ago
For sure is correct.
upvoted 3 times

Layer8 1 year, 4 months ago
I assume the reason roaming profiles won't work is because the users have already signed into all the windows 8.1 machines. therefore their roaming profiles won't be established on the network.
upvoted 2 times

Jeffoort 1 year, 7 months ago
Correct
upvoted 2 times

Question #54 *Topic 2*

You have computers that run Windows 8.1 or Windows 10. All the computers are enrolled in Microsoft Intune, Endpoint Configuration Manager, and Desktop
Analytics. Co-management is enabled for your environment.
You plan to upgrade the Windows 8.1 computers to Windows 10.
You need to identify which Windows 8.1 computers do NOT have supported Windows 10 drivers.
What should you use?

A. the General Hardware Inventory report in Configuration Manager

B. the List of devices in a specific device category report in Configuration Manager

C. Deployment plans in Desktop Analytics

D. the Device compliance report in Intune

Correct Answer: *C*
Desktop Analytics collects and analyzes device, application, and driver data in your organization. Based on this analysis and your input, you can use the service to create deployment plans for Windows 10. Deployment plans have the following features:
* Drivers:
See the list of drivers included with this deployment plan. Set the Upgrade decision, review Microsoft's recommendation, and see compatibility risk factors.
* etc.
Reference:
https://docs.microsoft.com/en-us/mem/configmgr/desktop-analytics/about-deployment-plans

Anthony_2770 Highly Voted 1 year, 7 months ago
Desktop Analytics collects and analyzes device, application, and driver data in your organization. Based on this analysis and your input, you can use the service to create deployment plans for Windows 10.
upvoted 35 times

TrustMebro 9 months, 2 weeks ago
Thank you for always giving the answers and confirmations !
upvoted 2 times

RodrigoT 5 months, 1 week ago
And here is the proof:
https://docs.microsoft.com/en-us/mem/configmgr/desktop-analytics/about-deployment-plans#readiness-rules
upvoted 3 times

Perycles Highly Voted 1 year, 3 months ago
C : desktop analytics for sure.
upvoted 5 times

b3arb0yb1m Most Recent 9 months, 2 weeks ago
C. Deployment plans in Desktop Analytics
upvoted 1 times

Question #55 *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 computer that runs Windows 8.1.
Two days ago, you upgraded the computer to Windows 10.
You need to downgrade the computer to Windows 8.1.
Solution: From the Settings app, you use the Recovery options.
Does this meet the goal?

A. Yes

B. No

Correct Answer: *A*
Windows 10 supports a ɹ€Rollbackɹ€ feature that allows you to go back (recover) to the version of Windows (Windows 10, Windows 7 or Windows 8.1) installed on your PC prior to upgrading to the latest version of Windows 10 or Windows 7 / 8.1
1) Click on Start > Settings >
2) In the Windows Setting options click on Update & security
3) In the column of option on the left side of Windows Update click on the 'Recovery' option.
4) Click on 'Get started' to start the Recovery / Rollback process
5) Etc.
Reference:
https://answers.microsoft.com/en-us/windows/forum/windows_10-windows_install/how-to-recover-restore-your-previous-version-of/94368560-9c64-4387-92b9-82a9234216ad

KiwE 1 month ago
Threadlink isn't working as of now for the answer
upvoted 1 times

mikl 9 months, 2 weeks ago
Selected Answer: A
Think A is valid.

Select the Start button > Settings > Update & Security > Recovery. Under Go back to the previous version of Windows 10,Go back to Windows 8.1, select Get started. By following the prompts, you'll keep your personal files but remove apps and drivers installed after the upgrade, plus any changes you made to settings.

https://support.microsoft.com/en-us/windows/go-back-to-windows-8-1-40e2d7dc-f640-b0e5-56e1-b41a27e28533
upvoted 4 times

Merma 1 year, 5 months ago
A is correct. Note: The option to go back to your previous version of Windows is available only for a limited time following the upgrade (10 days, in most cases).
Select the Start button > Settings > Update & Security > Recovery. Under Go back to the previous version of Windows 10, Go back to Windows 8.1, select Get started.
https://support.microsoft.com/en-us/search?query=how%20to%20rollback%20to%20previous%20version%20of%20windows
upvoted 4 times

DJHASH786 1 year, 6 months ago
From the Settings App, you then goto UPDATE AND SECURITY and then click Recovery... Answer is incomplete ..
upvoted 4 times

Slammer900 1 year, 5 months ago
so is it still yes then?
upvoted 2 times

petir 1 year, 5 months ago
A is correct. Recovery options are still within the Settings app they jsut didn't include the step by step path
upvoted 1 times

Perycles 1 year, 3 months ago
you 're right, Microsoft doesn't use to put the exact path. Just retain it's under Setting path.so answer is correct.
upvoted 2 times

Question #56 *Topic 2*

Note: This question is part of a series of questions that present the same scenario. Each question in the series contains a unique solution that might meet the stated goals. Some question sets might have more than one correct solution, while others might not have a correct solution.
After you answer a question in this section, you will NOT be able to return to it. As a result, these questions will not appear in the review screen.
You have a computer that runs Windows 8.1.
Two days ago, you upgraded the computer to Windows 10.
You need to downgrade the computer to Windows 8.1.
Solution: You restart the computer to Windows Recovery Environment (Windows RE) and use the Advanced options.
Does this meet the goal?

A. Yes

B. No

Correct Answer: *B*
Instead: From the Settings app, you use the Recovery options.
Note: Windows 10 supports a ɹ€Rollbackɹ€ feature that allows you to go back (recover) to the version of Windows (Windows 10, Windows 7 or Windows 8.1) installed on your PC prior to upgrading to the latest version of Windows 10 or Windows 7 / 8.1
1) Click on Start > Settings >
2) In the Windows Setting options click on Update & security
3) In the column of option on the left side of Windows Update click on the 'Recovery' option.
4) Click on 'Get started' to start the Recovery / Rollback process
5) Etc.
Reference:
https://answers.microsoft.com/en-us/windows/forum/windows_10-windows_install/how-to-recover-restore-your-previous-version-of/94368560-9c64-4387-92b9-82a9234216ad

Perycles Highly Voted 1 year, 3 months ago
just tested on W8.1 > Upgrade to W10. After upgrade completed , restart in WinRE. From winRE > Avanced Options > uninstall last Features Updates . Computer restart, uninstalls W10 and i could log on win 8.1 :) so answer is YES YES YES.
upvoted 21 times

Fourbell Highly Voted 1 year, 2 months ago
answer is YES
Two methods are avalable :
https://answers.microsoft.com/en-us/windows/forum/windows_10-windows_install/how-to-recover-restore-your-previous-version-of/94368560-9c64-4387-92b9-82a9234216ad
upvoted 7 times

MitchF Most Recent 2 months, 2 weeks ago
This Microsoft doc says the answer should be "YES"
https://answers.microsoft.com/en-us/windows/forum/all/cant-roll-back-to-win-10/145b5900-420f-4685-a12a-3f8efb25ef36

Here is how:
"Reset this PC and Go back buttons in Settings > System > Recovery do not function. Reset and roll back can be accessed from the Windows Recovery Environment by selecting System > Recovery > Advanced startup, and pressing Restart now. Once in Windows Recovery, choose Troubleshoot.
Choose Reset this PC to perform a reset.
Choose Advanced options > Uninstall Updates > Uninstall latest feature update to perform a rollback."
upvoted 1 times

MR_Eliot 5 months ago
Selected Answer: A
Answer is A.
upvoted 1 times

NZS 5 months, 1 week ago
The answer is definitely YES
upvoted 1 times

Moderator 6 months ago
Selected Answer: A
Should work, when I read this: https://answers.microsoft.com/en-us/windows/forum/all/how-to-recover-restore-your-previous-version-of/94368560-9c64-4387-92b9-82a9234216ad?auth=1
upvoted 1 times

bumbomele 6 months, 3 weeks ago
https://support.microsoft.com/en-us/windows/go-back-to-windows-8-1-40e2d7dc-f640-b0e5-56e1-b41a27e28533#:~:text=Select%20the%20Start%20button%20%3E%20Settings,changes%20you%20made%20to%20settings.

NO
upvoted 1 times

mayleni 8 months, 2 weeks ago

Selected Answer: A

Tested and answer is yes

upvoted 5 times

moobdoob 8 months, 2 weeks ago

Selected Answer: A

Tested this in lab enviroment, answer is YES.

upvoted 5 times

mikl 9 months, 2 weeks ago

Answer is yes.

https://www.thewindowsclub.com/uninstall-latest-quality-or-feature-update

upvoted 2 times

rovert94 10 months, 1 week ago

Selected Answer: A

I think the answer is yes

upvoted 4 times

BLYBOI 1 year, 4 months ago

https://support.microsoft.com/en-us/windows/go-back-to-windows-8-1-40e2d7dc-f640-b0e5-56e1-b41a27e28533#:~:text=Select%20the%20Start%20button%20%3E%20Settings,changes%20you%20made%20to%20settings.

upvoted 2 times

Merma 1 year, 5 months ago

As mentioned by Wilf32 accessing the troubleshooting menu is need to rollback or downgrade to a previous version of Windows.
"Uninstall Updates
Removing the latest updates recently installed to Windows 10 can be a good troubleshooting step if you are having trouble starting your PC or if you are having trouble uninstalling something within Windows 10. Simply select Uninstall latest quality update or Uninstall latest feature update to uninstall the desired update from WinRE with just a couple of steps. Please note; however, that you should reapply the latest updates as soon as possible to help keep your devices protected and productive."
https://techcommunity.microsoft.com/t5/windows-it-pro-blog/windows-recovery-environment-explained/ba-p/2273533

upvoted 2 times

Technik 1 year, 5 months ago

In the advanced option select 'go back to the previous build' which will restore win 8.1.

Think the answer should be yes

upvoted 3 times

Wilf32 1 year, 5 months ago

This is a tricky one to answer as there an many questions im MD-100 and MD-101 set out so that you know which menu to go into. If the question asked "You restart the computer to Windows Recovery Environment (Windows RE) **in troubleshooting menu** you use the Advanced options." it would be a solid YES, the key part being within the troubleshooting menu.

Im not sure how pedantic Microsoft would be about this.... but using the link from the next question i could be swayed to say the answer to this question is YES

https://answers.microsoft.com/en-us/windows/forum/windows_10-windows_install/how-to-recover-restore-your-previous-version-of/94368560-9c64-4387-92b9-82a9234216ad

upvoted 6 times

Danohav 1 year, 4 months ago

You are right, but this applies only if the OS has the same version = Win10 to Win10 = removing feature update among Win10 version. Please correct me if I am wrong. But i only found this:
https://support.microsoft.com/en-us/windows/go-back-to-windows-8-1-40e2d7dc-f640-b0e5-56e1-b41a27e28533#:~:text=Select%20the%20Start%20button%20%3E%20Settings,changes%20you%20made%20to%20settings.
= you would need a Win8.1 installation media created with Windows MCT (MediaCreationTool)

upvoted 2 times

Kryan 1 year, 6 months ago

yes,
https://www.yourwindowsguide.com/2018/10/rollback-windows-10-version-1803-upgrading-version-1809.html

upvoted 3 times

Question #57 *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 computer that runs Windows 8.1.
Two days ago, you upgraded the computer to Windows 10.
You need to downgrade the computer to Windows 8.1.
Solution: From Windows Update in the Settings app, you use the Advanced options.
Does this meet the goal?

A. Yes

B. No

Correct Answer: *B*
Instead: From the Settings app, you use the Recovery options.
Note: Windows 10 supports a ɹ€Rollbackɹ€ feature that allows you to go back (recover) to the version of Windows (Windows 10, Windows 7 or Windows 8.1) installed on your PC prior to upgrading to the latest version of Windows 10 or Windows 7 / 8.1
1) Click on Start > Settings >
2) In the Windows Setting options click on Update & security
3) In the column of option on the left side of Windows Update click on the 'Recovery' option.
4) Click on 'Get started' to start the Recovery / Rollback process
5) Etc.
Reference:
https://answers.microsoft.com/en-us/windows/forum/windows_10-windows_install/how-to-recover-restore-your-previous-version-of/94368560-9c64-4387-92b9-82a9234216ad

Whatsamattr81 3 months, 2 weeks ago
I think the answer is yes, the upgrade process should have created a restore point, and you can get to restore points from the advanced options under Settings / Windows Update / Advanced Options. No different than doing a recovery from a Windows RE environment.
upvoted 1 times

morito 7 months, 3 weeks ago
Selected Answer: A
Answer is (at least partially) correct when using Windows 11. Settings -> Windows Update -> Advanced Options -> Recovery -> Go Back
upvoted 2 times

RodrigoT 5 months ago
The exam is about Windows 10, not Windows 11.
upvoted 4 times

blitzyx 8 months, 1 week ago
On Windows 11 under Settings > Windows Update > Advanced options, there is an option that takes you to Recovery where you can go back to an older version. So if this question was W11 related, I would say the answer is yes.
upvoted 2 times

moobdoob 8 months, 2 weeks ago
Answer is no.
upvoted 1 times

mikl 9 months, 2 weeks ago
Answer is no - you can't uninstall from Windows Update.
upvoted 1 times

rovert94 10 months, 1 week ago
Selected Answer: B
The answer is NO because you would go under Settings > Update & Security > Recovery, NOT Windows Update.
upvoted 3 times

MikeMatt2020 1 year, 4 months ago
What an absolutely garbage question. How nonspecific is "Advanced Options"

- Do they mean "Advanced Options" under Update & Security > Windows Update? If so, I don't see an option to rollback

- Booting to Windows RE will work
- Navigating to Update & Security > Recovery will also work
upvoted 4 times

tf444 1 year ago
Yes, that is what the q is asking "setting up"!
Hello!!!!
upvoted 1 times

lucidgreen 1 year, 7 months ago

https://support.microsoft.com/en-us/windows/go-back-to-windows-8-1-40e2d7dc-f640-b0e5-56e1-b41a27e28533#:~:text=Select%20the%20Start%20button%20%3E%20Settings,changes%20you%20made%20to%20settings.
Settings>Update & Security > Recovery
Go back to previous version, etc.

upvoted 3 times

Question #58 *Topic 2*

DRAG DROP -

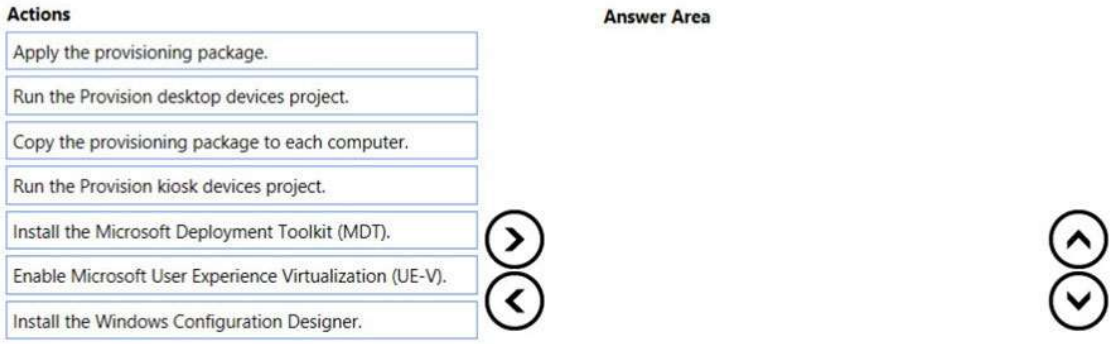
You have five computers that runs Windows 10.

You need to create a provisioning package to configure the computers to meet the following requirements:

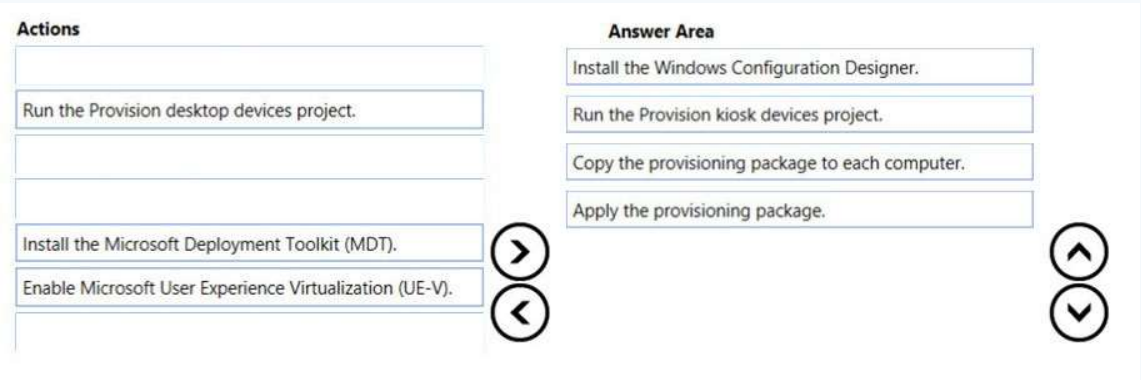
- Run an interactive app.
- Automatically sign in by using a local user account.
- Prevent users from accessing the desktop and running other applications.

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:



Correct Answer:



Step 1: Install Windows Configuration Designer

On devices running Windows client, you can install the Windows Configuration Designer app from the Microsoft Store.

Step 2: Run the Provision kiosk devices project.

A single-app kiosk uses the Assigned Access feature to run a single app above the lock screen. When the kiosk account signs in, the app is launched automatically. The person using the kiosk cannot do anything on the device outside of the kiosk app.

Step 3: Copy the provisioning package to each computer.

Provisioning packages can be applied to client devices during the first-run experience (out-of-box experience or "OOBE") and after ("runtime").

Step 4: Apply the provisioning package.

Apply the provisioning package to a device running Windows client.

Reference:

https://docs.microsoft.com/en-us/windows/configuration/provisioning-packages/provisioning-install-icd https://docs.microsoft.com/en-us/windows/configuration/kiosk-single-app

Perycles Highly Voted 1 year, 3 months ago

all is right :)

upvoted 10 times

Merma Highly Voted 1 year, 4 months ago

The given answer seems correct.
A single-app kiosk uses the Assigned Access feature to run a single app above the lockscreen.
When the kiosk account signs in, the app is launched automatically. The person using the kiosk cannot do anything on the device outside of the kiosk app.
https://docs.microsoft.com/en-us/windows/configuration/kiosk-single-app
https://docs.microsoft.com/en-us/windows/configuration/provisioning-packages/provisioning-install-icd

upvoted 5 times

moobdoob Most Recent 8 months, 2 weeks ago

Answer is correct.

upvoted 3 times

Cowok 1 year, 4 months ago

Seems it correct

upvoted 4 times

HOTSPOT -

You upgrade three computers from Windows 8.1 to Windows 10 as shown in the following table.

Name	Days since upgrade
Computer1	18
Computer2	9
Computer3	3

The in-place upgrade settings used to perform the upgrade are shown in the following table.

Name	Setting
Computer1	Keep personal files and apps
Computer2	*None*
Computer3	Keep personal files and apps

After the upgrade, you perform the following actions on each computer:

- Add a local user account named LocalAdmin1.
- Install Microsoft Office 2019.

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
You can roll back Computer1 to Windows 8.1	○	○
You can roll back Computer2 to Windows 8.1	○	○
You can roll back Computer3 to Windows 8.1	○	○

Correct Answer:

Answer Area

Statements	Yes	No
You can roll back Computer1 to Windows 8.1	○	●
You can roll back Computer2 to Windows 8.1	●	○
You can roll back Computer3 to Windows 8.1	●	○

Box 1: No -

More than 10 days.

Reference:

https://support.microsoft.com/en-us/windows/go-back-to-windows-8-1-40e2d7dc-f640-b0e5-56e1-b41a27e28533

BLYBOI Highly Voted 1 year, 4 months ago

No, Yes, Yes,
https://support.microsoft.com/en-us/windows/go-back-to-windows-8-1-40e2d7dc-f640-b0e5-56e1-b41a27e28533

upvoted 41 times

Evilcoocie Highly Voted 1 year, 3 months ago

Isnt it:
NO (more than 10 days ago)
NO (deleted everything)
YES (within 10 days & kept all files)

upvoted 35 times

daonga 1 year ago

It isn't asking if you can get the user data back, only if you can roll it back to Windows 8.1.

Since it's been less then 10 days, should be Yes (so NYY)

upvoted 15 times

rej0088 1 year ago

None = Fresh Install , you cannot revert back to anything as Windows.old will not exist, so its NO NO YES

upvoted 4 times

NKG123 9 months, 3 weeks ago
Start by reading all the question including the context...
upvoted 3 times

jcgm1990 3 months ago
At least read the question right, where does it say fresh install???
upvoted 1 times

Dbomb 9 months, 2 weeks ago
you are right, if you look at the link provided it clearly says that if you opted to keep nothing you cant rollback
upvoted 3 times

RodrigoT 6 months, 3 weeks ago
I don't thrust that link, non official information. In my opinion Windows 10 ALWAYS creates a windows.old folder on a in place upgrade. But the only way to be certain is checking by my self in a VM because I didn't find any official information about this.
upvoted 4 times

Zero_0 1 month, 3 weeks ago
And? Have you tested?
upvoted 1 times

TonySuccess Most Recent 2 weeks, 5 days ago
No, Yes, Yes.

Please ignore people posting answers that are not correct.
upvoted 1 times

raduM 1 month, 4 weeks ago
no yes yes. you do not keep personal files and apps but in 10 days you can still roll back. your apps wil not be saved
upvoted 1 times

shaolin_monk 2 months ago
In Place upgrade, so
No (more than 10 days)
Yes (less than 10 days)
Yes (less than 10 days)
upvoted 2 times

Hisandy 4 months, 1 week ago
N.Y.Y
https://answers.microsoft.com/en-us/windows/forum/all/how-to-recover-restore-your-previous-version-of/94368560-9c64-4387-92b9-82a9234216ad
upvoted 1 times

moobdoob 8 months, 2 weeks ago
I'm going with NO NO YES.

Reasoning:
1. More than 10 days
2. Opted to wipe, therefore rollback option is not available.
3. Within 10 days, and opted to keep all files (Windows.old)
upvoted 4 times

RodrigoT 6 months, 3 weeks ago
And where did you read about a wipe on the second PC? The question says that all 3 where in place upgrade and that only the user data was not saved on the second computer.
upvoted 5 times

mikl 9 months, 2 weeks ago
The option to go back to your previous version of Windows is available only for a limited time following the upgrade (10 days, in most cases).

https://support.microsoft.com/en-us/windows/go-back-to-windows-8-1-40e2d7dc-f640-b0e5-56e1-b41a27e28533
upvoted 1 times

Nen0 10 months, 2 weeks ago
Correct answer is "No, Yes, Yes". System rollback availability lasts for 10 days.
upvoted 3 times

ANDREVOX 11 months ago
NO, YES, YES..!!

Please take note!
The question state that "The in-place upgrade settings used to perform the upgrade are shown in the following table."
On Computer 2 the setting is None - i.e. Nothing: Everything will be deleted, including files, app and Settings. This is equal to a clean install...
The Windows.old folder will always be created during a upgrade install, even if you choose the "Nothing" option. "If you choose to “Keep nothing” when you upgrade to Windows 8.1, or if you reset, refresh, or reinstall Windows, your personal files are temporarily saved to the Windows.old" with a 10 day limit to do so....

https://support.microsoft.com/en-us/windows/retrieve-files-from-the-windows-old-folder-f668ada4-701b-204a-73c3-952bc5ceb1c8

https://answers.microsoft.com/en-us/windows/forum/all/how-to-recover-restore-your-previous-version-of/94368560-9c64-4387-92b9-82a9234216ad
upvoted 8 times

NKG123 9 months, 3 weeks ago

What an imagination !!!

upvoted 1 times

mikl 9 months ago

What ?

upvoted 1 times

RodrigoT 5 months ago

Another link that confirms this:
https://www.tenforums.com/tutorials/148005-how-restore-files-windows-old-folder-windows-10-a.html
"If you choose to “Keep nothing”, personal files of users from their profile folder are temporarily saved to the Windows.old folder, and will be automatically deleted in 10 days after the date you upgraded by default. The Windows.old folder will also contain a copy of the previous Windows installation"

upvoted 3 times

BMAN101 1 year ago

Its Def NO NO YES
https://www.pcmag.com/how-to/computer-acting-up-how-to-uninstall-a-windows-10-update#:~:text=There's%20one%20catch%3A%20you%20can,can%20no%20longer%20roll%20back.

upvoted 2 times

RodrigoT 6 months, 3 weeks ago

Why not the second computer? Only the user data was not saved during the in place upgrade.

upvoted 1 times

RodrigoT 5 months ago

And your link is just about rollback feature updates, not Windows version.

upvoted 1 times

Rick_C137 1 year, 3 months ago

Anyone know why Computer1 would be a "Yes" based on the question and info provided in it?

upvoted 1 times

RodrigoT 6 months, 3 weeks ago

It's because this question is very old and at that time you had until 30 days to rollback. Now you just have 10 days.

upvoted 3 times

Perycles 1 year, 3 months ago

10 days max to rollback : NO, YES, YES

upvoted 4 times

Vizsgazo1 1 year, 4 months ago

No; Yes; Yes https://answers.microsoft.com/en-us/windows/forum/windows_10-windows_install/how-to-extend-the-10-day-limit-to-go-back-to-your/22a013b0-0096-46fe-8e70-a5cbbdedb1ce

upvoted 4 times

AnoniMouse 1 year, 4 months ago

Technically the answer should be NO NO NO, because you have added users and installed applications. But if removing the users and uninstalling the applications is implicit, then

NO - Upgraded 18 days ago and you only have 10
Yes
Yes

upvoted 3 times

RodrigoT 5 months ago

https://support.microsoft.com/en-us/windows/recovery-options-in-windows-31ce2444-7de3-818c-d626-e3b5a3024da5#bkmk_go_back_previous_version

Just remove any user accounts you added after the upgrade.

upvoted 1 times

Testtest123 1 year, 5 months ago

This should be
1 - No
2 - No
3- Yes

After 10 days it should not be available anymore.

upvoted 2 times

FlitZ 1 year, 3 months ago

That's correct, if you upgrade to windows 10 and you don't keep the files and data you won't be able to revert to Windows 8.1. Maybe this question is old because in the past you were able to revert de system max 30 days . Today that policy changed. You have max 10 days to change to the old operative system.

upvoted 3 times

Testtest123 1 year, 5 months ago

1 - No
2 - Yes
3- Yes

Ignore previous comment

upvoted 10 times

Linny75 1 year, 5 months ago

You can't roll back Computer1, upgrade happened more than 10 days ago. The question does not say anything about other requirements, so in my opinion you can roll back Computer2 and 3. You have to remove the newly created user and Office2019 will be gone, but you can rollback.
https://answers.microsoft.com/en-us/windows/forum/windows_10-windows_install/how-to-recover-restore-your-previous-version-of/94368560-9c64-4387-92b9-82a9234216ad

upvoted 4 times

1morenickname 1 year, 5 months ago

I agree. The link they provided is very old (2016). It has changed from 30 days to 10. https://support.microsoft.com/en-us/windows/go-back-to-windows-8-1-40e2d7dc-f640-b0e5-56e1-b41a27e28533

upvoted 2 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.
Your network contains an Active Directory domain. The domain contains member computers that run Windows 8.1 and are enrolled in Microsoft Intune.
You need to identify which computers can be upgraded to Windows 10.
Solution: From the Microsoft Endpoint Manager admin center, you create a device compliance policy and assign the policy to the computers. After 24 hours, you view the Device compliance report in Intune.
Does this meet the goal?

A. Yes

B. No

Correct Answer: *B*
Instead use the Microsoft Assessment and Planning Toolkit.
The Microsoft Assessment and Planning (MAP) toolkit is something that has been around for a long time, you might have used it to inventory your environment or used it recently to upgrade your desktops to Windows 10.
Note: Microsoft recommends that you use Azure Migrate to simplify your migration process. Azure Migrate provides discovery, assessment, and migration capabilities for applications, infrastructure, and data.
Reference:
https://www.techielass.com/using-maps-azure-readiness/

Perycles Highly Voted 1 year, 3 months ago

answer is NO : Compliance policy define conditions that device must fulfill in order to be compliant and able to access company resources.

upvoted 16 times

mikl 9 months, 2 weeks ago

Agree!

upvoted 1 times

moobdoob Most Recent 8 months, 2 weeks ago

Compliance policy has nothing to do with upgrade readyness, answer is NO.

upvoted 3 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.
Your network contains an Active Directory domain. The domain contains member computers that run Windows 8.1 and are enrolled in Microsoft Intune.
You need to identify which computers can be upgraded to Windows 10.
Solution: From Windows on the Devices blade of the Microsoft Endpoint Manager admin center, you create a filter and export the results as a CSV file.
Does this meet the goal?

A. Yes

B. No

Correct Answer: *B*
Instead use the Microsoft Assessment and Planning Toolkit.
The Microsoft Assessment and Planning (MAP) toolkit is something that has been around for a long time, you might have used it to inventory your environment or used it recently to upgrade your desktops to Windows 10.
Note: Microsoft recommends that you use Azure Migrate to simplify your migration process. Azure Migrate provides discovery, assessment, and migration capabilities for applications, infrastructure, and data.
Reference:
https://www.techielass.com/using-maps-azure-readiness/

Perycles Highly Voted 1 year, 3 months ago
answer is NO : export devices informations to csv doesn't give you hardware incompatibility, just a inventory of devices.
upvoted 12 times

moobdoob Most Recent 8 months, 2 weeks ago
Answer is NO.
upvoted 2 times

john909 11 months, 2 weeks ago
I think we're looking for Desktop Analytics > Deployment plans (https://docs.microsoft.com/en-us/mem/configmgr/desktop-analytics/about-deployment-plans)
upvoted 4 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.
Your network contains an Active Directory domain. The domain contains member computers that run Windows 8.1 and are enrolled in Microsoft Intune.
You need to identify which computers can be upgraded to Windows 10.
Solution: You install the Microsoft Assessment and Planning Toolkit. From the Microsoft Assessment and Planning Toolkit, you collect inventory data and run the
Windows 10 Readiness scenario.
Does this meet the goal?

A. Yes

B. No

Correct Answer: *A*
The Microsoft Assessment and Planning (MAP) toolkit is something that has been around for a long time, you might have used it to inventory your environment or used it recently to upgrade your desktops to Windows 10.
Note: Microsoft recommends that you use Azure Migrate to simplify your migration process. Azure Migrate provides discovery, assessment, and migration capabilities for applications, infrastructure, and data.
Reference:
https://www.techielass.com/using-maps-azure-readiness/

Perycles Highly Voted 1 year, 3 months ago
MAP Toolkit is a agentless tool. You download it, install a a device in your domain, enter credential to map other devices, start the scan. When the scan is completed, you can create a report based on W10 readiness assessment. so answer is YES.
upvoted 16 times

Merma Highly Voted 1 year, 4 months ago
A. Yes is correct.
https://social.technet.microsoft.com/wiki/contents/articles/17804.map-toolkit-how-to-implement-the-phased-approach.aspx#Phase_5_Collect_Data
upvoted 5 times

moobdoob Most Recent 8 months, 2 weeks ago
Answer is YES.
upvoted 1 times

Question #63 *Topic 2*

You have a Microsoft 365 tenant that uses Microsoft Intune for mobile device management (MDM).
You associate a Microsoft Store for Business account with Intune.
You purchase an app named App1 from the Microsoft Store for Business.
You need to ensure that App1 can be deployed by using Intune.
What should you do?

A. Sync purchased apps from the Microsoft Store for Business.

B. Integrate the Windows Autopilot Deployment Program into the Microsoft Store for Business.

C. Create an app category in Intune.

D. Create an app protection policy in Intune.

Correct Answer: *A*
Synchronize apps -
If you've already associated your Microsoft Store for Business account with your Intune admin credentials, you can manually sync your Microsoft Store for
Business apps with Intune using the following steps.
1. Select Tenant administration > Connectors and tokens > Microsoft Store for Business.
2. Click Sync to get the apps you've purchased from the Microsoft Store into Intune.
Note: You can synchronize the list of apps you have purchased (or that are free) from the store with Intune.
Apps that are synchronized appear in the Intune administration console; you can assign these apps like any other apps.
Both Online and Offline licensed versions of Apps are synchronized to Intune. App names will be appended with "Online" or "Offline" in the portal.
Reference:
https://docs.microsoft.com/en-us/mem/intune/apps/windows-store-for-business

ThreeDay Highly Voted 1 year ago
I see nobody said this yet but A is correct
upvoted 16 times

BrentOn 6 months, 3 weeks ago
I see nobody has confirmed what you said yet, A is correct
upvoted 6 times

RodrigoT 6 months ago
I see nobody was capable of posting a decent link here to help who really wants to study:
https://docs.microsoft.com/en-us/mem/intune/apps/windows-store-for-business#synchronize-apps
upvoted 16 times

MR_Eliot 5 months ago
I see nobody had voted the answer is A, so I did.
upvoted 5 times

Perycles Highly Voted 1 year, 3 months ago
A is correct
upvoted 6 times

shaolin_monk Most Recent 2 months ago
A: (Click Sync to get the apps you've purchased from the Microsoft Store into Intune).
upvoted 1 times

MR_Eliot 5 months ago
Selected Answer: A
A is correct.
https://docs.microsoft.com/en-us/mem/intune/apps/windows-store-for-business#synchronize-apps
upvoted 1 times

shaolin_monk 5 months, 1 week ago
A is correct.
Tenant administration > Connectors and tokens > Microsoft Store for Business. Then click sync.
https://docs.microsoft.com/en-us/mem/intune/apps/windows-store-for-business#synchronize-apps
upvoted 1 times

HF_Lee 9 months ago
Tenant Admin -> Connector and token -> MSfB -> Enable sync
upvoted 5 times

moobdoob 8 months, 2 weeks ago
Great success!
upvoted 1 times

Nome2025 1 year, 3 months ago

A is correct

upvoted 4 times

HOTSPOT -

Your network contains an on-premises Active Directory domain named contoso.com that syncs to Azure Active Directory (Azure AD).

A user named User1 uses the domain-joined devices shown in the following table.

Name	Operating system
Device1	Windows 8.1 Pro
Device2	Windows 10 Pro

In the Azure Active Directory admin center, you assign a Windows 10 Enterprise E5 license to User1.

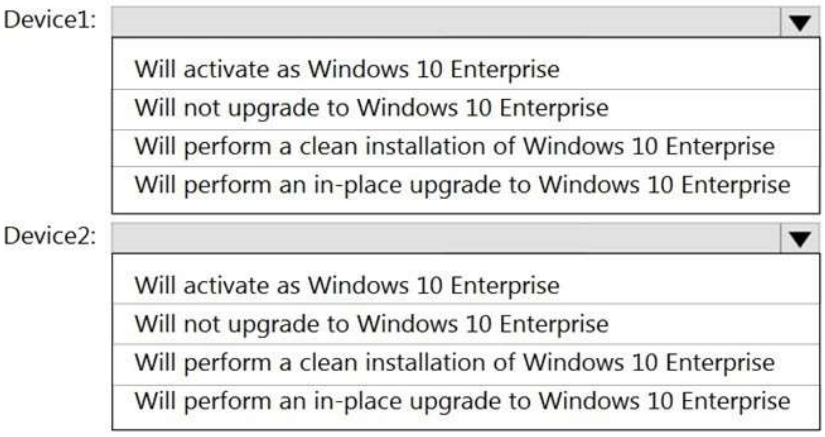
You need to identify what will occur when User1 next signs in to the devices.

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

NOTE: Each correct selection is worth one point.

Hot Area:

Answer Area



Correct Answer:

Answer Area

Box 1: Will not upgrade to Windows 10 Enterprise

Box 2: Will activate as Windows 10 Enterprise

Windows 10 Pro supports the Subscription Activation feature, enabling users to ג€step-upג€ from Windows 10 Pro or Windows 11 Pro to Windows 10 Enterprise or

Windows 11 Enterprise, respectively, if they are subscribed to Windows 10/11 Enterprise E3 or E5.

With Windows 10, version 1903 and later, the Subscription Activation feature also supports the ability to step-up from Windows 10 Pro Education or Windows 11

Pro Education to the Enterprise grade editions for educational institutionsג€"Windows 10 Education or Windows 11 Education.

Reference:

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

lahey69 Highly Voted 1 year, 4 months ago

Device1 is Windows 8.1 - Will not upgrade to Windows 10 Enterprise
Device2 is Windows 10 Pro- Will activate as Windows 10 Enterprise

upvoted 60 times

moobdoob 8 months, 2 weeks ago

Agreed. Correct answer above.

upvoted 1 times

mikl 9 months, 2 weeks ago

Agree!

upvoted 1 times

AzureLearner01 3 months, 3 weeks ago

Agree, if you read the following article from Microsoft you can verify that no hybrid-joined device is needed for subscription activation. I think this is the most discussed point in the comments. So yes, even with on-Prem AD-Joined devices it will activate as Windows 10 Enterprise.

https://docs.microsoft.com/en-us/windows/deployment/windows-10-subscription-activation
Organizations that have an Enterprise agreement can also benefit from the new service, using traditional Active Directory-joined devices. In this scenario, the Active Directory user that signs in on their device must be synchronized with Azure AD using Azure AD Connect Sync.

upvoted 3 times

Pleebb Highly Voted 1 year, 3 months ago

Device 1: does not upgrade
Device 2: Will activate as Windows 10 Enterprise because AD is on "Hybrid joined" to Azure. Devices will automatically join Azure AD and will be labelled as "Hybrid joined" devices.

https://docs.microsoft.com/en-us/windows/deployment/deploy-enterprise-licenses
https://www.orbid365.be/hybrid-azure-ad-join-p1/

upvoted 14 times

Rob69420 Most Recent 2 months, 3 weeks ago

This link shows tables which indicate you CAN UPGRADE BOTH IN PLACE and KEEP THE SETTINGS, FILES, ETC.....

https://docs.microsoft.com/en-us/windows/deployment/upgrade/windows-10-upgrade-paths

upvoted 1 times

jcgm1990 3 months ago

Can moderators please speak to whoever provided these answers and tell him to retake the exam as I am pretty sure whoever provided these answer did no pass if they used the answers provided here

upvoted 4 times

b3arb0yb1m 9 months, 2 weeks ago

Subscription Activation for Windows 10/11 Enterprise
Windows 10/11 Enterprise E3 and Windows 10/11 Enterprise E5 are available as online services via subscription. Deploying Windows 10 Enterprise or Windows 11 Enterprise in your organization can now be accomplished with no keys and no reboots.

If you are running Windows 10, version 1703 or later:

Devices with a current Windows 10 Pro license or Windows 11 Pro license can be seamlessly upgraded to Windows 10 Enterprise or Windows 11 Enterprise, respectively.
Product key-based Windows 10 Enterprise or Windows 11 Enterprise software licenses can be transitioned to Windows 10 Enterprise and Windows 11 Enterprise subscriptions.
Organizations that have an Enterprise agreement can also benefit from the new service, using traditional Active Directory-joined devices. In this scenario, the Active Directory user that signs in on their device must be synchronized with Azure AD using Azure AD Connect Sync.

upvoted 3 times

Mage7 11 months, 1 week ago

To much Comments on different answers here...
I'll give here my two cents after reading all the comments.
As most of the time if you miss one word from the sentence you can interpreter the answer however you want...

Device1 - for sure "Will not upgrade to Windows 10 Enterprise"
Device2 - here's where most depates are currently is...

I state several facts:
"on-premises Active Directory domain named contoso.com that syncs to Azure Active Directory (Azure AD)" - so User1 will be synced to AAD for sure - everyone agrees here.
"A user named User1 uses the domain-joined devices shown in the following table" - Please note "DOMAIN-JOINED" phrase (NOT Azure Joined, NOT Azure Registered, NOT Hybrid Azure AD Joined as someone assumed and mentioned = DOMAIN-JOINED). We, of course, could assume that AD Connect is configured to SYNC AD devices to Azure, but we can also assume it is not.

Based on my last two sentences I'm sticking with:
Device2 - "Will not upgrade to Windows 10 Enterprise"

As always - do your own research with all the questions/answers and stick to the answer you think fits the best.

Good luck with the exam.

upvoted 3 times

ken2ut 4 months, 1 week ago

You said "We, of course, could assume that AD Connect is configured to SYNC AD devices to Azure, but we can also assume it is not.". THERE IS NOTHING TO ASSUME. The scenario clearly states "...sync to Azure Active Directory (Azure AD)." Therefore AD Connect is configured.

Device2 - "Will activate as Windows 10 Enterprise"

upvoted 2 times

BMAN101 1 year ago

this is the reason i read the comments, im sure this answer was entered wrong on purpose

upvoted 1 times

BAbdalla 1 year ago

Reversed as responses.
Device1 which is a Windows 8.1, will not upgrade to Windows 10.
Device2, Windows 10 Pro, will upgrade to Windows Enterprise version (depending on W10Pro build). I tested it in Lab and it worked using a 21H2.

upvoted 8 times

RodrigoT 6 months, 2 weeks ago

That's what I'm talking about. Thanks for the lab.

upvoted 4 times

RodrigoT 6 months ago

But device2 will actually just ACTIVATE as Enterprise.
For example I had a Windows 10 Home, bought a Pro license, applied it and it just activated as 10 Pro. Of course I've got more features but there was not any visible "upgrade".

upvoted 3 times

Alfred666 1 year, 1 month ago

Now i think both devices won't upgrade. When the network syncs to AAD this is for user accounts and has nothing to do with devices.

upvoted 1 times

Mujja 1 year, 3 months ago

I have
-W10 Ent Domain-Joined device, it doesn't activate
-W10 Ent Hybrid-Joined device, it activates

The question doesn't say the device is Hybrid-joined, so I would say it doesn't activate.

upvoted 1 times

ercluff 1 year, 2 months ago

The given information states: "Your network contains an on-premises Active Directory domain named contoso.com that syncs to Azure Active Directory (Azure AD)." That is a Hybrid AD Domain.

upvoted 3 times

Tomtom11 1 year, 3 months ago

Subscription Activation Windows 10 Subscription Activation allows you to automati-
cally upgrade devices with Windows 10 Pro to Windows 10 Enterprise without needing
to enter a product key or perform a restart.

upvoted 1 times

Tomtom11 1 year, 3 months ago

If you are running Windows 10, version 1703 or later:

Devices with a current Windows 10 Pro license can be seamlessly upgraded to Windows 10 Enterprise.
Product key-based Windows 10 Enterprise software licenses can be transitioned to Windows 10 Enterprise subscriptions.

upvoted 1 times

egdeeptha 1 year, 3 months ago

Both Devices are Joined to On-Prem AD., not to AzureAD. For subscription activation to work, a device has to be joined to Azure AD.
And I do not think Windows 8.1 machine will get 10 Enperprse automatically when a user logs in even if it was azure AD joined. So answers are Will not upgrade to windows 10 enterprise.

upvoted 1 times

S4L4LMF 1 year, 3 months ago

https://www.microsoft.com/en-us/microsoft-365/blog/2017/01/19/new-windows-10-upgrade-benefits-windows-cloud-subscriptions-csp/

Windows 8.1 will be upgraded to 10 enterprise only if this is explicitly done by an admin in the azure portal. This isnt stated, so user one wont see any upgrade taking place.

on Device 2 im not sure, is synced the same as Azure AD joined? It will also depend if the windows 10 deployment is 1703 or above. Since its synced, im taking it is also a hybrid environment (which is NOT stated), which would mean it will automatically upgrade to 10 enterprise. If Synced = azure hybrid AD joined, then the device will upgrade (automatically) to windows 10:

https://docs.microsoft.com/en-us/windows/deployment/windows-10-subscription-activation
"Devices must be Azure AD-joined or Hybrid Azure AD joined. Workgroup-joined or Azure AD registered devices are not supported."

upvoted 2 times

Perycles 1 year, 3 months ago

Device 1 : no effect - "Modern Subscrition activation" only applied on Win 10 PRO, ENT, EDU.
device 2 : activate to Win10 ENT : "Modern Subscrition activation" is supported on both Azure AD join and Azure AD hybride Join Devices.

upvoted 2 times

RajeeMark 1 year, 4 months ago

As i understand from the question, both PC's are On-prem domain joined.
Domain joined PC's don't activate automatically.
So both will not upgrade to W10 Enterprise.

upvoted 4 times

Nome2025 1 year, 3 months ago

But they are synced.

upvoted 1 times

S4L4LMF 1 year, 3 months ago

Synced = / = joined, These arent Azure AD joined devices, so according to the given link Device 2 doesnt meet the requirement.

upvoted 1 times

Jimbob77 1 year, 4 months ago

Some details are missing from this question, the version of Windows 10 will determine whether the upgrade is successful (it wont work on 8.1):
Device 1: Will not upgrade to W10 Ent
Device 2: Will activate as W10 Ent (maybe)
From the URL provided: https://docs.microsoft.com/en-us/windows/deployment/windows-10-subscription-activation
If you are running Windows 10, version 1703 or later:
Devices with a current Windows 10 Pro license can be seamlessly upgraded to Windows 10 Enterprise.

upvoted 3 times

Question #65 *Topic 2*

You have a server that runs the Microsoft Deployment Toolkit (MDT). You have computers that run Windows 8.1 or Windows 10.
You have a Microsoft 365 tenant. Microsoft 365 Enterprise E5 licenses are assigned to all users.
You need to recommend a strategy to install Windows 10 on the Windows 8.1 computers. The installation must retain the user files, settings, and supported applications.
What should you recommend?

A. Refresh the Window 8.1 computers by using Windows 10 and use the User State Migration Tool (USMT).

B. Perform an in-place upgrade of Windows 8.1 to Windows 10.

C. Refresh the Window 8.1 computers by using Windows 10 and use Windows Autopilot white glove service to finalize the installation.

D. Refresh the Window 8.1 computers by using Windows 10 and use Windows Autopilot user-driven mode.

Correct Answer: *B*
The simplest path to upgrade PCs currently running Windows 7, Windows 8, or Windows 8.1 to Windows 10 is through an in-place upgrade. You can use a
Microsoft Endpoint Manager task sequence to completely automate the process.
Note: For Windows 10 deployment, Microsoft 365 includes a fantastic deployment advisor that can walk you through the entire process of deploying Windows 10.
The wizard supports multiple Windows 10 deployment methods, including:

Windows Autopilot -

In-place upgrade -
Deploying Windows 10 upgrade with Intune
Deploying Windows 10 upgrade with Microsoft Endpoint Configuration Manager
Deploying a computer refresh with Microsoft Endpoint Configuration Manager
Reference:
https://docs.microsoft.com/en-us/windows/deployment/deploy-m365 https://docs.microsoft.com/en-us/windows/deployment/deploy-windows-cm/upgrade-to-windows-10-with-configuration-manager

Perycles Highly Voted 1 year, 3 months ago
of course B : in place upgarde is the recommended way by microsoft in this case.
upvoted 11 times

NZS Most Recent 5 months, 1 week ago
B. Also, MDT can be used to do in-place upgrades.
upvoted 1 times

Angarali 5 months, 2 weeks ago
Selected Answer: B
B. Perform an in-place upgrade of Windows 8.1 to Windows 10.
upvoted 2 times

RodrigoT 6 months, 2 weeks ago
Correct B. The first link provided is useless, don't waste your time. The second link is good. You can in place upgrade even from a Windows 7.
upvoted 3 times

moobdoob 8 months, 2 weeks ago
In place upgrade is correct.
upvoted 2 times

mikl 9 months, 2 weeks ago
Selected Answer: B
B. Perform an in-place upgrade of Windows 8.1 to Windows 10.
upvoted 2 times

BAbdalla 11 months, 1 week ago
Why not option A (Refresh to Windows10 and use USMT)?
upvoted 1 times

AVP_Riga 11 months ago
Faster(cheaper) and "The installation must retain the user files, settings, and supported applications."
upvoted 3 times

mikl 9 months, 2 weeks ago
You could keep user files with USMT, but I still agree with you - and Im pretty sure that Micrsoft actually recommends an in-place-upgrade in these cases.
upvoted 1 times

RodrigoT 6 months ago

Because in this environment you have a Microsoft 365 tenant, you are already in the cloud using the modern way, not on-premisses. If you had just an on-premises Active Directory domain then you would use USMT. Check the Page 10 Question #55: https://www.examtopics.com/exams/microsoft/md-101/view/10/

upvoted 2 times

Question #66 *Topic 2*

You use the Microsoft Deployment Toolkit (MDT) to deploy Windows 10.

You create a new task sequence by using the Standard Client Task Sequence template to deploy Windows 10 Enterprise to new computers. The computers have a single hard disk.

You need to modify the task sequence to create a system volume and a data volume.

Which phase should you modify in the task sequence?

A. Preinstall

B. State Restore

C. Initialization

D. Postinstall

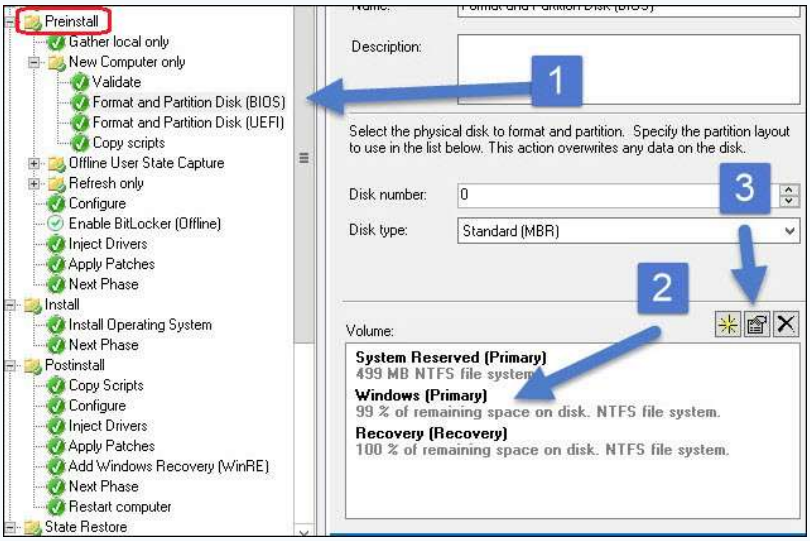
Correct Answer: *A*

Step 1 ג€" Create Extra Partition in MDT

1. First we will look to create extra partition in MDT. We will create a new task sequence for a machine that doesn't have an extra partition. Specify the TS name and comments. Click Next.

2. On the Select Template page, click the drop-down and select Standard Client Task Sequence. Complete the remaining steps.

3. Edit the task sequence and click the New Computer only step. Within that step, click Format and Partition Disk(BIOS) step and edit it.



Etc.

Reference:

https://www.prajwaldesai.com/create-extra-partition-in-mdt/

HOTSPOT -

You have the Microsoft Deployment Toolkit (MDT) installed in three sites as shown in the following table.

MDT instance name	Site	Default gateway
MDT1	New York	10.1.1.0/24
MDT2	London	10.5.5.0/24
MDT3	Dallas	10.4.4.0/24

You use Distributed File System (DFS) Replication to replicate images in a share named Production.

You configure the following settings in the Bootstrap.ini file.

```
[Settings]
Priority=DefaultGateway, Default
[DefaultGateway]
10.1.1.1=NewYork
10.5.5.1=London
[NewYork]
DeployRoot=\\MDT1\Production$
[London]
DeployRoot=\\MDT2\Production$

KeyboardLocale=en-gb -
[Default]
DeployRoot=\\MDT3\Production$

KeyboardLocale=en-us -
```

You plan to deploy Windows 10 to the computers shown in the following table.

Name	IP address
LT1	10.1.1.240
DT1	10.5.5.115
TB1	10.2.2.193

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
TB1 will download the image from MDT3.	○	○
DT1 will have a KeyboardLocale of en-gb.	○	○
LT1 will download the image from MDT1.	○	○

Correct Answer:

Answer Area

Statements	Yes	No
TB1 will download the image from MDT3.	○	●
DT1 will have a KeyboardLocale of en-gb.	●	○
LT1 will download the image from MDT1.	●	○

Reference:

https://docs.microsoft.com/en-us/windows/deployment/deploy-windows-mdt/build-a-distributed-environment-for-windows-10-deployment

Perycles Highly Voted 1 year, 3 months ago

all is correct.

upvoted 18 times

[Removed] 1 year, 3 months ago

can you please elaborate on why the 1st is yes?

upvoted 3 times

AVP_Riga 11 months ago

Because device has x.2.2.x IP address which didn't mention in first DefaultGateway table.

upvoted 1 times

RodrigoT 6 months, 2 weeks ago

So, how can TB1 comunicate if it's in a different subnet of all three MDTs?

upvoted 3 times

NZS 5 months, 1 week ago

Doesn't matter, the router (default gateway) will take care of that in the same way you can communicate with the outside world.

upvoted 2 times

ercluff Highly Voted 1 year, 1 month ago

N Y Y
Please note the Setting priority lists DefaultGateway, Default. DefaultGateway lists 10.1.1.1[NewYork] and 10.5.5.1[London]. TB1 [10.2.2.193] will route through DefautGateway first before routing through Default, hence it will route through NewYork's MDT1 unless NewYork is down. Only then would it route through Dallas' MDT3. Therefore, the first answer is NO. The other two are YES since they are in line with the bootstrap.ini Settings table.

upvoted 16 times

RodrigoT 6 months, 2 weeks ago

I agree with N Y Y, but I think that the first is N because TB1 (10.2.2.x) is in a different subnet of MDT3 (10.4.4.x). The link provided says that the device: "must be assigned a default gateway that matches the one you entered in the Boostrap.ini file". There is no mention of MDT3 ip address in the bootstrap.ini file. So, in my opinion TB1 won't find anyone.

upvoted 4 times

veteran_tech 6 months, 2 weeks ago

Agree, N Y Y as TB1 is on a different subnet and would therefore access the default GW.

upvoted 1 times

RodrigoT 5 months ago

And note that DeployRoot=\\ServerName\Production$ is a types of namespaces called "stand-alone", not domain-based. So, the communication is only local, not worldwide. On this link there is a very long and deep explanation about this, but what matters for this question is on the beginning of the article:
https://docs.microsoft.com/en-us/previous-versions/windows/it-pro/windows-server-2003/cc782417(v=ws.10)

upvoted 1 times

TonySuccess Most Recent 3 days, 11 hours ago

Nobody going to say it, okay I will. What a joke of a question.

upvoted 2 times

silver_bullet666 3 months, 2 weeks ago

It seems like some of the question may have changed since some of these comments where made, my understanding is this. Firstly I did some reading and MDT does work over VPN.

TB1 (10.2.2.193) will attempt to download from MDT3 as it is defined as the default and no more specific site is defined in bootstrap.ini, will it actually work though, probably yes, because MDT shares are replicated with DFS hence there must be inter-site connectivity.
DT1(10.5.5.115) will have KeyboardLocale of en-gb, this is defined in the bootstrap.ini for London site.
LT1 will download the image from MDT1 as this is defined in bootstrap.ini for NewYork site.

upvoted 1 times

PiPe 7 months, 4 weeks ago

LT1 (New York):
Deployroot : MDT1 (DefaultGateway) --> MDT3 (Default) = MDT3 wins (overwrite = true)
KeyboardLocale : en-US (Default) = en-US wins

DT1 (London):
Deployroot : MDT2 (DefaultGateway) --> MDT3 (Default) = MDT3 wins (overwrite = true)
KeyboardLocale : en-GB (DefaultGateway) --> en-US (Default) = en-GB wins (overwrite = false)

TB1 (Dallas):
Deployroot : MDT3 (Default) = MDT3 wins
KeyboardLocale : en-US (Default) = en-US wins

So:

TB1 will download the image from MDT3 : YES
DT1 will have a KeyboardLocale of en-GB : YES
LT1 will download the image from MDT1 : NO

upvoted 4 times

PiPe 7 months, 4 weeks ago

However... ZTIGather.xml stipulates that DeployRoot is one of the few properties that is set to overwrite=true, meaning the last value will win (in contrast to the previous statement)
https://scriptimus.wordpress.com/2011/07/06/mdt-2010-ztigather-xml/

So the Deployroot property in the 'Default' section will overwrite the previously set Deployroot property in the 'DefaultGateway' section, according to me.

Doesn't that mean that all 3 cases will use MDT3, which is specified in the 'Default' section only?

This looks like a relevant Technet forum question:

https://social.technet.microsoft.com/Forums/en-US/19cf3eb8-20a1-4371-81ab-7a3e431a1687/bootstrapini-and-defaultgateway-question?forum=mdt

In contrast, the KeyboardLocale property has overwrite=false, so there the first occurrence would win.

upvoted 3 times

PiPe 7 months, 4 weeks ago

https://www.techrepublic.com/article/microsoft-deployment-toolkit-advanced-settings-for-automating-deployments-using-bootstrap-ini/

"The entries stipulated after Priority= will be processed in the order in which they are read –from left to right–by the MDT scripts." Meaning, the 'DefaultGateway' section first, and the 'Default' section second.

"Typically, as the headers are read by the MDT script, the information is processed on a first-come, first-served basis. This means that if two or more conflicting entries are detected, the first entry read will be the one written. The subsequent entries will be disregarded."

upvoted 2 times

moobdoob 8 months, 2 weeks ago

YES, YES, YES

upvoted 2 times

ANDREVOX 11 months, 3 weeks ago

ALL = Y
Note the DeployRoot for every Location:
[NewYork] - DeployRoot= \\MDT1\Production$
[London] - DeployRoot= \\MDT2\Production$
KeyboardLocale=en-gb -
[Default] - DeployRoot= \\MDT3\Production$

Thus = Y Y Y

upvoted 3 times

BAbdalla 11 months, 1 week ago

But TB1 has a different IP range than MDT3. The exercise does not inform about the communication between the sites, but because it has a different range, I believe that TB1 would not be able to communicate with MDT3. Can you explain why the first option is also Yes instead of No?

upvoted 2 times

Mage7 11 months ago

We can assume that it has no communication between different sites...
I assume that it does (Site-To-Site VPN?). So for me: YYY

upvoted 2 times

AVR31 5 months, 1 week ago

That is too much assumption. Subnet 10.2.2.x doesn't have access to any of the shares. So it will fail.

upvoted 2 times

AVP_Riga 1 year ago

NYY there is no 10.2.2.x network...

upvoted 7 times

Ka1Nn 1 year, 1 month ago

N Y Y
N : 1st reason : the 1st character of the computer name should represent the state/country
LT1 for LONDON, DT1 for Dallas, TB1 not for NYC but maybe Texas.
2nd , The IP address CIDR can't reach the network provided in the Default Section in the Customsettings.ini. SO TB1 will try to connect on MDT3 without success.

"D" fo

upvoted 2 times

jibutoms 1 year, 3 months ago

N Y Y is correct. TB1 will take the Deployroot from [Default] section , ie. \\MDT3

upvoted 5 times

DPivc 1 year, 3 months ago

Which is exactly why the first answer "TB1 will download from MDT3" would also be Yes (MDT3 = Defaultroot). Why would you answer it as No then?

upvoted 5 times

Jvp21 1 year, 3 months ago

N Y Y is the correct answer

upvoted 4 times

cloudnothings 1 year, 3 months ago

Why would TB1 with an IP of 10.2.2.193 download from Texas at 10.4.4.0/24 ???

upvoted 3 times

S4L4LMF 1 year, 3 months ago

I think btecause MDT3 is the default site to go to, the others are linked to ip addresses and so can only be access by computers who have an IP address within that range.

upvoted 3 times

S4L4LMF 1 year, 3 months ago

To add to it, its default gateway is 10.4.4.0, but most likely TB1 would go to 10.2.2.1 default gateaway and from there on get routed towards 10.4.4.1 and arrive at MDT3 (Texas). Since its the default route it seems, while the others have defined gateways, meaning if the device gateway is what is pre-defined it will go to that location (NewYork/London).

upvoted 1 times

Question #68 *Topic 2*

You are replacing 100 company-owned Windows devices.
You need to use the Microsoft Deployment Toolkit (MDT) to securely wipe and decommission the devices. The solution must meet the following requirements:
⇨ Back up the user state.
⇨ Minimize administrative effort.
Which task sequence template should you use?

A. Litetouch OEM Task Sequence

B. Sysprep and Capture

C. Standard Client Replace Task Sequence

D. Standard Client Task Sequence

Correct Answer: *C*
Standard Client Replace task sequence. Used to run User State Migration Tool (USMT) backup and the optional full Windows Imaging (WIM) backup action. Can also be used to do a secure wipe of a machine that is going to be decommissioned.
Reference:
https://docs.microsoft.com/en-us/windows/deployment/deploy-windows-mdt/get-started-with-the-microsoft-deployment-toolkit

Jimbob77 Highly Voted 1 year, 4 months ago
Correct, C (least administrative effort)
(from their URL) Task Sequence Templates ...
Standard Client Replace task sequence. Used to run User State Migration Tool (USMT) backup and the optional full Windows Imaging (WIM) backup action. Can also be used to do a secure wipe of a machine that is going to be decommissioned.
upvoted 20 times

moobdoob Most Recent 8 months, 2 weeks ago
Replace task sequence is correct.
upvoted 2 times

HOTSPOT -

You have the devices shown in the following table.

Name	Operating system
Device1	Windows 10 Enterprise
Device2	Windows 8.1 Pro
Device3	Android 9.03
Device4	iOS

You plan to implement Desktop Analytics.

You need to identify which devices support the following:

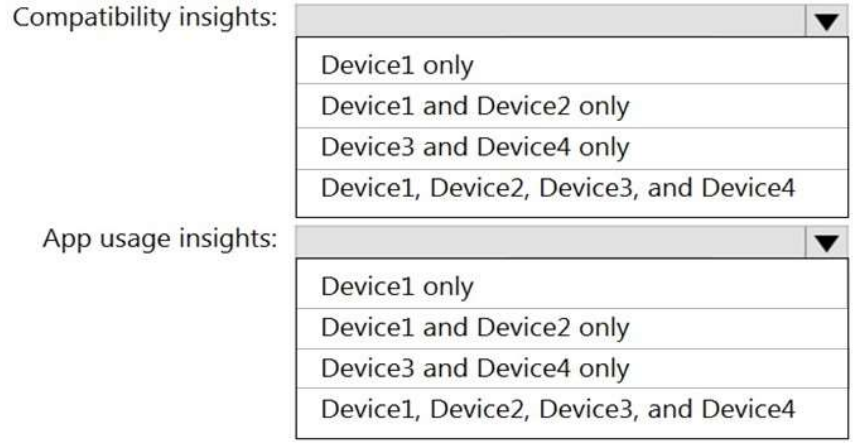
- Compatibility insights
- App usage insights

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

NOTE: Each correct selection is worth one point.

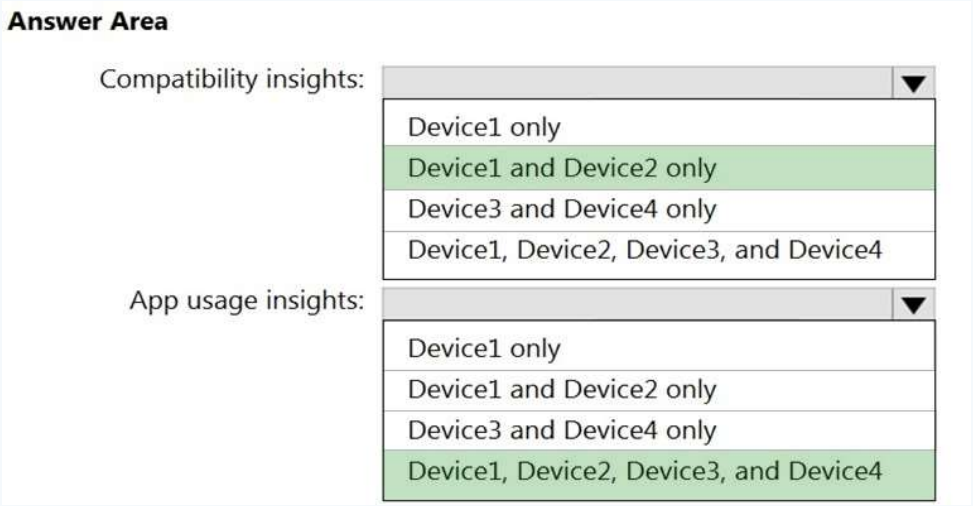
Hot Area:

Answer Area



Correct Answer:

Answer Area



Box 1: Device1 and Device2 only -

You can use the Compatibility Administrator Tool on the following operating systems:

Windows 10 -

Windows 8.1 -

Windows 8 -

Windows 7 -

Windows Server 2012 -

Windows Server 2008 R2 -
Box 2: Device1, Device2, Device3, and Device4
Application Insights adds support for iOS and Android apps.
Reference:
https://docs.microsoft.com/en-us/windows/deployment/planning/using-the-compatibility-administrator-tool https://azure.microsoft.com/en-us/updates/application-insights-adds-support-for-ios-and-android-apps-improved-java-app-support-and-fine-time-selection/

Perycles Highly Voted 1 year, 3 months ago
Desktop analytics only support Windows 7, 8.1 et W10. so answer is B for both question (device 1 and device 2).
upvoted 24 times

ozoz 1 year, 2 months ago
Incorrect:
From this link: Application Insights adds support for iOS and Android apps.....
https://azure.microsoft.com/en-us/updates/application-insights-adds-support-for-ios-and-android-apps-improved-java-app-support-and-fine-time-selection/
upvoted 5 times

cbjorn8931 1 year, 1 month ago
It talks about Compatibility insight, not Application insight... App Usage is all devices .. So the answer is correct
upvoted 10 times

[Removed] 11 months, 2 weeks ago
Confusing question - Application Insights is not part of Desktop Analytics...
upvoted 5 times

RodrigoT 5 months ago
You "plan" to implement Desktop Analytics.
upvoted 2 times

IykeP Highly Voted 8 months, 3 weeks ago
Below is the Correct Answer:

1. Compatibility Insights: Device 1 and Device 2 Only

2.App Usage Insights: Device 1 only.

App Usage Insights is not supported on windows 8.1, it is only supported on Windows 10 1803 and later.

https://www.anoopcnair.com/sccm-desktop-analytics-integration/
upvoted 13 times

RodrigoT 6 months, 2 weeks ago
What scares me is that you were upvoted 9 times, even giving a WRONG answer. Meaning everybody here has to study, a lot.

App Usage Insights is device independent. It focus on how the app is used, not the device.
https://docs.microsoft.com/en-us/azure/azure-monitor/app/mobile-center-quickstart
https://docs.microsoft.com/en-us/azure/azure-monitor/app/app-insights-overview
upvoted 6 times

cjanim03 Most Recent 7 months, 2 weeks ago
Lots of old information here. Since there have been changes over the last year (and it is being retired 11/30/22), thought I would put in my two cents:
1. Device 1 Only*
2. Device 1 Only**

*"The Windows diagnostic data processor configuration is supported on the following Windows 10 versions:
Pro, Education, and Enterprise editions
Version 1809 or later
July 2021 cumulative update or later
Important
Devices with an older OS version like Windows 7 will continue to show in Desktop Analytics until January 31, 2022. Use Desktop Analytics to update those devices to a supported version of Windows 10. After that date, Desktop Analytics will only display devices with supported versions of Windows 10." (https://docs.microsoft.com/en-us/mem/configmgr/desktop-analytics/whats-new)

**See above, and this is asking for App Usage Insights (which seems to be part of Desktop Analytics, though I can't find any info on MS documentation), NOT Application Insights (which would support IOS/Android, but is part of Azure Monitor).
upvoted 4 times

jage01 7 months, 2 weeks ago
Compatibility Insights: Device 1 & 2 only
App usage insights: Device 1

Devices with an older OS version like Windows 7 will continue to show in Desktop Analytics until January 31, 2022. Use Desktop Analytics to update those devices to a supported version of Windows 10. After that date, Desktop Analytics will only display devices with supported versions of Windows 10.

https://docs.microsoft.com/en-us/mem/configmgr/desktop-analytics/whats-new#support-for-the-windows-diagnostic-data-processor-configuration

Desktop Analytics will be retired on November 30, 2022.
upvoted 4 times

RodrigoT 5 months, 1 week ago

So, until there the question is still valid.

upvoted 1 times

moobdoob 8 months, 2 weeks ago

Compatibility Insights: Device 1 & 2 only
App usage insights: Device 1

upvoted 1 times

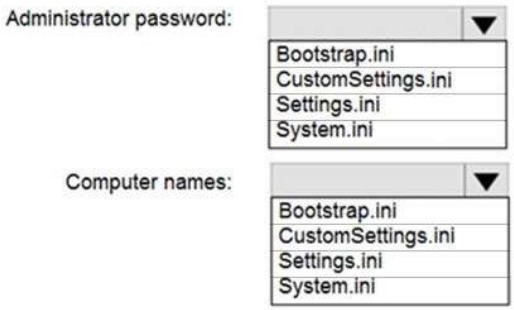
HellRaver80 10 months, 3 weeks ago

Desktop Analytics only supports the Windows 10 Enterprise LTSC 2019, which is equivalent to Windows 10, version 1809. It doesn't support Windows 10 Enterprise 2015 LTSB (version 1507) or Windows 10 Enterprise 2016 LTSB (version 1607).

upvoted 1 times

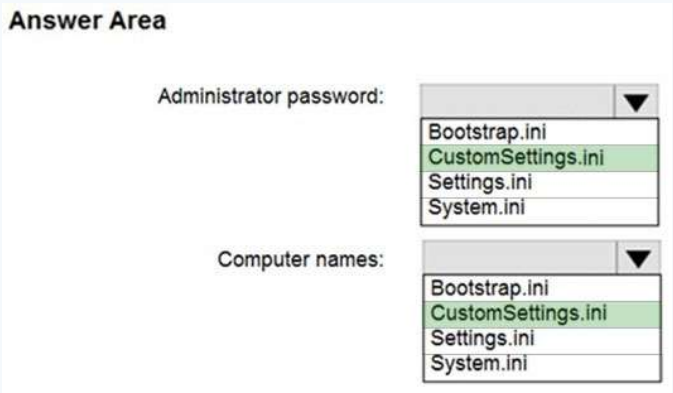
HOTSPOT -
You use the Microsoft Deployment Toolkit (MDT) to deploy Windows 10.
You need to modify the deployment share to meet the following requirements:
⇨ Ensure that the user who performs the installation is prompted to set the local Administrator password.
⇨ Define a rule for how to name computers during the deployment.
The solution must NOT replace the existing WinPE image.
Which file should you modify for each requirement? To answer, select the appropriate options in the answer area.
NOTE: Each correct selection is worth one point.
Hot Area:

Answer Area



Correct Answer:

Answer Area



Box 1: CustomSettings.ini -
You can skip the entire Windows Deployment Wizard by specifying the SkipWizard property in CustomSettings.ini. To skip individual wizard pages, use the following properties:

SkipAdminPassword -
Etc.
Note: The CustomSettings.ini file includes for example:

AdminPassword=pass@word1 -

DomainAdmin=CONTOSO\MDT_JD -

DomainAdminPassword=pass@word1 -
Some properties to use in the MDT Production rules file are as follows:
DomainAdmin. The account to use when joining the machine to the domain.
DomainAdminDomain. The domain for the join domain account.
DomainAdminPassword. The password for the join domain account.

Box 2: CustomSettings.ini -
Example of content in the CustomSettings.ini file:

SkipComputerName=YES -
OSDComputerName=%ComputerName%
Reference:
https://docs.microsoft.com/en-us/windows/deployment/deploy-windows-mdt/deploy-a-windows-10-image-using-mdt
https://docs.microsoft.com/en-us/mem/configmgr/mdt/samples-guide

Question #71 *Topic 2*

You have the Microsoft Deployment Toolkit (MDT) installed.
You install and customize Windows 10 on a reference computer.
You need to capture an image of the reference computer and ensure that the image can be deployed to multiple computers.
Which command should you run before you capture the image?

A. dism

B. wpeinit

C. bcdedit

D. sysprep

Correct Answer: *D*
Sysprep (System Preparation) prepares a Windows client or Windows Server installation for imaging. Sysprep can remove PC-specific information from a
Windows installation (generalizing) so it can be installed on different PCs.
Reference:
https://docs.microsoft.com/en-us/windows-hardware/manufacture/desktop/sysprep--system-preparation--overview

edpaz Highly Voted 1 year, 1 month ago
agreed
upvoted 7 times

moobdoob Most Recent 8 months, 2 weeks ago
Good answer.
upvoted 2 times

mikl 9 months, 2 weeks ago
Seems ok.

https://docs.microsoft.com/en-us/mem/configmgr/osd/deploy-use/create-a-task-sequence-to-capture-an-operating-system
upvoted 2 times

that_guy_eehh 1 year, 3 months ago
Agree
D: Sysprep
upvoted 4 times

Question #72 *Topic 2*

You have a Microsoft Deployment Toolkit (MDT) deployment share named DS1.
In the Out-of-Box Drivers node, you create folders that contain drivers for different hardware models.
You need to configure the Inject Drivers MDT task to use PnP detection to install the drivers for one of the hardware models.
What should you do first?

A. Create a selection profile

B. Import an OS package

C. Add a Validate task to the task sequence

D. Add a Gather task to the task sequence

Correct Answer: *A*
By default, MDT adds any storage and network drivers that you import to the boot images. However, you should add only the drivers that are necessary to the boot image. You can control which drivers are added by using selection profiles.
Reference:
https://docs.microsoft.com/en-us/windows/deployment/deploy-windows-mdt/deploy-a-windows-10-image-using-mdt

Davidchercm Highly Voted 1 year, 2 months ago
answer look correct
upvoted 6 times

RodrigoT Most Recent 6 months, 2 weeks ago
Check step 5 of the provided link under: Create the selection profiles for boot image drivers.
upvoted 2 times

moobdoob 8 months, 2 weeks ago
Good answer.
upvoted 1 times

Question #73 *Topic 2*

Your network contains an Active Directory domain. The domain contains computers that run Windows 8.1 and the users shown in the following table.

Name	Domain group membership	Local group membership
User1	Domain Users, Domain Admins	Administrators
User2	Domain Users, Remote Management Users	Users
User3	Domain Users	Administrators
User4	Domain Users	Remote Management Users

You plan to use the Microsoft Assessment and Planning (MAP) Toolkit to collect inventory data. The MAP Toolkit has the following configurations:

⇨ Inventory scenario: Windows computers

⇨ Discovery method: Use Active Directory Domain Services (AD DS)

You need to identify which user to use for the MAP Toolkit inventory discovery. The solution must use principle of least privilege.

What should you identify?

A. User3

B. User1

C. User4

D. User2

Correct Answer: *A*

Discovery method: Use Active Directory Domain Services (AD DS)

Credentials required â€" The wizard requires a domain account that is to be used to query AD DS. At a minimum, this account should be a member of the Domain

Users group in the domain. For each computer to be included in the WMI inventory process, the wizard also requires an account that is a member of the local

Administrators group on that computer.

Reference:

https://social.technet.microsoft.com/wiki/contents/articles/17808.map-toolkit-choose-a-discovery-method.aspx

Davidchercm Highly Voted 1 year, 2 months ago

Credentials required – The wizard requires a domain account that is to be used to query AD DS. At a minimum, this account should be a member of the Domain Users group in the domain. For each computer to be included in the WMI inventory process, the wizard also requires an account that is a member of the local Administrators group on that computer.

answer is correct

upvoted 15 times

Bradobrey Highly Voted 1 year, 2 months ago

Ok. May be user 1 or user3, but principle of least privilege- user3.

upvoted 5 times

RodrigoT 6 months ago

Exactly

upvoted 1 times

tf444 Most Recent 11 months, 2 weeks ago

Why not user 4?

upvoted 1 times

tf444 11 months, 2 weeks ago

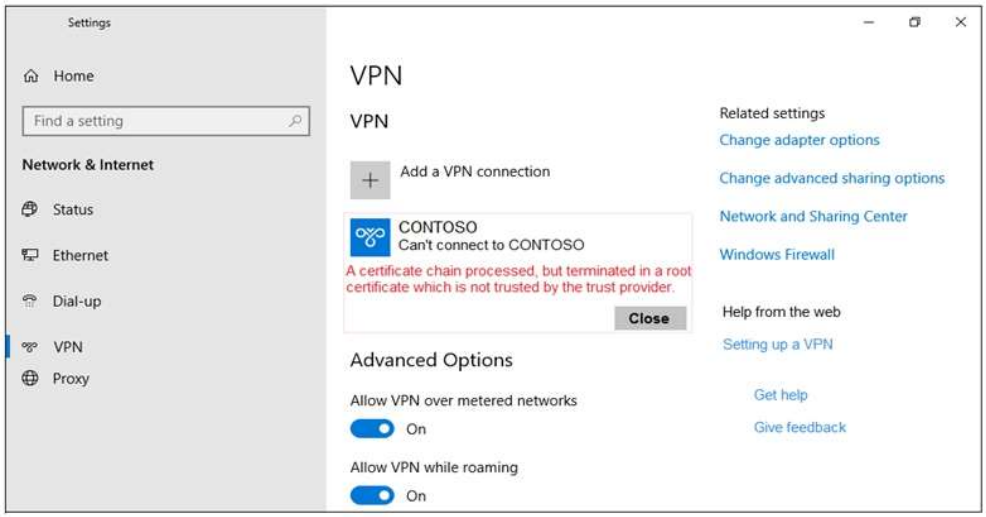
Got it ,the user must be a member of the local Administrators group.

upvoted 3 times

Question #74 *Topic 2*

You are configuring an SSTP VPN.

When you attempt to connect to the VPN, you receive the message shown in the exhibit. (Click the Exhibit tab.)



What should you do to ensure that you can connect to the VPN?

A. Change the VPN type

B. Generate a computer certificate from the root certification authority (CA)

C. Install the root certificate

Correct Answer: *C*

Error message: A certificate chain processed, but terminated in a root certificate which is not trusted by the trust provider.

We need to install a proper root certificate

Note: Each client computer that connects to a VNet using Point-to-Site must have a client certificate installed. You generate a client certificate from the self-signed root certificate, and then export and install the client certificate. If the client certificate is not installed, authentication fails.

Reference:

https://docs.microsoft.com/en-us/azure/virtual-wan/certificates-point-to-site

badguytoo Highly Voted 1 year, 1 month ago

I think should install the root certificate....

upvoted 13 times

AVP_Riga 1 year ago

It will work, but I assume it isn't a best practice...

upvoted 2 times

PiPe Highly Voted 7 months, 4 weeks ago

Selected Answer: C

https://docs.microsoft.com/en-us/windows-server/remote/remote-access/vpn/always-on-vpn/deploy/always-on-vpn-deploy-troubleshooting#error-code-0x800b0109

C is the right answer

upvoted 5 times

RodrigoT 5 months, 1 week ago

Thank you for the link.

upvoted 1 times

PHSmiffy Most Recent 6 months, 2 weeks ago

C is the correct answer. Generating certs from your root CA is bad practice

upvoted 1 times

cor_ 6 months, 3 weeks ago

See answer from PiPe.

upvoted 1 times

Marle 9 months ago

I would go with C. According to the MS docs this error message can be fixed by ensuring that the root certificate is installed on the client computer: https://docs.microsoft.com/en-us/windows-server/remote/remote-access/vpn/always-on-vpn/deploy/always-on-vpn-deploy-troubleshooting

upvoted 4 times

Goofer 11 months ago

The certificate chain includes the root certificate. If the computer is not a member of an domain the root certificate is not automatically deployed to the workstation.

Deploy the internal root certificate with intune(or something else)

upvoted 2 times

Prianishnikov 1 year, 1 month ago

https://social.msdn.microsoft.com/Forums/ie/en-US/5ed119ef-1704-4be4-8a4f-ef11de7c8f34/a-certificate-chain-processed-but-terminated-in-a-root-certificate-which-is-not-trusted-by-the?forum=WAVirtualMachinesVirtualNetwork

upvoted 1 times

FlailingLimbs 1 year, 1 month ago

This issue may occur if the appropriate trusted root certification authority (CA) certificate is not installed in the Trusted Root Certification Authorities store on the client computer.

Note Generally, if the client computer is joined to the domain and if you use domain credentials to log on to the VPN server, the certificate is automatically installed in the Trusted Root Certification Authorities store. However, if the computer is not joined to the domain or if you use an alternative certificate chain, you may experience this issue.

More reading here -
https://social.msdn.microsoft.com/Forums/sqlserver/en-US/5ed119ef-1704-4be4-8a4f-ef11de7c8f34/a-certificate-chain-processed-but-terminated-in-a-root-certificate-which-is-not-trusted-by-the?forum=WAVirtualMachinesVirtualNetwork

upvoted 1 times

HOTSPOT -

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

Name	UPN	Member of
User1	User1@contoso.com	Group1
User2	User2@contoso.com	*None*

You have Windows 10 devices enrolled in Microsoft Intune as shown in the following table.

Name	Ownership	Enrolled by UPN	Active hours
Device1	Personal	User1@contoso.com	10 AM to 6 PM
Device2	Corporate	User2@contoso.com	9 AM to 5 PM
Device3	Corporate	User1@contoso.com	10 AM to 6 PM

You create a Windows 10 update ring that has the following settings:

⇨ Basics:

- Name: Ring1

⇨ Update ring settings:

- Active hours start: 8 AM
- Active hours end: 8 PM

⇨ Assignments:

- Included Groups: All devices
- Excluded Groups: Group1

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 active hours of Device1 are from 8 AM to 8 PM	○	○
The active hours of Device2 are from 8 AM to 8 PM	○	○
The active hours of Device3 are from 8 AM to 8 PM	○	○

Correct Answer:

Answer Area

Statements	Yes	No
The active hours of Device1 are from 8 AM to 8 PM	○	○
The active hours of Device2 are from 8 AM to 8 PM	○	○
The active hours of Device3 are from 8 AM to 8 PM	○	○

Box 1: Yes -

Device1 is a personal device, but personal devices enrolled in Intune are included in the policies unless you use a specific FILTER to exclude personal devices.

Box 3: Yes -

You cannot mix User and Device Groups while Excluding groups. It is not supported, and the Excluded group will be ignored.

Reference:

https://docs.microsoft.com/en-us/mem/intune/fundamentals/filters https://docs.microsoft.com/en-us/mem/intune/protect/windows-10-update-rings

Alfred666 Highly Voted 1 year, 1 month ago

no, yes, yes

upvoted 8 times

RodrigoT 5 months, 1 week ago

Based on what? Link please. There is no mention on Microsoft documentation about update rings and personally-owned devices. I had to do the lab myself. And the result was Y Y Y. Check my comment above.
upvoted 3 times

RodrigoT 5 months ago
From Microsoft: with MDM mobile device management you can set rules and configure settings on "personal" and organization-owned devices. Once enrolled, they receive your rules and settings through policies configured in Intune.
https://docs.microsoft.com/en-us/mem/intune/fundamentals/what-is-intune
upvoted 1 times

Sir_Berus Highly Voted 1 year, 2 months ago
Provided answer is INCORRECT. You can't mix User and Device Groups while Excluding groups. It is not supported, and the Excluded group will be ignored.

Intune doesn't evaluate user-to-device group relationships, and devices of the included users will not be excluded.

https://docs.microsoft.com/en-us/mem/intune/configuration/device-profile-assign#exclude-groups-from-a-profile-assignment
upvoted 8 times

daonga 1 year, 1 month ago
So if I understand correctly, the Update ring applies to all devices regardless? Then this is YYY?
upvoted 3 times

AVP_Riga 1 year ago
NYY, personal device isn't property of company...
upvoted 6 times

[Removed] 11 months, 2 weeks ago
Is there a source that proves personal devices are not served? Can't find anything here: https://docs.microsoft.com/en-us/mem/intune/protect/windows-10-update-rings
upvoted 2 times

RodrigoT 6 months, 2 weeks ago
It doesn't matter, the device1 is enrolled in Microsoft Intune as Ownership: Personal, but this is not a filter. You still have to create a specific filter in Endpoint > Tenant administration > Filters to exclude personal owned devices. There is no filter created in this question. I tested in my lab. So, for me is Y Y Y.

https://docs.microsoft.com/en-us/mem/intune/fundamentals/filters#create-a-filter
upvoted 3 times

Angarali 5 months, 3 weeks ago
the answer is N Y Y, the device will be marked as non compliant, until updated by owner
upvoted 1 times

RodrigoT 5 months, 1 week ago
That's not true, I enrolled my personal laptop in my test MDM. After that I was unable to change my active hours. This setting disappeared, and the first two settings in Windows Update > Advanced options were disabled showing a message that it was because of policies from my organization. I checked in Azure and Endpoint and my device showed Personally owned. Then I disconnected the MDM and the settings came back. I insist Y Y Y.
upvoted 4 times

keenehteek 1 year, 1 month ago
"While update rings can deploy to both device and user groups, consider using only device groups when you also use feature updates."

See bullet point 6 under Create and Assign Update Rings:
https://docs.microsoft.com/en-us/mem/intune/protect/windows-10-update-rings
upvoted 3 times

PiPe Most Recent 7 months, 4 weeks ago
Personal devices are assigned to the update ring, as they are a member of the All Devices group.
You could filter these personal devices out with a filter on a dynamic device group, but that is beyond the scope of this question:
https://stealthpuppy.com/dynamic-software-update-rings/

The Group1 user group exclusion can be ignored as assigning a policy to a static device group and excluding user groups (both dynamic and static) isn't supported. (case 7 on the below URL)
https://docs.microsoft.com/en-us/mem/intune/configuration/device-profile-assign#exclude-groups-from-a-profile-assignment

Device1: Y
Device2: Y
Device3: Y
upvoted 6 times

PiPe 7 months, 4 weeks ago
Correction typo: *(case 4 & 7 on the below URL)
upvoted 2 times

RodrigoT 6 months, 2 weeks ago
After doing a lot of research I agree with you. Y Y Y, because personal devices enrolled in Intune are included in the policies unless you use a specific FILTER to exclude personal devices. Here is the link explaining this:
https://docs.microsoft.com/en-us/mem/intune/fundamentals/filters
upvoted 2 times

rovert94 8 months, 1 week ago
I believe the supplied answer is correct. I think the question is testing our knowledge of filters. In the example they give, they specifically talk about excluding personal devices. Now this would have to be explicitly configured, but I think because, in this question, they specifically point out some devices are personal and some are corporate, I think we have to assume the exclusion for them will be set. But

I would be happy to hear what others think.
https://docs.microsoft.com/en-us/mem/intune/fundamentals/filters

upvoted 1 times

RodrigoT 6 months, 2 weeks ago

Ok, the device1 is enrolled in Microsoft Intune as Ownership: Personal, but this is not a filter. You still have to create a specific filter in Endpoint > Tenant administration > Filters to exclude personal owned devices. There is no filter created in this question. I tested in my lab. So, for me is Y Y Y.

upvoted 1 times

Davidchercm 1 year, 2 months ago

answer looks correct as computer 1 and 3 are in the excluded group 1

upvoted 1 times

Question #76 *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.
Your company has an Azure Active Directory (Azure AD) tenant named contoso.com and a Microsoft Intune subscription.
Contoso.com contains a user named user1@contoso.com.
You have a computer named Computer1 that runs Windows 8.1.
You need to perform an in-place upgrade of Computer1 to Windows 10.
Solution: You start Computer1 from the Windows 10 installation media and use the Install option.
Does this meet the goal?

A. Yes

B. No

Correct Answer: *B*
Instead: From Windows 8.1, you run setup.exe from the Windows 10 installation media.
How To Upgrade To Windows 10 Using ISO File
1. Open your existing Windows edition and locate the ISO file. Now right click on this file and Mount, restart the machine. After rebooting, open File Explorer and locate the DVD drive, you'll find that the ISO file is already mounted to it with a temporary drive letter (as you can see in below shown window, where D: is temporary drive letter). Open this drive and click on the setup.exe file.
Reference:
https://www.kapilarya.com/how-to-upgrade-to-windows-10-using-iso-file

examkiller321 Highly Voted 11 months, 2 weeks ago
Answer is correct, I tested it.
1) I booted my computer (Win 8.1) from Windows 10 ISO
2) I clicked Install, then Upgrade
3) I got a message that the Upgrade option is not available if I run the computer using the Windows installation media.
4) Next is the recommendation to start Windows normally, insert the installation media and run the Windows installer (scenario from question #80)
upvoted 20 times

coppermine 8 months, 3 weeks ago
examkiller321 is correct.
Upon booting from Windows 10 install media using the "Upgrade: Install Windows and keep files, settings, and applications." option, you will be presented with the message "The upgrade option isn't available if you start your computer using Windows installation media."
upvoted 1 times

mikl 9 months, 1 week ago
Tricky question.
upvoted 2 times

verifedtomic Highly Voted 1 year ago
Why is this No? If you start the Windows 10 installation media and select Install, it will start the in-place upgrade wizard.
upvoted 6 times

AVP_Riga 11 months ago
Yes, if you start it from windows, but question about "You start Computer1 from the Windows 10 installation media".
upvoted 5 times

RodrigoT 6 months ago
If you do this you will wipe and install Win 10, not upgrade.
upvoted 1 times

Tanderson2491 Most Recent 6 months ago
Selected Answer: B
You cannot perform an in-place upgrade when booting to install media. It must be started from inside Windows.
upvoted 1 times

moobdoob 8 months, 2 weeks ago
Selected Answer: B
Answer is correct, by booting computer with installation media you do not have the option to keep files, settings and applications.
upvoted 1 times

handsofthelp 9 months, 3 weeks ago
Is correct. You can start Computer 1 from installation media, but will not be able to install.
upvoted 1 times

Jeff8989 1 year ago
Answer is not correct.
upvoted 4 times

Tanderson2491 6 months ago

You can only run in-place upgrades from inside windows. You cannot boot to install media to do an in-place upgrade.

upvoted 1 times

Question #77 *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.
Your company has an Azure Active Directory (Azure AD) tenant named contoso.com and a Microsoft Intune subscription.
Contoso.com contains a user named user1@contoso.com.
You have a computer named Computer1 that runs Windows 8.1.
You need to perform an in-place upgrade of Computer1 to Windows 10.
Solution: You assign a Windows 10 license to User1. You instruct User1 to sign in to Computer1.
Does this meet the goal?

A. Yes

B. No

Correct Answer: *B*
Instead: From Windows 8.1, you run setup.exe from the Windows 10 installation media.
How To Upgrade To Windows 10 Using ISO File
1. Open your existing Windows edition and locate the ISO file. Now right click on this file and Mount, restart the machine. After rebooting, open File Explorer and locate the DVD drive, you'll find that the ISO file is already mounted to it with a temporary drive letter (as you can see in below shown window, where D: is temporary drive letter). Open this drive and click on the setup.exe file.
Reference:
https://www.kapilarya.com/how-to-upgrade-to-windows-10-using-iso-file

verifedtomic Highly Voted 1 year ago

This is correct. Answer is No. User licenses don't have any effect on in-place upgrade.

upvoted 5 times

Cisco Most Recent 5 months, 2 weeks ago

I thought using an E3 or E5 licence would perform the upgrade as per Windows 10/11 Subscription Activation - Windows Deployment | Microsoft Docs
https://docs.microsoft.com/en-us/windows/deployment/windows-10-subscription-activation

upvoted 1 times

NZS 5 months, 1 week ago

Only from Windows 10 Pro to Windows 10 Enterprise

upvoted 1 times

mikl 9 months, 1 week ago

Selected Answer: B

B. No is correct.

upvoted 3 times

Question #78 *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.
Your company has an Azure Active Directory (Azure AD) tenant named contoso.com and a Microsoft Intune subscription.
Contoso.com contains a user named user1@contoso.com.
You have a computer named Computer1 that runs Windows 8.1.
You need to perform an in-place upgrade of Computer1 to Windows 10.
Solution: From Windows 8.1, you run setup.exe from the Windows 10 installation media.
Does this meet the goal?

A. Yes

B. No

Correct Answer: *A*
How To Upgrade To Windows 10 Using ISO File
1. Open your existing Windows edition and locate the ISO file. Now right click on this file and Mount, restart the machine. After rebooting, open File Explorer and locate the DVD drive, you'll find that the ISO file is already mounted to it with a temporary drive letter (as you can see in below shown window, where D: is temporary drive letter). Open this drive and click on the setup.exe file.
Reference:
https://www.kapilarya.com/how-to-upgrade-to-windows-10-using-iso-file

kalmann Highly Voted 1 year ago
Answer A is correct.
upvoted 5 times

Tanderson2491 Most Recent 6 months ago
Selected Answer: A
Answer is correct
upvoted 1 times

moobdoob 8 months, 2 weeks ago
A is correct.
upvoted 1 times

Anderp 8 months, 2 weeks ago
Selected Answer: A
A is correct
upvoted 1 times

mikl 9 months, 1 week ago
A is correct.
upvoted 1 times

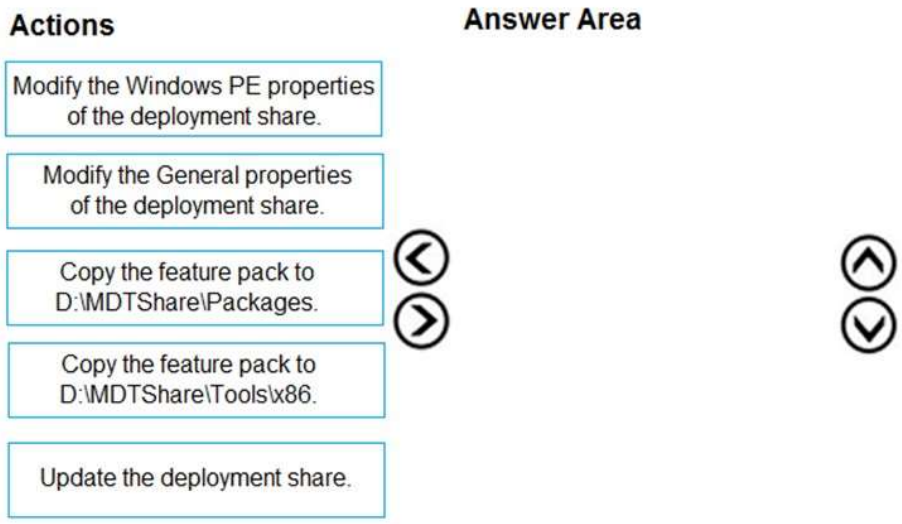
DRAG DROP -

You have a Microsoft Deployment Toolkit (MDT) deployment share that has a path of D:\MDTShare.

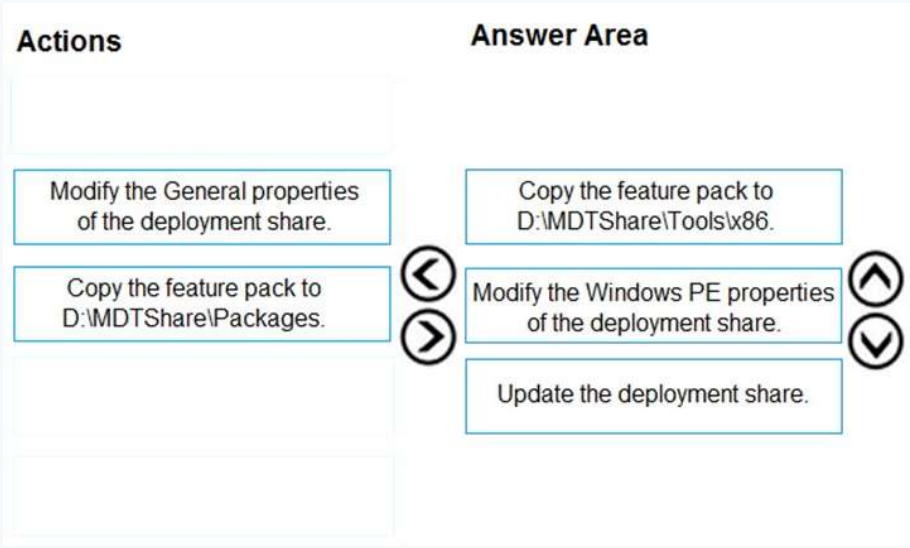
You need to add a feature pack to the boot image.

Which three actions should you perform in sequence? To answer, move the appropriate actions from the list of actions to the answer area and arrange them in the correct order.

Select and Place:



Correct Answer:



Step 1: Copy the feature pack to D:\MDTShare\Tools\x86

Add a feature pack, DaRT 10 (part of MDOP 2015), to the boot images.

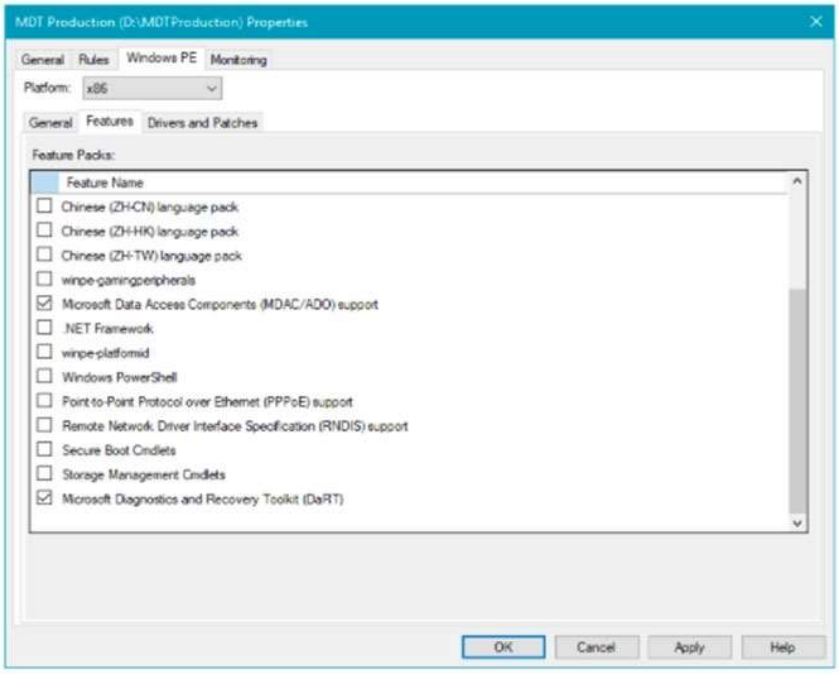
1. Copy the CAB files to the deployment share: MDTShare\Tools\x86

2. In the Deployment Workbench, right-click the MDTShare deployment share and select Properties.

Step 2: Modify the Windows PE properties of the deployment share

3. On the Windows PE tab, in the Platform drop-down list, make sure x86 is selected.

4. On the Features sub tab, select the Microsoft Diagnostics and Recovery Toolkit (DaRT) checkbox.



Etc.

Step 3: Update the deployment share

Like the MDT Build Lab deployment share, the MDT Production deployment share needs to be updated after it has been configured. This is the process during which the Windows PE boot images are created.

Reference:

https://docs.microsoft.com/en-us/windows/deployment/deploy-windows-mdt/deploy-a-windows-10-image-using-mdt

HOTSPOT -

You create a Windows Autopilot deployment profile.

You need to configure the profile settings to meet the following requirements:

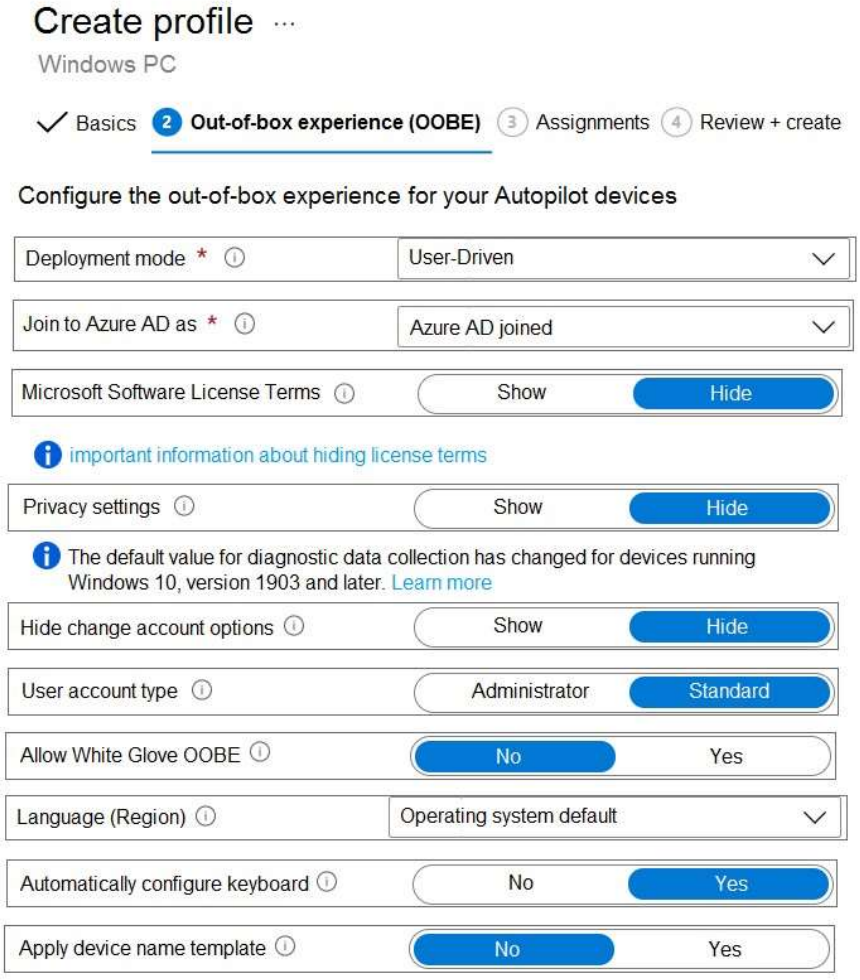
- Automatically enroll new devices and provision system apps without requiring end-user authentication.
- Include the hardware serial number in the computer name.

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

NOTE: Each correct selection is worth one point.

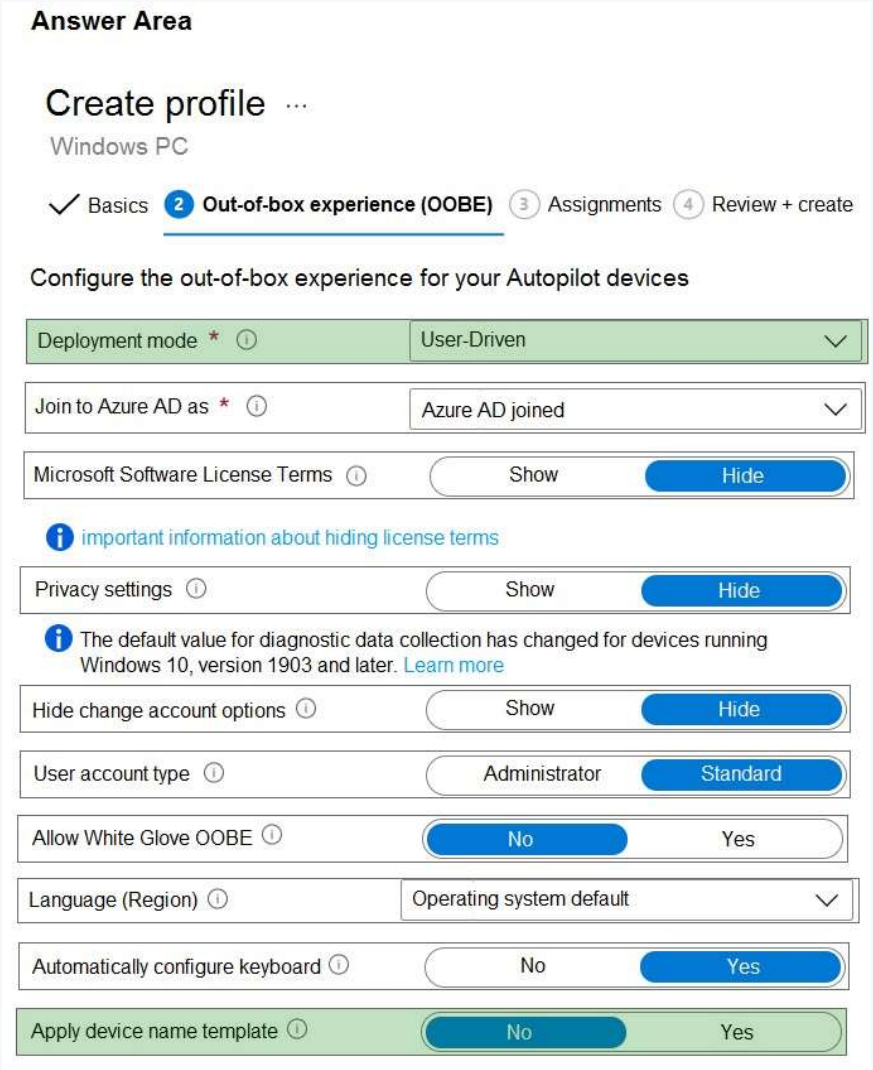
Hot Area:

Answer Area



Correct Answer:

Answer Area



Box 1: Deployment mode User-driven

User-driven: Devices with this profile are associated with the user enrolling the device. User credentials are required to enroll the device.

Change it to: Self-deploying (preview): (requires Windows 10, version 1809 or later) Devices with this profile aren't associated with the user enrolling the device.

User credentials aren't required to enroll the device. When a device has no user associated with it, user-based compliance policies don't apply to it. When using self-deploying mode, only compliance policies targeting the device will be applied.

Box 2: Apply device name template

Apply device name template (requires Windows 10, version 1809 or later, and Azure AD join type): Choose Yes to create a template to use when naming a device during enrollment. Names must be 15 characters or less, and can have letters, numbers, and hyphens. Names can't be all numbers. Use the %SERIAL% macro to add a hardware-specific serial number. Or, use the %RAND:x% macro to add a random string of numbers, where x equals the number of digits to add.

Reference:

https://docs.microsoft.com/en-us/mem/autopilot/profiles

TonySuccess 3 days, 11 hours ago

Mods please correct this, we are paying bro

upvoted 1 times

BRoald 1 week, 6 days ago

The question state: "⇨ Automatically enroll new devices and provision system apps without requiring end-user authentication."

But the answer give the "user driven" mode. But this is FALSE. You still need end-user authentication. (even the explination says that)

The real answer is WHITE GLOVE. If you tab the Windows button 5 times during booting, you enter a Windows screen where you can pre-provision the whole computer without needing any authentication from the end user. The computer will then install everything thats needed (aslong everything is assigned on device. User assigned apps/profiles dont work)

upvoted 3 times

bensrayan 2 weeks, 4 days ago

- Allow white Glove (provision system APPS without requiring....)
- Apply Device name

upvoted 1 times

rockhound 3 weeks, 5 days ago

Correct

upvoted 1 times

Question #81 *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 computer that runs Windows 8.1.
Two days ago, you upgraded the computer to Windows 10.
You need to downgrade the computer to Windows 8.1.
Solution: From View update history in the Settings app, you select Uninstall updates.
Does this meet the goal?

A. Yes

B. No

Correct Answer: *B*
Instead: From the Settings app, you use the Recovery options.
Note: Windows 10 supports a ɹ€Rollbackɹ€ feature that allows you to go back (recover) to the version of Windows (Windows 10, Windows 7 or Windows 8.1) installed on your PC prior to upgrading to the latest version of Windows 10 or Windows 7 / 8.1
1) Click on Start > Settings >
2) In the Windows Setting options click on Update & security
3) In the column of option on the left side of Windows Update click on the 'Recovery' option.
4) Click on 'Get started' to start the Recovery / Rollback process
5) Etc.
Reference:
https://answers.microsoft.com/en-us/windows/forum/windows_10-windows_install/how-to-recover-restore-your-previous-version-of/94368560-9c64-4387-92b9-82a9234216ad

RodrigoT 6 months, 2 weeks ago

Selected Answer: B

B. NO is correct

upvoted 2 times

ercluff 9 months, 1 week ago

B. NO – Uninstall Updates only pertains to quality updates, not feature updates, nor OS versions. Correct step is to choose Recovery and Go Back to the Previous Version of Windows.

upvoted 3 times

TrustMebro 9 months, 2 weeks ago

Answer is correct. Updates has not much do with Windows upgrades.

upvoted 1 times

Question #82 *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.
Your network contains an Active Directory domain. The domain contains member computers that run Windows 8.1 and are enrolled in Microsoft Intune.
You need to identify which computers can be upgraded to Windows 10.
Solution: You install the Microsoft Assessment and Planning Toolkit. From the Microsoft Assessment and Planning Toolkit, you collect inventory data and run the
Windows 8.1 Readiness scenario.
Does this meet the goal?

A. Yes

B. No

Correct Answer: *B*
Instead run the Windows 10 Readiness scenario.
Reference:
https://www.techielass.com/using-maps-azure-readiness/

ANDREVOX Highly Voted 11 months, 3 weeks ago
Answer is Correct.
You should collect inventory data and run the Windows 10 Readiness scenario (Not the Windows 8.1 Readiness scenario).
upvoted 14 times

MR_Eliot Most Recent 5 months ago
Selected Answer: B
B is the answer.
upvoted 1 times

moobdoob 8 months, 2 weeks ago
NOTE: Windows 8.1 readiness scenario, therefore answer is NO.
upvoted 3 times

Will_1_AM 11 months, 3 weeks ago
Should this be correct?
upvoted 1 times

Question #83 *Topic 2*

DRAG DROP -

You have a Microsoft Deployment Toolkit (MDT) deployment share named DS1.

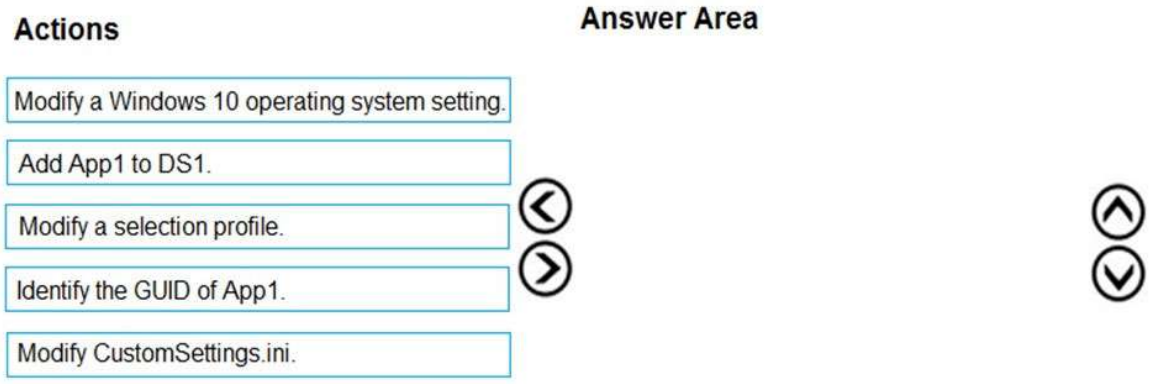
You import a Windows 10 image to DS1.

You have an executable installer for an application named App1.

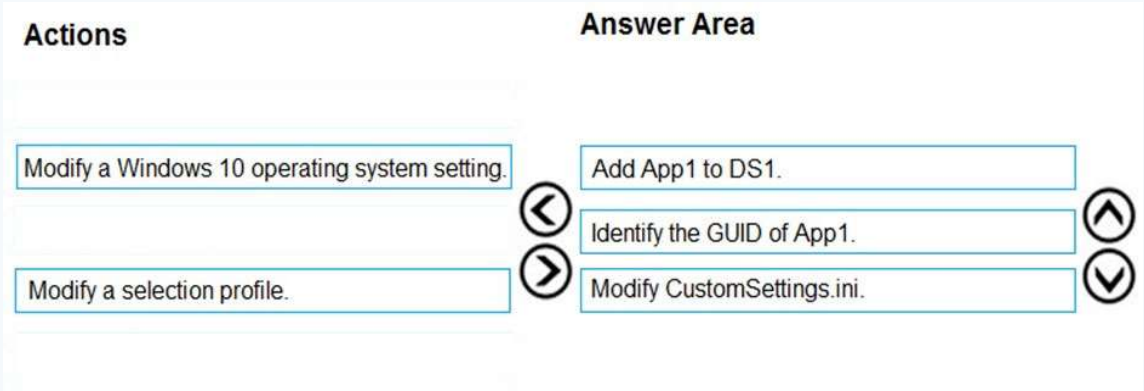
You need to ensure that App1 will be installed for all the task sequences that deploy the image.

Which three actions should you perform in sequence? To answer, move the appropriate actions from the list of actions to the answer area and arrange them in the correct order.

Select and Place:



Correct Answer:



Step 1: Add App1 to DS1 -

Add an application in the MDT console.

Step 2: Identify the GUID of App1.

Step 3: Modify the CustomSettings.ini

It is possible in the CustomSettings.ini file, to check the default program to add the following line:

ApplicationsXXX ={GUID-APPLICATION}

or to force the installation of the application box checked and grayed out:

MandatoryApplicationsXXX ={GUID-APPLICATION}

Reference:

https://rdr-it.com/en/mdt-installation-of-applications-when-deploying-windows/

czara6 Highly Voted 1 year ago

1. Add App to DS1, Identify the GUIS of App1, Modify CS.ini

upvoted 22 times

handsofthelp 10 months, 1 week ago

I have the same opinion.

upvoted 1 times

forummj 8 months, 3 weeks ago

I also thought this was the process to follow, however, in order to confirm, I managed to find this link.

https://rdr-it.com/en/mdt-installation-of-applications-when-deploying-windows/

1. Add the App to the Deployment Share (DS1)
2. Find the GUID
3. Add the GUID to the CustomSettings.ini file

upvoted 6 times

RodrigoT 6 months ago

I guess if you do this it will only affect one task sequence. But the question is to ensure that App1 will be installed for ALL the task sequences that deploy the image. So imagine the structure: You have one reference Win10 Image and several tasks sequences that

personalizes every department or machine type. But you have to alter ALL the tasks sequences to include App1. Then you have to follow the answer provided.

upvoted 1 times

RodrigoT 5 months ago

FINAL ASWER: Well guys, I talked today with a friend of mine. He works with MDT. Without seeing the answers he CONFIRMED the steps mentioned by czara6. Then I showed him the answer provided. He said that it's not "Modify a Windows 10 OS".

upvoted 1 times

RodrigoT 5 months ago

And selection profiles is usually for drivers. To mach drivers with device models.

upvoted 1 times

tcmaggio Highly Voted 1 year ago

I agree with czara6! Makes much more sense as we may see at https://docs.microsoft.com/en-us/previous-versions//bb490304(v=technet.10)?redirectedfrom=MSDN!

upvoted 5 times

Question #84 *Topic 2*

You have 100 computers that run Windows 8.1.

You need to identify which computers can be upgraded to Windows 10.

What should you use?

A. Microsoft Assessment and Planning (MAP) Toolkit

B. Update Compliance in Azure

C. Windows Assessment Toolkit

D. Microsoft Deployment Toolkit (MDT)

Correct Answer: *A*

The data and analysis provided by MAP streamline the planning process for software migration, help assess device driver availability, and allow you to make hardware upgrade recommendations. The MAP Toolkit also gathers performance metrics from computers you are considering for virtualization and includes a feature to model a library of potential host and storage hardware configurations. Use the MAP Toolkit to simplify the planning process for migration to Windows 10

Windows® 8.1, Windows Server 2012, Windows 7, Microsoft Office 2010, Microsoft Office 2013, Microsoft Office 365, Internet Explorer 11, Windows Azure

Platform, Windows Server 2008 R2, Microsoft SQL Server® 2012, Hyper-Vλ„¢, Hyper-V R2, and Microsoft Private Cloud Fast Track.

Reference:

https://social.technet.microsoft.com/wiki/contents/articles/17802.map-toolkit-what-is-the-microsoft-assessment-and-planning-toolkit.aspx

BAbdalla Highly Voted 11 months, 1 week ago

Correct. Option A (MAP).

upvoted 5 times

Beng_ali Most Recent 6 months, 4 weeks ago

Selected Answer: A

A is correct.

upvoted 2 times

Question #85 *Topic 2*

You have 100 computers that run Windows 8.1.
You need to create a report that will assess the Windows 10 readiness of the computers.
What should you use?

A. Windows Assessment and Deployment Kit (Windows ADK)

B. Microsoft Assessment and Planning (MAP) Toolkit

C. Windows Deployment Services (WDS)

D. Microsoft Desktop Optimization Pack (MDOP)

Correct Answer: *B*
The MAP Toolkit is used for multi-product assessment and planning. It assesses a network environment using agentless data collection technologies to gather inventory and performance information. Then provides assessment reports to aid organizations with their IT infrastructure planning.
The main areas of planning covered by MAP:

Migration Planning -

Consolidation/Virtualization -

Private/Public Cloud Planning -

Software Usage Tracking -
Note: The data and analysis provided by MAP streamline the planning process for software migration, help assess device driver availability, and allow you to make hardware upgrade recommendations. The MAP Toolkit also gathers performance metrics from computers you are considering for virtualization and includes a feature to model a library of potential host and storage hardware configurations. Use the MAP Toolkit to simplify the planning process for migration to Windows 10
Windows® 8.1, Windows Server 2012, Windows 7, Microsoft Office 2010, Microsoft Office 2013, Microsoft Office 365, Internet Explorer 11, Windows Azure
Platform, Windows Server 2008 R2, Microsoft SQL Server® 2012, Hyper-Vג„¢, Hyper-V R2, and Microsoft Private Cloud Fast Track.
Reference:
https://www.techielass.com/using-maps-azure-readiness/
https://social.technet.microsoft.com/wiki/contents/articles/1640.microsoft-assessment-and-planning-map-toolkit-getting-started.aspx

BAbdalla Highly Voted 11 months, 1 week ago
Option B (MAP) is Correct.
upvoted 6 times

HOTSPOT -

You have a Microsoft 365 tenant.

You have a Windows 10 update ring named Policy1 as shown in the following exhibit.

Basics

Name	Policy1
Description	– –

Update ring settings

Update settings

Servicing channel	Semi-Annual Channel
Microsoft product updates	Allow
Windows drivers	Block
Quality update deferral period (days)	0
Feature update deferral period (days)	0
Set feature update uninstall period (2–60 days)	14

A Windows 10 Feature update deployment named Policy2 is configured as shown in the following exhibit.

Deployment settings

Name	Policy2
Description	– –
Feature deployment settings	
Name	Windows 10 2004

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

Name	Windows 10 edition	Policy applied
Device1	Windows 10 Enterprise, version 20H2	Policy1
Device2	Windows 10 Pro, version 2004	Policy2
Device3	Windows 10 Enterprise, version 20H2	Policy2

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 will install feature updates twice a year.	○	○
Device2 will install feature update 20H2.	○	○
Device3 will be downgraded to feature update 2004.	○	○

Correct Answer:

Answer Area

Statements	Yes	No
Device1 will install feature updates twice a year.	○	○
Device2 will install feature update 20H2.	○	○
Device3 will be downgraded to feature update 2004.	○	○

Box 1: Yes -

Box 2: No -

Device2 already has feature update 20H2.

Box 3: No -

Device3 has a higher build than 2004.

Reference:

https://docs.microsoft.com/en-us/mem/intune/protect/windows-10-update-rings

Omar86 Highly Voted 12 months ago

Shouldnt it be Yes, No, No

The Feature Update Policy is set to 2004. Meaning Feature Updates would Freeze at 2004 and not update to 20H2 isnt that correct?

upvoted 19 times

[Removed] 11 months, 2 weeks ago

Yes, agree:
"With Feature updates for Windows 10 and later in Intune, you can select the Windows feature update version that you want devices to remain at, like Windows 10 version 1909 or a version of Windows 11. Intune supports setting a feature level to any version that remains in support at the time you create the policy."
https://docs.microsoft.com/en-us/mem/intune/protect/windows-10-feature-updates

upvoted 6 times

auton 11 months, 3 weeks ago

I'm guessing there's something left out of the question or it's missing severe context.

So; it could be a Yes, Yes, No for a good reason.
Essentially update ring "Policy1" is only applied to Device1, so it applies the SAC, deferral days etc. Hence Device1 will install feature updates twice a year.

Now, updates and features are not blocked even if they aren't specified with an update ring policy such as Policy1 for Device1.

The Device2 has the Policy2 which is a feature update, but yes, the computer is already in the targeted build. Now, just because Device2 is not configured with the "Policy1" update ring, it doesn't stop updating in the future, meaning it will eventually be updated to 20H2 most likely. Just not with the deferral days etc. that come through policy1.

Device3 is a no-brainer.

upvoted 2 times

Solaris2002 7 months, 1 week ago

We have this very setup in our environment. It is Yes, No, No

If Feature Update is set to say, 2004, and the computer has 2004. It will stay locked-in on that Feature Update unless otherwise changed. It will still receive monthly quality updates.

upvoted 1 times

RodrigoT 6 months ago

Well, the Policy2 feature update deployment has just the "Name" set as "Windows 10 2004". Obviously part of the image is cropped. I tried to find this image on the internet but no success. Anyway, I found a link:
https://docs.microsoft.com/en-us/mem/intune/protect/windows-10-feature-updates
that states: "With Feature updates for Windows 10 and later in Intune, you can select the Windows feature update version that you want devices to remain at, like Windows 10 version 1909... The device updates to the version of Windows specified in the policy. A device that already runs a later version of Windows remains at its current version... Devices won't install a new Windows version until you modify or remove the Feature updates policy". (tested in my lab). So, if in this question the Policy2 has a 2004 version set then the answer provided is wrong. The correct is Y N N.

upvoted 3 times

RodrigoT 5 months, 1 week ago

I get now the image. It is "Feature deployment settings Name". But this shows only when you check the properties of a Feature Updates policy on Endpoint > Devices | Feature updates for Windows 10 and later (Preview). When you are creating a policy (profile) it shows: "Feature update to deploy" and there you can choose, not type, the Windows version that you want to remain. I tested in my lab. Anyway, the answer provided is wrong. The correct is Y N N.

upvoted 2 times

Goofer Highly Voted 10 months, 3 weeks ago

Y - Policy 1
N - Policy 2 - Device is has already Feature update 2004 - No new Feature updates will be installed
N - Policy 2 - Device is has higher build than 2004 - No new Feature updates will be installed

upvoted 11 times

RodrigoT 5 months ago

Perfect simple answer 👌

upvoted 1 times

MR_Eliot Most Recent 5 months ago

Omar86 is right. Correct answer is Y,N,N

upvoted 1 times

PiPe 7 months, 4 weeks ago

This question is missing info to be able to answer the 2nd question.
Policy2 only has a name but the question is missing the policy settings.
So it could be either Yes, No, No or Yes, Yes, No
If on the exam the policy2 settings state a specific OS version to stick with (Win10 2004) then Device2 will not upgrade to 20H2. So I guess the answer is YNN if we go ahead with this assumption.

upvoted 3 times

RodrigoT 5 months, 1 week ago

Check my second comment above and you will understand.

upvoted 1 times

a92876 8 months ago

The answer is YYN. 1 and 3 are self-explanatory.
In 2 the only thing configured for the update ring is the Name. Just the display name! Implying everything else is on defaults --> Y.

upvoted 2 times

moobdoob 8 months, 2 weeks ago

Gotta go with goofer here.

Y
N
N

upvoted 1 times

Question #87 *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.
Your company has an Azure Active Directory (Azure AD) tenant named contoso.com and a Microsoft Intune subscription.
Contoso.com contains a user named user1@contoso.com.
You have a computer named Computer1 that runs Windows 8.1.
You need to perform an in-place upgrade of Computer1 to Windows 10.
Solution: You assign an Enterprise Mobility + Security license to User1. You instruct User1 to sign in to Computer1.
Does this meet the goal?

A. Yes

B. No

Correct Answer: *B*
Instead: From Windows 8.1, you run setup.exe from the Windows 10 installation media.
How To Upgrade To Windows 10 Using ISO File
1. Open your existing Windows edition and locate the ISO file. Now right click on this file and Mount, restart the machine. After rebooting, open File Explorer and locate the DVD drive, you'll find that the ISO file is already mounted to it with a temporary drive letter (as you can see in below shown window, where D: is temporary drive letter). Open this drive and click on the setup.exe file.
Reference:
https://www.kapilarya.com/how-to-upgrade-to-windows-10-using-iso-file

ercluff 9 months, 1 week ago

B. NO - Win 8.1 doesn't automatically upgrade to Enterprise Win10. "Devices must be running Windows 10 Pro, version 1703, or later and be Azure Active Directory joined, or hybrid domain joined with Azure AD Connect. Customers who are federated with Azure Active Directory are also eligible." See reference: https://docs.microsoft.com/en-us/windows/deployment/deploy-enterprise-licenses; https://blogs.technet.microsoft.com/skypehybridguy/2018/09/21/intune-upgrade-windows-from-pro-to-enterprise-automatically/

upvoted 4 times

MR_Eliot 5 months ago

I agree.

upvoted 1 times

HOTSPOT -

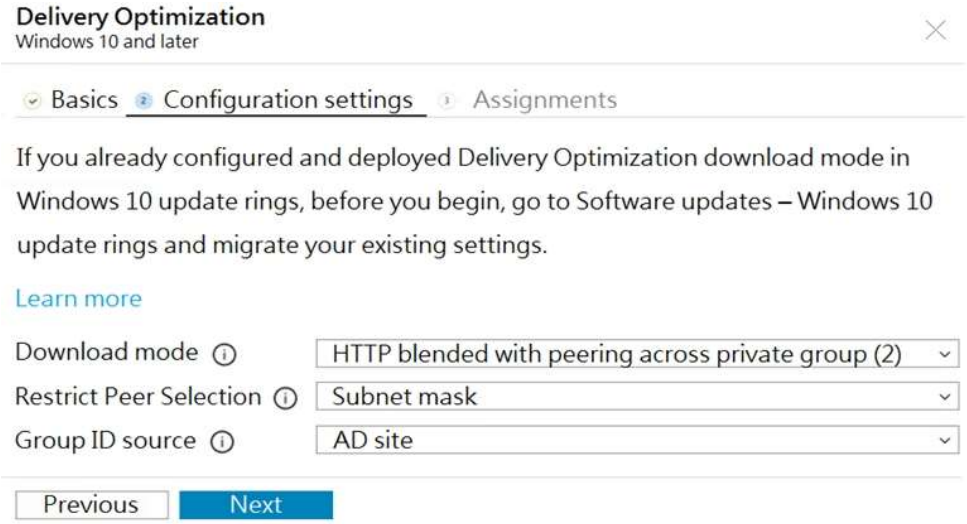
Your network contains an on-premises Active Directory domain that contains the locations shown in the following table.

Name	Internal IP address	Public Network Address Translation (NAT) IP address	Active Directory site
Location1	10.10.0.0/16	131.107.15.0/24	Site1
Location2	10.20.0.0/16	131.107.16.0/24	Site1
Location3	172.16.0.0/16	131.107.196.0/24	Site2

In Microsoft Intune, you enroll the Windows 10 devices shown in the following table.

Name	IP address
Device1	10.10.0.50
Device2	10.20.1.150
Device3	10.10.1.155
Device4	172.16.0.30

You have a Delivery Optimization device configuration profile applied to all the devices. The profile is configured as shown in the following exhibit.



From which devices can Device1 and Device2 get updates? To answer, select the appropriate options in the answer area.

NOTE: Each correct selection is worth one point.

Hot Area:

Answer Area

Device1:

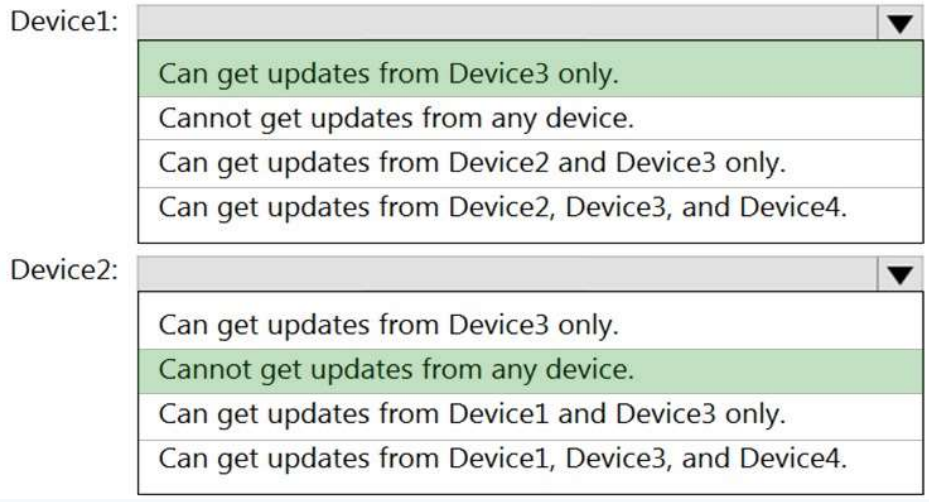
- Can get updates from Device3 only.
- Cannot get updates from any device.
- Can get updates from Device2 and Device3 only.
- Can get updates from Device2, Device3, and Device4.

Device2:

- Can get updates from Device3 only.
- Cannot get updates from any device.
- Can get updates from Device1 and Device3 only.
- Can get updates from Device1, Device3, and Device4.

Correct Answer:

Answer Area



Reference:

https://garvis.ca/2021/06/01/delivery-optimization-know-your-options/

czara6 Highly Voted 1 year ago

Device 1: only from Device 3
Device 2: cannot get updates from any device

upvoted 21 times

NorthBlueEdd 6 months, 2 weeks ago

This is correct. If logically answering the question.

upvoted 1 times

musiman 9 months, 3 weeks ago

I think czara6 is correct.

Select a method to restrict peer selection
Starting in Windows 10, version 1803, set this policy to restrict peer selection via selected option. Currently the available options include: 0 = NAT, 1 = Subnet mask, and 2 = Local Peer Discovery. The subnet mask option applies to both Download Modes LAN (1) and Group (2).

If Group mode is set, Delivery Optimization will connect to locally discovered peers that are also part of the same Group (have the same Group ID).
source: https://docs.microsoft.com/en-us/windows/deployment/update/waas-delivery-optimization-reference#select-a-method-to-restrict-peer-selection

upvoted 2 times

RodrigoT 6 months ago

No, he'not. The ip address are /16 not /24 meaning that the netmask is 255.255.0.0. So Device1 will talk to Device3 because they are in the same subnet 10.10.x.x. And since the Download mode is set to HTTP blended with peering across private group, Device1 will also talk to Device2 via NAT because they are in the same Site1. Following the logic Device2 will talk to Devices 1 and 3 via Site 1 NAT. The answer provided is correct.

upvoted 2 times

Nerovats74 4 days, 8 hours ago

Restrict Peer Selection is set to subnetmask, so answer is correct

upvoted 1 times

blueninja 12 months ago

Wrong. Based on my search, I reckon the given answers are correct.

HTTP blended with peering across a private group (2): Peering occurs on devices in the same Active Directory Site (if it exists) or the same domain. When this option is selected, peering crosses your NAT IP addresses

https://docs.microsoft.com/en-us/mem/intune/configuration/delivery-optimization-settings#delivery-optimization

upvoted 9 times

CGtheConqueror 9 months ago

I appreciate your use of the word reckon, blueninja is correct. the keyword here is HTTP blended with peering across a private group (2)

upvoted 4 times

DogeZaemon 11 months, 1 week ago

There is a restriction based on the Subnet.
Normally the Device1 gets updates from Device3
Device2 doesn't get update from any device

upvoted 7 times

RodrigoT 6 months, 2 weeks ago

But if Group mode (Group ID source in Endpoint) is set, Delivery Optimization will connect to locally discovered peers that are ALSO part of the same Group (have the same Group ID). In this case AD Site. And the devices are in the same Site1. So, for me the

answer provide is correct. Check the link:

https://docs.microsoft.com/en-us/windows/deployment/do/waas-delivery-optimization-reference#select-a-method-to-restrict-peer-selection

upvoted 1 times

LoganBundrant91 Highly Voted 9 months, 3 weeks ago

So who's correct?

upvoted 7 times

RodrigoT 6 months ago

The ip addresses are /16 not /24 meaning that the netmask is 255.255.0.0. So Device1 will talk to Device3 because they are in the same subnet 10.10.x.x. And since the Download mode is set to "HTTP blended with peering across private group", Device1 will also talk to Device2 via NAT because they are in the same Site1. Following the logic Device2 will talk to Devices 1 and 3 via Site 1 NAT. The answer provided is correct.

upvoted 1 times

randdrick Most Recent 5 months ago

I'm agree with czara.
Beacause if peering is doing with NAT Adresses, the devices must be in the same subnet.
Device 1 and Device 3 are in the same subnet (10.10.255.255), not Device 2 (10.20.255.255)
(see restrictions bellow)
https://docs.microsoft.com/en-us/windows/deployment/do/waas-delivery-optimization-reference#select-a-method-to-restrict-peer-selection

upvoted 1 times

MR_Eliot 5 months ago

Read follwing for the correct answer! Upvote to confirm.
- HTTP blended with peering across a private group (2): Peering occurs on devices in the same Active Directory Site (if it exists) or the same domain. When this option is selected, peering crosses your NAT IP addresses.
- Restricts peer selection: Restricts peer selection via the selected option. Applies to Download Modes NAT (1) and Group (2).
- Subnet Location 1 = Subnet Location 2
- Site1 has following locations: Location1 & Location2.

So, the correct answer should be:
Device1: Only device 2
Device2: Only device 1
Device3: none

https://docs.microsoft.com/en-us/mem/intune/configuration/delivery-optimization-settings#delivery-optimization

upvoted 1 times

PiPe 7 months, 4 weeks ago

Since 'Restrict Peer Selection' is set to limit based on subnet mask, the answers are:
Device1: Can get updates from device3 only
Device2: Cannot get updates from any device

upvoted 6 times

AVR31 5 months, 1 week ago

Yes, since peer selection is restricted to network mask, this is the correct answer.

upvoted 1 times

moobdoob 8 months, 2 weeks ago

My answer:
Device1: Can get updates from Device3 only.
Device2: Cannot get updates from any device.

Based on information from the following:
https://garvis.ca/2021/06/01/delivery-optimization-know-your-options/

HTTP blended with peering across private group: Computer can get updates from computers in the same Active Directory Domain Services (AD DS) site, or in the same domain. This option can be dangerous when computers are geographically dispersed, so all of a sudden your computers in Seattle are downloading from a cache in Paris. Only use this option if your AD sites are properly configured and maintained.

upvoted 2 times

forummj 8 months, 3 weeks ago

I found this guide, https://garvis.ca/2021/06/01/delivery-optimization-know-your-options/

This suggests that due to the Restriction option being available only when you choose one of the Peering options, and being able to limit the peering to a subnet, it is my belief that Device 1 can only get updates from Device 3, and Device 2 can't receive updates from any other device. That is what I'm going to go with anyway.

upvoted 2 times

Goofer 11 months ago

Download mode: HTTP blended with peering across a private group (2): Peering occurs on devices in the same Active Directory Site (if it exists) or the same domain. When this option is selected, peering crosses your NAT IP addresses.
Restrict Peer Selection: Restricts peer selection to a specific group of devices.
Group ID Source: Restricts peer selection to a specific group of devices by source.
An Ad site can have more than one Subnet. The Restrict Peer Selection is set on one Subnet. So updates can only download from other computers fron one subnet.
Device https://www.examtopics.com/exams/microsoft/md-101/view/14/#1: only from Device 3
Device 2: cannot get updates from any device

upvoted 3 times

lijk_manson 11 months, 3 weeks ago

@blueninja
So if i'm right? Device 1 and 2 from all devices?

upvoted 2 times

Question #89 *Topic 2*

DRAG DROP -

Your network contains an Active Directory domain.

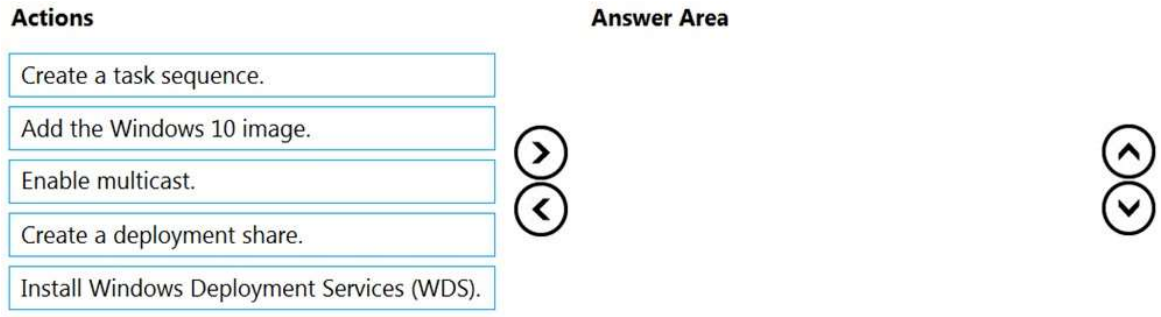
You install the Microsoft Deployment Toolkit (MDT) on a server.

You have a custom image of Windows 10.

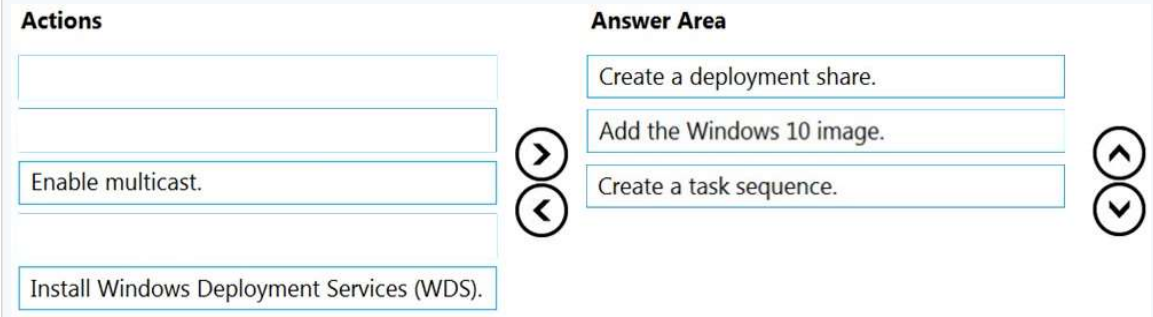
You need to deploy the image to 100 devices by using MDT.

Which three actions should you perform in sequence? To answer, move the appropriate actions from the list of actions to the answer area and arrange them in the correct order.

Select and Place:



Correct Answer:



Step 1: Create a deployment share.

Set up the MDT production deployment share.

Step 2:Add the Windows 10 image.

Add a custom image.

The next step is to add a reference image into the deployment share with the setup files required to successfully deploy Windows 10.

Step 3: Create a task sequence.

Create the deployment task sequence.

Reference:

https://docs.microsoft.com/en-us/windows/deployment/deploy-windows-mdt/deploy-a-windows-10-image-using-mdt

Moderator Highly Voted 8 months, 4 weeks ago

The given answer is correct.

upvoted 6 times

RodrigoT 6 months, 2 weeks ago

I agree.

upvoted 1 times

AVR31 Most Recent 5 months, 1 week ago

From the given list, first you need WDS. MDT does not install WDS and you cannot multicast to 100 devices without WDS.
You then need to enable multicast no WDS.
And the third step is to create the TS.

upvoted 1 times

RodrigoT 5 months ago

Totally wrong, sorry. WDS is a very old way to wipe and load static images. Welcome to MDT.

upvoted 1 times

TaboloDude 9 months, 2 weeks ago

@b3arb0yb1m
What are you talking about? Those options aren't even available in the answer?

upvoted 4 times

b3arb0yb1m 10 months, 2 weeks ago

Step 3: Add a custom image
The next step is to add a reference image into the deployment share with the setup files required to successfully deploy Windows 11.
When adding a custom image, you still need to copy setup files (an option in the wizard) because Windows 10/11 stores additional components in the Sources\SxS folder which is outside the image and may be required when installing components.

Add the Windows 11 Enterprise x64 custom image

Step 6: Create the deployment task sequence

upvoted 2 times

Question #90 *Topic 2*

You have a Microsoft 365 tenant.

You plan to enable Enterprise State Roaming.

Which three types of data will sync across devices? Each correct answer presents a complete solution.

NOTE: Each correct selection is worth one point.

A. Microsoft Teams settings

B. mouse settings

C. Microsoft Edge Chromium settings

D. internet passwords

E. desktop theme settings

Correct Answer: *CDE*

But what data is actually being roamed? You can divide the data into two different areas:

Windows settings -

Application data -

For Windows settings, these are settings that are built into the operating system, generally what personalize the users device. For an overview of what's being roamed, see the list below:

(E) Theme â€" desktop theme, taskbar settings, etc.

Internet Explorer settings â€" recently opened tabs, favorites, etc.

(C) Edge browser settings â€" favorites, reading list

(D) Passwords â€" Internet passwords, Wi-Fi profiles, etc.

Language preferences â€" keyboard layouts, system language, dateand time, etc.

Ease of access â€" high contrast theme, Narrator, Magnifier, etc.

Other Windows settings â€" command prompt settings, application list, etc.

Reference:

https://msendpointmgr.com/2016/02/14/synchronize-user-and-application-settings-to-azure-ad-with-enterprise-state-roaming/

fvibes Highly Voted 9 months, 1 week ago

Selected Answer: BDE

Should be BDE as Chromium based browser is not supported.
https://docs.microsoft.com/en-us/azure/active-directory/devices/enterprise-state-roaming-windows-settings-reference#windows-settings-overview

upvoted 10 times

RodrigoT 6 months, 2 weeks ago

The word Chromium is there just to confuse you. Microsoft Edge is "based" in the Chromium project. CDE is correct.

upvoted 5 times

veteran_tech 6 months, 2 weeks ago

Agreed, sticking with CDE

upvoted 1 times

MR_Eliot Most Recent 5 months ago

Selected Answer: BDE

What's changing with Microsoft Edge?
With the new Microsoft Edge, the sync solution isn't tied to Windows sync ecosystem. This enables us to offer Microsoft Edge across all the platforms, such as Windows 7, Windows 8.1, iOS, Android and macOS. This also enables us to offer sync for non-primary accounts on Windows. In addition, we can ship Microsoft Edge at a more frequent and flexible release cadence than Windows. (For more information, see Windows updates to support the next version of Microsoft Edge. All these factors highlighted the need to re-assess Microsoft Edge participation in the ESR offering.

ESR is framed as a Windows product offering with promises about how data from Windows devices is handled, but Microsoft Edge sync will extend beyond Windows devices. And, as the data roams across these devices, it makes it difficult to define the Microsoft Edge sync offering in the context of ESR. To simplify how sync works and is managed, and to accommodate the changes that are highlighted, a decision was made to pull Microsoft Edge out of the ESR offering.

upvoted 1 times

Cisco 5 months, 2 weeks ago

Edge is not supported due to it adopting the chromium platform, its removed from the ESR sync for this reason as outlined in this article:
https://docs.microsoft.com/en-us/deployedge/microsoft-edge-enterprise-state-roaming#:~:text=Enterprise%20State%20Roaming%20(ESR)%20provides,disconnected%20from%20Windows%20sync%20framework

So my vote is BDE

upvoted 2 times

RodrigoT 5 months ago

When it says: "its sync solution is now disconnected from Windows sync framework" it does NOT mean that Edge settings are not roaming with ESR. If you keep reading the article: "Microsoft Edge will continue to support most of the abilities provided in the ESR

offering. When a user is signed into their windows device with an Azure Active Directory (Azure AD account), Microsoft Edge will implicitly inherit that Identity on first launch of the new browser."
You will just need to take an extra step:
"After a user has explicitly consented to turning on sync in the new Microsoft Edge, the browser will sync all the browser data, such as favorites, passwords, and history."
Go for CDE and pass the test.
upvoted 1 times

Moderator 6 months ago
https://www.anoopcnair.com/how-to-use-enterprise-state-roaming-esr/

It's basically B, C, D and E. Kinda feels like an outdated question, or they intentionally have 4 right answers. Wouldn't surprise me that this question if worded differently and/or isn't on the actual exam anymore. We'll see :)
upvoted 1 times

Garito 7 months, 1 week ago
Selected Answer: BDE
Chromium settings not supported
upvoted 3 times

RodrigoT 6 months, 2 weeks ago
The word Chromium is there just to confuse you. Microsoft Edge is "based" in the Chromium project. CDE is correct.
upvoted 3 times

Deric 1 week, 3 days ago
I am afraid Fvibes and Cisco seem to be correct. "As a result of Microsoft Edge adopting the Chromium platform, its sync solution is now disconnected from Windows sync framework" https://learn.microsoft.com/en-us/deployedge/microsoft-edge-enterprise-state-roaming
upvoted 1 times

Mlt1865 7 months, 2 weeks ago
https://docs.microsoft.com/en-us/azure/active-directory/devices/enterprise-state-roaming-windows-settings-reference
BCE
upvoted 2 times

moobdoob 8 months, 2 weeks ago
Selected Answer: BDE
Correct
upvoted 2 times

IykeP 8 months, 3 weeks ago
Selected Answer: BDE
Correct Answer is BDE
upvoted 4 times

NKG123 9 months, 3 weeks ago
Mouse instead of Edge chromium

This article applies to the Microsoft Edge Legacy HTML-based browser launched with Windows 10 in July 2015. The article does not apply to the new Microsoft Edge Chromium-based browser released on January 15, 2020. For more information on the Sync behavior for the new Microsoft Edge, see the article Microsoft Edge Sync.
upvoted 2 times

b3arb0yb1m 10 months, 2 weeks ago
What data roams?
Windows settings: the PC settings that are built into the Windows operating system. Generally, these are settings that personalize your PC, and they include the following broad categories:

Theme, which includes features such as desktop theme and taskbar settings.
Internet Explorer settings, including recently opened tabs and favorites.
Microsoft Edge browser settings, such as favorites and reading list.
Passwords, including Internet passwords, Wi-Fi profiles, and others.
Language preferences, which include settings for keyboard layouts, system language, date and time, and more.
Ease of access features, such as high-contrast theme, Narrator, and Magnifier.
Other Windows settings, such as mouse settings.
upvoted 3 times

Skorne 10 months, 3 weeks ago
Should be BCDE 4 correct answer
https://docs.microsoft.com/en-us/azure/active-directory/devices/enterprise-state-roaming-faqs
"Other Windows settings, such as mouse settings."
upvoted 4 times

ercluff 9 months, 1 week ago
B, D, and E. Not C. Your reference clearly states it does not include Edge Chromium browser.
upvoted 1 times

Will_1_AM 11 months, 3 weeks ago
Correct. Internet password is included. https://docs.microsoft.com/en-us/azure/active-directory/devices/enterprise-state-roaming-faqs
upvoted 1 times

[Removed] 11 months, 2 weeks ago
I would even say there are 4 correct answers... :S. "Microsoft Edge browser settings, such as favorites and reading list." But I will stick CDE...
upvoted 1 times

[Removed] 11 months, 2 weeks ago

Sorry I meant also B, mouse settings, should be right: "Other Windows settings, such as mouse settings."

upvoted 1 times

Anon1212 8 months, 3 weeks ago

BDE, If exploder or edge were mentioned than perhaps CDE.

upvoted 1 times

Question #91 *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.
Your company uses Windows Autopilot to configure the computer settings of computers issued to users.
A user named User1 has a computer named Computer1 that runs Windows 10. User1 leaves the company.
You plan to transfer the computer to a user named User2.
You need to ensure that when User2 first starts the computer, User2 is prompted to select the language setting and to agree to the license agreement.
Solution: You perform a remote Windows Autopilot Reset.
Does this meet the goal?

A. Yes

B. No

Correct Answer: *B*
Instead:
Windows Autopilot user-driven mode lets you configure new Windows devices to automatically transform them from their factory state to a ready-to-use state. This process doesn't require that IT personnel touch the device.
The process is very simple. Devices can be shipped or distributed to the end user directly with the following instructions:
Unbox the device, plug it in, and turn it on.
Choose a language (only required when multiple languages are installed), locale, and keyboard.
Connect it to a wireless or wired network with internet access. If using wireless, the user must establish the Wi-Fi link.
Specify your e-mail address and password for your organization account.
The rest of the process is automated. The device will:
Join the organization.
Enroll in Intune (or another MDM service)
Get configured as defined by the organization.
Reference:
https://docs.microsoft.com/en-us/windows/deployment/windows-autopilot/windows-autopilot-reset

PESK Highly Voted 2 years, 11 months ago
Answer B is correct as these customizations are already done by the IT admin. Per the second link below: Windows Autopilot Reset removes personal files, apps, and settings and *reapplies a device's original settings*, maintaining its identity connection to Azure AD and its management connection to Intune so that the device is once again ready for use. Windows Autopilot Reset takes the device back to a business-ready state, allowing the next user to sign in and get productive quickly and simply. See https://www.youtube.com/watch?v=nE5XSOBV0rI and https://docs.microsoft.com/en-us/windows/deployment/windows-autopilot/windows-autopilot-reset
upvoted 21 times

RodrigoT 5 months, 1 week ago
I agree. To ensure that when User2 first starts the computer, User2 is prompted to select the language setting and to agree to the license agreement you need a user-driven profile. I simple reset does not ensure that.
upvoted 1 times

JohnxLarusso Highly Voted 2 years, 10 months ago
B is correct. The user does not set anything. User authenticates then device sets the configs. Once Autopilot Reset is triggered, the reset process starts.

After reset, the device:
- Sets the region, language, and keyboard.
- Connects to Wi-Fi.
- If you provided a provisioning package when Autopilot Reset is triggered, the system will apply this new provisioning package. Otherwise, the system will re-apply the original provisioning package on the device.
- Is returned to a known good managed state, connected to Azure AD and MDM.
upvoted 19 times

JN_311 Most Recent 2 months ago
Selected Answer: A
Answer A, done it many times
upvoted 1 times

4Shawsy 8 months ago
Selected Answer: B
Autopilot Reset removes personal files, apps, and settings on a device but retains the connection to Azure AD and Intune. The key here is personal data; Autopilot Reset basically only removes the user profile instead of wiping the entire OS drive. This makes Autopilot Reset a sort of middle-ground option, where you're wiping a device and maintaining the enrollment state but not maintaining the user data.
upvoted 3 times

BeamerV 9 months, 1 week ago
Selected Answer: B

Windows Autopilot Reset takes the device back to a business-ready state, allowing the next user to sign in and get productive quickly and simply. Specifically, Windows Autopilot Reset:

Removes personal files, apps, and settings.
Reapplies a device's original settings.
Sets the region, language, and keyboard to the original values.
Maintains the device's identity connection to Azure AD.
Maintains the device's management connection to Intune.

https://docs.microsoft.com/en-us/mem/autopilot/windows-autopilot-reset

upvoted 1 times

Moderator 9 months, 2 weeks ago

I'm actually strongly leaning to A.

While creating a Autopilot Deployment Profile, you can actually choose whether or not the user has to accept the User Agreement and Language Region.
You set the Language (Region) option to 'User Select' and the Microsoft Software License Terms to 'Show'.

Best example:
https://docs.microsoft.com/en-us/windows/deployment/windows-autopilot/demonstrate-deployment-on-vm

upvoted 3 times

Moderator 9 months, 2 weeks ago

I actually see the next question talks about a deployment profile, so the answer might be B afterall, since the default options make sure the language and license agreement will be hidden/automatically configured.

upvoted 1 times

Richmawdsley 1 year, 3 months ago

I think the key bit here is, as always in the question:

"User2 is prompted to select the language setting and to agree to the license agreement."

The user will of course be prompted for their language... but they won't be prompted to accept the license agreement because the device has remained attached to the tenant.

Thus Answer B is correct.

Probably.

upvoted 2 times

Jonasye 1 year, 3 months ago

I'm stick to Yes, I've tried it a few times, after reset and login, it requires me to select language

upvoted 1 times

Jeffoort 1 year, 6 months ago

The Windows Autopilot Reset process automatically keeps information from the existing device:

Set the region, language, and keyboard to the original values.
Wi-Fi connection details.
Provisioning packages previously applied to the device
A provisioning package present on a USB drive when the reset process is started
Azure Active Directory device membership and MDM enrollment information.

upvoted 1 times

_Rico 1 year, 6 months ago

Completed this process 4 times yesterday and remote autopilot reset does bring it back to the region screen but keeps all the apps etc that were provisioned.

upvoted 1 times

j0eyv 1 year, 10 months ago

Correct answer is B! This is because a remote AP reset from the Endpoint console does not show the region/language screens. The remote Fresh Start feature will show the region/language settings. So again, B is correct.

upvoted 6 times

Junh 2 years ago

so what is correct answer then?what should I do if I want user to select language?
should IT person do local windows autopilot reset?

upvoted 1 times

mikl 9 months, 2 weeks ago

Depends on how you have configured your Autopilot deployment profiles : https://docs.microsoft.com/en-us/mem/autopilot/profiles

upvoted 1 times

loganharris 2 years ago

From the reference link "Windows Autopilot Reset removes personal files, apps, and settings and reapplies a device's original settings, maintaining its identity connection to Azure AD and its management connection to Intune so that the device is once again ready for use. Windows Autopilot Reset takes the device back to a business-ready state, allowing the next user to sign in and get productive quickly and simply."

upvoted 2 times

Redders 2 years, 8 months ago

Definitely B as Windows Autopilot Reset process automatically retains information from the existing device including LANGUAGE.

upvoted 12 times

nolancl 3 years ago

Correct answer is A and the document you linked supports that. Device has already been configured once.

upvoted 11 times

Parzival 2 years, 10 months ago

I agree I have read it twice.

upvoted 2 times

Cronus1610 1 year, 5 months ago

The answer is A.

From the link...

"Windows Autopilot Reset takes the device back to a business-ready state, allowing the next user to sign in and get productive quickly and simply. Specifically, Windows Autopilot Reset:

- Removes personal files, apps, and settings.
- Reapplies a device's original settings.
- Maintains the device's identity connection to Azure AD.
- Maintains the device's management connection to Intune"

upvoted 3 times

HOTSPOT -

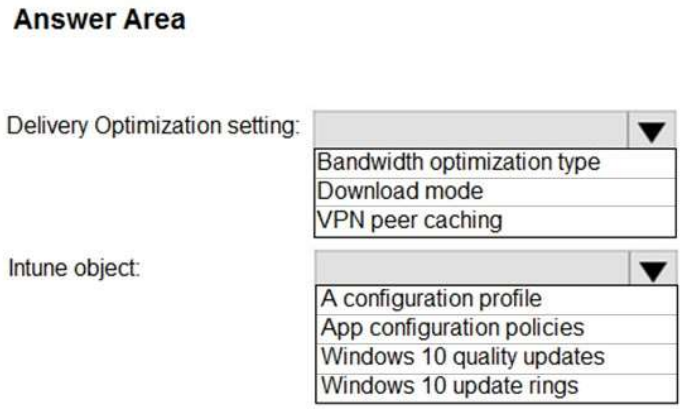
You have 100 Windows 10 devices enrolled in Microsoft Intune.

You need to configure the devices to retrieve Windows updates from the internet and from other computers on a local network.

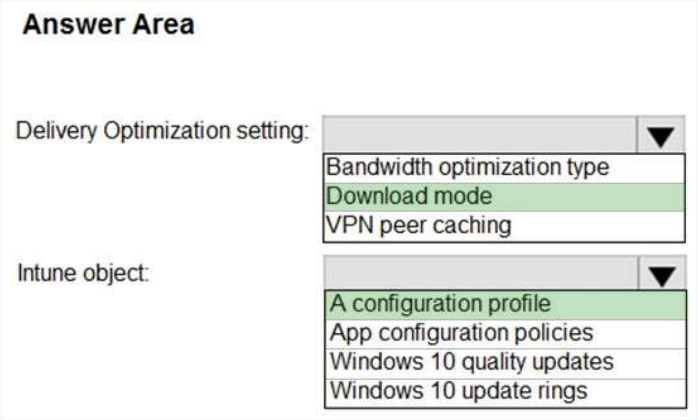
Which Delivery Optimization setting should you configure, and which type of Intune object should you create? To answer, select the appropriate options in the answer area.

NOTE: Each correct selection is worth one point.

Hot Area:



Correct Answer:



Box 1: Download mode -

Download mode specifies the download method that Delivery Optimization uses to download content.

Box 2: A configuration profile -

Delivery Optimization settings are configured as part of the device configuration profile.

Reference:

https://docs.microsoft.com/en-us/mem/intune/configuration/delivery-optimization-settings https://docs.microsoft.com/en-us/mem/intune/configuration/delivery-optimization-windows

MR_Eliot 5 months ago

Provided answer is correct.

upvoted 1 times

Question #93 *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.
Your company uses Windows Autopilot to configure the computer settings of computers issued to users.
A user named User1 has a computer named Computer1 that runs Windows 10. User1 leaves the company.
You plan to transfer the computer to a user named User2.
You need to ensure that when User2 first starts the computer, User2 is prompted to select the language setting and to agree to the license agreement.
Solution: You create a new Windows Autopilot user-driven deployment profile.
Does this meet the goal?

A. Yes

B. No

Correct Answer: *A*
Windows Autopilot user-driven mode lets you configure new Windows devices to automatically transform them from their factory state to a ready-to-use state. This process doesn't require that IT personnel touch the device.
The process is very simple. Devices can be shipped or distributed to the end user directly with the following instructions:
Unbox the device, plug it in, and turn it on.
Choose a language (only required when multiple languages are installed), locale, and keyboard.
Connect it to a wireless or wired network with internet access. If using wireless, the user must establish the Wi-Fi link.
Specify your e-mail address and password for your organization account.
The rest of the process is automated. The device will:
Join the organization.
Enroll in Intune (or another MDM service)
Get configured as defined by the organization.
Reference:
https://docs.microsoft.com/en-us/windows/deployment/windows-autopilot/user-driven

Mike666 Highly Voted 2 years, 9 months ago
A is correct, as the following link describes
https://docs.microsoft.com/en-us/windows/deployment/windows-autopilot/user-driven
upvoted 16 times

ercluff 1 year, 1 month ago
Your cited reference shows it will cause the required OOBE, but only on a NEW computer. A Fresh Start would have to precede the user-driver part.
upvoted 2 times

nolancl Highly Voted 3 years ago
Correct answer is B. Auto-driven deployment is meant for new machines from the factory for an OOBE. Cannot be used on a machine previously deployed without Remote reset.
upvoted 10 times

lucidgreen 1 year, 7 months ago
The question says user-driven.
upvoted 6 times

ercluff 1 year, 1 month ago
Mike666 reference shows: "Windows Autopilot user-driven mode lets you configure new Windows 10 devices to automatically transform them from their factory state to a ready-to-use state. " Note the NEW specification as nolancl cited. A user-driver mode only helps a machine in a previously unused state. The answer must be NO.
upvoted 1 times

Anon1212 Most Recent 9 months, 1 week ago
Exam reference MD101, page 18 table 1-6; Windows AutoPilot User-driven mode "Provision Windows 10 on a new windows 10 device. Devices will be set up by a member of the organization and configured for that person to use."
If org member configures user OBEE to ask for language and to accept MS license, I do not see why not. It accomplishes goal.
upvoted 3 times

Moderator 9 months, 2 weeks ago
Correct answer is indeed A.

While creating a Autopilot Deployment Profile, you choose 'User-driven' as Deployment Mode, you choose for 'Show' at Microsoft Software License Terms and at Language Region you select 'User Select'.
upvoted 1 times

Goofer 11 months ago
Answer is Yes, Under 'Windows Autopilot deployment profiles' you can set the option 'language (Region)' to 'User select' if the Deployment mode is User-Driven.
upvoted 2 times

Gonch 1 year, 4 months ago

I would say Yes to this, but the whole scenario is badly worded. Setting the option 'Convert all targeted devices to Autopilot' in the Basics screen when creating the new profile will allow for a redeployment using autopilot (which meets the objectives). The step that is missing, but assumed, is that you force the device into an OOBE experience again ready for the new user.

upvoted 2 times

MikeMatt2020 1 year, 4 months ago

Correct Answer is A:
The other two possible solutions are "Autopilot Reset" and "Self-Deploying Profile"
To start, this question SUCKS. Performing an Autopilot Reset does NOT achieve our goals of ensuring that User2 is prompted to agree to the license agreement. AP Reset will RETAIN previously configure OOBE settings, wipe user data, settings, and apps. The user will immediately be prompted to sign-in with his/her AAD creds. It is also NOT self-deploying profile as the option to prompt the user to accept the license agreement is GREYED OUT when configuring a self-deploying profile. Self-deployment mode is also specifically for shared devices/kiosks and isn't intended for individual users. A user-driven profile is our best answer here, although it's incomplete. To answer this question, we'd need to first create a NEW user-driven profile that allows the user to accept the license agreement. THEN, we'll need to reset the device so that the new user can configure language, locale, Wi-Fi connection, pull down the user-driven profile, and be prompted to accept the license agreement.

upvoted 7 times

Merma 1 year, 5 months ago

B. No is the correct answer. Yes with AutoPilot you can create a User-driven profile with the option for User2 to be "prompted to select the language setting". However, the option to agree to the license agreement is not available. The only choice is to Show or Hide the Microsoft Software License Terms. See link:
https://docs.microsoft.com/en-us/mem/autopilot/profiles

upvoted 2 times

Mr01z0 1 year, 6 months ago

The problem with this question is the phrasing of it.

"Does this meet the goal"

Creating the new Autopilot profile is a possible step in the right direction, but not the last step that is needed to actually set the computer in the desired state.

So the question remains, how close to the goal does the question giver wants us to be?

Obviously we all want to fresh start the device or wipe it, that would be a much faster approach, but then nowhere is stated that the specific machine is already in Intune or that they wish to use an existing Autopilot profile.

Still I would lean towards A because following that path will lead to a working solution.
- create deployment profile
- assign computer to it
- reset computer

upvoted 2 times

Anthony_2770 1 year, 7 months ago

B (No)
People are correctly pointing out that you can setup this user-driven deployment profile with the required settings and hence the answer must be Yes, but the question is testing you out if you know whether or not it is the correct action to be doing in this scenario and as has been pointed out by various other people it is NOT.

upvoted 7 times

ExamStudy101 1 year, 2 months ago

"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." Sorry Anthony, I normally trust your answers but a lot of people are getting incorrectly caught up with these questions thinking that it needs to be done the 'correct' way. The correct way is not what these questions ask, it only asks if the answer will give the desired outcome which in this case it appears to do so.

upvoted 3 times

hawkens 1 year, 7 months ago

Answer is YES! YOu can select that the users is asked for a language and agreement.

Out-of-box experience (OOBE) (user drive).
Edit
Deployment mode
User-Driven
Join to Azure AD as
Hybrid Azure AD joined
Skip AD connectivity check (preview)
Yes
Language (Region)
User select
Microsoft Software License Terms
Hide
Privacy settings
Hide
Hide change account options
Hide
User account type
Administrator
Allow White Glove OOBE
Yes
Apply device name template
No

upvoted 3 times

amymay101 1 year, 7 months ago

Answer is not correct, its B, this is a deployment profile and does get the 'used' device in a state ready for the next user

upvoted 2 times

Anthony_2770 1 year, 7 months ago
Do you mean "It does not get the used device in a state ready for the next user."
upvoted 1 times

mfalkjunk 1 year, 7 months ago
Answer is correct.

You can configure the AutoPilot User Driven mode in a configuration profile.

Navigate to: Endpoint Manager admin center > Devices > Windows > Windows Deployment Autopilot profiles. On Step 2, select "User-Driven" for the Deployment Mode. There you can configure to have the end-user accept the EULA.

Also, you can choose "No" under the "Automatically configure keyboard" setting. This will force the end-user to make that choice.
upvoted 2 times

amymay101 1 year, 8 months ago
there seems to be missing info to make an informed decision, but with that there is i would say NO. Creating a new AutoPilot user-driven deployment profile is irrelevant as the device would need to be wiped and assigned to the new deployment profile. It also does not detail what settings are configured eg. auto accept license agreement
upvoted 3 times

amymay101 1 year, 8 months ago
ok so after reading the 3 scenarios for this question this one probably seems the most likely..
upvoted 1 times

vinnyct 1 year, 9 months ago
It's Yes
upvoted 1 times

CvdK 1 year, 10 months ago
B. first comment by nolancl is correct. De device has already been enrolled. First needs a Wipe (back to OOBE) before a (new) profile can be applied. See also https://deviceadvice.io/2019/08/09/autopilot-reset-what-does-it-do-how-is-it-different/
upvoted 5 times

loganharris 2 years ago
I believe B is correct. After reading the reference link it does not mention the license agreement just selecting a language.
upvoted 3 times

loganharris 2 years ago
disregard is Yes as you can configure additional settings to have the user accept
upvoted 2 times

Question #94 *Topic 2*

You have a Microsoft 365 subscription.
You have 20 computers that run Windows 10 and are joined to Microsoft Azure Active Directory (Azure AD).
You plan to replace the computers with new computers that run Windows 10. The new computers will be joined to Azure AD.
You need to ensure that the desktop theme, taskbar settings, and Bluetooth settings are available on the new computers.
What should you use?

A. Folder Redirection

B. The Microsoft SharePoint Migration Tool

C. Enterprise State Roaming

D. Roaming user profiles

Correct Answer: *D*
Roaming User Profiles redirects user profiles to a file share so that users receive the same operating system and application settings on multiple computers.
When a user signs in to a computer by using an account that is set up with a file share as the profile path, the user's profile is downloaded to the local computer and merged with the local profile (if present). When the user signs out of the computer, the local copy of their profile, including any changes, is merged with the server copy of the profile. Typically, a network administrator enables Roaming User Profiles on domain accounts.
Reference:
https://docs.microsoft.com/en-us/windows-server/storage/folder-redirection/folder-redirection-rup-overview

Henkjanarie 2 days ago
Selected Answer: C
Enterprise State Roaming is the correct answer - Azure AD.
upvoted 1 times

Deric 1 week, 3 days ago
Selected Answer: C
C - Enterprise State Roaming. This is Azure AD, not AD.
upvoted 1 times

thuba_TD 2 weeks, 4 days ago
Selected Answer: C
correct answer is C
upvoted 2 times

MR_Eliot 5 months ago
Selected Answer: C
Correct answer is C
upvoted 2 times

mathlete1083 5 months, 1 week ago
Selected Answer: C
C for the win!
upvoted 2 times

AVR31 5 months, 1 week ago
Selected Answer: C
That would be C, Enterprise State Roaming.
upvoted 2 times

RodrigoT 5 months, 1 week ago
Wrong link and wrong answer. The correct is C. ESR.
upvoted 2 times

Question #95 *Topic 2*

You have a Microsoft 365 E5 subscription that contains 100 iOS devices enrolled in Microsoft Intune.
You need to deploy a custom line-of-business (LOB) app to the devices by using Intune.
Which extension should you select for the app package file?

A. .intunemac

B. .apk

C. .ipa

D. .appx

Correct Answer: *C*
iOS/iPadOS LOB apps: Select Line-of-business app as the app type, select the App package file, and then enter an iOS/iPadOS installation file with the extension
.ipa.
Reference:
https://docs.microsoft.com/en-us/mem/intune/apps/apps-add

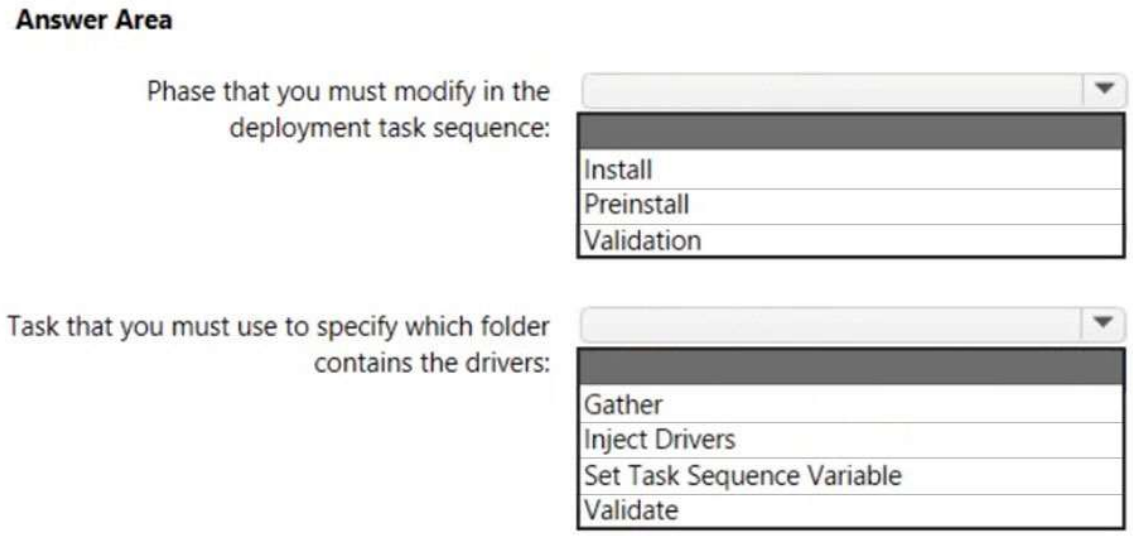
raduM 4 weeks, 1 day ago
i stand corrected ios sorry. ipa is correct
upvoted 1 times

raduM 1 month ago
https://docs.microsoft.com/en-us/mem/intune/apps/lob-apps-windows
appx all the way
upvoted 1 times

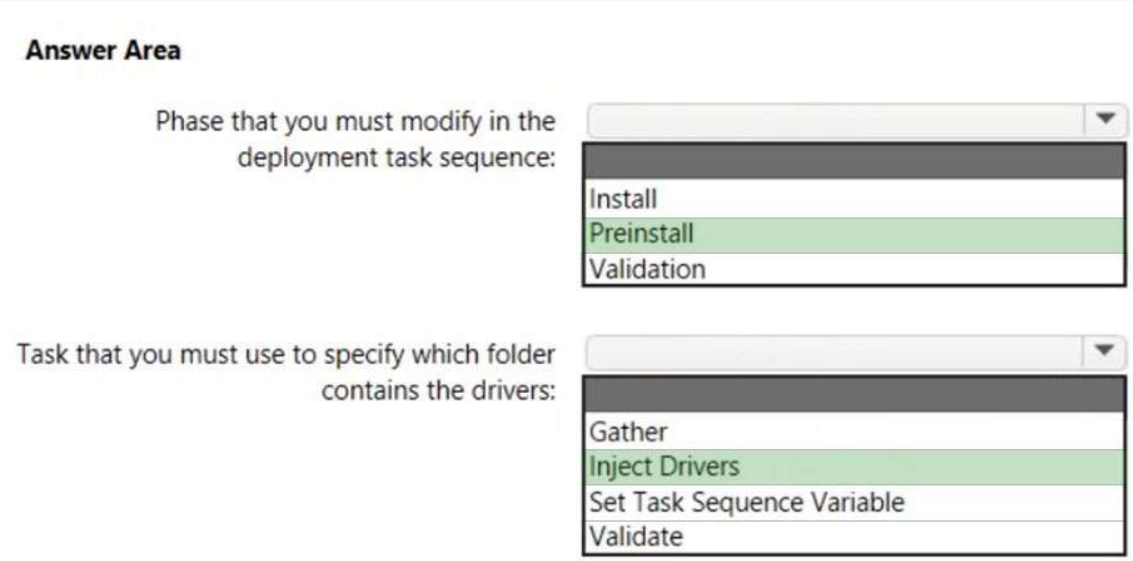
neobahamutk 1 month ago
Wrong ref. For IOS use .ipa
https://docs.microsoft.com/en-us/mem/intune/apps/lob-apps-ios
upvoted 1 times

Question #96 *Topic 2*

HOTSPOT -
You manage a Microsoft Deployment Toolkit (MDT) deployment share named DS1. DS1 contains an Out-of-Box Drivers folder named Windows 10 x64 that has subfolders in the format of {make name}\{model name}.
You need to modify a deployment task sequence to ensure that all the drivers in the folder that match the make and model of the computers are installed without using PnP detection or selection profiles.
What should you do? To answer, select the appropriate options in the answer area.
NOTE: Each correct selection is worth one point.
Hot Area:



Correct Answer:



Box 1: Preinstall -

PREINSTALL -
Completes any tasks that need to be done (such as creating new partitions) before the target operating system is deployed.
Incorrect:
* INSTALL
Installs the target operating system on the target computer.
* VALIDATION
Identifies that the target computer is capable of running the scripts necessary to complete the deployment process.

Box 2: Inject Drivers -

Inject Drivers -
This task sequence step injects drivers that have been configured for deployment to the target computer.
The unique properties and settings for the Inject Drivers task sequence step type are:
* Property: TypeSet this read-only type to Inject Drivers.
* Settings

Install only matching drivers: Injects only the drivers that the target computer requires and that match what is available in Out-of-Box Drivers
Install all drivers: Installs all drivers
Selection profile: Installs all drivers in the selected profile
Reference:
https://docs.microsoft.com/en-us/mem/configmgr/mdt/toolkit-reference

Question #97 *Topic 2*

You use the Microsoft Deployment Toolkit (MDT) to manage Windows 10 deployments.
From Deployment Workbench, you modify the WinPE settings and add PowerShell support.
You need to generate a new set of WinPE boot image files that contain the updated settings.
What should you do?

A. From the Operating Systems node, import a new operating system.

B. From the Deployment Shares node, update the deployment share.

C. From the Packages node, import a new operating system package.

D. From the Advanced Configuration node, create new media.

Correct Answer: *B*
Distribute content to the CM01 (for example) distribution portal.
In Configuration Manager, you can distribute all packages needed by a task sequence in a single task. In this section, you distribute packages that have not yet been distributed to the CM01 distribution point.
On CM01:
1. Open the Deployment Workbench, right-click Deployment Shares and click New Deployment Share. Use the following settings for the New Deployment Share
Wizard:
Deployment share path: D:\MDTProduction
Share name: MDTProduction$
Deployment share description: MDT Production
Options: <default settings>
2. Etc.
Reference:
https://docs.microsoft.com/en-us/windows/deployment/deploy-windows-cm/finalize-the-os-configuration-for-windows-10-deployment-with-configuration-manager

DRAG DROP -

You have a Microsoft Deployment Toolkit (MDT) server named MDT1.

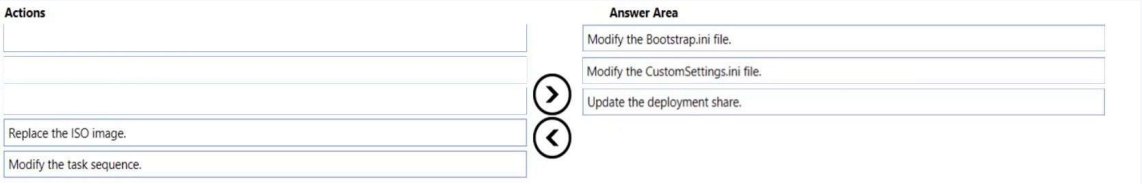
When computers start from the LiteTouchPE_x64.iso image and connect to MDT1, the welcome screen appears as shown in the following exhibit.

You need to prevent the welcome screen from appearing when the computers connect to MDT1.

Which three actions should you perform in sequence? To answer, move the appropriate actions from the list of actions to the answer area and arrange them in the correct order.

Select and Place:

Correct Answer:



Box 1: Modify the Bootstrap.ini file.

Add this to your bootstrap.ini file and then update the deployment share and use the new boot media created in that process:

SkipBDDWelcome=YES -

Box 2: Modify the CustomSettings.ini file.

SkipBDDWelcome -

Indicates whether the Welcome to Windows Deployment wizard page is skipped.

For this property to function properly it must be configured in both CustomSettings.ini and BootStrap.ini. BootStrap.ini is processed before a deployment share

(which contains CustomSettings.ini) has been selected.

Box 3: Update the deployment share.

Reference:

https://docs.microsoft.com/en-us/mem/configmgr/mdt/toolkit-reference#table-6-deployment-wizard-pages

rockhound 3 weeks, 5 days ago

Correct

upvoted 1 times

HOTSPOT -

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

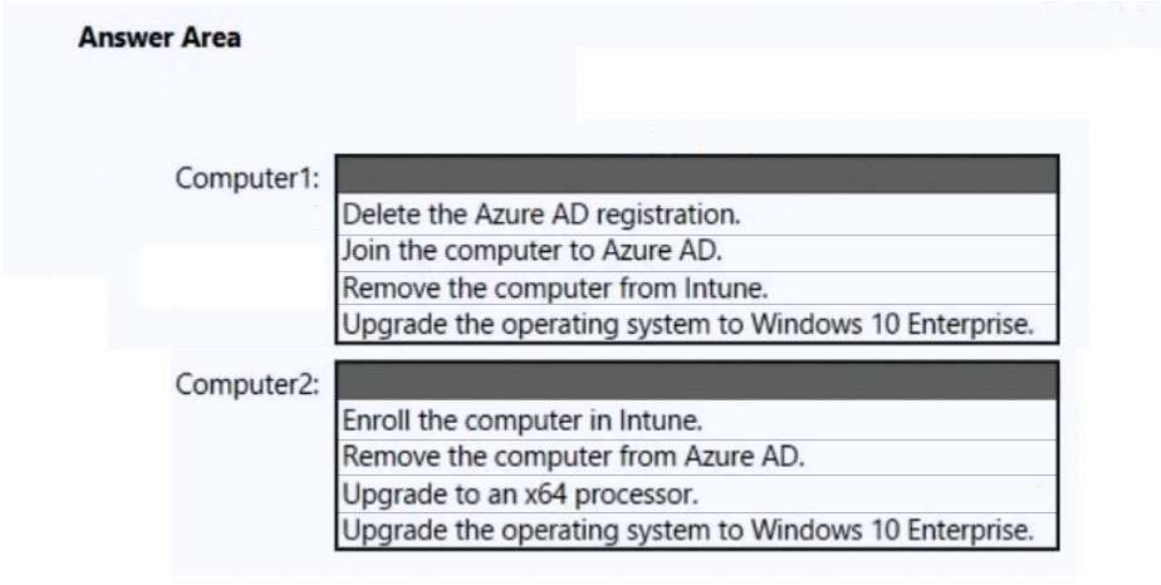
Name	Azure AD join type	Enrolled in Microsoft Intune	Operating system	Processor type
Computer1	Azure Active Directory (Azure AD) registered	Yes	Windows 10 Pro	x64
Computer2	Azure Active Directory (Azure AD) joined	No	Windows 8.1	x86

You plan to use Windows Autopilot.

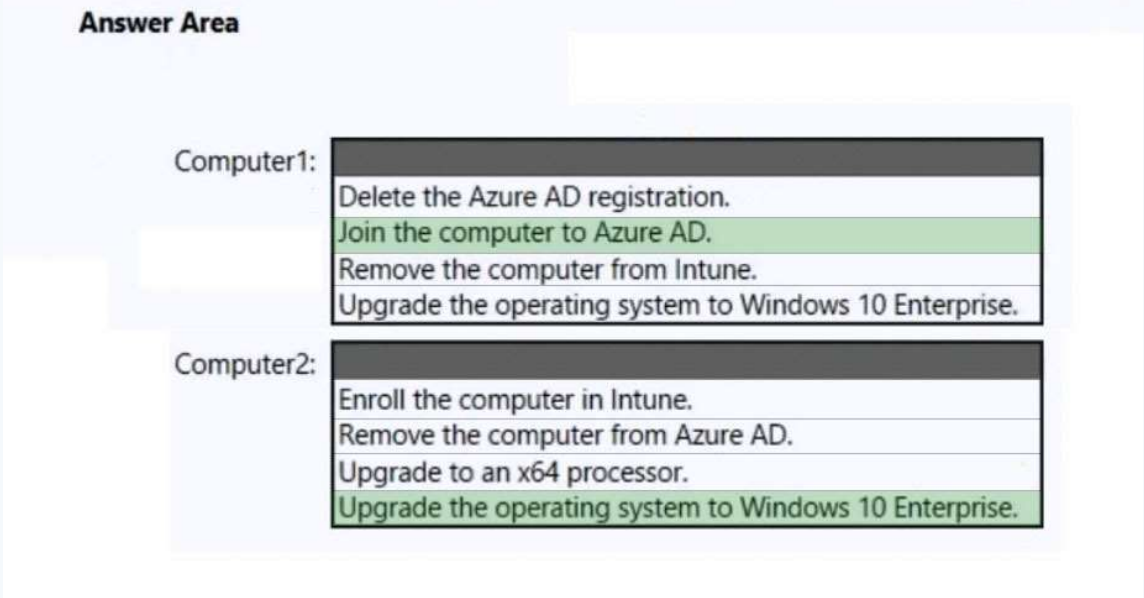
You need to ensure that the computers support automatic registration in Windows Autopilot.

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

Hot Area:



Correct Answer:



Box 1: Join the computer to Azure AD.

You can deploy hybrid Azure AD-joined devices by using Intune and Windows Autopilot.

Box 2: Upgrade the operating system to Windows 10 Enterprise

The device to be enrolled must follow these requirements:

Use Windows 11 or Windows 10 version 1809 or later.

Reference:

https://docs.microsoft.com/en-us/mem/autopilot/windows-autopilot-hybrid

TonySuccess 2 weeks, 4 days ago

I'm not sure on the validity of this question, unless anybody else can clarify for the rest of us?

Computer 1: This has Windows 10 Pro (Valid, as is Enterprise for Auto Registration to Autopilot). It also is in Intune already, which as per the links provided by jenread and asturmark means it is already ready for Autopilot.

I presume the options will differ if the questions still appears in the Exam.

upvoted 1 times

jenraed 2 weeks, 4 days ago

According to https://docs.microsoft.com/en-us/mem/autopilot/software-requirements, computers need Win 10/11 to enroll in Autopilot, so it looks right to me.

upvoted 1 times

asturmark 3 weeks, 4 days ago

i think the provided answer is wrong according to this link:
https://docs.microsoft.com/en-us/mem/autopilot/automatic-registration
For automatic registration in autopilot is necessary that the device is enrolled in intune (azure ad join is not a requirement) and it is windows 10/11

upvoted 2 times

Question #100 *Topic 2*

HOTSPOT -

You have a server named Server1 and computers that run Windows 8.1. Server1 has the Microsoft Deployment Toolkit (MDT) installed.

You plan to upgrade the Windows 8.1 computers to Windows 10 by using the MDT deployment wizard.

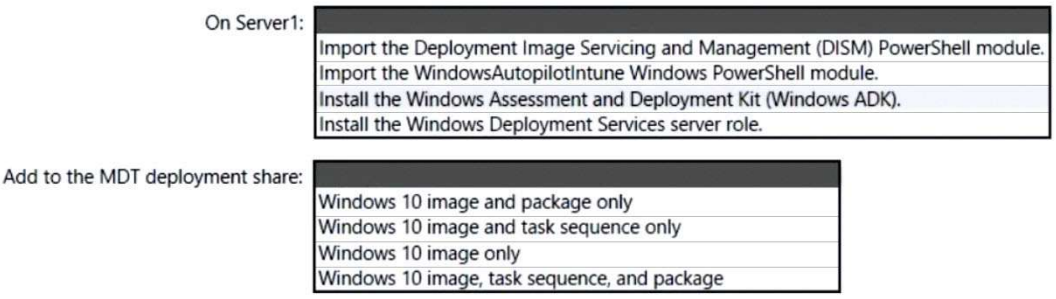
You need to create a deployment share on Server1.

What should you do on Server1, and what are the minimum components you should add to the MDT deployment share? To answer, select the appropriate options in the answer area.

NOTE: Each correct selection is worth one point.

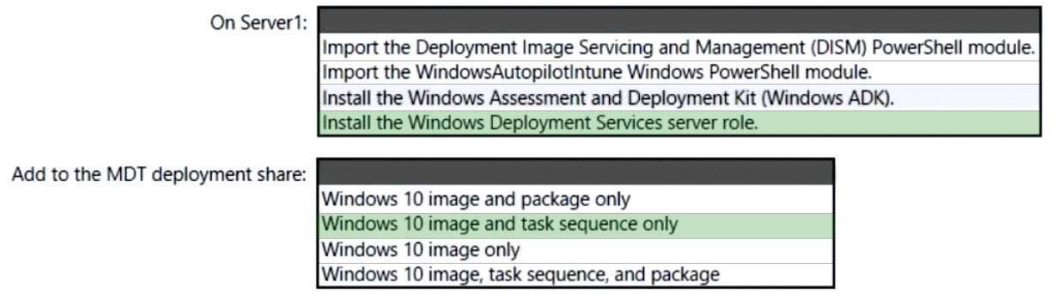
Hot Area:

Answer Area



Correct Answer:

Answer Area



Box 1: Install the Windows Deployment Services role.

Install and initialize Windows Deployment Services (WDS)

On the server:

Open an elevated Windows PowerShell prompt and enter the following command:

Install-WindowsFeature -Name WDS -IncludeManagementTools

WDSUTIL /Verbose /Progress /Initialize-Server /Server:MDT01 /RemInst:"D:\RemoteInstall"

WDSUTIL /Set-Server /AnswerClients:All

Incorrect:

* Install the Windows Assessment and Deployment Kit (Windows ADK)

MDT installation required the ADK, but MDT is already installed.

Box 2: Windows 10 image and task sequence only

Create the reference image task sequence

In order to build and capture your Windows 10 reference image for deployment using MDT, you will create a task sequence.

Reference:

https://docs.microsoft.com/en-us/windows/deployment/deploy-windows-mdt/prepare-for-windows-deployment-with-mdt

https://docs.microsoft.com/en-us/windows/deployment/deploy-windows-mdt/create-a-windows-10-reference-image

bensrayan 2 weeks, 4 days ago

My picks:
-install ADK
-windows 10 image and task sequence only

upvoted 4 times

Deric 1 week, 3 days ago

The MDT installation would require ADK, but it states that MDT is already installed on the server. Therefore I think the given answer is correct.

upvoted 2 times

Question #101 *Topic 2*

You have 25 computers that run Windows 8.1 Pro.

You have a Microsoft 365 E5 subscription that uses Microsoft Intune.

You need to upgrade the computers to Windows 10 Enterprise by using an in-place upgrade. The solution must minimize administrative effort.

What should you use?

A. Microsoft Endpoint Configuration Manager and a custom image of Windows 10 Enterprise

B. Subscription Activation

C. Microsoft Deployment Toolkit (MDT) and a default image of Windows 10 Enterprise

D. Windows Autopilot

Correct Answer: *B*

Deric 1 week, 3 days ago

Selected Answer: A

It's not B, the license will not automatically upgrade the OS. Based on this link, I believe it's A: https://learn.microsoft.com/en-us/mem/autopilot/existing-devices

upvoted 3 times

daye 9 hours, 57 minutes ago

I agree

A - Only solution that offer IPU
B- Doesn't upgrade from W8.1, only activates and upgrade within W10 versions
C - No
D - Autopilot doesn't offer in place upgrade

upvoted 1 times

thuba_TD 2 weeks, 4 days ago

Selected Answer: B

answer is correct B
https://docs.microsoft.com/en-us/windows/deployment/windows-10-subscription-activation

upvoted 2 times

TonySuccess 3 days, 11 hours ago

But it says in the link that it only applies to Windows 10 and 11, so we'd have to choose Autopilot. Although I admit, like in most cases the certain answer is difficult to find in plain English.

upvoted 1 times

TonySuccess 3 days, 11 hours ago

Then again it also says the same for Autopilot, but in the same link:

Windows Autopilot for existing devices lets you reimage and provision a Windows 8.1 device for Autopilot user-driven mode using a single, native Configuration Manager task sequence.

upvoted 1 times

raduM 4 weeks, 1 day ago

if you have windows 8.1 pro will subscription activation update to windows 10 enterprise? as far as i know... no.
i would go with autopilot here

upvoted 3 times

junior6995 3 weeks, 6 days ago

The question did not mention any on premises resources, I assume It is a Cloud Only environment so, I'd go for Autopilot too

upvoted 1 times

bensrayan 2 weeks, 4 days ago

windows autopilot Applies to, not to windows 8.1 :
Windows 10
Windows 11
Windows Holographic, version 2004
https://docs.microsoft.com/en-us/mem/autopilot/windows-autopilot

upvoted 2 times

HOTSPOT -

You have the x64 devices shown in the following table.

Name	Operating system	Installed apps
Computer1	64-bit version of Windows 8.1 Pro	Microsoft Office 2013
Computer2	32-bit version of Windows 8.1 Enterprise	*None*

You have the Windows 10 Enterprise images shown in the following table.

Name	Platform	Description
Image1	x64	Custom Windows 10 Enterprise image that has Microsoft Office 2019 installed
Image2	x64	Default Windows 10 Enterprise image created by Microsoft
Image3	x86	Custom Windows 10 Enterprise image that has Microsoft Office 2019 installed
Image4	x86	Default Windows 10 Enterprise image created by Microsoft

You need to identify which images can be used to perform an in-place upgrade of Computer1 and Computer2.

Which images 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

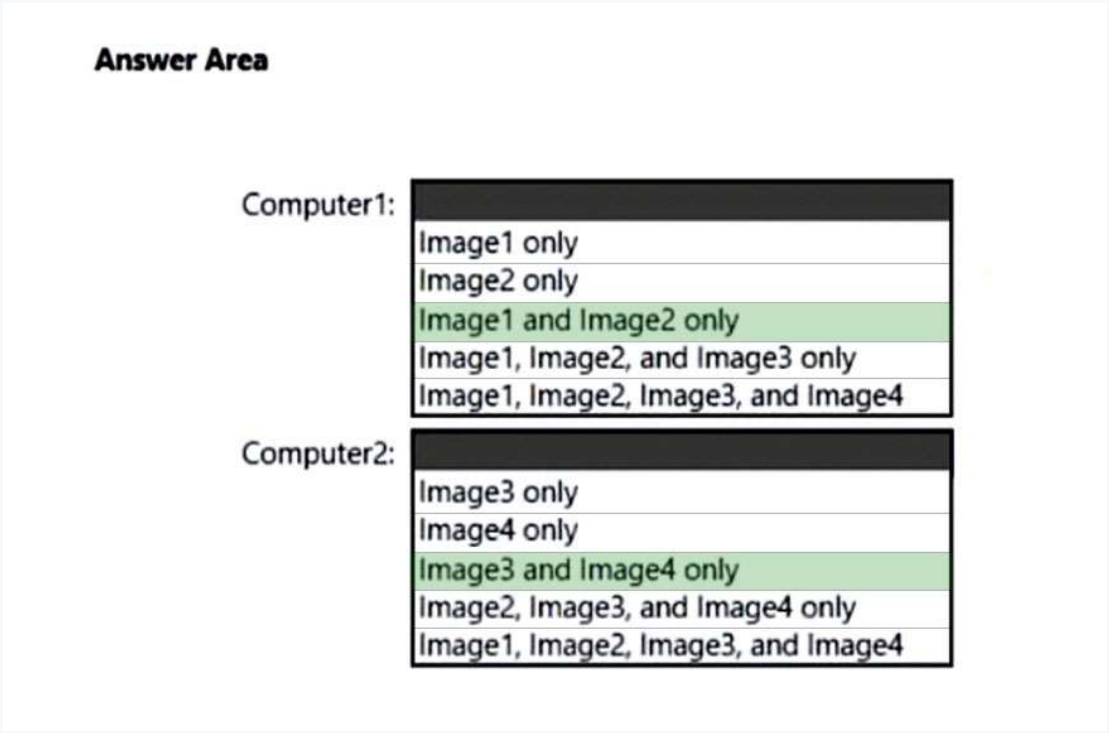
Computer1:

- Image1 only
- Image2 only
- Image1 and Image2 only
- Image1, Image2, and Image3 only
- Image1, Image2, Image3, and Image4

Computer2:

- Image3 only
- Image4 only
- Image3 and Image4 only
- Image2, Image3, and Image4 only
- Image1, Image2, Image3, and Image4

Correct Answer:



Box 1: Image1 and Image2 only -

Computer1 is a x64 system so Image1 and Image2 are fine.

Note: x86 refers to a 32-bit CPU and operating system while x64 refers to a 64-bit CPU and operating system.

Box 2: Image3 and Image4 only -

There is no upgrade path from 32 bit versions of Windows to Windows 8 64 bit.

Reference:

https://answers.microsoft.com/en-us/windows/forum/all/switch-from-x86-to-x64/a69b5aae-9d20-414b-86b8-004bece700c0

neobahamutk 2 weeks, 4 days ago

Correct.

upvoted 1 times

rockhound 3 weeks, 5 days ago

Correct. X64 or X86 is important. The Office version is not.

upvoted 2 times

Question #103 *Topic 2*

HOTSPOT -

You have 100 computers that run Windows 10. You have no servers. All the computers are joined to Microsoft Azure Active Directory (Azure AD).

The computers have different update settings, and some computers are configured for manual updates.

You need to configure Windows Update. The solution must meet the following requirements:

- The configuration must be managed from a central location.
- Internet traffic must be minimized.
- Costs must be minimized.

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

NOTE: Each correct selection is worth one point.

Hot Area:

Answer Area

Windows Update technology to use:
- Windows Server Update Services (WSUS)
- Microsoft Endpoint Configuration Manager
- Windows Update for Business

Manage the configuration by using:
- A Group Policy object (GPO)
- Microsoft Endpoint Configuration Manager
- Microsoft Intune

Manage the traffic by using:
- Delivery Optimization
- BranchCache
- Peer cache

Correct Answer:

Answer Area

Windows Update technology to use:
- Windows Server Update Services (WSUS)
- Microsoft Endpoint Configuration Manager
- Windows Update for Business

Manage the configuration by using:
- A Group Policy object (GPO)
- Microsoft Endpoint Configuration Manager
- Microsoft Intune

Manage the traffic by using:
- Delivery Optimization
- BranchCache
- Peer cache

Box 1: Windows Server Update Services (WSUS)

Windows Server Update Services (WSUS) enables information technology administrators to deploy the latest Microsoft product updates. You can use WSUS to fully manage the distribution of updates that are released through Microsoft Update to computers on your network.

Windows Server Update Services is a built-in server role that includes the following enhancements:

Can be added and removed by using the Server Manager

Includes Windows PowerShell cmdlets to manage the most important administrative tasks in WSUS

Etc.

Box 2: A Group Policy object -

In an Active Directory environment, you can use Group Policy to define how computers and users can interact with Windows Update to obtain automatic updates from Windows Server Update Services (WSUS).

Box 3: BranchCache -

BranchCache is a bandwidth-optimization feature that has been available since the Windows Server 2008 R2 and Windows 7 operating systems. Each client has a cache and acts as an alternate source for content that devices on its own network request. Windows Server Update Services (WSUS) and Microsoft Endpoint

Manager can use BranchCache to optimize network bandwidth during update deployment, and it's easy to configure for either of them.

BranchCache has two operating modes: Distributed Cache mode and Hosted Cache mode.

Reference:

https://docs.microsoft.com/en-us/windows/deployment/update/waas-branchcache https://docs.microsoft.com/en-us/windows-server/administration/windows-server-update-services/deploy/4-configure-group-policy-settings-for-automatic-updates

raduM Highly Voted 4 weeks, 1 day ago

device is joined to azure ad not to activtive directory. so solution is update for business, intune, delivery optimization

upvoted 9 times

rockhound 3 weeks, 5 days ago

correct

upvoted 1 times

TonySuccess Highly Voted 3 weeks, 6 days ago

Yeah, I'm surprised there aren't more people discussing this one. No server in place, no AD, I'd be using Endpoint.microsoft.com to create a configuration profile with delivery optimization...

upvoted 6 times

Henkjanarie Most Recent 2 days ago

Definitely wrong.. It's Azure AD without a server, so I also would go for: Business, Intune and Delivery Optimization. As the most cost effective solution.

upvoted 1 times

bensrayan 2 weeks, 4 days ago

The answer given is wrong.. ! so should be :
- windows update for business and not WSUS (there is no server!)
- intune
-delivery optimization

upvoted 5 times

Question #104 *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.
Your network contains an Active Directory domain. The domain contains a computer named Computer1 that runs Windows 8.1.
Computer1 has apps that are compatible with Windows 10.
You need to perform a Windows 10 in-place upgrade on Computer1.
Solution: You add Windows 10 startup and install images to a Windows Deployment Services (WDS) server. You start Computer1 by using WDS and PXE, and then you initiate the Windows 10 installation.
Does this meet the goal?

A. Yes

B. No

Correct Answer: *A*
Reference:
https://docs.microsoft.com/en-us/windows/deployment/windows-deployment-scenarios-and-tools

raduM Highly Voted 4 weeks ago
i think the answer is no. you cannot do in place upgrade with wds
upvoted 5 times

bensrayan 2 weeks, 4 days ago
Correct!
upvoted 1 times

Deric Most Recent 1 week, 3 days ago
Selected Answer: B
Correct answer is B
upvoted 1 times

geggio 2 weeks ago
correct foe me b
upvoted 1 times

Question #105 *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.
Your network contains an Active Directory domain. The domain contains a computer named Computer1 that runs Windows 8.1.
Computer1 has apps that are compatible with Windows 10.
You need to perform a Windows 10 in-place upgrade on Computer1.
Solution: You copy the Windows 10 installation media to a network share. You start Computer1 from Windows PE (WinPE), and then you run setup.exe from the network share.
Does this meet the goal?

A. Yes

B. No

Correct Answer: *B*
Instead: You add Windows 10 startup and install images to a Windows Deployment Services (WDS) server. You start Computer1 by using WDS and PXE, and then you initiate the Windows 10 installation.
Reference:
https://docs.microsoft.com/en-us/windows/deployment/windows-deployment-scenarios-and-tools

TonySuccess 3 days, 10 hours ago
Selected Answer: A
Mod please sort these questions out
upvoted 1 times

RADYN 4 days ago
Selected Answer: A
A for me
upvoted 1 times

Deric 1 week, 3 days ago
Selected Answer: A
A is correct.
upvoted 1 times

thuba_TD 2 weeks, 4 days ago
Selected Answer: A
a is the correct answer.
upvoted 1 times

raduM 4 weeks ago
yes. seems like standard procedure
upvoted 2 times

Question #106 *Topic 2*

You have a Microsoft Deployment Toolkit (MDT) deployment share.
You plan to deploy Windows 10 by using the Standard Client Task Sequence template.
You need to modify the task sequence to perform the following actions:
⇨ Format disks to support Unified Extensible Firmware Interface (UEFI).
⇨ Create a recovery partition.
Which phase of the task sequence should you modify?

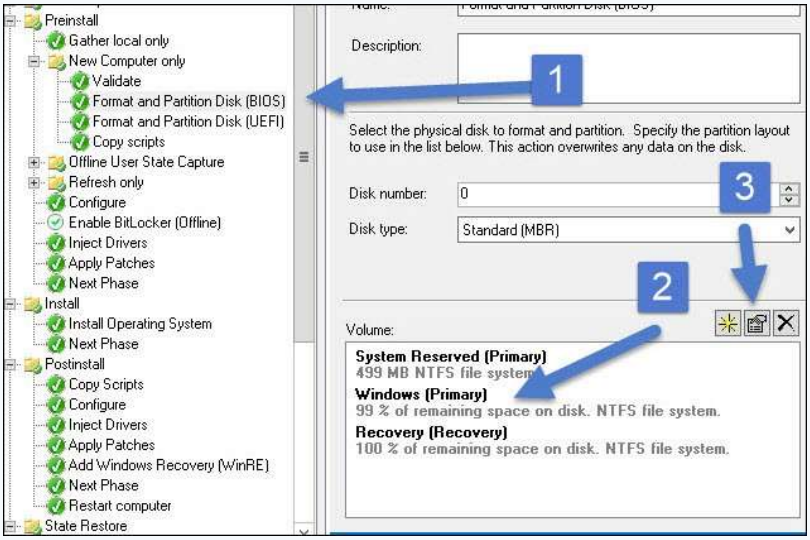
A. Initialization

B. Install

C. PostInstall

D. Preinstall

Correct Answer: *D*
Create Extra Partition in MDT -
We will create a new task sequence for a machine that doesn't have an extra partition.
1. On the Select Template page, click the drop-down and select Standard Client Task Sequence. Complete the remaining steps.
2. Edit the task sequence and click the New Computer only step. Within that step, click Format and Partition Disk(BIOS) step and edit it.



Etc.
Reference:
https://www.prajwaldesai.com/create-extra-partition-in-mdt/

neobahamutk 2 weeks, 4 days ago
Correct.
upvoted 2 times

Deric 1 week, 3 days ago
Agreed.
upvoted 1 times

HOTSPOT -

Your network contains an Active Directory domain. The domain contains the users shown in the following table.

Name	Member of
User1	Group1
User2	Group2

You have a server named Server that runs Windows Server 2019 and has the Windows Deployment Services role installed. Server1 contains an x86 boot image and three Windows 10 install images. The install images are shown in the following table.

Name	Architecture	User permission
Image1	x64	Full control: Administrators, WDSServer
Image2	x64	Full control: Administrators Read: Group1
Image3	x86	Full control: Administrators, WDSServer Read: Group2

You purchase a computer named Computer1 that is compatible with the 64-bit version of Windows 10.

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 Image1 on Computer1 by using Windows Deployment Services (WDS).	○	○
User1 can install Image2 on Computer1 by using Windows Deployment Services (WDS).	○	○
User2 can install Image3 on Computer1 by using Windows Deployment Services (WDS).	○	○

Correct Answer:

Answer Area

Statements	Yes	No
User1 can install Image1 on Computer1 by using Windows Deployment Services (WDS).	○	●
User1 can install Image2 on Computer1 by using Windows Deployment Services (WDS).	●	○
User2 can install Image3 on Computer1 by using Windows Deployment Services (WDS).	●	○

Box 1: No -

User1 is a member of Group1. User1 does not have any permission to Image1.

Box 2: Yes -

User1 has read permissions to Image2 through Group1.

Box 3: Yes -

User2 has read permissions to Image3 through Group2.

DragonSlayer848 4 weeks, 1 day ago

Shouldn't it be No Yes No? x86 version will not work on a 64bit computer right>

upvoted 1 times

Deric 1 week, 3 days ago

It will work, it's just not ideal / wise. It will install fine though.

upvoted 1 times

raduM 3 weeks, 6 days ago

wrong. 32 bit works on 64 bit. the other way around it does not work

upvoted 2 times

HOTSPOT -

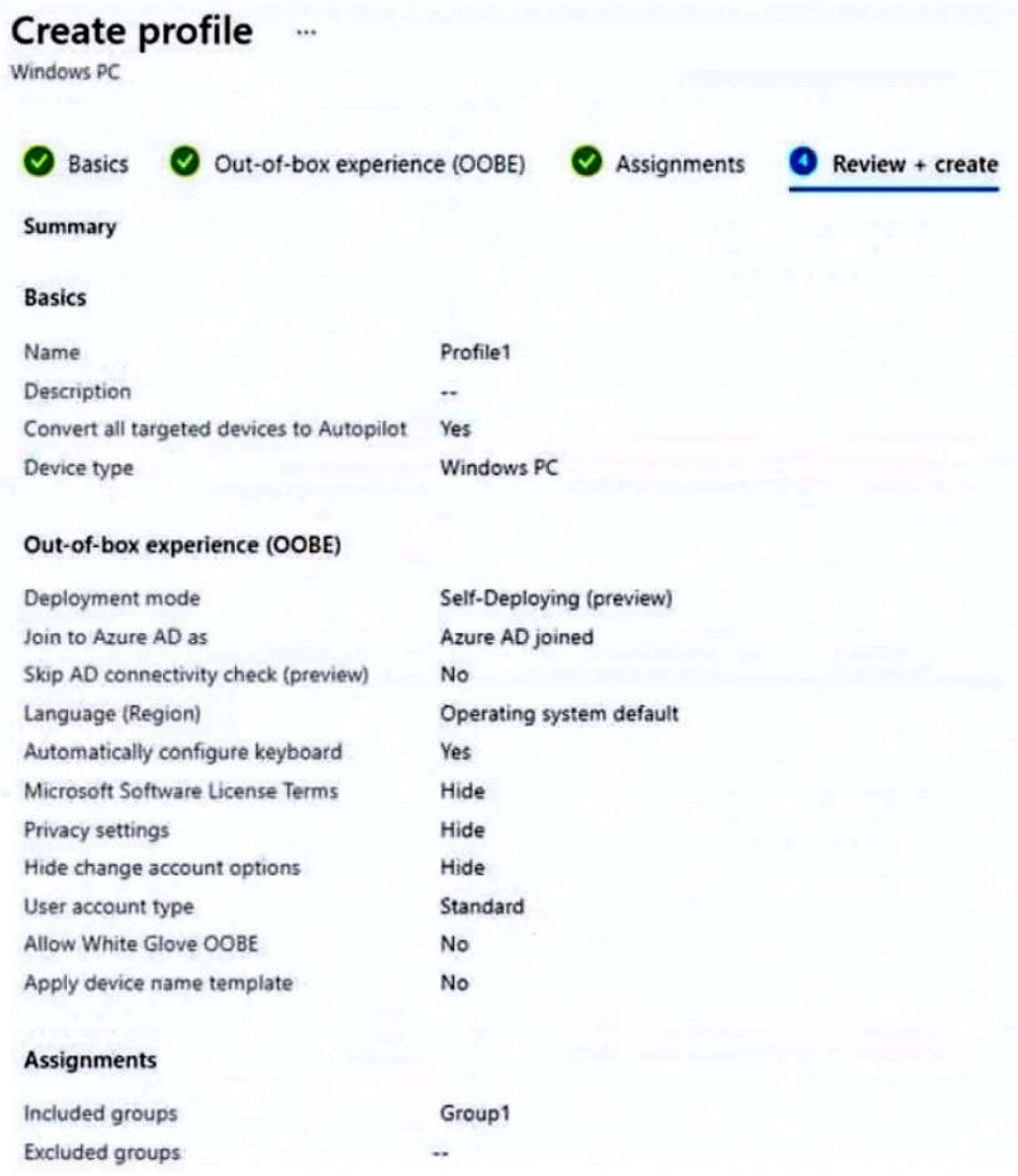
You have an Azure Active Directory (Azure AD) tenant named contoso.com that contains the devices shown in the following table.

Name	Operating system	Azure AD status	Mobile device management (MDM)
Device1	Windows 8.1	Registered	*None*
Device2	Windows 10	Joined	*None*
Device3	Windows 10	Joined	Microsoft Intune

Contoso.com contains the Azure Active Directory groups shown in the following table.

Name	Members
Group1	Group2, Device1, Device3
Group2	Device2

You add a Windows Autopilot deployment profile. The profile is configured 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
If Device1 starts in Out of Box Experience (OOBE) mode, the device will be deployed by using Autopilot.	○	○
If Device2 starts in Out of Box Experience (OOBE) mode, the device will be deployed by using Autopilot.	○	○
If Device3 starts in Out of Box Experience (OOBE) mode, the device will be deployed by using	○	○

Correct Answer:

Answer Area

Statements	Yes	No
If Device1 starts in Out of Box Experience (OOBE) mode, the device will be deployed by using Autopilot.	○	○
If Device2 starts in Out of Box Experience (OOBE) mode, the device will be deployed by using Autopilot.	○	○
If Device3 starts in Out of Box Experience (OOBE) mode, the device will be deployed by using	○	○

Box 1: No -
Device1 has no Mobile device Management (MDM) configured.
Note: Device1 is running Windows 8.1, and is registered, but not joined.
Device1 is in Group1.
Profile1 is assigned to Group1.

Box 2: No -
Device2 has no Mobile device Management (MDM) configured.
Note: Device2 is running Windows 10, and is joined.
Device2 is in Group2.
Group2 is in Group1.
Profile1 is assigned to Group1.

Box 3: Yes -
Device3 has Mobile device Management (MDM) configured.
Device3 is running Windows 10, and is joined
Device1 is in Group1.
Profile1 is assigned to Group1.
Mobile device management (MDM) enrollment: Once your Windows 10 device joins Azure AD, Autopilot ensures your device is automatically enrolled with MDMs such as Microsoft Intune. This program can automatically push configurations, policies and settings to the device, and install Office 365 and other business apps without you having to get IT admins to manually sort the device. Intune can also apply the latest updates from Windows Update for Business.
Reference:
https://xo.xello.com.au/blog/windows-autopilot

Mage10 1 day, 4 hours ago
I say it's no no yes
No - device is registered and not joined
No-if you look in the profile included group 1(device 2 is in group to so its not in the profile)
Yes- Device 3 is joined and also has mdm, mainly its in group 1 which is part of thr profile
upvoted 1 times

geggio 2 weeks ago
no
y
y
upvoted 1 times

bensrayan 2 weeks, 3 days ago

For me is :
- No (windows 8.1 means we are using Autopilot existing devices scenario, bit required SCCM to update 8.1 to windows 10)
- yes : nested group
- yes

Question #109 *Topic 2*

You have a Microsoft 365 Business Standard subscription and 100 Windows 10 Pro devices.
You purchase a Microsoft 365 E5 subscription.
You need to upgrade the Windows 10 Pro devices to Windows 10 Enterprise. The solution must minimize administrative effort.
Which upgrade method should you use?

A. Subscription Activation

B. an in-place upgrade by using Windows installation media

C. a Microsoft Deployment Toolkit (MDT) lite-touch deployment

D. Windows Autopilot

Correct Answer: *A*
Windows 10/11 Subscription Activation
Windows 10 Pro supports the Subscription Activation feature, enabling users to ג€step-upג€ from Windows 10 Pro or Windows 11 Pro to Windows 10 Enterprise or
Windows 11 Enterprise, respectively, if they are subscribed to Windows 10/11 Enterprise E3 or E5.
Reference:
https://docs.microsoft.com/en-us/windows/deployment/windows-10-subscription-activation

Deric 1 week, 3 days ago
Selected Answer: A
Correct, A
upvoted 1 times

raduM 3 weeks, 6 days ago
correct
upvoted 1 times

HOTSPOT -

You have a Microsoft Deployment Toolkit (MDT) deployment share named Share1.

You add Windows 10 images to Share1 as shown in the following table.

Name	In WIM file	Description
Image1	Install1.wim	Default Windows 10 Pro image from the Windows 10 installation media
Image2	Install1.wim	Default Windows 10 Enterprise image from the Windows 10 installation media
Image3	Install2.wim	Default Windows 10 Pro for Workstations image from the Windows 10 installation media
Image4	Custom1.wim	Custom Windows 10 Enterprise image without any additional applications
Image5	Custom2.wim	Custom Windows 10 Enterprise image that includes custom applications

Which images can be used in the Standard Client Task Sequence, and which images can be used in the Standard Client Upgrade Task Sequence?

NOTE: Each correct selection is worth one point.

Hot Area:

Answer Area

Standard Client Task Sequence:

- Image3 only
- Image3, Image4, and Image5 only
- Image1, Image2, and Image3 only
- Image1, Image2, Image3, and Image4 only
- Image1, Image2, Image3, Image4, and Image5

Standard Client Upgrade Task Sequence:

- Image3 only
- Image3, Image4, and Image5 only
- Image1, Image2, and Image3 only
- Image1, Image2, Image3, and Image4 only
- Image1, Image2, Image3, Image4, and Image5

Correct Answer:

Answer Area

Standard Client Task Sequence:

- Image3 only
- Image3, Image4, and Image5 only
- Image1, Image2, and Image3 only
- Image1, Image2, Image3, and Image4 only
- **Image1, Image2, Image3, Image4, and Image5**

Standard Client Upgrade Task Sequence:

- Image3 only
- Image3, Image4, and Image5 only
- Image1, Image2, and Image3 only
- **Image1, Image2, Image3, and Image4 only**
- Image1, Image2, Image3, Image4, and Image5

Box 1: Image1, Image2, Image3, Image4, and Image5.

All images.

Standard Client Task Sequence -
Standard Client task sequence. The most frequently used task sequence. Used for creating reference images and for deploying clients in production.
Box 2: Image1, Image2, Image3, and Image4 only.
Exclude image5 with applications.
Standard Client Upgrade Task Sequence
Standard Client Upgrade task sequence. A simple task sequence template used to perform an in-place upgrade from Windows 7, Windows 8, or Windows 8.1 directly to Windows 10, automatically preserving existing data, settings, applications, and drivers.
Reference:
https://docs.microsoft.com/en-us/windows/deployment/deploy-windows-mdt/get-started-with-the-microsoft-deployment-toolkit

Topic 3 - Question Set 3

Question #1 *Topic 3*

HOTSPOT -

You have an Azure Active Directory (Azure AD) tenant named contoso.com that contains a user named User1. User1 has the devices shown in the following table.

Name	Platform	Registered in contoso.com
Device1	Windows 10	No
Device2	Android	Yes
Device3	iOS	Yes

On September 5, 2019, you create and enforce a terms of use (ToU) in contoso.com. The ToU has the following settings:

- Name: Terms1
- Display name: Terms1 name
- Require users to expand the terms of use: Off
- Require users to consent on every device: On
- Expire consents: On
- Expire starting on: October 10, 2019
- Frequency: Monthly

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:

Correct Answer:

Reference:

https://docs.microsoft.com/en-us/azure/active-directory/conditional-access/terms-of-use#frequently-asked-questions

Perycles Highly Voted 1 year, 3 months ago

just tested :TOu are displayed when user logs to login.microsoftonline.com for example,so when He tries to connect his web portal. If device is not registered in to AAD, he receive the a message to ask. him to enroll his device. When Enrolled, and only when enrolled, TOu appears when accessing this same URL. So anwser are NO, YES,YES

upvoted 16 times

Angarali 5 months, 2 weeks ago

You will only need to enroll a device if you're trying to access the resources locally, not via web. The given answer is correct.

upvoted 1 times

RodrigoT 6 months, 2 weeks ago

The link provided says:
Q: When is the terms of use policy triggered?
A: The terms of use policy is triggered during the sign-in experience.
User1 is an Azure AD user, not a local user. He has to sign-in to access the resources. So, for me is Y Y Y.

upvoted 2 times

Tomtom11 Highly Voted 1 year, 4 months ago

No Yes Yes
Per-device terms of use has the following constraints:

A device can only be joined to one tenant.
A user must have permissions to join their device.
The Intune Enrollment app is not supported. Ensure that it is excluded from any Conditional Access policy requiring Terms of Use policy.
Azure AD B2B users are not supported.
If the user's device is not joined, they will receive a message that they need to join their device. Their experience will be dependent on the platform and software

upvoted 6 times

Goofer 10 months, 3 weeks ago

huh... AAD Join, The question is about AAD registration. You can register a device to more than one tenant. You can create (and use) Terms of Use under Conditional Access policies.
upvoted 1 times

NKG123 10 months, 1 week ago
Hahaha you can register a device in a single azure tenant.
upvoted 2 times

Angarali Most Recent 5 months, 2 weeks ago
The answer is Y Y Y. The question clearly states "User1 will be prompted" therefore regardless of what device they're using, they will be prompted to accept the ToU. I see some comments saying you need to register the device, let's not forget this isn't a requirement when accessing the web portal. Therefore you will only be prompted to accept the ToU when accessing through a browser. Below article and video from Microsoft will back up my point.

Good luck to everyone taking the exam.

https://docs.microsoft.com/en-us/azure/active-directory/conditional-access/terms-of-use
https://www.youtube.com/embed/N4vgqHO2tgY
upvoted 2 times

PChi 6 months ago
https://support.microsoft.com/en-us/account-billing/join-your-work-device-to-your-work-or-school-network-ef4d6adb-5095-4e51-829e-5457430f3973#to-join-an-already-configured-windows-10-device
upvoted 1 times

PChi 6 months ago
https://docs.microsoft.com/en-us/azure/active-directory/conditional-access/terms-of-use
Yes, yes, and yes. I agree with RodrigoT and due to my own finding in the given docs above.
upvoted 1 times

moobdoob 8 months, 2 weeks ago
Answer is: NO, YES, YES
upvoted 3 times

moobdoob 8 months, 2 weeks ago
N - Device is not registered in AzureAD
Y - registered in AzureAD
Y - registered in AzureAD
upvoted 3 times

RodrigoT 5 months, 4 weeks ago
It doesn't matter. When an Azure user signs in it will be prompted. The TOU is for the USER, not the device.
upvoted 1 times

Goofer 10 months, 4 weeks ago
N - Device is not registered in AzureAD
Y - registered in AzureAD
Y - registered in AzureAD
upvoted 2 times

BLYBOI 1 year, 4 months ago
I think Y,Y,Y, because the question says User1 will be prompted TOU?
upvoted 2 times

Danohav 1 year, 4 months ago
Should be no:

https://docs.microsoft.com/en-us/azure/active-directory/conditional-access/terms-of-use

In Section: Per-Device terms of use > "...user's device is not joined, they will receive a message that they need to join their device..."
=
prompt to accept terms will not appear, only prompt to join / register
upvoted 4 times

Moorebid 1 year, 4 months ago
I agree with the first question being "No".
In the same section you mentioned, it says: "The end user will be required to register their device in Azure AD. When the device is registered, the device ID is used to enforce the terms of use policy on each device."
upvoted 3 times

GohanF2 1 year, 4 months ago
the correct answer is : no, yes , yes
the terms of user applies to users with a premium azure license but the devices must be registered to the domain
upvoted 3 times

Alexbz 1 year, 5 months ago
The answer is correct. The challenging one is Device 1. Require users to consent on every device is on.
The Require users to consent on every device setting enables you to require end users to accept your terms of use policy on every device they are accessing from. The end user will be required to register their device in Azure AD. When the device is registered, the device ID is used to enforce the terms of use policy on each device.
https://docs.microsoft.com/en-us/azure/active-directory/conditional-access/terms-of-use
upvoted 5 times

Layer8 1 year, 4 months ago
anyone know when the user would be prompted to accept this ToU? would it be when they tried to access company resources (exchange or something like that)?

upvoted 1 times

RomeIndian 1 year, 4 months ago

Right answer - If the user's device is not joined, they will receive a message that they need to join their device. Their experience will be dependent on the platform and software.
Look under Per-device terms of use in here https://docs.microsoft.com/en-us/azure/active-directory/conditional-access/terms-of-use#frequently-asked-questions

upvoted 1 times

Merma 1 year, 5 months ago

"The Require users to consent on every device setting enables you to require end users to accept your terms of use policy on every device they are accessing from. The end user will be required to register their device in Azure AD. When the device is registered, the device ID is used to enforce the terms of use policy on each device."
https://docs.microsoft.com/en-us/azure/active-directory/conditional-access/terms-of-use#frequently-asked-questions

upvoted 1 times

petir 1 year, 5 months ago

if device 1 is not registered with contoso how does it know to require the user to consent? I don't think you can log in with an azure account if it's not registered

upvoted 1 times

Perycles 1 year, 3 months ago

TOu are displayed when user logs to login.microsoftonline.com for example,so when He tries to connect his web portal. If device is not registered in to AAD, he receive the a message to ask. him to enroll his device. When Enrolled, and only when enrolled, TOu appears when accessing this same URL. So anwser are NO, YES,YES

upvoted 2 times

petir 1 year, 5 months ago

i think first one should be no

upvoted 2 times

Layer8 1 year, 4 months ago

I think the question assumes that the user used their Azure AD sign in when going through OOBE on that Win10 device

upvoted 2 times

Question #2 *Topic 3*

HOTSPOT -

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

Name	Operating system
Device1	Windows 10
Device2	Android 8.0
Device3	Android 9
Device4	iOS 11.0
Device5	iOS 11.4.1

All devices contain an app named App1 and are enrolled in Microsoft Intune.

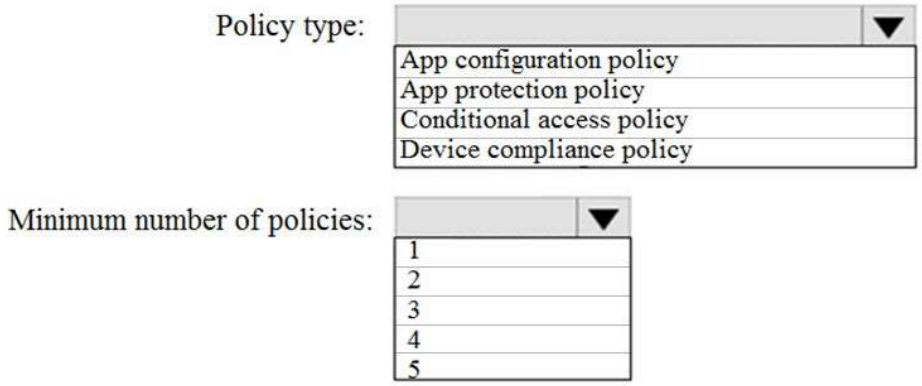
You need to prevent users from copying data from App1 and pasting the data into other apps.

Which type of policy and how many policies should you create in Intune? To answer, select the appropriate options in the answer area.

NOTE: Each correct selection is worth one point.

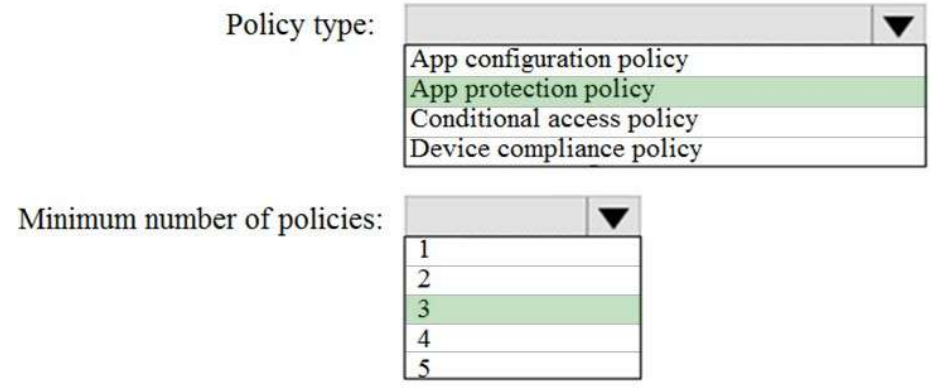
Hot Area:

Answer Area



Correct Answer:

Answer Area



Box 2: 3 -

One for Windows, one for Android, and one for iOS.

Reference:

https://docs.microsoft.com/en-us/mem/intune/apps/app-protection-policies https://docs.microsoft.com/en-us/mem/intune/apps/app-protection-policies-configure-windows-10

Perycles Highly Voted 1 year, 3 months ago

when creating Apps Protection Policy , you have 3 choice possible : IOS, ANDROID , WINDOWS. SO 3 policies necessary.

upvoted 14 times

mikl 9 months, 1 week ago

I agree.

upvoted 1 times

us3r Most Recent 9 months, 2 weeks ago

applies also for ms-101.

upvoted 1 times

lijk_manson 10 months, 3 weeks ago

Is it not 4 Policy's ?
Windows need to have 2 right?
By making a windows policy you have 2 options: with and without enrolment ;)
upvoted 1 times

lijk_manson 10 months, 2 weeks ago
You need to follow the table, so yes it is 3 not 4
upvoted 1 times

RodrigoT 6 months, 2 weeks ago
https://docs.microsoft.com/en-us/mem/intune/apps/app-protection-policies
This link says: "App protection policies can apply to apps running on devices that may or may not be managed by Intune". So, only 3 policies.
upvoted 1 times

RodrigoT 5 months ago
When you are creating an app protection policy for Windows 10 just chose "Without enrollment" and you're good to go.
upvoted 1 times

Angarali 1 year, 2 months ago
Answer is correct

https://docs.microsoft.com/en-us/microsoft-365/business/protection-settings-for-windows-10-devices
upvoted 4 times

GohanF2 1 year, 4 months ago
the answer is correct
upvoted 1 times

Layer8 1 year, 4 months ago
in Intune when you think "policy", think "platform" as well (that's what i've gathered in the learning process at least).
upvoted 1 times

Merma 1 year, 5 months ago
The given answer is correct. If you watch the interactive video:
https://docs.microsoft.com/en-us/mem/intune/apps/app-management
When creating a policy you have to select one of these options: Windows, Android & for iOS
upvoted 3 times

Danohav 1 year, 4 months ago
Thank you for the link.
However, in the "App management capabilities by platform" table, under "Protect company data in apps with app protection policies" > Win10 is set to NO, as it works only with Windows Information Protection = not App Protection Policies
upvoted 2 times

Poncho25 1 year, 5 months ago
The correct answer is App Protection Policy - 4. You can control the data only in Android and IOS - not Windows 10:
https://docs.microsoft.com/en-us/mem/intune/apps/app-management
upvoted 3 times

1morenickname 1 year, 5 months ago
Correct, but then it should be 2 policies - 1 for iOS, 1 for Android
upvoted 6 times

Moorebid 1 year, 4 months ago
The correct answer is 3, one for each platform (Windows, Android, iOS).
upvoted 3 times

IrvSus 1 year, 4 months ago
https://docs.microsoft.com/en-us/mem/intune/apps/app-protection-policies-configure-windows-10 <-- you can - I have walked through it in a live tenant.
upvoted 3 times

Question #3 *Topic 3*

Your company has an internal portal that uses a URL of http://contoso.com.
The network contains computers that run Windows 10. The default browser on all the computers is Microsoft Edge.
You need to ensure that all users only use Internet Explorer to connect to the internal portal. The solution must ensure that Microsoft Edge can be used to connect to all other websites.
What should you do from each computer?

A. From Internet Explorer, configure the Compatibility View settings

B. From the local policy, configure Enterprise Mode

C. From Microsoft Edge, configure the Advanced Site Settings

D. From the Settings app, configure the default web browser settings

Correct Answer: *B*
Using Enterprise Mode means that you can continue to use Microsoft Edge as your default browser, while also ensuring that your apps continue working on IE11.
If you have specific websites and apps that have compatibility problems with Microsoft Edge, you can use the Enterprise Mode site list so that the websites open in
Internet Explorer 11 automatically. Additionally, if you know that your intranet sites aren't going to work correctly with Microsoft Edge, you can set all intranet sites to automatically open using IE11 with the Send all intranet sites to IE group policy.
Reference:
https://docs.microsoft.com/en-us/microsoft-edge/deploy/emie-to-improve-compatibility

tezawynn Highly Voted 1 year, 9 months ago
I will get them to use Chrome or Firefox.
upvoted 18 times

asturmark 3 weeks, 3 days ago
Or Brave :)
upvoted 1 times

Anthony_2770 Highly Voted 1 year, 8 months ago
B
https://docs.microsoft.com/en-us/internet-explorer/ie11-deploy-guide/what-is-enterprise-mode
For Windows 10 and Windows 10 Mobile, Microsoft Edge is the default browser experience. However, Microsoft Edge lets you continue to use IE11 for sites that are on your corporate intranet or included on your Enterprise Mode Site List.
Using Enterprise Mode means that you can continue to use Microsoft Edge as your default browser, while also ensuring that your apps continue working on IE11.
upvoted 14 times

NZS Most Recent 5 months, 1 week ago
Enterprise Mode... but IE is gone from both Windows 10 and 11 now
upvoted 2 times

letters1234 7 months, 2 weeks ago
This answer may change:
The IE11 application is being deprecated in June 2022, around then it will only allow opening in IE11 mode WITHIN Edge Chromium, not redirecting to IE11 (the application)
upvoted 1 times

mikl 9 months, 1 week ago
Enterprise Mode is the solution.
upvoted 2 times

Perycles 1 year, 3 months ago
B : enterprise mode allow you to put desired web site and choose wich browser to use for each URL.
upvoted 2 times

vinnyct 1 year, 10 months ago
It's B
upvoted 2 times

lijk_manson 1 year, 10 months ago
I dont believe this question will be on the exam :)
upvoted 3 times

Question #4 *Topic 3*

Your company uses Microsoft Intune.
More than 500 Android and iOS devices are enrolled in the Intune tenant.
You plan to deploy new Intune policies. Different policies will apply depending on the version of Android or iOS installed on the device.
You need to ensure that the policies can target the devices based on their version of Android or iOS.
What should you configure first?

A. Corporate device identifiers in Intune

B. Device settings in Microsoft Azure Active Directory (Azure AD)

C. Device categories in Intune

D. Groups that have dynamic membership rules in Microsoft Azure Active Directory (Azure AD)

Correct Answer: *D*
We can create dynamic groups by using the deviceOSVersion or deviceOSType properties, and then apply Intune configuration policies to those groups.
Reference:
https://docs.microsoft.com/en-us/archive/blogs/pauljones/dynamic-group-membership-in-azure-active-directory-part-2
https://docs.microsoft.com/en-ie/mem/intune/enrollment/device-group-mapping

Mendel Highly Voted 3 years ago
Why not answer D?
https://blogs.technet.microsoft.com/pauljones/2017/08/29/dynamic-group-membership-in-azure-active-directory-part-2/

B does not make sense and the links does not answer why this should be the right answer.
upvoted 24 times

nolancl 3 years ago
Agreed, the device settings in the device compliance would address setting an OS range before devices can be joined not different configurations for specific OS. Need Dynamic Group settings to accomplish this like Mendel stated.
upvoted 3 times

Mike_Row 2 years, 6 months ago
Agreed, you can create dynamic groups with a deviceOSVersion and or deviceOSType property and use that for the Intune configuration policies.
upvoted 9 times

mikl 9 months, 1 week ago
Exactly.
upvoted 1 times

DUSHIWORLD Highly Voted 2 years, 7 months ago
Answer is D!
upvoted 12 times

gotrekk Most Recent 1 month, 2 weeks ago
Selected Answer: D
Dynamic groups
upvoted 1 times

raduM 1 month, 3 weeks ago
i would also go with dynamic groups here
upvoted 1 times

mikl 9 months, 1 week ago
Selected Answer: D
D. Groups that have dynamic membership rules in Microsoft Azure Active Directory (Azure AD) is correct.
upvoted 3 times

Perycles 1 year, 3 months ago
D is the good answer, by using "deviceOSversion" setting, whith can type the version of the desired OS.
upvoted 2 times

Tomtom11 1 year, 4 months ago
C when you read the below
https://docs.microsoft.com/en-ie/mem/intune/enrollment/device-group-mapping
They you choose D
upvoted 2 times

BLYBOI 1 year, 4 months ago
I would go with D. Groups that have dynamic membership rules in Microsoft Azure Active Directory (Azure AD)
upvoted 2 times

George_83 1 year, 5 months ago
Correct aswer is D

upvoted 4 times

slaoui 1 year, 5 months ago

It's either Device Restrictions or Identity Protection.
Since the latter is not in the list of answers, it has to be Device Restrictions (under Password)

upvoted 1 times

slaoui 1 year, 5 months ago

Disregard my comment, it was meant for the previous question

upvoted 1 times

Tomtom11 1 year, 6 months ago

Answer is D
https://docs.microsoft.com/en-ie/azure/active-directory/enterprise-users/groups-dynamic-membership
Rules for devices
deviceOSType and deviceOSVersion

upvoted 2 times

Rstilekar 1 year, 9 months ago

@RGM, the link you shared doesnt say anything related to question requirement asked. Yes you can manage device using the setting B, but it still doesnt solves the purpose. What should you do first is asked and you can still create Dynamic groups (Option D) before anything. So i would go for D. B doesnt makes any sense here.

upvoted 2 times

Dauti 1 year, 9 months ago

There are two locations to manage devices in Azure AD:
Azure portal > Azure Active Directory > Devices
Azure portal > Azure Active Directory > Users > Select a user > Devices

upvoted 1 times

RGM 1 year, 10 months ago

https://docs.microsoft.com/nl-nl/azure/active-directory/devices/device-management-azure-portal
its B

upvoted 1 times

j0eyv 1 year, 10 months ago

This was a question in the exam last week.. i gave answer A cause two test exams say its A but i assume it should be D.. Still not sure about what is the right answer for this question in the exam. Will go for A again next week..

upvoted 1 times

j0eyv 1 year, 10 months ago

Sorry i mean B.

upvoted 2 times

DJM 1 year, 10 months ago

I am looking at Device Settings in AAD right now, it gives me the option to:

Specify which users may join devices to AD,
Allow or block users from registering devices with AzureAD,
Require MFA to join devices
Maximum number of devices, nothing relevant to this question, for me the answer is D,

B makes no sense.

upvoted 2 times

Coopmsb 2 years ago

Its D for Sure !!! you can create Device Dynamic group based upon there Versions

upvoted 3 times

surbento 2 years, 2 months ago

Answer is D . I have tested

upvoted 3 times

Question #5 *Topic 3*

You have computers that run Windows 10 Pro. The computers are joined to Microsoft Azure Active Directory (Azure AD) and enrolled in Microsoft Intune.
You need to upgrade the computers to Windows 10 Enterprise.
What should you configure in Intune?

A. A device enrollment policy

B. A device cleanup rule

C. A device compliance policy

D. A device configuration profile

Correct Answer: *D*
Intune: Upgrade Windows Pro to Enterprise.
1. First, create a Microsoft Intune configuration policy. In the Azure Portal navigate to Microsoft Intune -> Device Configuration -> Profiles. Click Create Profile.
2. Next, create a new Windows 10 and later profile, with a type of Edition Upgrade. Click Settings
3. Etc.
Reference:
https://blogs.technet.microsoft.com/skypehybridguy/2018/09/21/intune-upgrade-windows-from-pro-to-enterprise-automatically/

Tomtom11 Highly Voted 1 year, 6 months ago
Answer D = Windows | Configuration profiles - Edition upgrade and mode switch
upvoted 14 times

miki Most Recent 9 months, 1 week ago
D. A device configuration profile is correct
upvoted 1 times

john909 11 months, 1 week ago
Yes, D (configuration profiles -> then select Template -> Edition upgrade)
upvoted 3 times

AzZnLuVaBol 1 year, 7 months ago
D. is correct.
upvoted 4 times

Question #6 *Topic 3*

You are creating a device configuration profile in Microsoft Intune.
You need to implement an ADMX-backed policy.
Which profile type should you use?

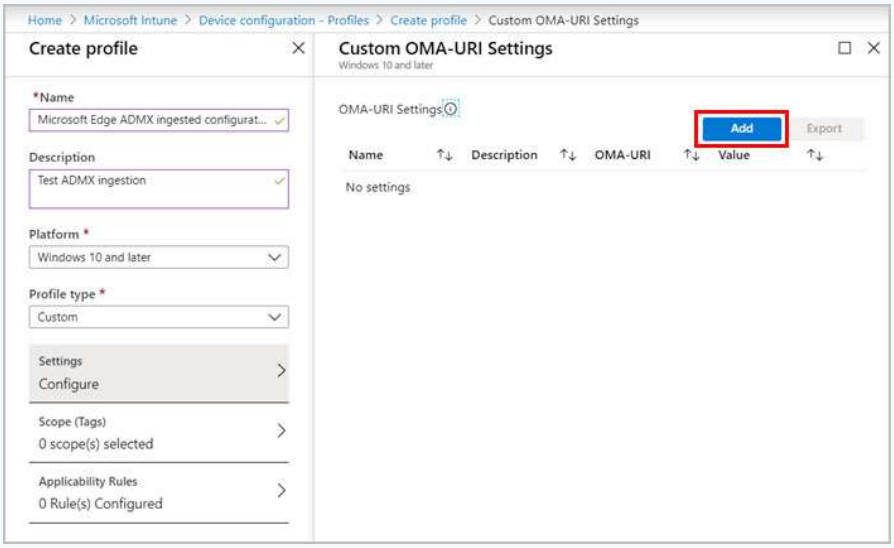
A. Identity protection

B. Custom

C. Device restrictions

D. Device restrictions (Windows 10 Team)

Correct Answer: *B*
Ingest the Microsoft Edge ADMX file into Intune
To ingest the ADMX file, follow these steps:
1. Download the Microsoft Edge policy templates file (MicrosoftEdgePolicyTemplates.cab) from the Microsoft Edge Enterprise landing page and extract the contents. The file that you want to ingest is msedge.admx.
2. Sign in to the Microsoft Azure portal.
3. Select Intune from All Services, or search for Intune in the portal search box.
4. From Microsoft Intune - Overview, select Device configuration | Profiles.
5. On the top command bar, select + Create profile.
6. Provide the following profile information:
Name: Enter a descriptive name. For this example, "Microsoft Edge ADMX ingested configuration".
Description: Enter an optional description for the profile.
Platform: Select "Windows 10 and later"
Profile type: Select "Custom"
7. On Custom OMA-URI Settings, click Add to add an ADMX ingestion.



8. Etc.
Reference:
https://docs.microsoft.com/en-us/deployedge/configure-edge-with-mdm

Question #7 *Topic 3*

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

Contoso.com contains the devices shown in the following table.

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

In Intune, you create the app protection policies shown in the following table.

Name	Platform	Enrollment state	Assigned to
Policy1	Windows 10	With enrollment	Group1
Policy2	Windows 10	Without enrollment	Group2
Policy3	Windows 10	With enrollment	GroupA
Policy4	Windows 10	Without enrollment	GroupB

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

NOTE: Each correct selection is worth one point.

Hot Area:

Answer Area

Statements	Yes	No
When User1 signs in to Device1, Policy1 applies.	○	○
When User2 signs in to Device1, Policy2 applies.	○	○
When User2 signs in to Device2, Policy2 applies.	○	○

Correct Answer:

Answer Area

Statements	Yes	No
When User1 signs in to Device1, Policy1 applies.	○	○
When User2 signs in to Device1, Policy2 applies.	○	○
When User2 signs in to Device2, Policy2 applies.	○	○

Reference:

https://docs.microsoft.com/en-us/mem/intune/apps/app-protection-policy

petir Highly Voted 1 year, 5 months ago

looks right, had to pay attention to enrollment state

upvoted 15 times

RodrigoT 5 months, 4 weeks ago

App protection policies are assigned to users, not devices. For devices you just choose the platform (3 options, Windows, IOS, Android). If in the Windows policy you left the default "Enrollment state > Without enrollment" then the policy applies anyway by MAM, not MDM. Check the point 3 of this link:
https://docs.microsoft.com/en-us/windows/security/information-protection/windows-information-protection/create-wip-policy-using-intune-azure#create-a-wip-policy
Using the "Enrollment state > Without enrollment" is also the recommendation of Microsoft because is the more restrictive. Check the source:
https://docs.microsoft.com/en-us/mem/intune/apps/windows-information-protection-policy-create#to-add-a-wip-policy

upvoted 3 times

RodrigoT 5 months, 4 weeks ago

The app is always protected by its policy. It doesn't matter if the device is not enrolled because the policy is for the app. Otherwise you are saying that the app is not protected just because the device is not enrolled. That doesn't make sense.
If you say Y N Y then in the Question #8 in this same page the second answer would be "Minimum 4 policies", Android, IOS, Windows with enrollment e Windows without enrollment.
So, for me the answer is Y Y Y.

upvoted 5 times

RodrigoT 5 months, 4 weeks ago

"because the device1 is enrolled" I meant.

upvoted 1 times

51007 4 months ago

Ok I think I've got it.

https://docs.microsoft.com/en-us/windows/security/information-protection/windows-information-protection/create-wip-policy-using-intune-azure#create-a-wip-policy

"If the same user and device are targeted for both MDM and MAM, the MDM policy will be applied to devices joined to Azure AD.""

So for the second item you are right in the sense that the app will not go policy-less just bc the device is enrolled. BUT the MDM device policy will take precedent over the MAM user policy.. MAMPolicy2 is assigned to Group2/User2.. MDMPolicy3 is assigned to Device1. The question asks will Policy2 apply when User2 signs into Device1 and my answer is NO.. Policy3 would apply. Y-N-Y

upvoted 2 times

MitchF 2 months, 2 weeks ago

I agree Y, Y, Y -- It doesn't matter if the devices are enrolled or not. The app protection policy still protects your data anyways. This is the proof:
"You can use Intune app protection policies independent of any mobile-device management (MDM) solution. This independence helps you protect your company's data with or without enrolling devices in a device management solution"
Source (near the top of page):
https://docs.microsoft.com/en-us/mem/intune/apps/app-protection-policy

upvoted 1 times

Merma Highly Voted 1 year, 4 months ago

Box 1: Yes - User1 is a member of Group1, Device1 is Intune managed, Policy1 is enrolled and assigned to Group1.
Box 2: No - User2 is a member of Group2, Device1 is Intune managed, Policy2 is not enrolled & is assigned to Group2.
Box 3: Yes - User2 is a member of Group2,Device2 is not Intune managed, Policy2 is assigned to Group2

upvoted 11 times

RodrigoT 5 months ago

When an app protection policy is created for Windows 10 "without enrollment" it will be applied anyway by MAM.

upvoted 1 times

BRoald Most Recent 1 week, 2 days ago

I would say Y Y Y

" Because mobile app management doesn't require device management, you can protect company data on both managed and unmanaged devices"

https://learn.microsoft.com/en-us/mem/intune/apps/app-protection-policy

upvoted 1 times

bensrayan 2 weeks, 3 days ago

we can apply a app protection policies to windows 10 devices (with or without enrollement), so the answer is YES YES YES

upvoted 1 times

Whatsamattr81 3 months, 1 week ago

Answer is Y Y Y

upvoted 3 times

Whatsamattr81 3 months, 1 week ago

App protection policies apply security at the app level and do not require device enrollment. You can use them with devices enrolled into Intune or not. Additionally, you can apply them to devices enrolled into a third-party MDM provider. They also only apply to users (not devices) so basically whatever group the user is in, they will get the policy applied to that group - regardless of device group or enrollment status.

upvoted 1 times

hawkens 9 months, 2 weeks ago

@nkg123, isn't that only for mobile devices? https://xenit.se/tech-blog/app-protection-policies-for-managed-and-unmanaged-devices-in-intune/

upvoted 1 times

NKG123 9 months, 1 week ago

You are wrong. When you create it you specify with or without enrollment.

upvoted 1 times

RodrigoT 5 months, 4 weeks ago

But "with" or "without enrollment" is available just for Windows (tested in lab). If you choose the default "without enrollment" the policy is more restrictive and applies anyway by MAM, independently if the device is enrolled or not. But if you choose "with enrollment" then i doesn't apply if the device is not enrolled. I don't know why this 2 options even exist if it's just for Windows.

upvoted 2 times

tf444 11 months, 3 weeks ago

Yes, No, No.
Box 1: Yes - User1 is a member of Group1, Device1 is Intune managed, Policy1 is enrolled and assigned to Group1.

Box 2: No - User2 is a member of Group2, Device1 is Intune managed, Policy2 is not enrolled & is assigned to Group2.
Box 3: Yes - User2 is a member of Group2, Device2 is not Intune managed, Policy2 is not enrolled assigned to Group2.

upvoted 2 times

rajpatel007 6 months ago

so Yes No No or Yes No Yes

upvoted 2 times

Layer8 1 year, 4 months ago

App protection policies should effect regardless of intune enrollment then?

upvoted 1 times

NKG123 9 months, 3 weeks ago

You are wrong. You can chose to apply on an unmanaged device!

upvoted 1 times

Pleebb 1 year, 2 months ago

correct

upvoted 1 times

Question #8 *Topic 3*

Your network contains an Active Directory named contoso.com. The domain contains two computers named Computer1 and Computer2 that run Windows 10.
Folder Redirection is configured for a domain user named User1. The AppData\Roaming folder and the Desktop folder are redirected to a network share.
User1 signs in to Computer1 and performs the following tasks:
- Configures screen saver to start after five minutes of inactivity
- Modifies the default save location for Microsoft Word
- Creates a file named File1.docx on the desktop
- Modifies the desktop background

What will be retained when User1 signs in to Computer2?

A. File1.docx and the desktop background only

B. File1.docx, the screen saver settings, the desktop background, and the default save location for Word

C. File1.docx only

D. File1.docx, the desktop background, and the default save location for Word only

Correct Answer: *B*
* Folder Redirection enables users and administrators to redirect the path of a known folder to a new location, manually or by using Group Policy. The new location can be a folder on the local computer or a directory on a file share. Users interact with files in the redirected folder as if it still existed on the local drive. For example, you can redirect the Documents folder, which is usually stored on a local drive, to a network location. The files in the folder are then available to the user from any computer on the network.
* Roaming User Profiles redirects user profiles to a file share so that users receive the same operating system and application settings on multiple computers.
When a user signs in to a computer by using an account that is set up with a file share as the profile path, the user's profile is downloaded to the local computer and merged with the local profile (if present). When the user signs out of the computer, the local copy of their profile, including any changes, is merged with the server copy of the profile. Typically, a network administrator enables Roaming User Profiles on domain accounts.
Reference:
https://docs.microsoft.com/en-us/windows-server/storage/folder-redirection/folder-redirection-rup-overview

Technik Highly Voted 1 year, 4 months ago
See for older discussion:

https://www.examtopics.com/discussions/microsoft/view/5328-exam-md-101-topic-2-question-9-discussion/
upvoted 9 times

Mage7 11 months ago
So the answer is C.
Personally I didn't knew which one it was because I didn't knew where EACH of these settings (background, were saved. Now I'll know - NTUSER.DAT (which is in APPDATA folder).
upvoted 3 times

Bouncy 7 months, 2 weeks ago
ntuser.dat is in %userprofile% folder (.\username), two tiers above %appdata% (the variable leads to .\username\appdata\roaming folder). Hence folder redirection for %appdata% won't catch any registry related settings
upvoted 4 times

Y2 Highly Voted 6 months, 3 weeks ago
Why are there SOO many wrong anwer in MD-101 past papers. i have never seen anything like this
upvoted 9 times

BrentOn 6 months, 3 weeks ago
IKR, really forces you to actually try understand things because no one can be trusted.
upvoted 8 times

raduM Most Recent 3 weeks, 5 days ago
the answer should be c
upvoted 2 times

raduM 1 month, 3 weeks ago
Selected Answer: C
c should be correct
upvoted 1 times

raduM 1 month, 3 weeks ago
i believe it should be c. why whould the desktop settings be saved? these settings are in registry and in the ntuser.dat folder.
upvoted 1 times

silver_bullet666 3 months ago

it may interest you to know that mapped drive information is actually also stored in HKU;

foreach ($1 in (Get-ChildItem -Path Registry::HKEY_USERS|?{$_.name -like '*-*-*-*-*-*' -and $_.name -notlike '*_Classes'})){gci -Path ('Registry::\'+$1.name+'\Network') -Recurse}

upvoted 1 times

Whatsamattr81 3 months, 1 week ago

OK, so the question doesnt actually mention roaming profiles... Just Folder redirection. Screensaver settings and desktop settings will be stored in %USERPROFILE% which if just using folder redirection, wil be the local C:\Users\<username>... it wont follow you around, only the stuff in the redirected folders.

upvoted 1 times

Whatsamattr81 3 months, 1 week ago

With roaming profiles enabled, HKCU gets saved to the profile path specified in the policy setting (\\server\profiles$\user\profile). Folder redirection just prevents the contents of the well known folders being copied at login / logout. This network location will have a copy of HKCU.

upvoted 1 times

ken2ut 4 months, 1 week ago

A is the answer.

Default save location for MS Word is the Documents folder.

upvoted 1 times

MR_Eliot 5 months ago

Selected Answer: A

Answer is A for sure!
Desktop background is saved in:
"C:\Users\<username>\AppData\Roaming\Microsoft\Windows\Themes\TranscodedWallpaper".

upvoted 2 times

AVR31 5 months, 1 week ago

Desktop background, screen saver settings, default Word location are stored in the registry. The user registry file is not in %appdata%\roaming. So none of these will be syncronized.
Only the file created on the desktop will appear on another computer, when the user logs in.

upvoted 2 times

Angarali 5 months, 2 weeks ago

Selected Answer: A

Your user profile stores your individual settings under Windows. It is used to re-create your preferred system environment when you log on. This includes everything from your wallpaper and desktop, to your email settings and network connections. A roaming profile is stored on a central server which can be accessed from all domain computers. This allows you to have the same environment settings on every machine to which you log on. Your roaming profile is copied to a machine when you log on, and the synchronized back to the server when you log off.

upvoted 1 times

RodrigoT 5 months, 3 weeks ago

Selected Answer: A

FINAL ANSWER: Guys, today I got this question in a KAPLAN exam. The only difference is that in their question there was not a Desktop background change. In their official explanation they say that the document in the desktop folder surely is retained. The other settings like screen saver, default save location for Word, and map a network drive (their option instead of our desktop background) are NOT retained. They explained that the Appdata\Roaming folder stores default templates, some configuration files (like desktop background, and support data. To redirect everything you would have to use a roaming user profile, not Folder Redirection.
So for this scenario the final answer is A. the file and desktop background.
Study more, guess less.

upvoted 4 times

MitchF 2 months, 1 week ago

The only supported answer that I see from Microsoft is answer:
"C. File1.docx only"

They say Folder Redirections is for folders only.

If you want redirect desktop settings too, you must use Roaming User Profiles (see title: Primary computers for Folder Redirection and Roaming User Profiles) to designate “primary computers for users”, which will allow you to “...redirected data (e.g., File1.docx in our question) and settings (e.g., Desktop settings in our question)."
Source:
https://docs.microsoft.com/en-us/windows-server/storage/folder-redirection/folder-redirection-rup-overview

upvoted 1 times

Adhikari123 5 months, 3 weeks ago

Selected Answer: B

B is correct

upvoted 1 times

distortion 6 months ago

Stupid question. What idiot would redirect the appdata\roaming folder....

upvoted 1 times

Tanderson2491 6 months ago

Selected Answer: C

C is the correct answer as only desktop redirection has been configured.
Desktop background and default Word save location would only apply if Roaming Profiles were in place which in this example they are not.

upvoted 1 times

Tanderson2491 6 months ago

I redact this comment. I missed the fact that appdata\roaming was also redirected. Correct answer is A.

upvoted 1 times

IykeP 8 months, 3 weeks ago

Selected Answer: A

Through group policy, you can specify folder redirection for the following four system folders on the user system: Application Data, Desktop, My Documents, Start Menu.

upvoted 1 times

Tanderson2491 6 months ago

Yes, you CAN configure that, but only the desktop is redirected in this example. The correct answer is C.

upvoted 1 times

HOTSPOT -

You have a computer named Computer1 that runs Windows 10.

Computer1 has the users shown in the following table.

Name	Member of
User1	Administrators
User2	Replicator
User3	Guests

User1 signs in to Computer1, creates the following files, and then signs out:

- File1.docx in C:\Users\User1\Desktop
- File2.docx in C:\Users\Public\Public Desktop
- File3.docx in C:\Users\Default\ Desktop

User3 then signs in to Computer1 and creates a file named File4.docx in C:\Users\User3\Desktop.

User2 has never signed in to Computer1.

How many DOCX files will appear on the desktop of each user the next time each user signs in? To answer, select the appropriate options in the answer area.

NOTE: Each correct selection is worth one point.

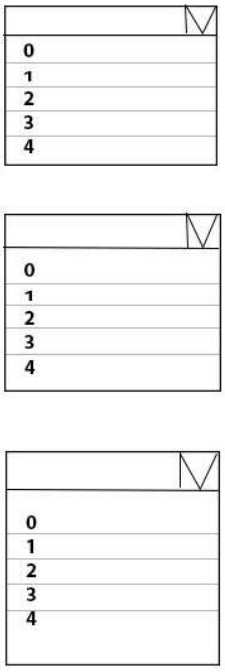
Hot Area:

Answer Area

Number of documents that will appear for User1:

Number of documents that will appear for User2:

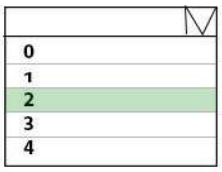
Number of documents that will appear for User3:



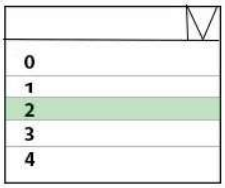
Correct Answer:

Answer Area

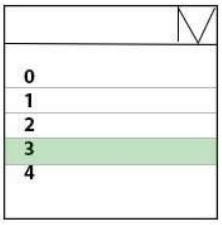
Number of documents that will appear for User1:



Number of documents that will appear for User2:



Number of documents that will appear for User3:



Box 1: 2 -

File1.docx (Created by User1) and File2.docx (public)

Box 2: 2 -

File2.docx (public) and File3.docx (default),

Box 3: 3 -

File2 (public) + File3 (Default, user1 creates File3 then User3 signs in) + File4 (desktop, user3)

Forsmark Highly Voted 2 years, 7 months ago

User1: File1.docx and File2.docx = 2 files (file3.docx is only for new users)
User2: File2.docx and File3.docx = 2 files (File3.docx because he has never been logged on before)
User3: Fil12.docx and File3.docx = 2 files. (User3 is a guest user, and there fore he will get a new profile every time he logs on. Therefore he will get File3.docx and File4 was deleted (with the profile) when he logged off after creating the file)

upvoted 69 times

RodrigoT 5 months, 4 weeks ago

User2 is in the Replicator group. A group for computers, not users. Here is the link explaining this:
https://docs.microsoft.com/en-us/previous-versions/windows/it-pro/windows-server-2008-r2-and-2008/cc771990(v=ws.10)
And User3 is not the "guest" user because Windows 10 deprecated this, he is just member of the guest group, meaning less privileges.
So this question is very, very strange.

upvoted 1 times

RodrigoT 5 months, 2 weeks ago

FINAL ANSWER TESTED IN A WINDOWS 10 PRO 21H2 build, replicating the exact same conditions step-by-step:
User1 - 2 - File1 and File2
User2 - 2 - File2 and File3
User3 - 2 - File2 and File4
It doesn't matter if User2 is a Replicator member, it works anyway.
It doesn't matter if User3 is a Guest MEMBER (not the deprecated guest user), he does NOT load a new profile every time from the Default profile and he KEEPS the files that he created before Sign Out - Sign In.
The question is "How many DOCX files will APPEAR on the desktop of each user the next time each user signs in". So, obviously, User1 will NOT see File3 because he will NOT load the Default profile every time. The answer provided couldn't be more wrong.
Tested in lab for you. You're welcome.

upvoted 13 times

Mendel Highly Voted 3 years ago

Isn't it User1: 2, User 2: 2 and User3: 3?

User 1: File1 and File2
User 2: File 2 and File3
User 3: File 2, File 3 and File 4

File 2 on Public desktop appears on all existing and new users
File 3 on Default desktop only appears on new users

upvoted 25 times

stepient 2 years, 1 month ago

User3 won't see File4, because Guest setttings and files are not saved. I just tested it i lab.

upvoted 13 times

RodrigoT 5 months, 2 weeks ago
Wrong, User3 KEEPS the files that he created before. Tested in a Win10 Pro 21H2.
upvoted 1 times

mistrzkungfu 2 years, 8 months ago
I confirm this. I checked this on my Win 10 v1909 vm and files are present as per Mendel's comment:
- User 1: File1 and File2
- User 2: File 2 and File3
- User 3: File 2, File 3 and File 4
upvoted 11 times

h3nk13 2 years, 7 months ago
User 3 is an existing user, so it won't get file 3.
upvoted 3 times

Saldi 2 years, 5 months ago
Every time a guest user logs in, they will be treated as new.
upvoted 10 times

RodrigoT 6 months, 1 week ago
But he is not the "guest" user because Windows 10 deprecated this, he is just member of the guest group, meaning less privileges.
upvoted 2 times

Anthony_2770 1 year, 8 months ago
User 3 is a guest and will not get File4
upvoted 6 times

PinkyK 4 months, 1 week ago
I want to say special thanks to you, I passed my MD-100 and now preparing MD-101.
Your comments are always valuable and I trust what you say. Thank you so much
Pinky:)
upvoted 2 times

tf444 1 year ago
not true, it keeps all the 3 files.
upvoted 1 times

Jnorris Most Recent 1 month, 1 week ago
2 files - User 1 File 2 on public desktop and file 1 on desktop
2 files - User 2 file 2 on public desktop and file 3 on default desktop
3 files - User 3 file 2 on public desktop, file 3 on default desktop, and file4 on desktop

It specifies "user 3 then signs in" implying they sign in after User 1 created the file on the default desktop so they would get it.

Description of Guests group on Windows 10 Pro 21H2 machine
"Guests have the same access as members of the Users group by default, except for the Guest account which is further restricted"
upvoted 1 times

raduM 1 month, 3 weeks ago
3-2-2 should be correct
upvoted 1 times

Whatsamattr81 3 months, 1 week ago
Forget the theory, I just tested this out.
User 1 gets 2 files (1 and 2)
User 2 CANT even log in, he's a member of the replicator group only (doesn't mention Users...) so he gets 0 files.
User 3 gets 3 files - W10 doesnt do the TEMP thing. This is a user named User3, who is a member of guests (and not the Guest).

Final answer as tested... 2, 0, 3
upvoted 2 times

Whatsamattr81 3 months, 1 week ago
Rules. Default is a 1 time creation on first login. Guest users get a temporary profile, recreated every time they log in. Default wont apply for already created profiles.
upvoted 1 times

BrentOn 6 months, 3 weeks ago
Beginning to wonder if these answers are pulled out of a hat.
upvoted 1 times

jage01 7 months, 2 weeks ago
2, 2, 2 if user3 has already signed in before user1 created the files.

2, 2, 3 if user3 signs in for the first time after user1 created the files.
upvoted 3 times

coppermine 8 months, 3 weeks ago
User1: File1.docx (Created by User1) and File2.docx (public)
User2: File2.docx (public) and File3.docx (default) (Question specifically indicates User2 has never signed in before.)
User3: File2.docx (public) and File4.docx (Created by User3)
(Question did not indicate User3 has never signed in before so he won't get File3.docx, Also need to note that User3 is in Guests group, it is not a guest account, therefore profile won't be re-created so File4.docx remains. The difference between Guests and Users Group is Guests Group is more restrictive)

upvoted 2 times

RodrigoT 6 months, 1 week ago

I almost agree with you, but User2 is in the Replicator group. A group for computers, not users. Here is the link explaining this: https://docs.microsoft.com/en-us/previous-versions/windows/it-pro/windows-server-2008-r2-and-2008/cc771990(v=ws.10)
So this question is very, very strange.

upvoted 2 times

jage01 8 months, 3 weeks ago

Content from public folder does not get copied to the logged in user, they only have access to that folder. 1, 1, 2

upvoted 1 times

Goofer 10 months, 4 weeks ago

User1: File2 (public) + File1 (desktop, user1) = 2 files
User2: File2 (public) + File3 (Default,never signed in) = 2 files
User3: File2 (public) + File3 (Default, user1 creates File3 then User3 signs in) + File4 (desktop, user3) = 2 files
Deleting of Guest profiles depents on Windows 10 build version. Newer builds don't remove guest profiles.

upvoted 2 times

Goofer 10 months, 4 weeks ago

Typo: User3 = 3files

upvoted 2 times

ANDREVOX 11 months ago

Note the Question - "How many DOCX files will appear on the desktop of each user THE NEXT TIME each user signs in?"

User1 = 2 (C:\Users\Default\ Desktop will only be referenced upon first creating of a profile). Thus only File1.docx in C:\Users\User1\Desktop & File2.docx in C:\Users\Public\Public Desktop.

User2 = 2 Has never signed in to Computer1. First login will reference C:\Users\Public\Public Desktop & C:\Users\Default\Desktop thus having File2.docx & File3.docx

User3 = 2 Although User3 is part of the Guest group (meaning that the entire profile will be deleted upon logoff). When logging back in, C:\Users\Public\Public Desktop & C:\Users\Default\Desktop will be referenced again, thus having File2.docx & File3.docx

https://ss64.com/nt/syntax-security_groups.html

upvoted 2 times

ANDREVOX 11 months, 3 weeks ago

User 3 signs in after User 1 added the files, thus Used 3 will have File 2, File 3 and File 4 = 3

upvoted 1 times

tf444 1 year ago

2,2,2 tested, on the desktop is the question!

upvoted 4 times

Smanga1 1 year ago

2 / 2 / 2 for me

upvoted 3 times

Pleebb 1 year, 2 months ago

Question asks "How many DOCX files will appear on the desktop of each user"
"DESKTOP OF EACH USER" not "PUBLIC FOLDER"

upvoted 1 times

tf444 1 year ago

Lol, the public folder has a desktop folder!

upvoted 2 times

Perycles 1 year, 3 months ago

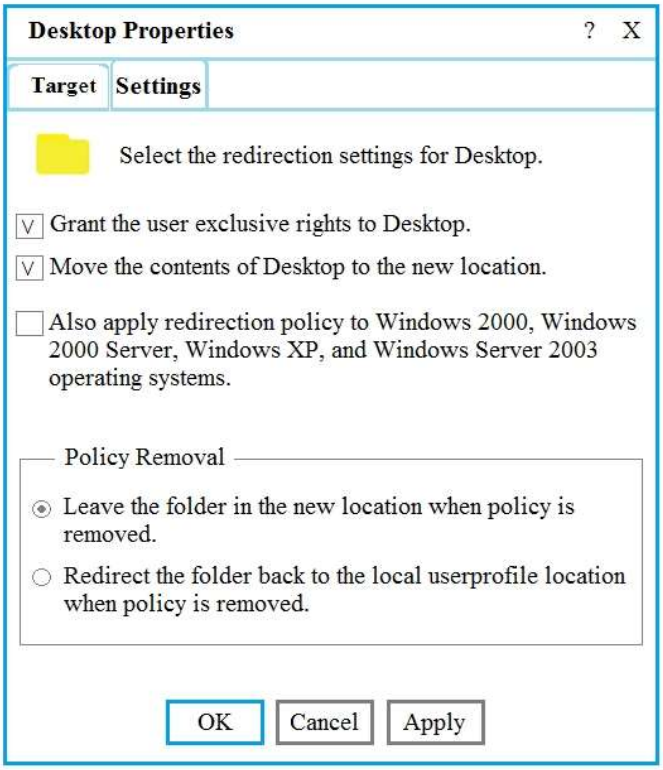
tested , tested and tested again ..... 2,2,2 be carrefull if you made the test, consider user 3 has already log on to the computers , even if answer will be 2,2,3. but in the question, user3 not mentioned as "first login" as user2.

upvoted 6 times

Question #10 *Topic 3*

Your network contains an Active Directory domain named contoso.com. The domain contains 200 computers that run Windows 10.

Folder Redirection for the Desktop folder is configured as shown in the following exhibit.



The target is set to Server1.

You plan to use known folder redirection in Microsoft OneDrive for Business.

You need to ensure that the desktop content of users remains on their desktop when you implement known folder redirection.

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

NOTE: Each correct selection is worth one point.

A. Clear the Grant the user exclusive rights to Desktop check box.

B. Change the Policy Removal setting.

C. Disable Folder Redirection.

D. Clear the Move the contents of Desktop to the new location check box.

Correct Answer: *AB*

Reference:

https://docs.microsoft.com/en-us/onedrive/redirect-known-folders

nolancl Highly Voted 3 years ago

Correct answer is BC as per Microsoft's important tip:
"Important

The OneDrive Known Folder Move Group Policy objects won't work if you previously used Windows Folder Redirection Group Policy objects to redirect the Documents, Pictures, or Desktop folders to a location other than OneDrive. Remove the Windows Group Policy objects for these folders before you enable the OneDrive Group Policy objects. The OneDrive Group Policy objects won't affect the Music and Videos folders, so you can keep them redirected with the Windows Group Policy objects. For info about Windows Folder Redirection, see Deploy Folder Redirection with Offline Files."

upvoted 40 times

thesystem 2 years, 10 months ago

Agreed, I think it should also be BC.

upvoted 5 times

DUSHIWORLD 2 years, 7 months ago

Correct

upvoted 2 times

Layer8 1 year, 4 months ago

if it's anything, it's BC

upvoted 3 times

Notinmybrain Highly Voted 2 years, 3 months ago

Clear the Grant the user exclusive rights to Desktop check box.
and check the redirect the folder. in policy
those were the answers i got on the md-101 Microsoft practice test
upvoted 5 times

gotrekk Most Recent 1 month, 2 weeks ago

Selected Answer: BC

Change the policy and disabile redirection
upvoted 1 times

MitchF 2 months, 1 week ago

Answer should be B & D.

Question asks: You need to ensure that the desktop content of users remains on their desktop...which means....KEEP IT ON THE DESKTOP!

We should pick:
B. Change the Policy Removal setting ("Redirect the folder back to the local userprofile location when policy is removed")---YES...that will put the data BACK ON THE DESKTOP!

D. Clear the "Move the contents of Desktop to the new location" check box. --If you don't "move" the contents...YES it will STAY ON THE DESKTOP!
upvoted 1 times

Dedutch 2 months ago

B: changes the policy removal setting so when the policy is removed the files are moved from the redirect location to the local desktop.

C: remove the policy so the action in B occurs.

Then when you implement the one drive solution it will check the local known folders and sync successfully, it won't sync if the folders are redirected.
upvoted 1 times

silver_bullet666 3 months ago

Selected Answer: BC

The answer is indeed as voted;
B. Change the Policy Removal setting.
C. Disable Folder Redirection.
I have personally done this irl a few years back
upvoted 1 times

Whatsamattr81 3 months, 1 week ago

https://docs.microsoft.com/en-us/onedrive/redirect-known-folders

B and C it is then... Doing B will do A by default as the exclusive access permission is set at the server level (on the share).
upvoted 2 times

RodrigoT 5 months, 2 weeks ago

Selected Answer: AB

FINAL ANSWER, got this in a KAPLAN practice exam:
-Uncheck Grant the user exclusive rights to Documents. When this is enabled, Folder Redirection fist checks preexisting folders to determine if the user is the owner. If the administrator previously created the folder, this check will fail and redirection will be cancelled. If you create folders for users, the permissions must be set correctly.
-Change Policy Removal to Redirect the folder back... to ensure that the desktop content of users still remains on their desktop after you implement known folder redirection.
upvoted 5 times

ken2ut 4 months, 1 week ago

One of the requirements for setting up Known Folder Redirection to OneDrive is "NO GPO for Folder Redirection must exist" and if you had setup a KFR and decided to use OneDrive for KFR, the 2nd policy removal option must be selected.
This is one of the video lesson in CBTNuggets.

Answer is B,C.
upvoted 1 times

Adhikari123 5 months, 3 weeks ago

Selected Answer: BC

This is the answer
upvoted 1 times

Adhikari123 6 months, 1 week ago

Selected Answer: BC

B and C
upvoted 1 times

Harold 6 months, 2 weeks ago

Selected Answer: BC

Agree with the other explanations.
upvoted 1 times

rj_client 6 months, 3 weeks ago

Selected Answer: BC

Given this scenario best choices appear to be B and C

B
You need to copy the relevant files back to users pc so that one drive folder redirection can user the current folders/files.

C
Folder redirection has to be disabled as it does not work with OneDrive known Folder Move
upvoted 1 times

PiPe 7 months, 4 weeks ago

Selected Answer: BC

https://diychris.com/index.php/2019/05/24/your-it-administrator-has-set-a-policy-that-prevents-changes-to-known-folders-please-remove-this-policy-and-try-again/

https://docs.microsoft.com/en-us/answers/questions/360973/disable-folder-redirection-policy.html

I'm going for BC
upvoted 3 times

auton 11 months, 3 weeks ago

AB is correct;

"If folders have been redirected to a network file share:

Note

We recommend using Windows 10 Fall Creators Update (version 1709 or later) or Windows Server 2019 and the current version of OneDrive to get the benefits from Files On-Demand.

Use Migration Manager to copy contents in the network file share location to a user's OneDrive, making sure that all contents go into the existing Documents, Pictures, or Desktop folders.
Disable the Window Folder Redirection Group Policy and make sure to leave the folder and contents on the network file share.
Enable KFM Group Policy. Known folders move to OneDrive and will merge with the existing Desktop, Documents, and Pictures folders, which contain all the file share content that you moved in the first step."

Migration Manager needs administrator rights and through that we have opt the user exclusivity to the desktop.

We also need to change the settings specified in Policy Removal to ensure that data stays on the desktop.

Which is why I'm leaning towards AB.
upvoted 2 times

Merma 1 year, 5 months ago

B & C are correct. In addition to the original reference link please see:
https://4sysops.com/archives/remove-unneeded-settings-from-group-policy-objects/
https://docs.microsoft.com/en-us/onedrive/redirect-known-folders
upvoted 3 times

Millsy 1 year, 8 months ago

A: is not helpful at all as the administrator does not need access to these files all the processing happens user side so weather or not the user has exclusive rights is moot
B: is a must because we need the files to return to the default desktop location on the users PC so onedrive can take them over
C: This is required to kick off the move of the data back to the regular location
D: We need the contents moved so we leave this setting alone.
upvoted 3 times

Millsy 1 year, 8 months ago

This is one of those questions that want the Microsoft way... so to do it the microsoft way it's AB -
Use a migration tool to copy contents in the network file share location to a user's OneDrive, making sure that all contents go into the existing Documents, Pictures, or Desktop folders.
Disable the Window Folder Redirection Group Policy and make sure to leave the folder and contents on the network file share.
Enable KFM Group Policy. Known folders move to OneDrive and will merge with the existing Desktop, Documents, and Pictures folders which contain all the file share content that you moved in the first step.
upvoted 2 times

goape 1 year, 10 months ago

Had this question come up in Kaplan practice test today. Answer was AB
upvoted 4 times

RodrigoT 6 months, 1 week ago

Me too. AB
upvoted 1 times

Justin0020 1 year, 12 months ago

Answer is B and C. This reference is very clear: https://docs.microsoft.com/en-us/onedrive/redirect-known-folders
upvoted 3 times

DJM 1 year, 10 months ago

"Disable the Window Folder Redirection Group Policy and make sure to leave the folder and contents on the network file share." The reference says to leave the folders i.e. not change the policy removal setting.
upvoted 1 times

Question #11 *Topic 3*

HOTSPOT -

You have a Microsoft 365 subscription.

All computers are enrolled in Microsoft Intune.

You have business requirements for securing your Windows 10 environment as shown in the following table.

Requirement	Detail
Requirement1	Ensure that Microsoft Exchange Online can be accessed from known locations only.
Requirement2	Lock a device that has a high Microsoft Defender for Endpoint risk score.

What should you implement to meet each requirement? To answer, select the appropriate options in the answer area.

NOTE: Each correct selection is worth one point.

Hot Area:

Answer Area

Requirement1

- A conditional access policy
- A device compliance policy
- A device configuration profile

Requirement2

- A conditional access policy
- A device compliance policy
- A device configuration profile

Correct Answer:

Answer Area

Requirement1

- **A conditional access policy**
- A device compliance policy
- A device configuration profile

Requirement2

- A conditional access policy
- **A device compliance policy**
- A device configuration profile

Box 1: A conditional access policy

Box 2: A device compliance policy

Compliance policies in Intune:

Define the rules and settings that users and devices must meet to be compliant.

Include actions that apply to devices that are noncompliant. Actions for noncompliance can alert users to the conditions of noncompliance and safeguard data on noncompliant devices.

Can be combined with Conditional Access, which can then block users and devices that don't meet the rules.

Reference:

https://docs.microsoft.com/en-us/mem/intune/protect/device-compliance-get-started

john909 Highly Voted 11 months ago

Looks ok

Check also https://docs.microsoft.com/en-us/mem/intune/protect/actions-for-noncompliance

upvoted 8 times

chapinoli Most Recent 8 months, 1 week ago

I disagree here. Device compliance policy cannot "lock" a device, it can only flag it as non-compliant. It is the conditional access policy that actually performs the "lock" or "block" action.

Compliance policies in Intune:

Define the rules and settings that users and devices must meet to be compliant.

Include actions that apply to devices that are noncompliant. Actions for noncompliance can alert users to the conditions of noncompliance and safeguard data on noncompliant devices.

Can be combined with Conditional Access, which can then block users and devices that don't meet the rules.
https://docs.microsoft.com/en-us/mem/intune/protect/device-compliance-get-started

upvoted 1 times

pogap64757 7 months, 4 weeks ago

For iOS and Android, compliance can remotely lock a device under "Actions for noncompliance".
Best answer for the question as the MS Defender for Endpoint Rating is in the compliance policy settings

upvoted 1 times

RodrigoT 6 months, 1 week ago

The link provided states: "Support actions that apply to devices that don't meet your compliance rules. Examples of actions include being remotely locked". So the answers provided are correct.

upvoted 2 times

RodrigoT 5 months ago

Conditional access uses that compliance status to determine whether to grant or block access to email and other organization resources. You can configure your Conditional Access policies to use the results of your device compliance policies. Meaning, you have to "start" with a device compliance policy to fulfill the Requirement2.

https://docs.microsoft.com/en-us/mem/intune/protect/device-compliance-get-started#integrate-with-conditional-access

upvoted 1 times

mayleni 8 months, 2 weeks ago

correct

upvoted 1 times

Moderator 8 months, 3 weeks ago

Correct answers.

upvoted 1 times

mikl 9 months, 1 week ago

I agree.

upvoted 1 times

HOTSPOT -

Your company has computers that run Windows 10. The employees at the company use the computers.

You plan to monitor the computers by using the Update Compliance solution.

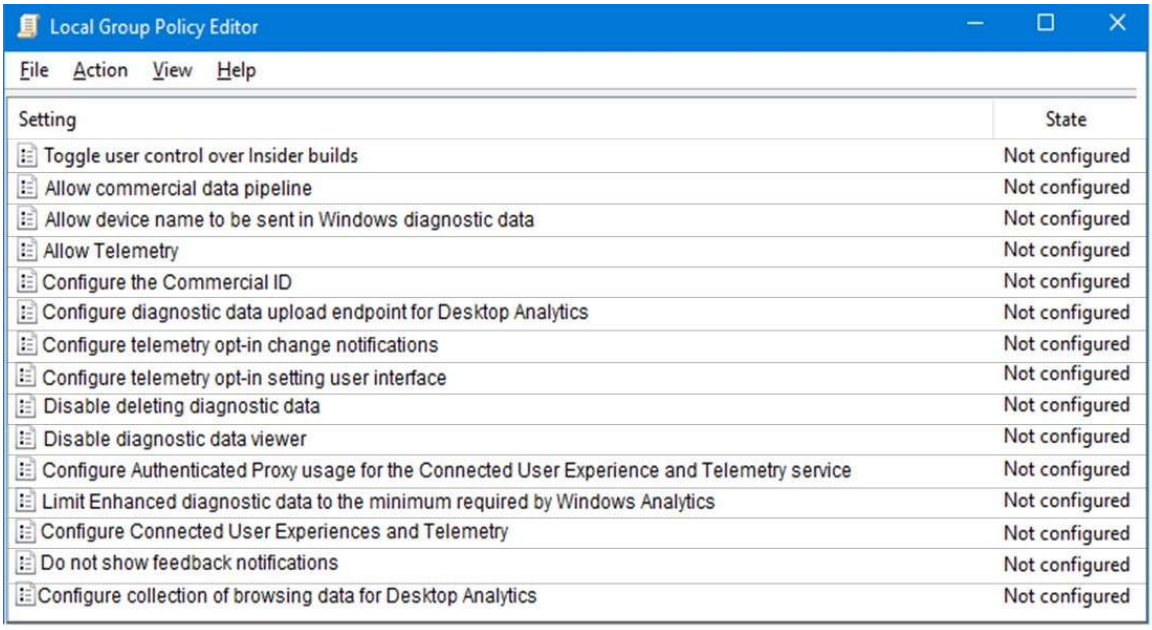
You create the required resources in Azure.

You need to configure the computers to send enhanced Update Compliance data.

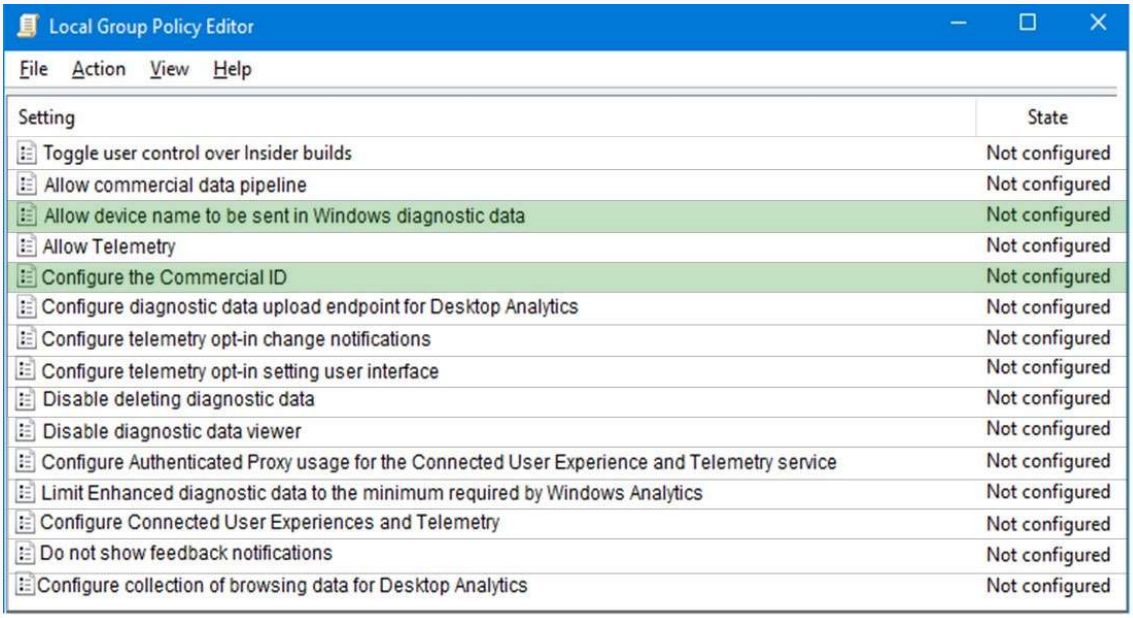
Which two Group Policy settings should you configure? To answer, select the appropriate settings in the answer area.

NOTE: Each correct selection is worth one point.

Hot Area:



Correct Answer:



Box 1: Configure the Commercial ID

All Group policies that need to be configured for Update Compliance are under Computer Configuration>Administrative Templates>Windows Components\Data

Collection and Preview Builds. All of these policies must be in the Enabled state and set to the defined Value below.

* Configure the Commercial ID

Identifies the device as belonging to your organization.

Box 2: Allow device name to be sent in Windows diagnostic data

* Allow device name to be sent in Windows diagnostic data

Allows device name to be sent for Windows Diagnostic Data. If this policy is Not Configured or Disabled, Device Name will not be sent and will not be visible in

Update Compliance, showing # instead.

Reference:

https://docs.microsoft.com/en-us/windows/deployment/update/update-compliance-configuration-manual

Poncho25 Highly Voted 1 year, 5 months ago

The question itself is flawed. The correct answer must include the Allow Telemetry policy set to 2 (Enhanced). So that means you must select the 3 group policies to get the correct answer, not two. The correct answer is actually Configure Commercial ID, Allow Telemetry, & Allow device name to be sent in Windows diagnostic data.

upvoted 10 times

raduM Most Recent 1 month, 3 weeks ago

configure commercial id and allow telemetry

upvoted 2 times

silver_bullet666 2 months ago

check the link https://docs.microsoft.com/en-us/windows/deployment/update/update-compliance-configuration-manual
there are actually more items that need to be set than are mentioned here

upvoted 1 times

Whatsamattr81 3 months, 1 week ago

Bad question. Update Compliance requires at least Basic (or Required) diagnostic data, but can function off Enhanced or Full (or Optional). Mandatory GPO settings are here - https://docs.microsoft.com/en-us/windows/deployment/update/update-compliance-configuration-manual#required-policies.
To focus on 'enhanced' though, its in the Allow telemetry setting, also commercial ID. Not sending the name wont stop the enhanced data flowing -If this policy is Not Configured or Disabled, Device Name will not be sent and will not be visible in Update Compliance, showing # instead.

upvoted 1 times

ken2ut 4 months, 1 week ago

Answer is correct.
"Allow telemetry" mainly used for collecting your computer data and sending it to Microsoft. This is useful for beta tester and insider program.
This is similar to apple like enabling sending analytics from iOS devices to help improve product and services. That is exactly what the policy does in Windows.

upvoted 1 times

PiPe 7 months, 4 weeks ago

Allow Telemetry & Configure the Commercial ID
I don't see a requirement to send the device name together with the telemetry, so they're fine with the anonymized data, I guess.

upvoted 4 times

moobdoob 8 months, 2 weeks ago

Commercial ID + Telemetry is what im going with.

upvoted 3 times

forummj 8 months, 3 weeks ago

Finally I see the answer lol.

We all agree that Commercial ID needs to be configured.

The question also states "enhanced" data needs to be sent, this option is is Allow Telemetry which can be set to Basic or Enhanced, so this must be the second option.

upvoted 2 times

petersed 10 months ago

Configure the Commercial ID and Allow Telemetry
https://docs.microsoft.com/en-us/windows/deployment/update/update-compliance-configuration-manual#:~:text=%20The%20requirements%20are%20separated%20into%20different%20categories%3A,all%20necessary%20data%20points%20are%20collected.%20See%20More.

upvoted 2 times

Perycles 1 year, 3 months ago

commercial ID and Telemetry. Device computer name is not mandatory. if this gpo is not applied data will be sent to Dekstop analytics , but computer name not. https://docs.microsoft.com/en-us/windows/deployment/update/update-compliance-configuration-manual

upvoted 1 times

Tiit 1 year, 4 months ago

Actually - if question is, "Which TWO Group Policy settings" then, *Configure the Commercial ID and *Allow device name to be sent in Windows diagnostic data are "Must be", because "If you disable or do not configure this policy setting, then device name will not be sent to Microsoft as part of Windows diagnostic data".- but "allow telemetry" is optional, because If you disable or do not configure this policy setting, users can configure the Telemetry level in Settings.

upvoted 1 times

Poncho25 1 year, 4 months ago

Like I said, the question is flawed. The questions states: you need "enhanced Update Compliance data". You can only send enhanced compliance data by enabling Enhanced on the Allow Telemetry policy. That means you need all three options enabled to satisfy the requirements.

upvoted 2 times

Merma 1 year, 5 months ago

Why not:
4. Allow Telemetry
6. Configure diagnostic data upload endpoint for Desktop Analytics
"After adding the solution to Azure and configuring devices, there will be a waiting period of up to 72 hours before you can begin to see devices in the solution. Before or as devices appear, you can learn how to Use Update Compliance to monitor Windows Updates and Delivery Optimization."
https://docs.microsoft.com/en-us/windows/deployment/update/update-compliance-get-started

upvoted 1 times

Merma 1 year, 4 months ago

After reading and thinking about it, I'll go with the answers provided.
3. Allow device name to be sent in Windows diagnostic date
5.Configure the Commercial ID

upvoted 1 times

Merma 1 year, 4 months ago

The question & answer is likely to changing in the future:
"As of May 10, 2021, a new policy is required to use Update Compliance: "Allow Update Compliance Processing." For more details, see the Mobile Device Management policies and Group policies tables."

upvoted 1 times

HOTSPOT -

You are licensed for Microsoft Endpoint Manager.

You use Microsoft Endpoint Configuration Manager and Microsoft Intune.

You have devices enrolled in Configuration Manager as shown in the following table.

Name	Collection
Device1	Collection1
Device2	Collection2
Device3	Collection1, Collection2

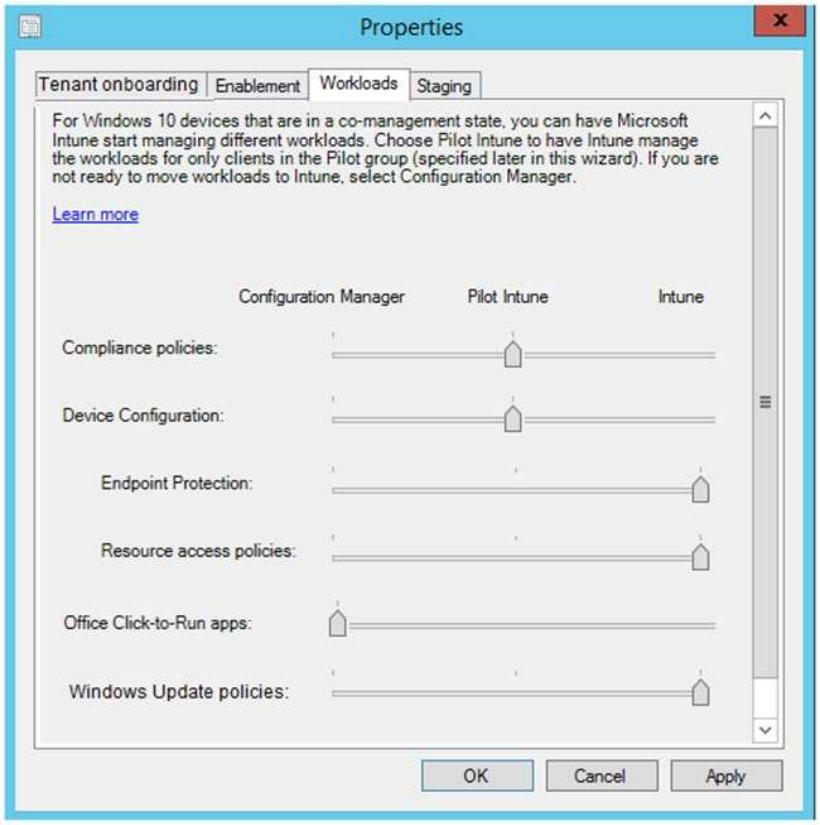
In Configuration Manager, you enable co-management and configure the following settings:

- Automatic enrolment in Intune: Pilot
- Intune Auto Enrollment: Collection1

In Configuration Manager, you configure co-management staging to have the following settings:

- Compliance policies: Collection2
- Device Configuration: Collection1

In Configuration Manager, 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.

Hot Area:

Answer Area

Statements	Yes	No
You can use the Microsoft Endpoint Manager admin center to monitor the compliance status of Device1.	○	○
You can use the Microsoft Endpoint Manager admin center to monitor the compliance status of Device2.	○	○
You can use the Microsoft Endpoint Manager admin center to monitor the compliance status of Device3.	○	○

Correct Answer:

Answer Area

Statements	Yes	No
You can use the Microsoft Endpoint Manager admin center to monitor the compliance status of Device1.	○	○
You can use the Microsoft Endpoint Manager admin center to monitor the compliance status of Device2.	○	○
You can use the Microsoft Endpoint Manager admin center to monitor the compliance status of Device3.	○	○

Box 2: No -

Members of Collection2 are not enrolled in Intune.

Box 3: Yes -

Device3 has Collection2 which has compliance policies.

Reference:

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

Perycles Highly Voted 1 year, 3 months ago

No,No,Yes see Anonimouse explains, it's correct.

upvoted 22 times

asdaa Highly Voted 11 months, 2 weeks ago

This is the first question where I can say confidently that the answer is wrong. Answer should be NO,NO,YES.

Microsoft documentation:
https://docs.microsoft.com/en-us/mem/configmgr/comanage/how-to-enable
"Pilot - Only the Configuration Manager clients that are members of the Intune Auto Enrollment collection are automatically enrolled to Intune."

So members of collection 2 are NOT enrolled in Intune. Therefore you will not be able to see their compliance status in MEM.

upvoted 7 times

RodrigoT 6 months, 1 week ago

I agree.
NO. Device1 is enrolled but not assigned.
NO. Device2 is assigned but not enrolled.
YES. Device3 is enrolled and assigned, because is included in both collections.

upvoted 2 times

RodrigoT 5 months, 4 weeks ago

Explaining better:
I agree.
NO. Device1 is enrolled in Intune, but not compliance policy assigned.
NO. Device2 is compliance policy assigned, but not enrolled in Intune.
YES. Device3 is enrolled and assigned, because is included in both collections.

upvoted 3 times

raduM Most Recent 1 month, 2 weeks ago

No No Yes. Given answer is wrong

upvoted 1 times

MitchF 2 months, 1 week ago

Answers look correct based on this:

1) Can you use the Endpt Mgr Admin Center to monitor the compliance status of Device1---No, it is auto-enrolled (Collection1), but no compliance policy assigned (Collection2)

2) Can you use the Endpt Mgr Admin Center to monitor the compliance status of Device2----Yes, it is co-managed & has compliance policy assigned (Collection2)
Note on co-managed devices: "As an administrator, you can see co-managed devices in the Microsoft Endpoint Manager admin center. You can do remote actions from the admin center"...so you can see if the device is compliant via co-management.
Source:
https://docs.microsoft.com/en-us/mem/configmgr/comanage/faq

3) Can you use the Endpt Mgr Admin Center to monitor the compliance status of Device3 (Collection 1&2): Yes, it is auto-enrolled (Collection1) & has a compliance policy (Collection2)

upvoted 1 times

raduM 1 month, 2 weeks ago

device 2 is not comanaged because you set the auto enrollment just for collection 1

upvoted 1 times

Merma 1 year, 4 months ago

Box 1: No, compliance policies are assigned to Collection2 and not Collection1, therefore Device1 which is a assigned to Collection1 cannot be monitored for compliance status.
Box 2: Yes, compliance policies are assigned to Collection2, assigned with Device2.
Box 3: Yes, compliance policies are assigned to Collection2, assigned with Device3.

upvoted 1 times

AnoniMouse 1 year, 4 months ago

No: compliance policies are assigned to Collection2 and not Collection1, therefore Device1 which is a assigned to Collection1 cannot be monitored for compliance status.
No: Members of Collection2 are NOT enrolled in Intune
YES: Compliance policies are assigned to Collection2, assigned with Device3

upvoted 31 times

Question #14 *Topic 3*

You have an Azure Active Directory group named Group1. Group1 contains two Windows 10 Enterprise devices named Device1 and Device2.
You create a device configuration profile named Profile1. You assign Profile1 to Group1.
You need to ensure that Profile1 applies to Device1 only.
What should you modify in Profile1?

A. Scope (Tags)

B. Settings

C. Applicability Rules

D. Assignments

Correct Answer: *D*
You create a profile, and it includes all the settings you entered. The next step is to deploy or "assign" the profile to your user or device groups. When it's assigned, the users and devices receive your profile, and the settings you entered are applied.
Reference:
https://docs.microsoft.com/en-us/mem/intune/configuration/device-profile-assign

Mage7 Highly Voted 11 months ago
D - correct.

Scope - limits administrators view does not have effect whether Profile will be applied or not.
Settings - we have correct settings already. Question is not about this..
Applicability Rules - could be used but in this case question states that BOTH devices are Windows 10 Enterprise - you cannot use this.

Only correct answer is Settings (you'll have either to replace INCLUDE Group1 with other group or do not touch INCLUDE and add EXCLUDE GROUPX where device2 is a member).
upvoted 12 times

ercluff 9 months ago
Didn't you mean "assignments" as the only correct answer?
upvoted 4 times

randdrick Most Recent 5 months ago
Selected Answer: A
I think the correct answer is A beacause device 1 and device 2 are in the same group.
Policy is apply for the group. You can ONLY include or exclude a group, not a device.
But you can use tag to apply rules (see : https://docs.microsoft.com/en-us/mem/intune/configuration/device-profile-assign#use-scope-tags-or-applicability-rules)
upvoted 1 times

Moderator 8 months, 3 weeks ago
Selected Answer: D
Assigments (D) should be the correct answer here, imo: https://docs.microsoft.com/en-us/mem/intune/configuration/device-profile-assign
upvoted 1 times

b3arb0yb1m 9 months, 1 week ago
C. Applicability Rules
upvoted 1 times

CARO54 9 months, 1 week ago
Could be used but in this case question states that BOTH devices are Windows 10 Enterprise - you cannot use this.
upvoted 2 times

encxorblood 10 months, 2 weeks ago
D is correct. Include or Exclude Devices in assigment.
upvoted 2 times

DogeZaemon 11 months, 1 week ago
There is no way to specify an individual device in Assignments (include or exclude)
The only possible way is using tags
https://docs.microsoft.com/en-us/mem/intune/fundamentals/scope-tags
upvoted 1 times

Angarali 5 months, 2 weeks ago
you're confused..
upvoted 1 times

Mage7 11 months ago
Tags limit Administrators view,
upvoted 3 times

Question #15 *Topic 3*

Your network contains an on-premises Active Directory domain and an Azure Active Directory (Azure AD) tenant.

The Default Domain Policy Group Policy Object (GPO) contains the settings shown in the following table.

Name	GPO value
LockoutBadCount	0
MaximumPasswordAge	42
MinimumPasswordAge	1
MinimumPasswordLength	7
PasswordComplexity	True
PasswordHistorySize	24

You need to migrate the existing Default Domain Policy GPO settings to a device configuration profile.

Which type of device configuration profile should you create?

A. Custom

B. Endpoint protection

C. Administrative Templates

D. Device restrictions

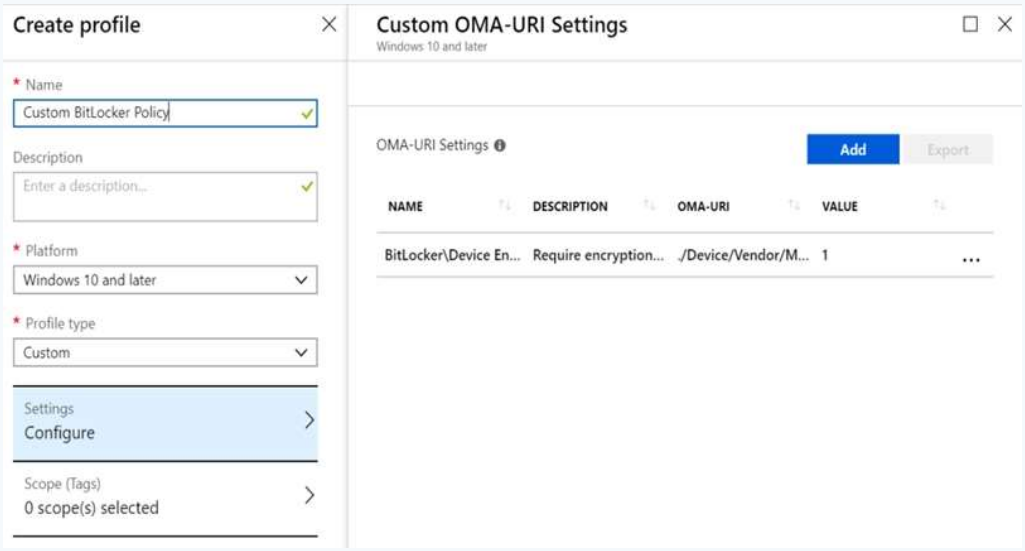
Correct Answer: *A*

Intune (and other MDM solutions) build there policy configurations and user interfaces on top of CSPs(Configuration Service Providers) .

However, some CSPs and its settings might not be exposed in the interface directly but such a setting can be set anyway by entering its OMA-URI manually. Think of an OMA-URI as sort of a registry key that you can set to make the underlying configuration setting happen.

In Intune this is called a Custom Policy.

Example:



Reference:

https://danielchronlund.com/2018/11/27/how-to-replace-your-old-gpos-with-intune-configuration-profiles/

asturmark 3 weeks, 3 days ago

The answer should be ¨device restrictions¨. From there you have the options for password complexity

upvoted 1 times

Question #16 *Topic 3*

Your company plans to deploy tablets to 50 meeting rooms.
The tablets run Windows 10 and are managed by using Microsoft Intune. The tablets have an application named App1.
You need to configure the tablets so that any user can use App1 without having to sign in. Users must be prevented from using other applications on the tablets.
Which device configuration profile type should you use?

A. Kiosk

B. Endpoint protection

C. Identity protection

D. Device restrictions

Correct Answer: *A*
Reference:
https://docs.microsoft.com/en-us/windows/configuration/kiosk-single-app

Dong1999 Highly Voted 1 year, 2 months ago
Answer is correct
upvoted 7 times

MR_Eliot Most Recent 5 months, 2 weeks ago
Selected Answer: A
Kiosk is the answer.
upvoted 1 times

mikl 9 months, 2 weeks ago
A. Kiosk

https://docs.microsoft.com/en-us/mem/intune/configuration/kiosk-settings-windows
upvoted 2 times

Question #17 *Topic 3*

HOTSPOT -

Your network contains an Active Directory domain named contoso.com that syncs to Azure Active Directory (Azure AD). The domain contains computers that run

Windows 10. The computers are configured as shown in the following table.

Name	Member of
Computer1	Group1
Computer2	Group2

All the computers are enrolled in Microsoft Intune.

You configure the following Maintenance Scheduler settings in the Default Domain Policy:

- Turn off auto-restart for updates during active hours: Enabled
- Active hours start: 08:00
- Active hours end: 22:00

In Intune, you create a device configuration profile named Profile1 that has the following OMA-URI settings:

- ./Device/Vendor/MSFT/Policy/Config/ControlPolicyConflict/MDMWinsOverGP set to value 1
- ./Device/Vendor/MSFT/Policy/Config/Update/ActiveHoursStart set to value 9
- ./Device/Vendor/MSFT/Policy/Config/Update/ActiveHoursEnd set to value 21

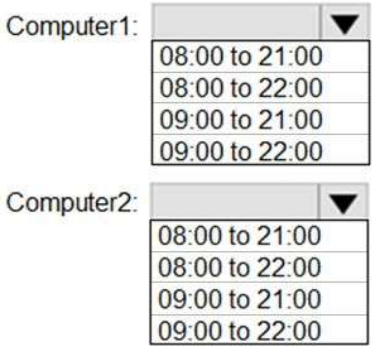
You assign Profile to Group1.

How are the active hours configured on Computer1 and Computer2? To answer, select the appropriate options in the answer area.

NOTE: Each correct selection is worth one point.

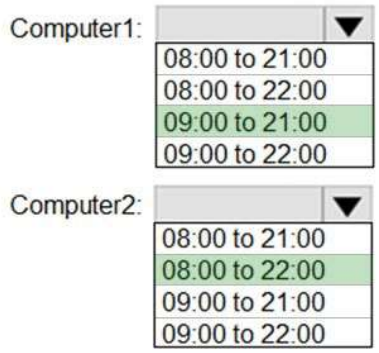
Hot Area:

Answer Area



Correct Answer:

Answer Area



Box 1: 09:00 to 21:00 -

For Computer1 Profile1 overrides the Default Domain Policy.

Box 2: 08:00 to 22:00 -

Computer2 uses the default Domain Policy.

Reference:

https://docs.microsoft.com/en-us/windows/client-management/mdm/policy-csp-controlpolicyconflict

Perycles Highly Voted 1 year, 3 months ago

if all questions could be like this one :)
Answer is correct/

upvoted 21 times

RodrigoT 6 months, 1 week ago

Two points easy peasy.

upvoted 1 times

raduM Most Recent 1 month, 3 weeks ago

if it all would be that easy

upvoted 1 times

Anon1212 7 months, 2 weeks ago

Literally the easiest question on this test <~

upvoted 4 times

krisbla 7 months, 3 weeks ago

The part of "Device/Vendor/MSFT/Policy/Config/ControlPolicyConflict/MDMWinsOverGP set to value 1" threw me off a bit. But answer should be correct.

upvoted 1 times

Kumargvm 8 months, 1 week ago

hehe...straight forward one...

upvoted 1 times

mikl 9 months, 1 week ago

I agree.

upvoted 1 times

lollo1234 1 year, 4 months ago

Answer is correct

upvoted 4 times

Question #18 *Topic 3*

HOTSPOT -

You have a Microsoft 365 subscription.

You have 25 Microsoft Surface Hub devices that you plan to manage by using Microsoft Endpoint Manager.

You need to configure the devices to meet the following requirements:

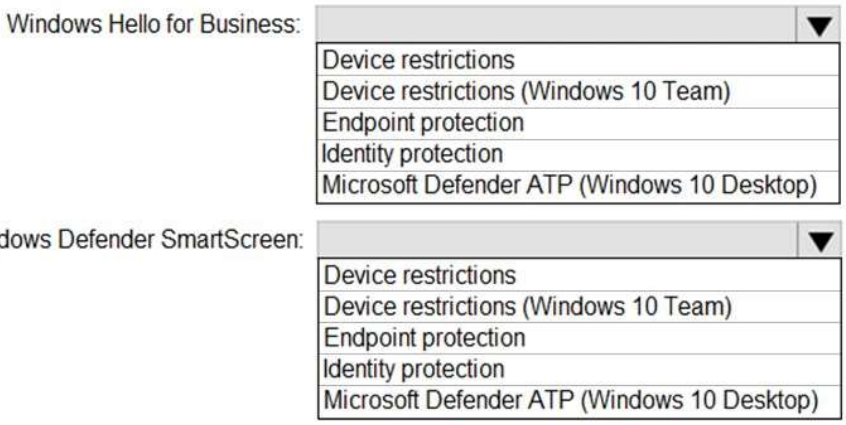
- Enable Windows Hello for Business.
- Configure Microsoft Defender SmartScreen to block users from running unverified files.

Which profile types should you configure? To answer, select the appropriate options in the answer area.

NOTE: Each correct selection is worth one point.

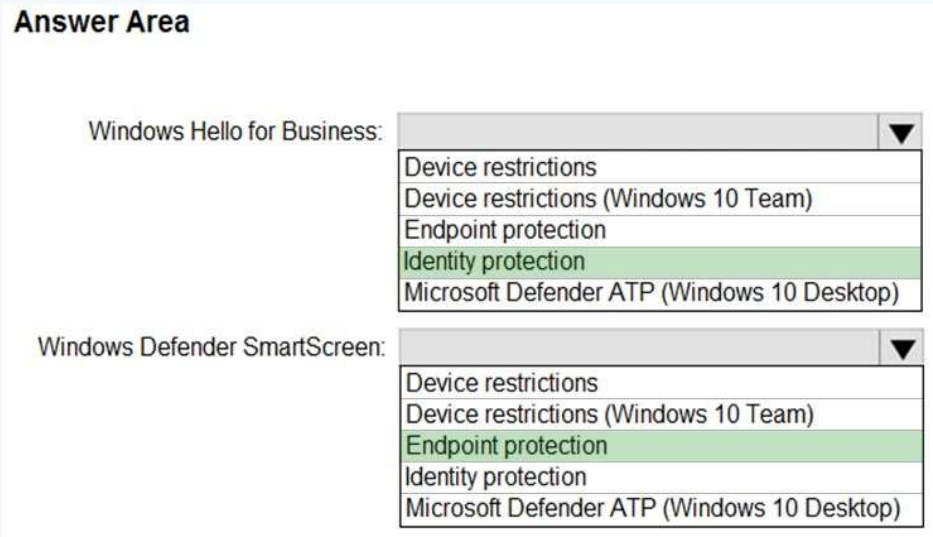
Hot Area:

Answer Area



Correct Answer:

Answer Area



Box 1: Identity protection -

In the Windows Hello for Business settings you can configure in an Identity protection profile. Identity protection profiles are part of device configuration policy in

Microsoft Intune. With an Identity protection profile, you can configure settings on discrete groups of Windows 10/11 devices.

Box 2: Endpoint protection -

Microsoft Intune includes many settings to help protect your devices. These settings are created in an endpoint protection configuration profile in Intune to control security, including BitLocker and Microsoft Defender.

Reference:

https://docs.microsoft.com/en-us/mem/intune/protect/identity-protection-windows-settings?toc=/intune/configuration/toc.json&bc=/intune/configuration/breadcrumb/ toc.json https://docs.microsoft.com/en-us/mem/intune/protect/endpoint-protection-windows-10?toc=/intune/configuration/toc.json&bc=/intune/configuration/breadcrumb/ toc.json

Perycles Highly Voted 1 year, 3 months ago

answers are correct.

upvoted 10 times

MikeMatt2020 Highly Voted 1 year, 4 months ago

Windows Hello for Business can be configure within Identity Protection

But it seems that this SmartScreen setting can be configured in BOTH Device Restrictions and Endpoint Protection. Literally the same exact setting.

upvoted 6 times

MikeMatt2020 1 year, 4 months ago

I suppose I'll go with Endpoint Protection. Still confusing.

https://docs.microsoft.com/en-us/mem/intune/protect/endpoint-protection-windows-10

upvoted 4 times

RodrigoT 6 months, 1 week ago

They are NOT the same thing. Microsoft Defender SmartScreen under Device restrictions is only for Microsoft Edge. The right answer is indeed Endpoint protection > Microsoft Defender SmartScreen settings.
https://docs.microsoft.com/en-us/windows/client-management/mdm/policy-csp-smartscreen#smartscreen-enablesmartscreeninshell

upvoted 6 times

Question #19 *Topic 3*

DRAG DROP -

Your network contains an Active Directory domain that is synced to Microsoft Azure Active Directory (Azure AD). All computers are joined to the domain and registered to Azure AD.

The network contains a Microsoft Endpoint Configuration Manager deployment that is configured for co-management with Microsoft Intune.

All the computers in the finance department are managed by using Endpoint Configuration Manager. All the computers in the marketing department are managed by using Intune.

You install new computers for the users in the marketing department by using the Microsoft Deployment Toolkit (MDT).

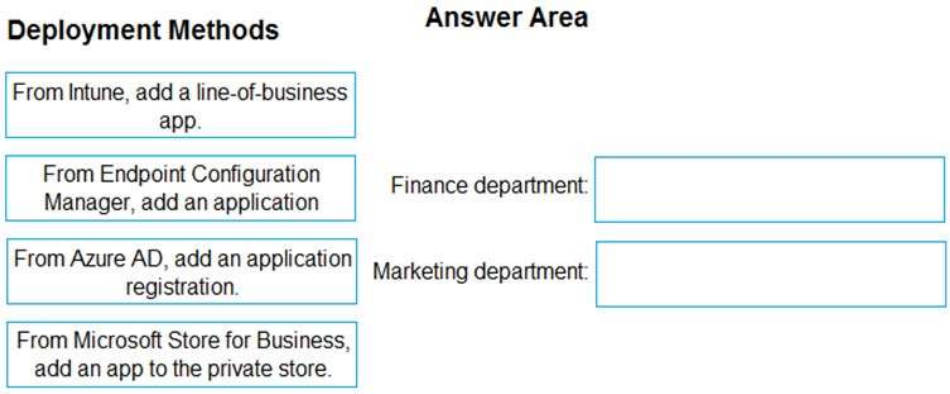
You purchase an application named App1 that uses an MSI package.

You need to install App1 on the finance department computers and the marketing department computers.

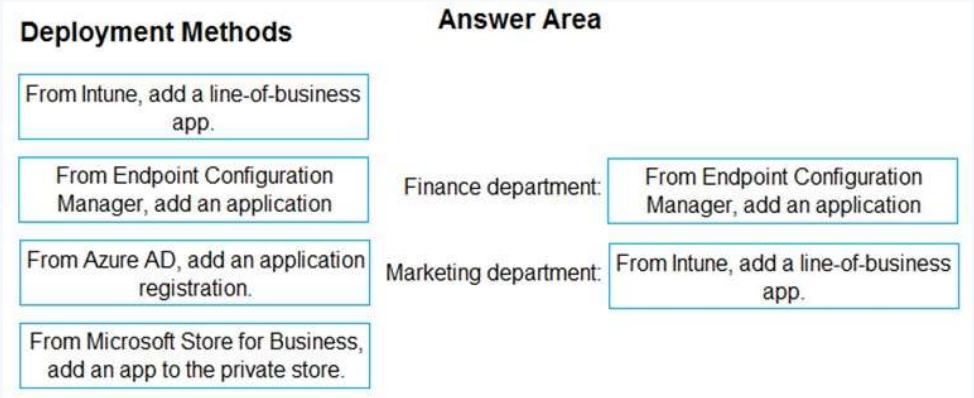
How should you deploy App1 to each department? To answer, drag the appropriate deployment methods to the correct departments. Each deployment method may be used once, more than once, or not at all. You may need to drag the split bat between panes or scroll to view content.

NOTE: Each correct selection is worth one point.

Select and Place:



Correct Answer:



Box 1: From Endpoint Configuration Manager, add an application

All the computers in the finance department are managed by using Endpoint Configuration Manager.

Distribute the application content.

1. In the Configuration Manager console, choose Software Library.
2. In the Software Library workspace, expand Applications. Then, in the list of applications, select the application.
3. Etc.

Box 2: From Intune, add a line-of-business app

All the computers in the marketing department are managed by using Intune.

Before you can configure, assign, protect, or monitor apps, you must add them to Microsoft Intune.

You can add an app in Microsoft Intune by selecting Apps > All apps > Add. The Select app type pane is displayed and allows you to select the App type.

Note: An LOB app is one that you add from an app installation file.

Reference:

https://docs.microsoft.com/en-us/intune/apps-add

https://docs.microsoft.com/en-us/sccm/apps/get-started/create-and-deploy-an-application

AVP_Riga Highly Voted 10 months, 4 weeks ago

For MECM answer is correct!

upvoted 6 times

RodrigoT Most Recent 6 months, 1 week ago

Correct answer. Two easy points.

upvoted 2 times

Question #20 *Topic 3*

Your company has a Microsoft 365 subscription.
The company uses Microsoft Intune to manage all devices.
The company uses conditional access to restrict access to Microsoft 365 services for devices that do not comply with the company's security policies.
You need to identify which devices will be prevented from accessing Microsoft 365 services.
What should you use?

A. The Device tab in Desktop Analytics.

B. Microsoft Defender Security Center.

C. The Device compliance blade in the Microsoft Endpoint Manager admin center.

D. The Conditional access blade in the Azure Active Directory admin center.

Correct Answer: *C*
Monitor Intune Device compliance policies.
1. Open the Intune Device compliance dashboard:
2. Sign in to the Microsoft Endpoint Manager admin center.
3. Select Devices > Overview > Compliance status tab.
Note: Compliance reports help you review device compliance and troubleshoot compliance-related issues in your organization. Using these reports, you can view information on:
- The overall compliance states of devices
- The compliance status for an individual setting
- The compliance status for an individual policy
- Drill down into individual devices to view specific settings and policies that affect the device

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

MikeMatt2020 Highly Voted 1 year, 4 months ago
Correct:

I believe this can be found under "Reports" > "Device Compliance"
upvoted 9 times

Perycles 1 year, 3 months ago
you're right
upvoted 3 times

chalitha Most Recent 1 year, 3 months ago
https://docs.microsoft.com/en-us/mem/intune/fundamentals/tutorial-walkthrough-endpoint-manager
upvoted 1 times

Merma 1 year, 4 months ago
3. From the navigation pane, select Devices to display details about the enrolled devices in your Intune tenant.
The Devices - Overview pane has several tabs that allow you to view a summary of the following statuses and alerts:
Compliance status - Review compliance status based on device, policy, setting, threats, and protection. Additionally, this pane provides a list of devices without a compliance policy.
4. From the Devices - Overview pane, select Compliance policies to display details about compliance for devices managed by Intune.
5. From the Devices - Overview pane, select Conditional Access to display details about access policies.
6. From the navigation pane, select Devices > Configuration profiles to display details about device profiles in Intune.
https://docs.microsoft.com/en-us/mem/intune/fundamentals/tutorial-walkthrough-endpoint-manager
upvoted 1 times

HOTSPOT -

You have 200 computers that run Windows 10.

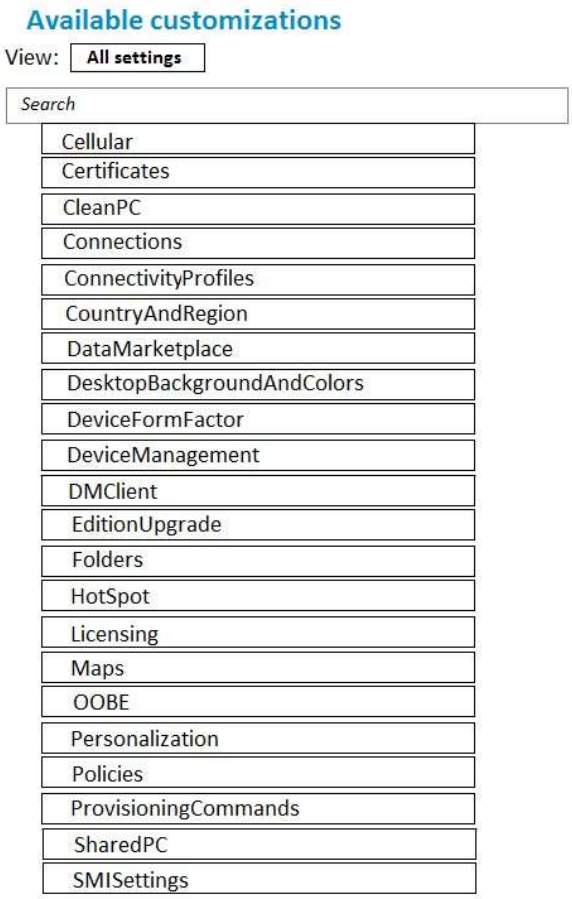
You need to create a provisioning package to configure the following tasks:

- Remove the Microsoft News and the Xbox Microsoft Store apps.
- Add a VPN connection to the corporate network.

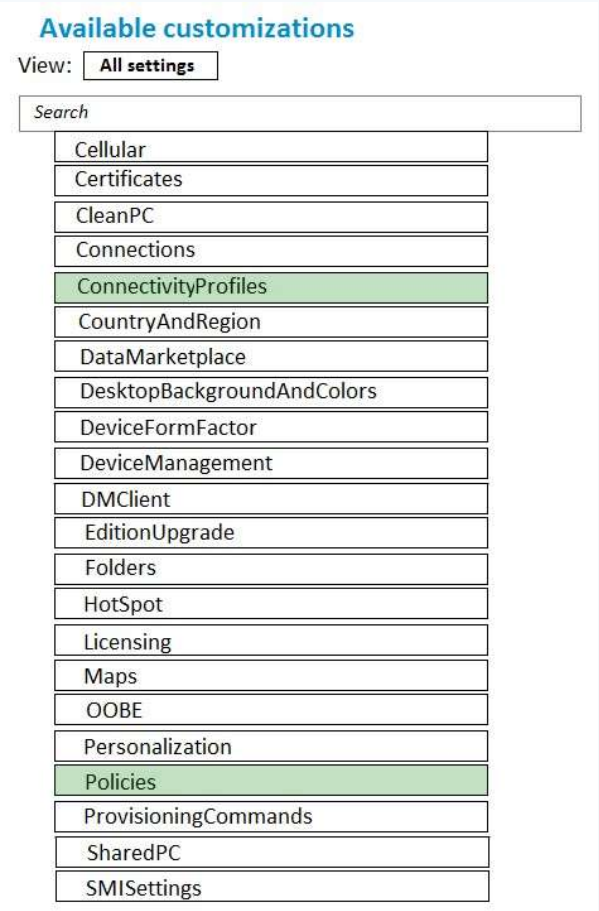
Which two customizations should you configure? To answer, select the appropriate customizations in the answer area.

NOTE: Each correct selection is worth one point.

Hot Area:



Correct Answer:



Box 1: ConnectivityProfiles -

Add a VPN connection to the corporate network.

ConnectivityProfiles is used to configure profiles that a user will connect with, such as an email account or VPN profile.

Box 2: Policies -

Remove the Microsoft News and the Xbox Microsoft Store apps.

ApplicationManagement policies, such as ApplicationManagement/DisableStoreOriginatedApps, are included in policies on Windows 10.

Reference:

https://docs.microsoft.com/en-us/windows/configuration/wcd/wcd-connectivityprofiles https://docs.microsoft.com/en-us/windows/client-management/mdm/policy-configuration-service-provider#applicationmanagement-applicationrestrictions https://docs.microsoft.com/en-us/windows/configuration/wcd/wcd-policies

josekast Highly Voted 2 years, 3 months ago

- Remove the Microsoft News and the Xbox Microsoft Store apps.
UniversalAppUninstall
- Add a VPN connection to the corporate network.
ConnectivityProfiles

Delete the previous message.

upvoted 31 times

nolancl Highly Voted 3 years ago

Missing half the available customizations. UniversalAppUninstall should be an options and is the correct method to Remove the desired apps.

upvoted 19 times

LauLauLauw 2 years, 6 months ago

You are correct, checked it in a lab environment

upvoted 7 times

silver_bullet666 Most Recent 2 months, 4 weeks ago

It seems that Policy may be able to 'block/disallow' the Microsoft News and the Xbox Microsoft Store apps but it can't 'remove' them I don't think; policy > ApplicationManagement > ApplicationRestrictions

"An XML blob that specifies app restrictions, such as an allow list, disallow list, etc."
Although the documentation is a bit complicated, talks about needing an ADMX file
https://docs.microsoft.com/en-us/windows/configuration/wcd/wcd-policies
https://docs.microsoft.com/en-us/windows/client-management/mdm/policy-configuration-service-provider#applicationmanagement-applicationrestrictions

So in reality we would want to use the UniversalAppUninstall...

upvoted 1 times

Goofer 10 months, 3 weeks ago

See Question #23 Topic 1
https://www.examtopics.com/exams/microsoft/md-101/view/3/
Same question, Answer B
ConnectivityProfiles and Policies

upvoted 6 times

Perycles 1 year, 3 months ago

just checked under ICD : answer are : ConnectivityProfile and UniversaleAppUninstall

upvoted 2 times

Perycles 1 year, 3 months ago

BUT as "UniversaleAppUninstall" is not display , we can use "ProvisioningCommands/DeviceContext/CommandLine" and type a powershell comand to uninstall desired APPs.

upvoted 6 times

Merma 1 year, 5 months ago

"VPN
In Available customizations, select VPNSetting, enter a friendly name for the account, and then click Add.
In Available customizations, select the name that you just created. The following table describes the settings you can configure. Settings in bold are required."
https://docs.microsoft.com/en-us/windows/configuration/wcd/wcd-connectivityprofiles
"Use UniversalAppUninstall settings to uninstall or remove Windows apps."
https://docs.microsoft.com/en-us/windows/configuration/wcd/wcd-UniversalAppUninstall

upvoted 1 times

cubalondon 1 year, 7 months ago

here is the solution
https://techcommunity.microsoft.com/t5/windows-blog-archive/yet-another-way-to-clean-up-in-box-apps/ba-p/706389

upvoted 2 times

josekast 2 years, 3 months ago

- Remove the Microsoft News and the Xbox Microsoft Store apps.
ConnectivityProfiles
- Add a VPN connection to the corporate network.
UniversalAppUninstall

upvoted 2 times

Question #22 *Topic 3*

You have an Azure Active Directory (Azure AD) tenant named contoso.com.
You create a terms of use (ToU) named Terms1 in contoso.com.
You are creating a conditional access policy named Policy1 to assign a cloud app named App1 to the users in contoso.com.
You need to configure Policy1 to require the users to accept Terms1.
What should you configure in Policy1?

A. Grant in the Access controls section

B. Conditions in the Assignments section

C. Cloud apps or actions in the Assignments section

D. Session in the Access controls section

Correct Answer: *A*
Before accessing certain cloud apps in your environment, you might want to get consent from users in form of accepting your terms of use (ToU). Azure Active
Directory (Azure AD) Conditional Access provides you with:
A simple method to configure ToU
The option to require accepting your terms of use through a Conditional Access policy
Reference:
https://docs.microsoft.com/en-us/azure/active-directory/conditional-access/require-tou

VCE_player Highly Voted 1 year, 9 months ago
Answer A is correct. I just configured this in the MD-101 lab.
Though, the "Terms Of Use" itself should be setup first before this option becomes available in the "grant" part of the policy. But that is not part of the question..
upvoted 20 times

[Removed] Most Recent 1 year, 3 months ago
Conditional Access
-Access Control
-Require app protection policy
-ToU
upvoted 2 times

Perycles 1 year, 3 months ago
A is correct.
upvoted 3 times

bertik 1 year, 4 months ago
Definitely A.

https://docs.microsoft.com/en-us/azure/active-directory/conditional-access/require-tou#create-your-conditional-access-policy
upvoted 3 times

MikeMatt2020 1 year, 4 months ago
Answer is A
"If your organization has created terms of use, additional options may be visible under grant controls. These options allow administrators to require acknowledgment of terms of use as a condition of accessing the resources protected by the policy"

https://docs.microsoft.com/en-us/azure/active-directory/conditional-access/concept-conditional-access-grant#require-approved-client-app
upvoted 3 times

Merma 1 year, 5 months ago
I believe B. Conditions in the Assignments section is the correct answer here.
"Within a Conditional Access policy, an administrator can make use of signals from conditions like risk, device platform, or location to enhance their policy decisions."
A. Grant in the Access controls section - "Within a Conditional Access policy, an administrator can make use of access controls to either grant or block access to resources. Block takes into account any assignments and prevents access based on the Conditional Access policy configuration. Administrators can choose to enforce one or more controls when granting access." Such as MFA.
https://docs.microsoft.com/en-us/azure/active-directory/conditional-access/concept-conditional-access-Conditions
https://docs.microsoft.com/en-us/azure/active-directory/conditional-access/concept-conditional-access-grant
Other thoughts?
upvoted 1 times

Merma 1 year, 4 months ago
How to deploy Terms of Use in Azure Active Directory - https://www.youtube.com/watch?v=N4vgqHO2tgY
upvoted 1 times

marz 1 year, 7 months ago
https://docs.microsoft.com/en-us/azure/active-directory/conditional-access/concept-conditional-access-grant#terms-of-use
upvoted 1 times

Anthony_2770 1 year, 8 months ago
Answer is either A or B.
What should you do first

It is not uncommon for the 2nd step to be listed as an option, to really see if you know what you are doing. Option B initially could be a candidate for this aspect.
This question is referring to the manual registration of devices to autopilot.

NOT C
If B,C,D needs to be considered then we need a CSV file not a XML file.

NOT D
Refers to win7/8.1 I believe

upvoted 1 times

Anthony_2770 1 year, 8 months ago

Additionally:
Manually register devices with Windows Autopilot\
https://docs.microsoft.com/en-us/mem/autopilot/add-devices
Windows Autopilot device registration can be done within your organization by manually collecting the hardware identity of devices (hardware hashes) and uploading this information in a comma-separated-value (CSV) file. Capturing the hardware hash for manual registration requires booting the device into Windows 10. Device owners can only register their devices with a hardware hash. Other methods (PKID, tuple) are available through OEMs or CSP partners.
Website talks about sysprep if the devices have already been connected to the internet.
Phoenix computers are to be used at home.
Answer is either A or B.
Need more discussion.....

upvoted 1 times

HOTSPOT -

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

Name	Platform	Group
Device1	Windows 10	Group1, Group2
Device2	Android	Group2
Device3	iOS	Group2, Group3

You create device configuration profiles in Intune as shown in the following table.

Name	Platform	Minimum password length
Profile1	Windows 10 and later	4
Profile2	Android	5
Profile3	iOS	6
Profile4	Android	7
Profile5	iOS	8

You assign the device configuration profiles to groups as shown in the following table.

Group	Profile
Group1	Profile3
Group2	Profile1, Profile2, Profile4
Group3	Profile3, Profile5

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 must have a minimum password length of seven characters.	○	○
Device2 must have a minimum password length of seven characters.	○	○
Device3 must have a minimum password length of six characters.	○	○

Correct Answer:

Answer Area

Statements	Yes	No
Device1 must have a minimum password length of seven characters.	○	●
Device2 must have a minimum password length of seven characters.	●	○
Device3 must have a minimum password length of six characters.	○	●

Box 1: No -

Windows 10 Device1 belongs to Group1 and Group2. Group 1 has Profile3. Group2 has Profile1, Profile2 and Profile 4. Profile1, for the correct platform, is the only that applies, with Minimum password length set to 4.

Box 2: Yes -

Android Device2 belongs to Group2. Group2 has Profile1, Profile2 and Profile 4, but only Profile2 applies to Android. Profile2 has a Minimum password length set to 5.

Box 3: No -

iOS Device3 belongs to Group2 and Group3. Group2 has Profile1, Profile2 and Profile 4. Group3 has Profile3 and Profile5. Only Profile3 and Profile5 applies to iOS. Profile5 is the most restrictive with Minimum password length set to 8.

Note: If a compliance policy evaluates against the same setting in another compliance policy, then the most restrictive compliance policy setting applies.

Reference:

https://docs.microsoft.com/en-us/mem/intune/configuration/device-profile-troubleshoot

Perycles Highly Voted 1 year, 3 months ago

NO,YES,NO : be carrefull , most restrectived so bigger password lenght applied.

upvoted 35 times

mikl 9 months, 1 week ago

I agree.

upvoted 2 times

RodrigoT 5 months ago

Agreed. Answer provided is correct.
upvoted 3 times

Merma Highly Voted 1 year, 4 months ago
No - Device1 (Windows) is in Group1 & Group2, applies to Profiles 1-4, only Profile1 is Windows with a minimum password length of 4.
Yes - Device2 (Android) is in Group2, applies to Profile 1,2 & 4, Profile 2 & 4 are Android with a minimum password length of 7 for Profile4.
No - Device 3 (iOS) is in Group2 & Group3, applies to Profile 1-5, only Profile3 & Profile5 are iOS with a minimum password length of 8 for Profile5.
upvoted 15 times

RodrigoT 5 months, 4 weeks ago
Good explanation, the bigger password applies because is the more restrictive.
upvoted 4 times

gotrekk Most Recent 1 month, 2 weeks ago
No yes no
upvoted 2 times

TonySuccess 3 days, 9 hours ago
Agreed
upvoted 1 times

Nome2025 1 year, 3 months ago
1 - No
2 - Yes
3 - Yes
device 3 got 8, and they are saying minimum is 6 and the minimum here is 8, so i think it's a YES
upvoted 1 times

Nome2025 1 year, 3 months ago
they saying must have 6, so i think its a NO then.
upvoted 2 times

Tomtom11 1 year, 4 months ago
When two profi le settings are applied to the same device, the most restrictive value will be applied. Any settings that are the same in each policy are applied as confi gured.
upvoted 3 times

George_83 1 year, 4 months ago
The correct answer is No, Yes, Yes
upvoted 1 times

MikeMatt2020 1 year, 4 months ago
No. The given answer (No, Yes, No) is correct.

I think you're missing that Device 3 is a member of Group2 and Group3
This means that it is receiving Policy 1,2,3,4,5
The only iOS policies are 3 and 5 (most restrictive wins so it is 8 characters)
upvoted 6 times

mikl 9 months, 1 week ago
True !
upvoted 1 times

Technik 1 year, 5 months ago
Device 3 is part of group 2 and 3 (profile 3 and 5 applied). Length of profile 5 is 8.

Given answers are correct
upvoted 4 times

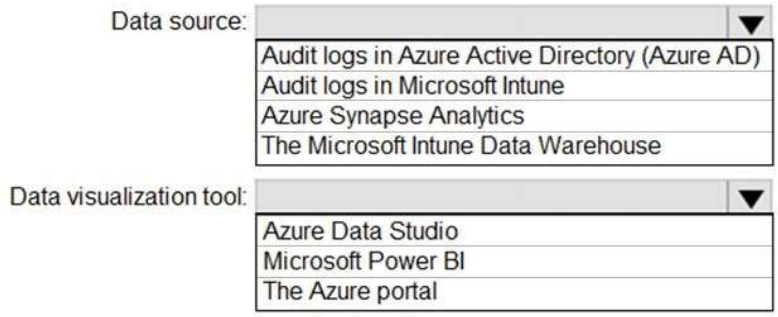
Testtest123 1 year, 5 months ago
This should be:
1 - No
2 - Yes
3 - Yes
Please can some one explain why device 3 is not Yes in the giving answer.
upvoted 1 times

1morenickname 1 year, 5 months ago
For the same reason Device 2 is yes. Multiple profiles apply to it, but the most restrictive is 8 characters.
upvoted 7 times

DavyB 1 year, 5 months ago
Non of the profiles match the OS
upvoted 1 times

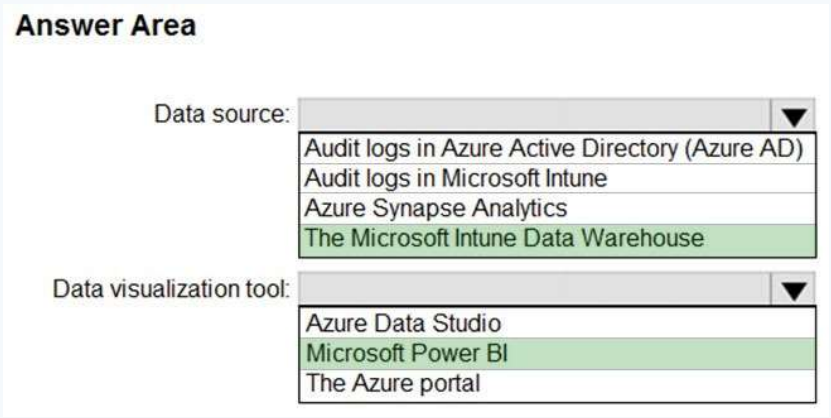
HOTSPOT -
You use Microsoft Endpoint Manager to manage Windows 10 devices.
You are designing a reporting solution that will provide reports on the following:
⇨ Compliance policy trends
⇨ Trends in device and user enrolment
⇨ App and operating system version breakdowns of mobile devices
You need to recommend a data source and a data visualization tool for the design.
What should you recommend? To answer, select the appropriate options in the answer area.
NOTE: Each correct selection is worth one point.
Hot Area:

Answer Area



Correct Answer:

Answer Area



Box 1: The Microsoft Intune Data Warehouse
Use the Intune Data Warehouse to build reports that provide insight into your enterprise mobile environment. For example, some of the reports include:
Trend of users enrolling in Intune so you can optimize your license purchases
App and OS versions breakdown so you can review that status of mobile devices
Enrollment and device compliance trends so you can smoothly roll out policy updates.

Box 2: Microsoft Power BI -
You can use the Power BI Compliance app to load interactive, dynamically generated reports for your Intune tenant. Additionally, you can load your tenant data in
Power BI using the OData link. Intune provides connection settings to your tenant so that you can view the following sample reports and charts related to:

Devices -

Enrollment -

App protection policy -

Compliance policy -

Device configuration profiles -

Software updates -

Device inventory logs -

Reference:
https://docs.microsoft.com/en-us/mem/intune/developer/reports-nav-create-intune-reports https://docs.microsoft.com/en-us/mem/intune/developer/reports-proc-get-a-link-powerbi

MikeMatt2020 Highly Voted 1 year, 4 months ago

ANSWER:
Data Source = The Microsoft Intune Data Warehouse
Data Visualization Tool = Microsoft Power BI

"Use the Intune Data Warehouse to build reports that provide insight into your enterprise mobile environment. For example, some of the reports include:

Trend of users enrolling in Intune so you can optimize your license purchases
App and OS versions breakdown so you can review that status of mobile devices
Enrollment and device compliance trends so you can smoothly roll out policy updates"
https://docs.microsoft.com/en-us/mem/intune/developer/reports-nav-create-intune-reports

upvoted 12 times

Perycles Highly Voted 1 year, 3 months ago

answer are correct.

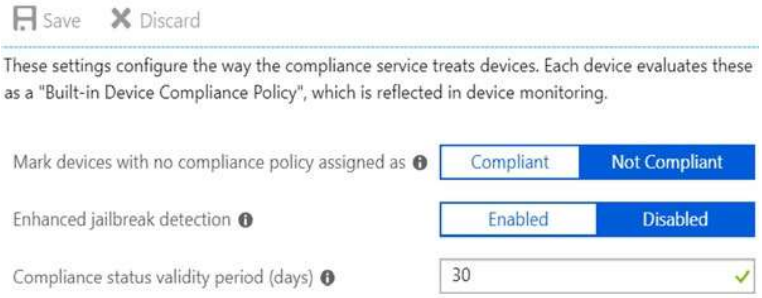
upvoted 6 times

HOTSPOT -

In Microsoft Intune, you have the device compliance policies shown in the following table.

Name	Type	Encryption	Windows Defender antimalware	Mark device as not compliant	Assigned to
Policy1	Windows 8	Require	*Not applicable*	5 days	Group1
Policy2	Windows 10	Not configured	Require	7 days	Group2
Policy3	Windows 10	Required	Require	10 days	Group2

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



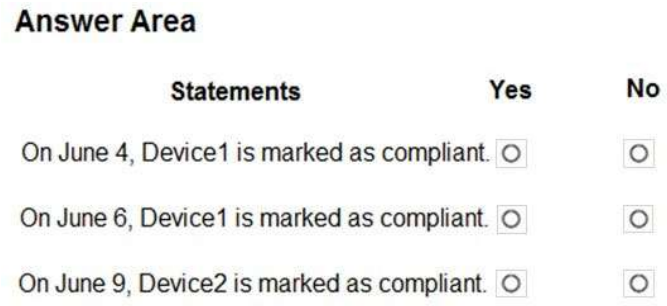
On June 1, you enroll Windows 10 devices in Intune as shown in the following table.

Name	Use BitLocker Drive Encryption (BitLocker)	Windows Defender	Member of
Device1	No	Enabled	Group1
Device2	No	Enabled	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:



Correct Answer:

Box 1: No -

Policy1 requires encryption, but on June 4 Device1 is configured with No Drive Encryption, so it is not compliant.

Box 2: No -

Policy1 requires encryption, but on June 6 Device1 is configured with No Drive Encryption, so it is not compliant.

Box 3: Yes -

Both Policy2 and Policy3 applies to Device2. Policy3, which is the most restrictive applies, which result in Mark device as not compliant = 10 days.

Note: If you have deployed multiple compliance policies, Intune uses the most restrictive of these policies.

Reference:

https://docs.microsoft.com/en-us/mem/intune/protect/actions-for-noncompliance https://docs.microsoft.com/en-us/mem/intune/protect/compliance-policy-monitor#how-intune-resolves-policy-conflicts

MikeMatt2020 Highly Voted 1 year, 4 months ago

I believe the answer is NO, NO, NO. That said, we need to understand some key settings:

1) *Mark devices as not compliant*, which is the "Schedule (days after noncompliance)" setting under the "Actions for Non-Compliance" tab when creating a Compliance Policy. Setting this to 5 days will put a non-compliant device in a "In-Grace Period" state. This does NOT make the device compliant. A device that is "In-Grace Period" is a level 4 severity status. https://docs.microsoft.com/en-us/mem/intune/protect/create-compliance-policy

2) *Compliance status validity period (days)*
This sets the amount of days that a device MUST report its compliance status. "Specify a period in which devices must successfully report on all their received compliance policies. If a device fails to report its compliance status for a policy before the validity period expires, the device is treated as noncompliant"

upvoted 24 times

LordCaine 1 year ago

Yes I agree with this, device 1 has no policy assigned (windows 8 policy is applied but a windows 10 device is enrolled) and it is specifically mentioned in the image that devices without a compliance policy are listed as non compliant.

Device 2 has a policy but is not compliant and enters a grace period for 7 days. So whatever action is set to non-compliant devices doesn't matter in this question, the device is marked not compliant.

upvoted 2 times

LordCaine 1 year ago

I want to edit this. I think the answer is No, No, Yes.
Device 1 is Windows 10 - and policy 1 is for Windows 8. Default compliance for devices without a policy is not compliant so first 2 questions are NO.
Then the third device has 2 policies, the first one is compliant and the second policy is not compliant but the device is not marked as non-compliant due to the fact that mark device as non-compliant is set to 10 days. This means that the machine will be compliant until june 10th.

Source:
Mark device non-compliant: By default, this action is set for each compliance policy and has a schedule of zero (0) days, marking devices as noncompliant immediately.

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

This action is supported on all platforms supported by Intune.
https://docs.microsoft.com/en-us/mem/intune/protect/actions-for-noncompliance

upvoted 16 times

john909 11 months ago

Thank you!

Indeed it says:

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

upvoted 2 times

pogap64757 7 months, 3 weeks ago

From MikeMatt2020's link:

"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."

So policy 2 and 3 will we applied. even though policy 2 is giving it compliant status, policy 3 is overriding it as "ingrace" until policy 3 eventually marks it outright non compliant

upvoted 1 times

Gonch Highly Voted 1 year, 4 months ago

I think it is No, No, Yes:

1 No - Device 1 does not have a Compliance Policy (assigned a Windows 8 policy) so will be marked as non-compliant, as per Compliance Policy Settings (Mark devices with no compliance policy assigned as: Not compliant)
2 No - As above
3 Yes - Device 2 will have Policy 3 applied rather than Policy 2 (most secure as it requires encryption as well as AV - https://docs.microsoft.com/en-us/mem/intune/protect/compliance-policy-monitor#how-intune-resolves-policy-conflicts). On June 9th this will still be seen as compliant as within the 10 day compliance window for Policy 3.

upvoted 8 times

FrancisLai 1 year, 4 months ago

I agreed 1 & 2 however for 3 I don't agree, as you said most secure and stricter rules applied then it is with Policy 3, however Policy 3 required encryption but Device 2 not encrypted.

upvoted 2 times

RodrigoT 5 months, 4 weeks ago

Policy3 will mark Device2 as non-compliant only on the 10th day. On day 9 Device2 is still compliant with Policy2. So, N N Y.

upvoted 5 times

raduM Most Recent 3 weeks, 5 days ago

no no no. it will be in grace period not compliant

upvoted 1 times

raduM 1 month ago

the correct answer is no, no,no. the devices will be in grace period and not compliant.just tested this fyi. :)

upvoted 1 times

gotrekk 1 month, 2 weeks ago

NNN.. i agree with others

upvoted 1 times

CARO54 9 months ago

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

Device 1 is Windows 10 - and policy 1 is for Windows 8. Default compliance for devices without a policy is not compliant so first 2 questions are NO COMPLIANT

Device 2 is no compliant but are in grace preriod so status is IN GRACE PERIOD

upvoted 1 times

Goofer 10 months, 3 weeks ago

N - Device1 = Group1 = Policy1 = Device requires Encryption --> Device1: No Drive Encryption = Not Compliant
N - Device1 = Group1 = Policy1 = Device requires Encryption --> Device1: No Drive Encryption = Not Compliant
N - Device2 = Group2 = Policy2 and 3 (policy conflict) = Device requires Encryption --> Device2: No Drive Encryption = Not Compliant
- If you have deployed multiple compliance policies, Intune uses the most secure of these policies.
- https://docs.microsoft.com/en-us/mem/intune/protect/compliance-policy-monitor#how-intune-resolves-policy-conflicts

upvoted 2 times

RodrigoT 6 months, 1 week ago

Policy1 is just for Windows 8 and Device1 is a Windows 10. So, Policy1 doesn't apply.

upvoted 1 times

bensrayan 2 weeks, 3 days ago

Policy1 is for Windows 8 AND LATER !

upvoted 1 times

Perycles 1 year, 3 months ago

on june 4 : device 1: no policy applies (groupe 1 only affect win8): so marked as non compliant because of "Markdevice with no compliance policy assigned" = NOT COMPLIANT

on june 6: : device 1: no policy applies (groupe 1 only affect win8): so marked as non compliant because of "Markdevice with no compliance policy assigned" = NOT COMPLIANT

on june 9 :Device 2: effected by 2 polycies (policicy 2 and 3) - when we have a confit,the most secure applies , so policy 3 applies ; "Mark device as not compliant = 10 days" understand " 10 Days before to be market as NON compliance"; That lets time for user to fix his problem (here for example, he has 10 days to activate is TPM, after that, his device will be non compliant). COMPLIANT

upvoted 5 times

Tomtom11 1 year, 3 months ago

Yes Default has 30 day to become compliant
Yes Default has 30 day to become compliant
No Policy from group 2 Excecced time limt

No

upvoted 2 times

S4L4LMF 1 year, 3 months ago

This seems the correct answer. Its compliant because its windows 10 so it doesnt fall under windows 8 policy. Default time is 30 days. The last one is not compliant because the stricter rule applies. THe stricter rule is 7 days, not 10 days, so device 2 will not be compliant on 9th of june.

upvoted 2 times

S4L4LMF 1 year, 3 months ago

I think im changing this to NO - YES - NO. Why? Because even if the device isnt Win 8, it still has a policy asigned. It just isnt compliant to it (because its Win10, not W8), so it will be marked as non compliant in 5 days.

upvoted 1 times

S4L4LMF 1 year, 3 months ago

Okay. i mean the reverse -> Yes, NO, Yes. 1. is yes because 5 days arent done. 2. is No because those 5 days are over and the device isnt Win8 so it isnt complying to the policy. And again Yes because device 2 complies to policy 2 but not 3, which marks non compliant in 10 days, so on the 8th day it still complies.

upvoted 1 times

Tomtom11 1 year, 4 months ago

Compliance status validity period (days)

Specify a period in which devices must successfully report on all their received compliance policies. If a device fails to report its compliance status for a policy before the validity period expires, the device is treated as noncompliant.

upvoted 3 times

George_83 1 year, 4 months ago

No, No, Yes:
Policy1 require encryption and Device1 doesn't have BitLocker therefore wont be marked as compliant on the first two question
Device 2 also doesn't have BitLocker but because policy2 is set to not configured will mark it as compliance

upvoted 5 times

MikeMatt2020 1 year, 4 months ago

Right...but Device2 receives policy 2 *AND* 3. So Device2 will not be marked as compliant for Policy3. A 10-day grace period is set but this does NOT mark the device as compliant. This puts the device in a level 4 severity status (next severity would be non-compliant)

Also, it's irrelevant because even if Device2 was compliant with Policy2, it would still be marked generally as "non-compliant" because of its failure to comply with Policy3

upvoted 3 times

Alexbz 1 year, 4 months ago

No
No
Yes

upvoted 4 times

RodrigoT 6 months, 1 week ago

I agree.
Endpoint > Devices > Compliance policies > Mark devices with no compliance policy assigned as NOT COMPLIANT
Device1 is Win10 and Group1 - Policy1 (for Win8 so, doesn't apply). So, no policy assigned: NOT COMPLIANT by default, end of story. NO for the first and second answers.
Device2 is Win10 and Group2 - Policy2 requires Win Defender that is enabled: COMPLIANT until day 9. YES for the third answer.
Policy3 requires Encryption but is disabled: NOT COMPLIANT just from day 10.

upvoted 2 times

Test99 1 year, 5 months ago

Should be NO NO NO, first is no as it's windows 10 so no policy applied and then device is marked as non compliant as per https://docs.microsoft.com/en-us/mem/intune/protect/device-compliance-get-started

Last is no as policy is applied for 10 as can see

upvoted 3 times

jeroenski 1 year, 4 months ago

Agreed, answer should be NO, NO, NO. A Grace Period does not make it compliant. Actions have to be performed to make it compliant

"Mark device non-compliant: By default, this action is set for each compliance policy and has a schedule of zero (0) days, marking devices as noncompliant immediately.
When you change the default schedule, you provide a grace period in which a user can remediate issues or become compliant without being marked as non-compliant."

upvoted 4 times

RodrigoT 6 months, 1 week ago

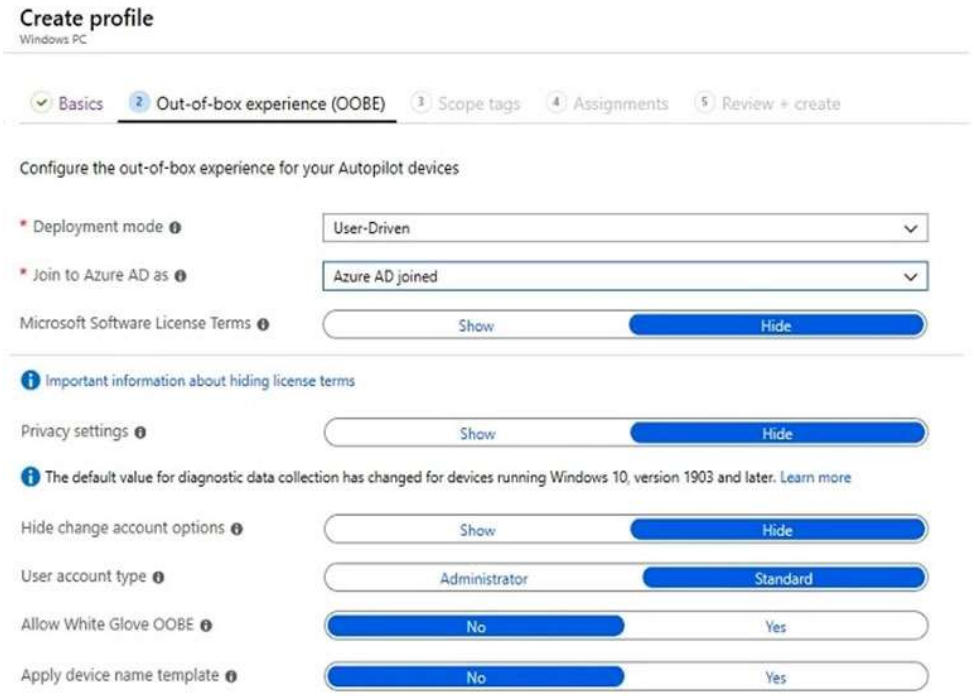
But Device2 is compliant because of Policy2. It won't be compliant just on the 10th day. On day 9 it's still compliant. So, NO NO YES.

upvoted 2 times

HOTSPOT -

You have a Microsoft Intune subscription.

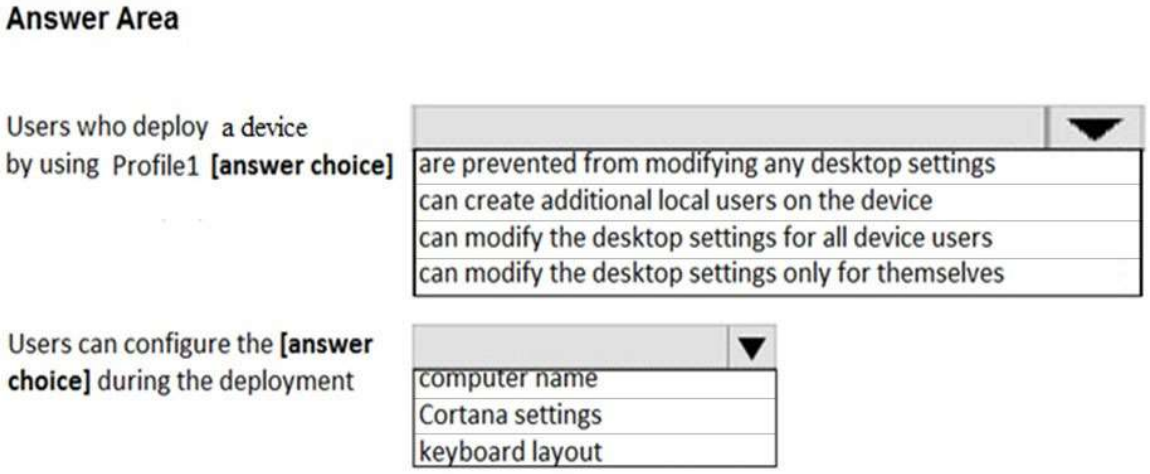
You create the Windows Autopilot deployment profile-shown in the following exhibit.



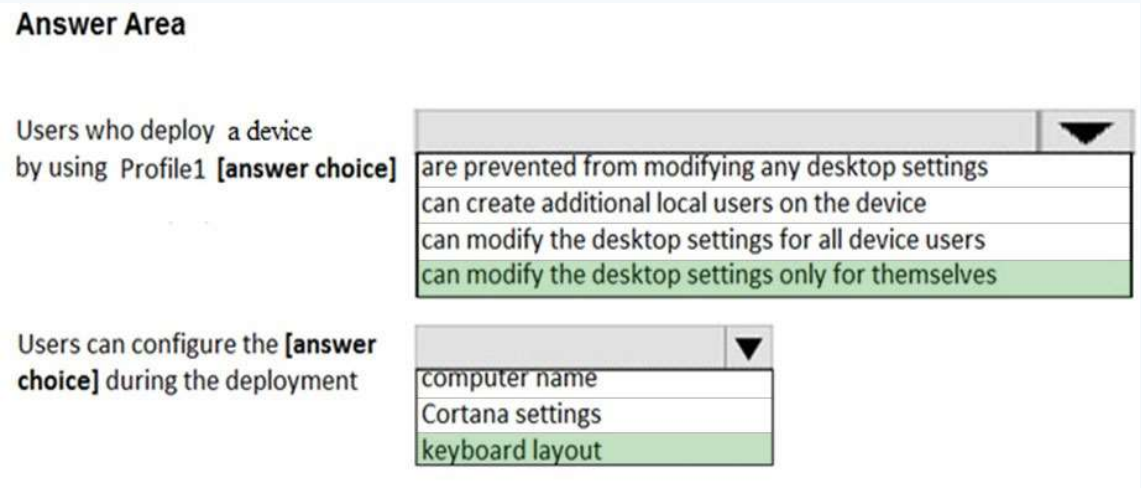
Use the drop-down menus to select the answer choice that completes each statement based on the information presented in the graphic.

NOTE: Each correct selection is worth one point.

Hot Area:



Correct Answer:



Reference:

https://docs.microsoft.com/en-us/windows/deployment/windows-autopilot/user-driven

MikeMatt2020 Highly Voted 1 year, 4 months ago

Answer given is correct

upvoted 6 times

RosalindFranklin Highly Voted 11 months, 1 week ago

That's almost the same question as in Topic 2, question 53. Except, you don't have the options "Language" & "Automatically configure keyboard". Anybody know why that is?

upvoted 6 times

ercluff 8 months, 2 weeks ago

Users who deploy a device by using Profile1: Can modify the desktop settings only for themselves Users can configure the : COMPUTER NAME during the deployment, (apply device name template = NO & Language and keyboard options are not represented.) References: https://docs.microsoft.com/en-us/mem/autopilot/profiles

upvoted 3 times

camino 7 months, 2 weeks ago

if no device name template is applied windows takes the minit-name, users cannot change the device name during autopilot.
Cortana is not an option in AP
-> must be keyboard settings, but they are simply not shown in the exhibit

upvoted 2 times

RodrigoT 5 months, 4 weeks ago

Second part wrong, check my answer above, and the demo video.

upvoted 2 times

RodrigoT 5 months, 4 weeks ago

Actually is the exact same Question #53 on Page 10, but here they provided the correct answers: change desktop settings only for themselves, keyboard layout.
https://www.examtopics.com/exams/microsoft/md-101/view/10/

And here I have the proof that you will able to change the keyboard layout:
In the link below there is a LAB with the exact same scenario. There is also a demo video that shows and says: "You should see the region selection screen, the keyboard selection screen, and the second keyboard selection screen".
https://docs.microsoft.com/en-us/windows/deployment/windows-autopilot/demonstrate-deployment-on-vm

upvoted 5 times

raduM Most Recent 1 month ago

correct

upvoted 1 times

gotrekk 1 month, 2 weeks ago

Agree with given answers.

upvoted 1 times

raduM 1 month, 2 weeks ago

during the deployment you have the option to modify the language. anyway it is the only viable solrution as computer name and cortana cannot be modified during the deployment

upvoted 1 times

Y2 6 months, 3 weeks ago

is the answer "Can modify the desktop settings only for themselves" because the keyboard option isn't available?

upvoted 1 times

RodrigoT 6 months, 1 week ago

No, it's because he is a standard user, not an administrator. The option of changing the keyboard layout will be present during deploy.

upvoted 2 times

Perycles 1 year, 3 months ago

all is correct.

upvoted 5 times

Question #27 *Topic 3*

You need to assign the same deployment profile to all the computers that are configured by using Windows Autopilot.
Which two actions should you perform? Each correct answer presents part of the solution.
NOTE: Each correct selection is worth one point.

A. Join the computers to Microsoft Azure Active Directory (Azure AD)

B. Assign a Windows Autopilot deployment profile to a group

C. Join the computers to an on-premises Active Directory domain

D. Create a Microsoft Azure Active Directory (Azure AD) group that has dynamic membership rules and uses the operatingSystem tag

E. Create a Group Policy object (GPO) that is linked to a domain

F. Create a Microsoft Azure Active Directory (Azure AD) group that has dynamic membership rules and uses the ZTDID tag

Correct Answer: *BF*
B: It is possibly to automatically assign a Windows AutoPilot deployment profile to Windows AutoPilot devices. That makes it a lot easier for administrators, as this prevents the administrators from potentially forgetting to assign the deployment profile to newly imported devices.
F: ZTDId: A unique value assigned to all imported Windows AutoPilot devices.
Reference:
https://www.petervanderwoude.nl/post/automatically-assign-windows-autopilot-deployment-profile-to-windows-autopilot-devices/

lucidgreen Highly Voted 1 year, 7 months ago
To create a group that includes all of your Autopilot devices, enter: (device.devicePhysicalIDs -any (_ -contains "[ZTDId]")).
https://docs.microsoft.com/en-us/mem/autopilot/enrollment-autopilot
upvoted 11 times

Moorebid 1 year, 4 months ago
ZTD stands for "Zero Touch Deployment" for anyone wondering.
upvoted 30 times

MikeMatt2020 Highly Voted 1 year, 4 months ago
Answer given is correct
upvoted 9 times

gotrekk Most Recent 1 month, 2 weeks ago
Selected Answer: BF
Correct
upvoted 2 times

raduM 1 month, 2 weeks ago
correct
upvoted 2 times

silver_bullet666 2 months, 4 weeks ago
B. Assign a Windows Autopilot deployment profile to a group
&
F. Create a Microsoft Azure Active Directory (Azure AD) group that has dynamic membership rules and uses the ZTDID tag
upvoted 1 times

Perycles 1 year, 3 months ago
correct.
upvoted 8 times

Question #28 *Topic 3*

Your company has a Microsoft Azure Active Directory (Azure AD) tenant named contoso.com. All users have computers that run Windows 10. The computers are joined to Azure AD and managed by using Microsoft Intune.
You need to ensure that you can centrally monitor the computers by using Windows Analytics.
What should you create in Intune?

A. a device configuration profile

B. a conditional access policy

C. a device compliance policy

D. an update policy

Correct Answer: *A*
To configure the setting go to Device configuration â€" Profiles > Device Restriction â€" Properties > Device restrictions > Reporting and Telemetry.

Reference:
https://www.scconfigmgr.com/2019/03/27/windows-analytics-onboarding-with-intune/

Question #29 *Topic 3*

HOTSPOT -

You have 200 computers that run Windows 10. The computers are joined to Microsoft Azure Active Directory (Azure AD) and enrolled in Microsoft Intune.

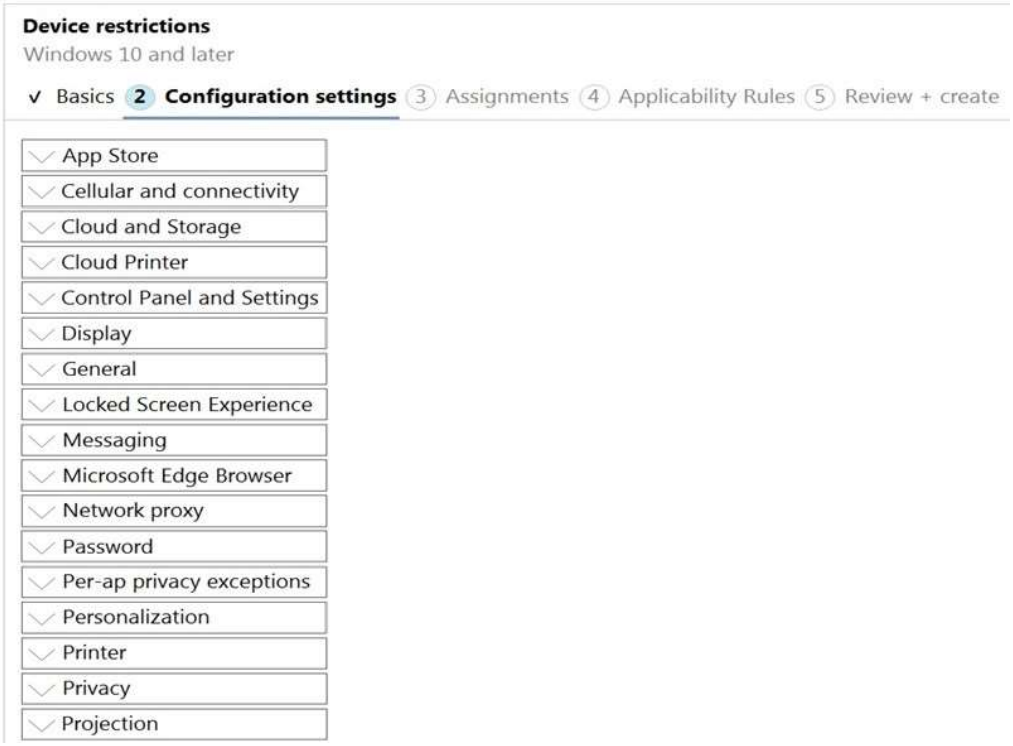
You need to set a custom image as the wallpaper and sign-in screen.

Which two settings should you configure in Device restrictions? To answer, select the appropriate settings in the answer area.

NOTE: Each correct selection is worth one point.

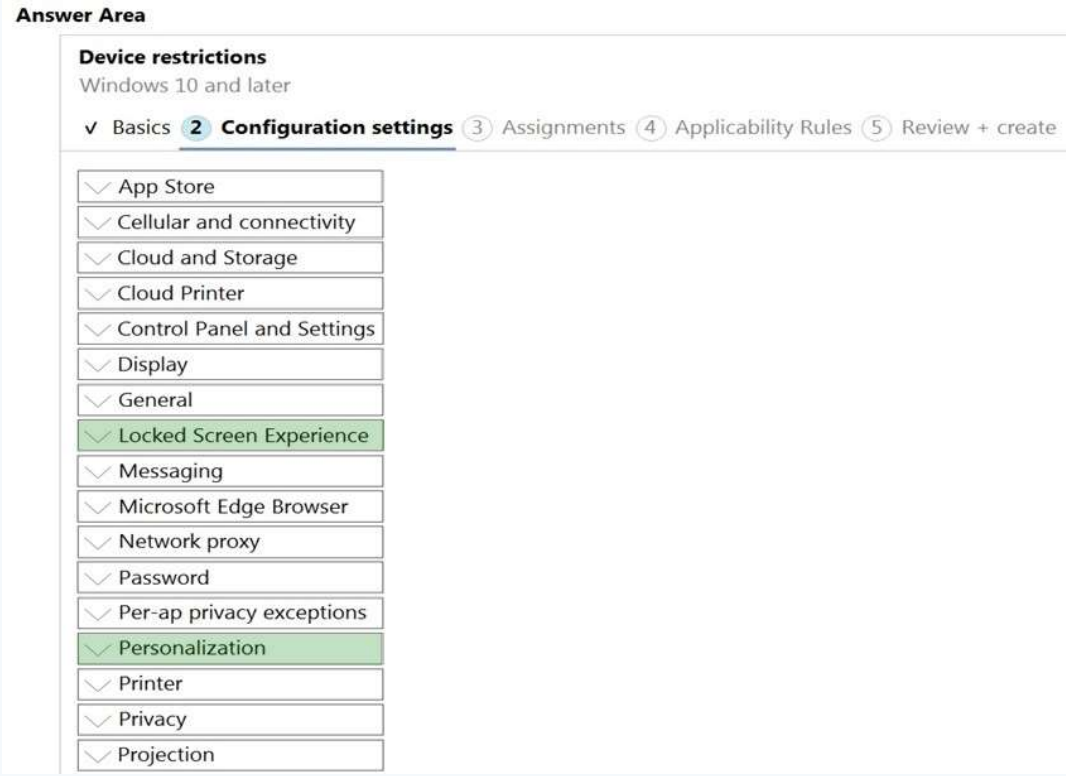
Hot Area:

Answer Area



Correct Answer:

Answer Area



Sign-in screen, or Locked screen, image is set under Locked screen experience

Wallpaper image, or Desktop background picture, URL is set under Personalization.

Reference:

https://docs.microsoft.com/en-us/intune/device-restrictions-windows-10

Perycles Highly Voted 1 year, 3 months ago

lock screen Experience > "locked screen picture url" option.
Personnalization > "Desktop background picture url" option.
so answers are correct.

upvoted 15 times

john909 11 months ago

Yes, correct, found these settings under Configuration Profiles > Templates > Device Restrictions

upvoted 3 times

raduM Most Recent 1 month, 2 weeks ago

correct

upvoted 1 times

JCkD4Ni3L 6 months ago

Important to note that this feature is only good under Windows 10 ENTEPRISE, this will NOT work on Windows 10 Pro or Business.

upvoted 3 times

mikl 9 months, 1 week ago

I agree!

upvoted 3 times

Question #30 *Topic 3*

Your company has a Microsoft Azure Active Directory (Azure AD) tenant named contoso.com. All users have computers that run Windows 10. The computers are joined to Azure AD and managed by using Microsoft Intune.
You need to ensure that you can centrally monitor the computers by using the Update Compliance solution.
What should you create in Intune?

A. a device configuration profile

B. a conditional access policy

C. a device compliance policy

D. an update policy

Correct Answer: *A*
With CommercialID in hand, you're ready to go to the MEM admin center portal and start putting your keyboard to work making a custom OMA-URI device configuration profile to enable Update Compliance settings. You're going to need a total of four custom policy settings to configure devices to play nice with

Update Compliance -
Reference:
https://www.jeffgilb.com/update-compliance-with-intune/

RodrigoT 5 months ago

Selected Answer: A

Correct. And here is how you do it:
https://docs.microsoft.com/en-us/mem/intune/protect/windows-update-compliance-reports#configure-data-collection

upvoted 2 times

MitchF 2 months, 1 week ago

This source could also help:
https://docs.microsoft.com/en-us/windows/deployment/update/update-compliance-get-started

upvoted 1 times

Perycles 1 year, 3 months ago

correct : to use Update Compliane (iclude in Desktop analytics solution), Commercial ID and telemetry must be enable. Device configuration (cith custom OMA-URI settings) allow to do that. https://docs.microsoft.com/en-us/windows/deployment/update/update-compliance-configuration-mem

upvoted 3 times

MikeMatt2020 1 year, 4 months ago

Answer is correct

upvoted 1 times

Wilf32 1 year, 4 months ago

After reading the provided article (august 2020) and the following links (last updated today) from offcial Microsoft. I agree with the answer given, but i suspect the actual question / answer will differ in the exam.

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

https://docs.microsoft.com/en-us/windows/deployment/update/update-compliance-configuration-manual

upvoted 4 times

Question #31 *Topic 3*

HOTSPOT -

You have a Microsoft Intune subscription that has the following device compliance policy settings:

- Mark devices with no compliance policy assigned as: Compliant
- Compliance status validity period (days): 14

On January 1, you enroll Windows 10 devices in Intune as shown in the following table.

Name	BitLocker Drive Encryption (BitLocker)	Firewall	Scope (Tags)	Member of
Device1	Enabled	Off	Tag1	Group1
Device2	Disabled	On	Tag2	Group2

On January 4, you create the following two device compliance policies:

- Name: Policy1
- Platform: Windows 10 and later
- Require BitLocker: Require
- Mark device noncompliant: 5 days after noncompliance
- Scope (Tags): Tag1
- Name: Policy2
- Platform: Windows 10 and later
- Firewall: Require
- Mark device noncompliant: Immediately
- Scope (Tags): Tag2

On January 5, you assign Policy1 and Policy2 to Group1.

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

NOTE: Each correct selection is worth one point.

Hot Area:

Answer Area

Statements	Yes	No
On January 7, Device1 is marked as compliant.	○	○
On January 8, Device1 is marked as compliant.	○	○
On January 8, Device2 is marked as compliant.	○	○

Correct Answer:

Answer Area

Statements	Yes	No
On January 7, Device1 is marked as compliant.	○	○
On January 8, Device1 is marked as compliant.	○	○
On January 8, Device2 is marked as compliant.	○	○

Box 1: No.

Policy1 and Policy2 apply to Group1 which Device1 is a member of. Device1 does not meet the firewall requirement in Policy2 so the device will immediately be marked as non-compliant.

Box 2: No -

For the same reason as Box1.

Box 3: Yes -

Policy1 and Policy2 apply to Group1. Device2 is not a member of Group1 so the policies don't apply.

The Scope (tags) have nothing to do with whether the policy is applied or not. The tags are used in RBAC.

Perycles Highly Voted 1 year, 3 months ago

all is correct

upvoted 12 times

raduM Most Recent 1 month, 2 weeks ago

if every question was so easy :)
upvoted 1 times

AZUREMAN2022 4 months, 1 week ago
Compliance status validity period (days)

Specify a period in which devices must successfully report on all their received compliance policies. If a device fails to report its compliance status for a policy before the validity period expires, the device is treated as noncompliant.

https://docs.microsoft.com/en-us/mem/intune/protect/device-compliance-get-started
upvoted 1 times

maggie_petrova 6 months ago
Policy2 has a scope tag2, why would policy2 be applied to computer1, which has scope tag1?
upvoted 1 times

silver_bullet666 2 months, 4 weeks ago
as stated in the answer, policy tags are for RBAC, ie. who can see/modify the object/policy, it does not define the scope of what the policy applies to.
upvoted 1 times

distortion 7 months, 2 weeks ago
It should all be no. The firewall is turned of on device 1 so that is a no 2 times. On device 2 bitlocker is not enabled, the policy states the device is non compliant after 5 days so again no.
upvoted 1 times

distortion 7 months, 2 weeks ago
Sorry misread the question. The policies only apply to group 1. Given answer is correct
upvoted 1 times

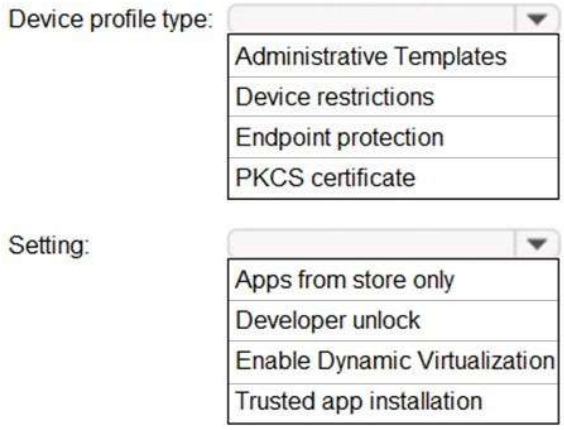
AVP_Riga 10 months, 4 weeks ago
Device will be uncomlined by this policy ASAP. Mark device noncompliant: Immediately
Devices will use default settings.
upvoted 1 times

AVP_Riga 10 months, 4 weeks ago
*Devices - Device2
upvoted 1 times

AVP_Riga 10 months, 4 weeks ago
*Device - Device1
upvoted 1 times

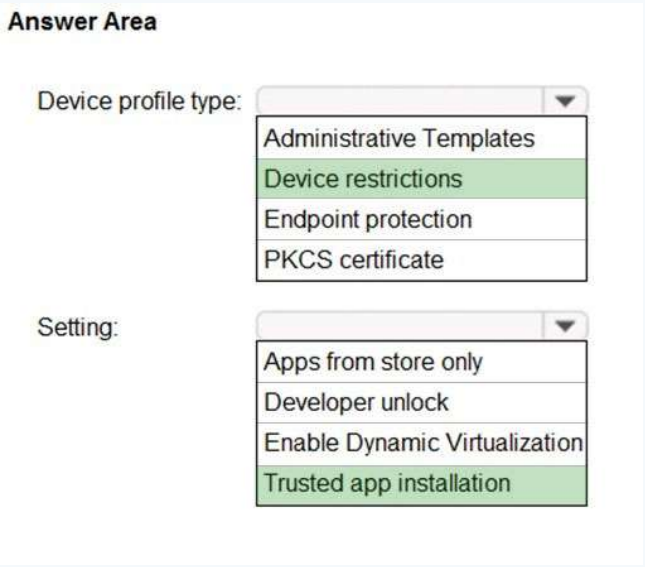
HOTSPOT -
You have 100 Windows 10 devices that are managed by using Microsoft Endpoint Manager.
You plan to sideload an app to the devices.
You need to configure Microsoft Endpoint Manager to enable sideloading.
Which device profile type and setting should you configure? To answer, select the appropriate options in the answer area.
NOTE: Each correct selection is worth one point.
Hot Area:

Answer Area



Correct Answer:

Answer Area



Box 1: Device restrictions -
In a Windows 10/11 device restrictions profile, most configurable settings are deployed at the device level using device groups. Policies deployed to user groups apply to targeted users. The policies also apply to users who have an Intune license, and users that sign in to that device.

Box 2: Trusted app installation -
Trusted app installation: Choose if non-Microsoft Store apps can be installed, also known as sideloading. Sideloading is installing, and then running or testing an app that isn't certified by the Microsoft Store. For example, an app that is internal to your company only.
Reference:
https://docs.microsoft.com/en-us/mem/intune/configuration/device-restrictions-windows-10

jibutoms Highly Voted 1 year, 3 months ago
It is moved under Device Restrictions --> Appstore --> Trusted app installation
upvoted 7 times

john909 11 months ago
thank you
upvoted 1 times

MikeMatt2020 Highly Voted 1 year, 4 months ago

Answer is correct

Under Device Restrictions > Trusted app installation
Description: "Specifies whether apps from Appx packages signed with a trusted certificate can be sideloaded"

https://docs.microsoft.com/en-us/mem/intune/apps/app-sideload-windows

upvoted 7 times

Sironin Most Recent 1 year, 1 month ago

While signing an app isn't particularly difficult, the question doesn't actually specify this. If an unsigned app is needed, the answer is Developer Unlock (allow) rather than Trusted App Installation (allow). In the scenario where an app is being deployed to 100 devices, we can assume this is not a development scenario where an unsigned app is required for early testing. So the given answer is correct in context.

upvoted 6 times

Question #33 *Topic 3*

Note: This question is part of a series of questions that present the same scenario. Each question in the series contains a unique solution that might meet the stated goals. Some question sets might have more than one correct solution, while others might not have a correct solution.
After you answer a question in this section, you will NOT be able to return to it. As a result, these questions will not appear in the review screen.
You have an Azure Directory group named Group1 that contains Windows 10 Enterprise devices and Windows 10 Pro devices.
From Microsoft Intune, you create a device configuration profile named Profile1.
You need to ensure that Profile1 applies to only the Windows 10 Enterprise devices in Group1.
Solution: You create a scope tag, and then you add the scope tag to the Windows 10 Enterprise devices and Profile1.
Does this meet the goal?

A. Yes

B. No

Correct Answer: *B*
Instead: You configure an applicability rule for Profile1. You assign Profile1 to Group1.
Note: Applicability rules allow administrators to target devices in a group that meet specific criteria. For example, you create a device restrictions profile that applies to the All Windows 10/11 devices group. And, you only want the profile assigned to devices running Windows Enterprise.
To do this task, create an applicability rule.
Reference:
https://docs.microsoft.com/en-us/mem/intune/configuration/device-profile-create

Anna_Peters Highly Voted 1 year, 4 months ago
I think it should be Applicability rules/Assignments.
upvoted 10 times

MikeMatt2020 Highly Voted 1 year, 4 months ago
So this does not meet our goal
(We'd want an Applicability Rule and specify the OS that will receive the policy)
upvoted 6 times

Russ_A7x Most Recent 2 months ago
Scope tags= filtering
upvoted 1 times

MikeMatt2020 1 year, 4 months ago
Scope tags are used for RBAC, NOT for filtering which devices receive policies.
upvoted 6 times

ja0000 1 year, 4 months ago
Doesn't scope let you specify devices/groups?
upvoted 1 times

Layer8 1 year, 4 months ago
it seems what i've gathered from reading on this site is that scope tags are ways of delegating permissions to user groups, not delegating policies to devices.
upvoted 3 times

Moorebid 1 year, 4 months ago
Scope tags are only used to limit view access to specific objects in Intune. An applicability rule would solve the issue in this question; it would allow you to apply the device configuration to only the Enterprise devices in Group1.
upvoted 3 times

Question #34 *Topic 3*

Your company has a System Center Configuration Manager deployment that uses hybrid mobile device management (MDM). All Windows 10 devices are Active
Directory domain-joined.
You plan to migrate from hybrid MDM to Microsoft Intune standalone.
You successfully run the Intune Data Importer tool.
You need to complete the migration.
Which two actions should you perform? Each correct answer presents part of the solution.
NOTE: Each correct selection is worth one point.

A. In Intune, add a device enrollment manager (DEM).

B. Change the tenant MDM authority to Intune.

C. Assign all users Intune licenses.

D. Create a new Intune tenant.

Correct Answer: *BC*
Reference:
https://docs.microsoft.com/en-us/sccm/mdm/deploy-use/migrate-hybridmdm-to-intunesa https://docs.microsoft.com/en-us/sccm/mdm/deploy-use/migrate-prepare-intune

Rstilekar Highly Voted 1 year, 9 months ago
I think this Question is not valid anymore as Microsoft retired the hybrid MDM service offering as of September 1, 2019. Ref - https://docs.microsoft.com/en-us/mem/configmgr/mdm/understand/what-happened-to-hybrid
upvoted 7 times

lucidgreen 1 year, 7 months ago
It's now called Co-Management.
upvoted 15 times

rovert94 8 months ago
Does that change the answer of this question?
upvoted 1 times

thuba_TD Most Recent 2 weeks, 3 days ago
Too easy
upvoted 1 times

RodrigoT 6 months, 1 week ago
BC. Easy peasy by elimination.
upvoted 2 times

LordCaine 1 year ago
But when it's hybrid isn't MDM already assigned to Intune? Since they are already half in Intune.
upvoted 2 times

Question #35 *Topic 3*

Your company has 200 computers that run Windows 10. The computers are managed by using Microsoft Intune.
Currently, Windows updates are downloaded without using Delivery Optimization.
You need to configure the computers to use Delivery Optimization.
What should you create in Intune?

A. a device configuration profile

B. a device compliance policy

C. an app protection policy

D. a Windows 10 update ring

Correct Answer: *A*
With Intune, use Delivery Optimization settings for your Windows devices to reduce bandwidth consumption when those devices download applications and updates. Configure Delivery Optimization as part of your device configuration profiles.
Reference:
https://docs.microsoft.com/en-us/intune/delivery-optimization-windows

TaboloDude Highly Voted 9 months, 2 weeks ago
Of course a device configuration profile, as usual..
upvoted 9 times

TestTaker72 Highly Voted 1 year, 6 months ago
Correct
Devices > Configuration profiles > Create profile
upvoted 5 times

john909 11 months ago
Profile type: Templates > Delivery Optimization
upvoted 5 times

Adilh99 Most Recent 6 months, 4 weeks ago
Is this not under update rings now?
upvoted 3 times

Martinvd 6 months, 1 week ago
Checked it, but it's not in the Update Rings.
upvoted 4 times

Koetjeboe 6 months, 3 weeks ago
That was my understanding as well but didn't checked it.
upvoted 1 times

mikl 9 months, 1 week ago
Correct!
upvoted 1 times

Perycles 1 year, 3 months ago
correct
upvoted 2 times

MikeMatt2020 1 year, 4 months ago
Correct
upvoted 2 times

Question #36 *Topic 3*

You have 500 computers that run Windows 10. The computers are joined to Microsoft Azure Active Directory (Azure AD) and enrolled in Microsoft Intune.

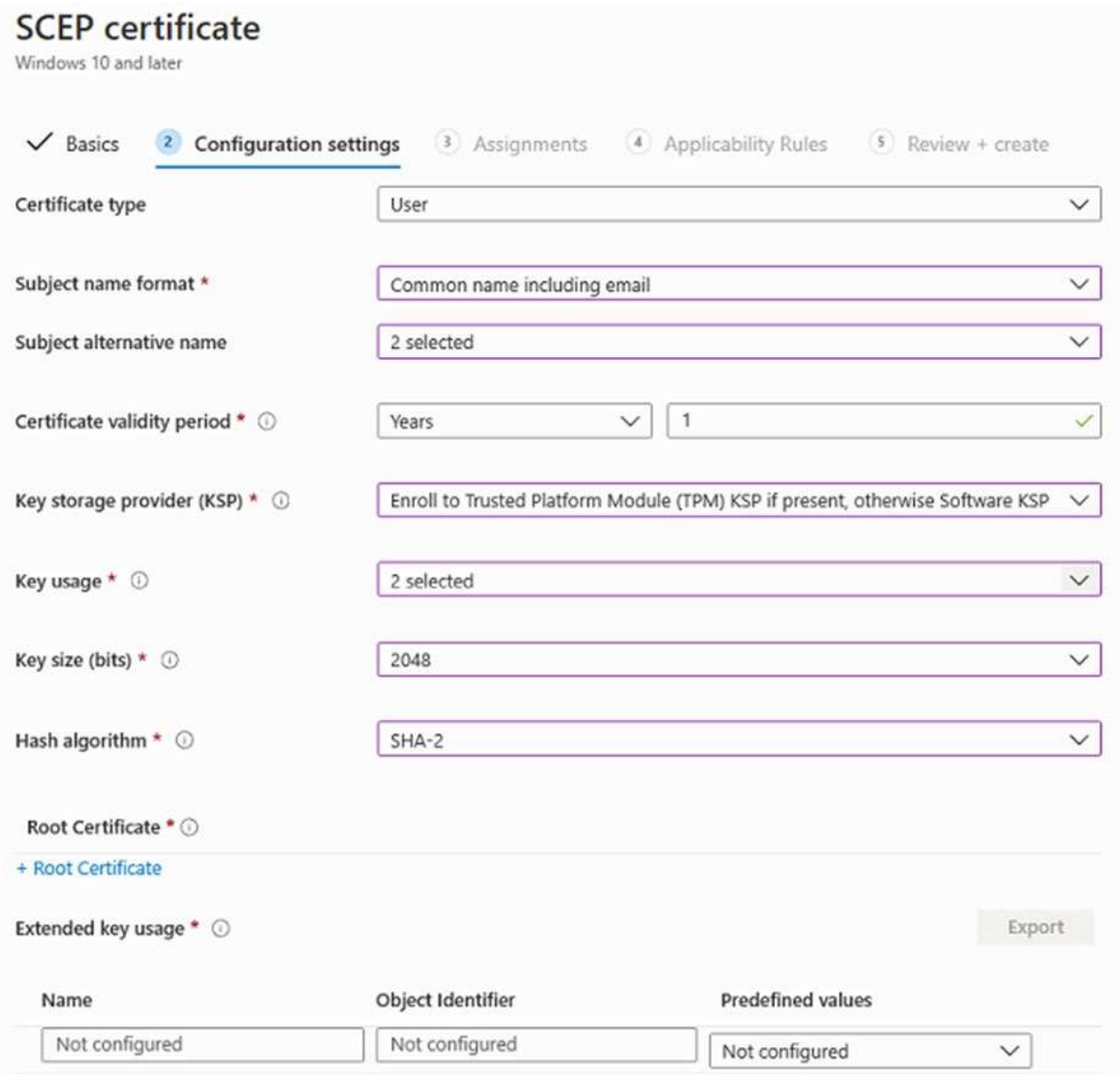
You plan to distribute certificates to the computers by using Simple Certificate Enrollment Protocol (SCEP).

You have the servers shown in the following table.

Name	Configuration
Server1	Domain controller
Server2	Root certification authority (CA)
Server3	Subordinate certification authority (CA)
Server4	Network Device Enrollment Service (NDES)

NDES issues certificates from the subordinate CA.

You are configuring a device profile as shown in the exhibit. (Click the Exhibit tab.)



On which server is the required root certificate located?

A. Server1

B. Server2

C. Server3

D. Server4

Correct Answer: *C*

As NDES issues certificates from the subordinate CA located at Server3, the root certificate should be used for Server3.

RodrigoT 5 months ago

Selected Answer: C

The CA is Server3.
Check NDES functions:
1-Generates and provides one-time enrollment passwords to administrators
2-Submits enrollment requests to the CA (in this case Server3)
3-Retrieves enrolled certificates from the CA and forwards them to the network device

Source:
https://docs.microsoft.com/en-us/previous-versions/windows/it-pro/windows-server-2012-R2-and-2012/hh831498(v=ws.11)

upvoted 1 times

MR_Eliot 5 months ago

Selected Answer: D

NDES server role – To support using the Certificate Connector for Microsoft Intune with SCEP, you must configure the Windows Server that will host the certificate connector with the Network Device Enrollment Service (NDES) server role. The connector supports installation on Windows Server 2012 R2 or later. In a later section of this article, we guide you through installing NDES.

The server that hosts NDES and the connector must be domain-joined and in the same forest as your Enterprise CA.
Do not use NDES that's installed on the server that hosts the Enterprise CA. This configuration represents a security risk when the CA services internet requests, and installation of the connector isn't supported on the same server as your issuing Certification Authority (CA).

https://docs.microsoft.com/en-us/mem/intune/protect/certificates-scep-configure

upvoted 1 times

Question #37 *Topic 3*

You have 200 computers that run Windows 10. The computers are joined to Microsoft Azure Active Directory (Azure AD) and enrolled in Microsoft Intune.

You redirect Windows known folders to Microsoft OneDrive for Business.

Which folder will be included in the redirection?

A. Saved Games

B. Desktop

C. Music

D. Downloads

Correct Answer: *B*

Reference:

https://docs.microsoft.com/en-us/onedrive/redirect-known-folders

saran1987 Highly Voted 2 years, 5 months ago

There are two primary advantages of moving or redirecting Windows known folders (Desktop, Documents, Pictures, Screenshots, and Camera Roll) to OneDrive for the users in your domain.

The answer is B

upvoted 10 times

mikl Most Recent 9 months, 1 week ago

Selected Answer: B

B. Desktop

upvoted 2 times

RodrigoT 5 months ago

Agreed.
Windows Known folders with Ms Onedrive for Business:
1-Screenshots
2-Pictures
3-Camera Roll
4-Documents
5-Desktop

upvoted 1 times

Perycles 1 year, 3 months ago

B is correct.

upvoted 1 times

Anilw 2 years, 6 months ago

Correct but if a user logs in two different pcs some shortcuts on the desktop e.g edge duplicate. E.g you will end up edge and edge (copy) as 2 shortcuts.

upvoted 2 times

vm007 2 years, 7 months ago

OneDrive known folder: Picture, Desktop, Documents.. ans is correct: D

upvoted 1 times

TestTaker72 1 year, 6 months ago

Not D - Downloads
B - Desktop

upvoted 2 times

Question #38 *Topic 3*

You have a Microsoft Azure Active Directory (Azure AD) tenant. All corporate devices are enrolled in Microsoft Intune.
You have a web-based application named App1 that uses Azure AD to authenticate.
You need to prompt all users of App1 to agree to the protection of corporate data when they access App1 from both corporate and noncorporate devices.
What should you configure?

A. Notifications in Device compliance

B. Terms and Conditions in Device enrollment

C. Terms of use in Conditional access

D. an Endpoint protection profile in Device configuration

Correct Answer: *C*
Use an Intune terms and conditions policy to present relevant disclaimers for legal or compliance requirements to device users. A terms and conditions policy requires targeted users to accept your terms in Company Portal before they can enroll devices or access protected resources.
Reference:
https://docs.microsoft.com/en-us/mem/intune/enrollment/terms-and-conditions-create

vm007 Highly Voted 2 years, 7 months ago
Term of Use require users or devices to agree before getting access: ans. is correct. C
upvoted 13 times

lucidgreen 1 year, 8 months ago
That's great but where should it be applied. Each answer can be termed a Terms of Use categorical statement.
Only one of them can be used for granting access, which would be conditional. So yes, you are correct, but for the wrong reasons.
Conditional Access can be applied to an app, provided it's supported.
https://docs.microsoft.com/en-us/mem/intune/protect/app-based-conditional-access-intune
Device Compliance has nothing to do with accessing an app, just accessing and maintaining the device.
Device Enrollment is also a throw-away.
An Endpoint Protection Profile, is also unlikely.
upvoted 1 times

raduM Most Recent 1 month, 2 weeks ago
correct
upvoted 1 times

cdhoesje 5 months ago
go to azure > Security > Conditional Acces > term of use

You can see C is correct.

https://docs.microsoft.com/nl-nl/azure/active-directory/conditional-access/terms-of-use
upvoted 1 times

Perycles 1 year, 3 months ago
C is correct.
upvoted 4 times

Question #39 *Topic 3*

You are creating a device configuration profile in Microsoft Intune.
You need to configure specific OMA-URI settings in the profile.
Which profile type should you use?

A. Identity protection

B. Custom

C. Device restrictions (Windows 10 Team)

D. Device restrictions

Correct Answer: *B*
Windows client custom profiles use Open Mobile Alliance Uniform Resource Identifier (OMA-URI) settings to configure different features. These settings are typically used by mobile device manufacturers to control features on the device.
Reference:
https://docs.microsoft.com/en-us/mem/intune/configuration/custom-settings-windows-10

Tiit Highly Voted 1 year, 4 months ago
Custom is right - Windows 10 custom profiles use Open Mobile Alliance Uniform Resource Identifier (OMA-URI) settings to configure different features. These settings are typically used by mobile device manufacturers to control features on the device.
upvoted 10 times

Perycles Highly Voted 1 year, 3 months ago
so easy , i like this :)
upvoted 5 times

Question #40 *Topic 3*

DRAG DROP -

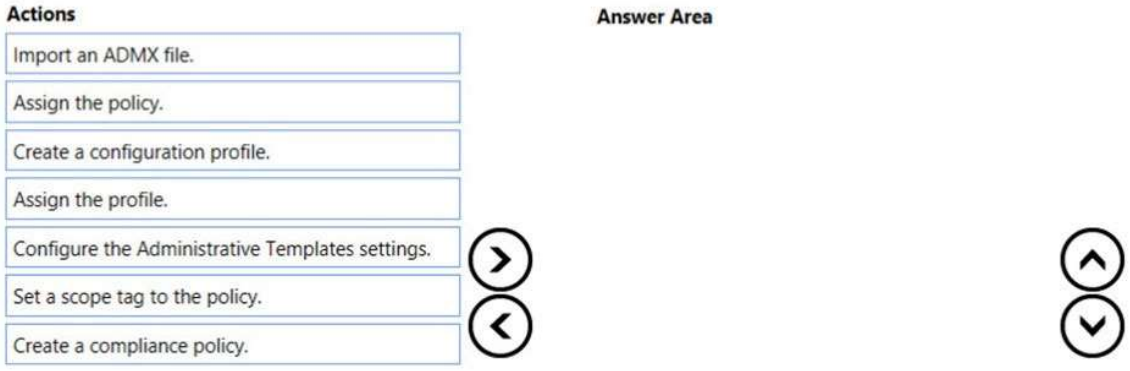
You have an Azure Active Directory (Azure AD) tenant that syncs to an on-premises Active Directory domain.

The tenant contains computers that run Windows 10. The computers are hybrid Azure AD joined and enrolled in Microsoft Intune. The Microsoft Office settings on the computers are configured by using a Group Policy Object (GPO).

You need to migrate the GPO to Intune.

Which three actions should you perform in sequence? To answer, move the appropriate actions from the list of actions to the answer area and arrange them in the correct order.

Select and Place:



Correct Answer:

Step 1: Create a configuration profle

Create the template -

1. Sign in to the Microsoft Endpoint Manager admin center.
2. Select Devices > Configuration profiles > Create profile.
3. Etc.

Step 2: Configure the Administrative Template settings.

Find some settings. There are thousands of settings available in these templates.

Step 3: Assign the profile.

The template is created, but may not be doing anything yet. Be sure to assign the template (also called a profile) and monitor its status.

Reference:

https://docs.microsoft.com/en-us/mem/intune/configuration/administrative-templates-windows

Mujja Highly Voted 1 year, 3 months ago

Correct answer.

The admin templates include settings for MS Office

upvoted 9 times

51007 Most Recent 4 months ago

Recreating the settings from scratch within Intune doesnt exactly seem like 'migrating' but ok

upvoted 2 times

forummj 1 year, 2 months ago

I presume that "Set a scope tag to the policy" doesn't come third because it's listed as Optional in the Windows Docs guide, then?

upvoted 1 times

Barrie 1 year, 1 month ago

Scope tags are for RBAC, has no control over the policy or settings

upvoted 2 times

Perycles 1 year, 3 months ago

correct method.

upvoted 2 times

Merma 1 year, 4 months ago

"Administrative Templates are built in to Intune, and don't require any customizations, including using OMA-URI. As part of your mobile device management (MDM) solution, use these template settings as a one-stop shop to manage your Windows 10 devices."

upvoted 2 times

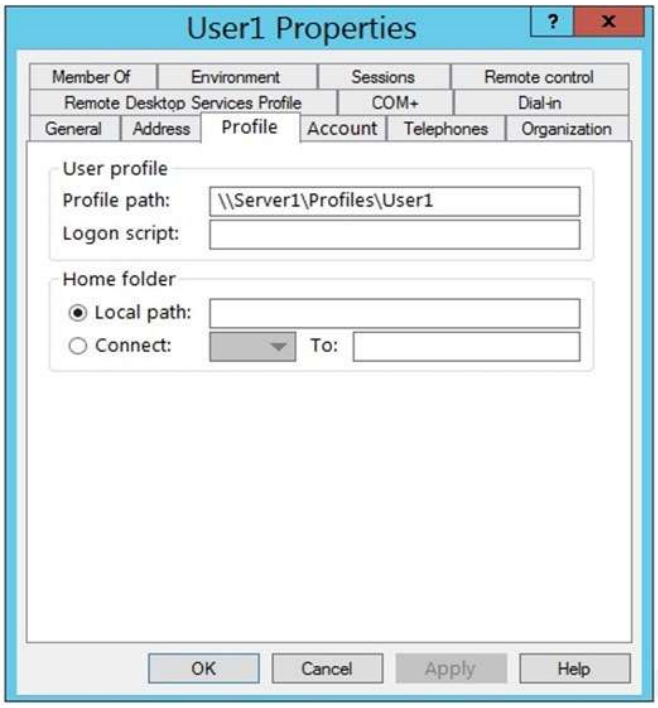
Question #41 *Topic 3*

HOTSPOT -

Your network contains an on-premises Active Directory forest named contoso.com. The forest contains a user named User1 and two computers named

Computer1 and Computer2 that run Windows 10.

User1 is configured as shown in the following exhibit.



You rename file \\Server1\Profiles\User1.V6\NTUSER.DAT as NTUSER.MAN.

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

NOTE: Each correct selection is worth one point.

Hot Area:

Answer Area

Statements	Yes	No
On Computer1, if User1 adds a shortcut to the desktop, the shortcut will appear when the user signs in to Computer2.	○	○
On Computer1, if User1 modifies the background, and then signs out, the user will see the modified background when signing back in to Computer1.	○	○
On Computer1, if User1 modifies the background, and then signs out, the user will see the modified background when signing in to Computer2.	○	○

Correct Answer:

Answer Area

Statements	Yes	No
On Computer1, if User1 adds a shortcut to the desktop, the shortcut will appear when the user signs in to Computer2.	○	○
On Computer1, if User1 modifies the background, and then signs out, the user will see the modified background when signing back in to Computer1.	○	○
On Computer1, if User1 modifies the background, and then signs out, the user will see the modified background when signing in to Computer2.	○	○

A mandatory user profile is a roaming user profile that has been pre-configured by an administrator to specify settings for users. Settings commonly defined in a mandatory profile include (but are not limited to): icons that appear on the desktop, desktop backgrounds, user preferences in Control Panel, printer selections, and more. Configuration changes made during a user's session that are normally saved to a roaming user profile are not saved when a mandatory user profile is assigned.

The .man extension causes the user profile to be a read-only profile.

Reference:

https://docs.microsoft.com/en-us/windows/client-management/mandatory-user-profile

Perycles Highly Voted 1 year, 3 months ago

correct.
upvoted 10 times

tf444 Highly Voted 11 months, 2 weeks ago
NTUSER.MAN MANADTORY
NTUSER.MAN.V6 SUPER MANADTORY
upvoted 6 times

raduM Most Recent 1 month, 2 weeks ago
correct
upvoted 1 times

tf444 11 months, 2 weeks ago
In mandatory profile, the user can sign in with local cache if the DC is down, in super mandatory the user is unable to sign in.
upvoted 3 times

badguytoo 1 year, 1 month ago
A mandatory user profile is a roaming user profile that has been pre-configured by an administrator to specify settings for users. Settings commonly defined in a mandatory profile include (but are not limited to): icons that appear on the desktop, desktop backgrounds, user preferences in Control Panel, printer selections, and more. Configuration changes made during a user's session that are normally saved to a roaming user profile are not saved when a mandatory user profile is assigned.
upvoted 3 times

Question #42 *Topic 3*

You have a Windows 10 device named Device1 that is joined to Active Directory and enrolled in Microsoft Intune.
Device 1 is managed by using Group Policy and Intune.
You need to ensure that the Intune settings override the Group Policy settings.
What should you configure?

A. a device configuration profile

B. an MDM Security Baseline profile

C. a device compliance policy

D. a Group Policy Object (GPO)

Correct Answer: *A*
Creating the policy -
Let's create a new policy in Intune to control the GP vs. MDM winner
1. Navigate to portal.azure.com and locate Intune
2. Select ↄ€Device configuration „ Profiles „ Create profileↄ€
3. Under Platform select Windows 10 and later
4. Under Profile type select ↄ€customↄ€ and ↄ€addↄ€
5. Name the custom setting with something intuitive
6. For OMA-URI add the policy OMA-URI string: ./Device/Vendor/MSFT/Policy/Config/ControlPolicyConflict/MDMWinsOverGP
7. For Data type select Integer and add the number
Note: The following describes which policy wins according to Windows 10 version.
Windows 10 versions 1709 and earlier Group Policy will override MDM policies, even if an identical policy is configured in MDM.
Windows 10 version 1803 and beyond there is a new Policy CSP (configuration service provider) setting called ControlPolicyConflict that includes the policy of
MDMWinsOverGP, where the preference of which policy wins can be controlled, i.e. Microsoft Intune MDM policy.
Note 2: the ControlPolicyConflict policy allows the IT admin to control which policy will be used whenever both the MDM policy and its equivalent Group Policy
(GP) are set on the device.
Reference:
https://docs.microsoft.com/en-us/windows/client-management/mdm/policy-csp-controlpolicyconflict
https://uem4all.com/2018/04/02/windows-10-group-policy-vs-intune-mdm-policy-who-wins/

Dong1999 Highly Voted 1 year, 2 months ago
Given answer A is correct.

Creating the policy

Let's create a new policy in Intune to control the GP vs. MDM winner

Navigate to portal.azure.com and locate Intune
Select "Device configuration à Profiles à Create profile"
Under Platform select Windows 10 and later
Under Profile type select "custom" and "add"
Name the custom setting with something intuitive
For OMA-URI add the policy OMA-URI string: ./Device/Vendor/MSFT/Policy/Config/ControlPolicyConflict/MDMWinsOverGP
For Data type select Integer and add the number 1
upvoted 24 times

Question #43 *Topic 3*

You use a Microsoft Intune subscription to manage iOS devices.
You configure a device compliance policy that blocks jailbroken iOS devices.
You need to enable Enhanced jailbreak detection.
What should you configure?

A. the device compliance policy

B. the Compliance policy settings

C. a network location

D. a configuration profile

Correct Answer: *A*
Compliance policy settings include the following settings:
* Enhanced jailbreak detection (applies only to iOS/iPadOS)
* Etc.
Reference:
https://docs.microsoft.com/en-us/mem/intune/protect/device-compliance-get-started

Jana08 Highly Voted 1 year, 3 months ago
Answer is B. The Compliance Policy settings.

In the Device compliance policy itself, you can't enable Enhanced Jailbreak Detection.

Go to Home>Devices>Compliance Policies>Compliance Policy Settings
upvoted 17 times

Cabanna94 1 year, 2 months ago
I agree with B. There are two parts to compliance policies in Intune:
Compliance policy settings & Device compliance policy.

Under "Compliance Policy Settings" itself, you can find the setting "Enhanced Jailbreak Detection (applies only to iOS/iPadOS)"

https://docs.microsoft.com/en-us/mem/intune/protect/device-compliance-get-started
upvoted 2 times

RodrigoT 5 months ago
Thank you for the path.
upvoted 1 times

[Removed] Most Recent 6 months, 3 weeks ago
Selected Answer: B
I also checked it just now, B is correct.
upvoted 1 times

4Shawsy 7 months, 3 weeks ago
Selected Answer: B
B is correct
upvoted 2 times

missa1 8 months ago
Selected Answer: B
B is the Correct answer.
upvoted 2 times

IykeP 8 months, 3 weeks ago
Selected Answer: B
B is the Correct answer.
https://docs.microsoft.com/en-us/mem/intune/protect/device-compliance-get-started
upvoted 1 times

Goofer 10 months, 3 weeks ago
Answer B. Compliance policy settings
These settings are generic and define the default behavior of the compliance policy. Here you can define what happens with a device which has no compliance policy assigned, by default this device will be marked as “Not Compliant”. You can also configure the usage of “Enhanced jailbreak detection” which is only supported on iOS/iPadOS and uses location services to more regularly check for a jailbreak.
upvoted 3 times

mgciba 1 year, 2 months ago
answer A is Correct.
From Reference Link
Enhanced jailbreak detection (applies only to iOS/iPadOS)
This setting works only with devices that you target with a device compliance policy that blocks jailbroken devices
upvoted 2 times

ExamStudy101 1 year, 2 months ago

The information you just listed is under "Compliance Policy settings" in the link, so the answer is B

upvoted 6 times

Question #44 *Topic 3*

Your network contains an Active Directory domain. The domain contains computers that run Windows 10.

All users use Roaming User Profiles.

You have a user named Public1 that is used to sign-in to a public computer.

You need to prevent changes to the user settings of Public1 from being saved to the user profile.

What should you do?

A. Rename the Roaming User Profile folder to Public1.man

B. Rename Ntuser.dat to Ntuser.v6

C. Rename Ntuser.dat to Ntuser.man

D. Rename the Roaming User Profile folder to Public1.v1

Correct Answer: *C*

User profiles become mandatory profiles when the administrator renames the NTuser.dat file (the registry hive) of each user's profile in the file system of the profile server from NTuser.dat to NTuser.man. The .man extension causes the user profile to be a read-only profile.

Reference:

https://docs.microsoft.com/en-us/windows/client-management/mandatory-user-profile

PersoDaniels Highly Voted 1 year, 3 months ago

C. is correct.

https://docs.microsoft.com/en-us/windows/client-management/mandatory-user-profile

upvoted 11 times

tf444 Most Recent 11 months, 2 weeks ago

To create a mandatory roaming profile, the ntuser.dat file (located at the root of the profile) is renamed to ntuser.man. This may be stored in a network share identified as \\DC1\Profiles.

upvoted 4 times

jorlloen 1 year, 1 month ago

I think A is the correct answer. All users have roaming profiles, and the request says "You need to prevent changes to the user settings of Public1 from being saved to the user profile" (only Public1). C option applies to all users, if you choose super-mandatory profile, you can set mandatory profile only to Public1 (https://docs.microsoft.com/en-us/previous-versions/windows/desktop/legacy/bb776895(v=vs.85))

upvoted 4 times

tf444 11 months, 2 weeks ago

Every user has a NTUSER.DAT when the user signs in, you rename the NTUSER.DAT to NTUSER.MAN for that user.

upvoted 4 times

Question #45 *Topic 3*

You have a hybrid deployment of Azure Active Directory (Azure AD) that contains 50 Windows 10 devices. All the devices are enrolled in Microsoft Endpoint
Manager.
You discover that Group Policy settings override the settings configured in Microsoft Endpoint Manager policies.
You need to ensure that the settings configured in Microsoft Endpoint Manager override the Group Policy settings.
What should you do?

A. From the Microsoft Endpoint Manager admin center, create an Administrative Templates device profile

B. From Group Policy Management Editor, configure the Computer Configuration settings in the Default Domain Policy

C. From the Microsoft Endpoint Manager admin center, create a custom device profile

D. From Group Policy Management Editor, configure the User Configuration settings in the Default Domain Policy

Correct Answer: *C*
Creating the policy -
Let's create a new policy in Intune to control the GP vs. MDM winner
1. Navigate to portal.azure.com and locate Intune
2. Select ɹ€Device configuration „ Profiles „ Create profileɹ€
3. Under Platform select Windows 10 and later
4. Under Profile type select ɹ€customɹ€ and ɹ€addɹ€
5. Name the custom setting with something intuitive
6. For OMA-URI add the policy OMA-URI string: ./Device/Vendor/MSFT/Policy/Config/ControlPolicyConflict/MDMWinsOverGP
7. For Data type select Integer and add the number
Note: The following describes which policy wins according to Windows 10 version.
Windows 10 versions 1709 and earlier Group Policy will override MDM policies, even if an identical policy is configured in MDM.
Windows 10 version 1803 and beyond there is a new Policy CSP (configuration service provider) setting called ControlPolicyConflict that includes the policy of
MDMWinsOverGP, where the preference of which policy wins can be controlled, i.e. Microsoft Intune MDM policy.
Note 2: the ControlPolicyConflict policy allows the IT admin to control which policy will be used whenever both the MDM policy and its equivalent Group Policy
(GP) are set on the device.
Reference:
https://docs.microsoft.com/en-us/windows/client-management/mdm/policy-csp-controlpolicyconflict
https://uem4all.com/2018/04/02/windows-10-group-policy-vs-intune-mdm-policy-who-wins/

PersoDaniels Highly Voted 1 year, 3 months ago
C. is correct.

https://docs.microsoft.com/en-us/archive/blogs/cbernier/windows-10-group-policy-vs-intune-mdm-policy-who-wins
upvoted 14 times

moobdoob Highly Voted 8 months, 2 weeks ago
C.

Navigate to portal.azure.com and locate Intune
Select “Device configuration à Profiles à Create profile”
Under Platform select Windows 10 and later
Under Profile type select “custom” and “add”
Name the custom setting with something intuitive
For OMA-URI add the policy OMA-URI string: ./Device/Vendor/MSFT/Policy/Config/ControlPolicyConflict/MDMWinsOverGP
For Data type select Integer and add the number 1
upvoted 5 times

Question #46 *Topic 3*

You have computers that run Windows 10, are joined to Azure Active Directory (Azure AD), and are enrolled in Microsoft Intune.
You have an Azure web app named App1. App1 only allows connections over HTTPS. App1 uses a certificate from an on-premises certification authority (CA).
You need to ensure that the computers can connect to App1 from Microsoft Edge.
Which type of device configuration profile should you create in Microsoft Endpoint Manager?

A. trusted certificate

B. Simple Certificate Enrollment Protocol (SCEP) certificate

C. imported public key pair (PKCS) certificate

D. public key pair (PKCS) certificate

Correct Answer: *B*
Intune supports use of the Simple Certificate Enrollment Protocol (SCEP) to authenticate connections to your apps and corporate resources.
Reference:
https://docs.microsoft.com/en-us/mem/intune/protect/certificates-scep-configure

Goofer Highly Voted 10 months, 3 weeks ago
SCEP is to onroll certificates to Intune Devices (not necessary)
PKCS is to onroll certificates to Intune Devices (not necessary)
To trust the (internal) certificate of app1 you need to import the internal root certificate to the 'trused root certification authorities' of the device.
You must create a configuration Profile - Trusted certificate to deploy the root certificate to the intune devices
Answer = trusted certificate
upvoted 7 times

MR_Eliot 5 months ago
Agreed.
upvoted 1 times

Jana08 Highly Voted 1 year, 3 months ago
SCEP Appears to be correct:

Intune supports use of the Simple Certificate Enrollment Protocol (SCEP) to authenticate connections to your apps and corporate resources.

https://docs.microsoft.com/en-us/mem/intune/protect/certificates-scep-configure
upvoted 6 times

IykeP Most Recent 8 months, 3 weeks ago
Selected Answer: B
B is the correct answer.
upvoted 4 times

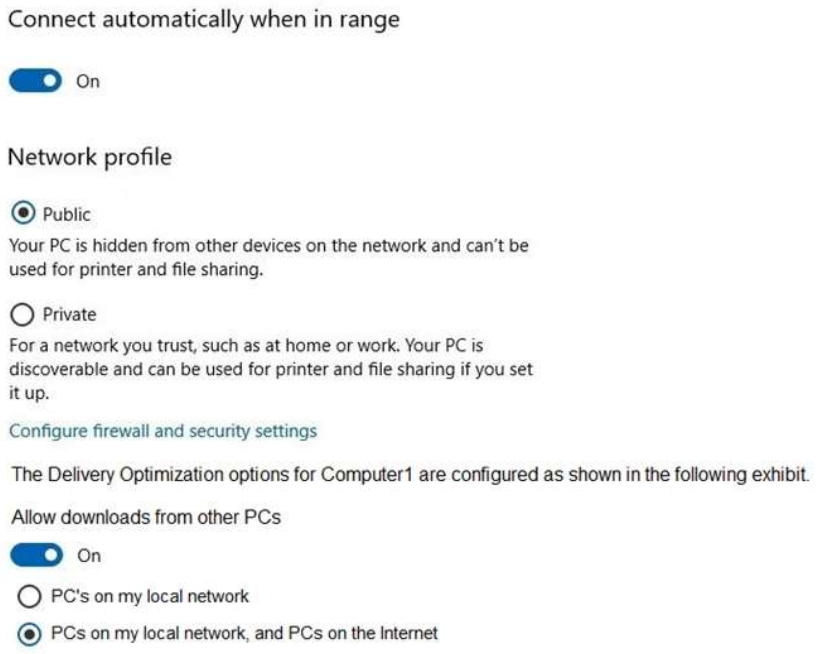
jorlloen 1 year, 1 month ago
In my opion. MS Edge needs to trust with App1 certificate, if not a "can't connect securely to this page" message will be showed on Edge, so you need to deploy the Root CA certificate in Trusted root certification Authorities. A is my ssugested answer.
upvoted 4 times

forExamCert2023 6 months, 3 weeks ago
While that can be a solution, have this in mind that Microsoft wants us to see if we know the new way of doing the business. That is their goal.
upvoted 2 times

HOTSPOT -

You have a computer named Computer1 that runs Windows 10.

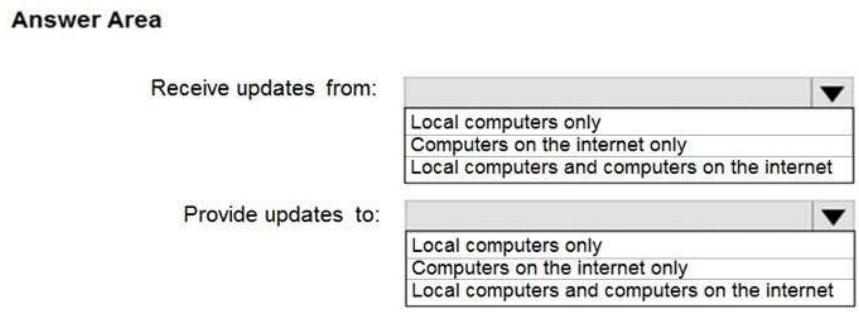
The Wi-Fi network profile for Computer1 is configured as shown in the following exhibit.



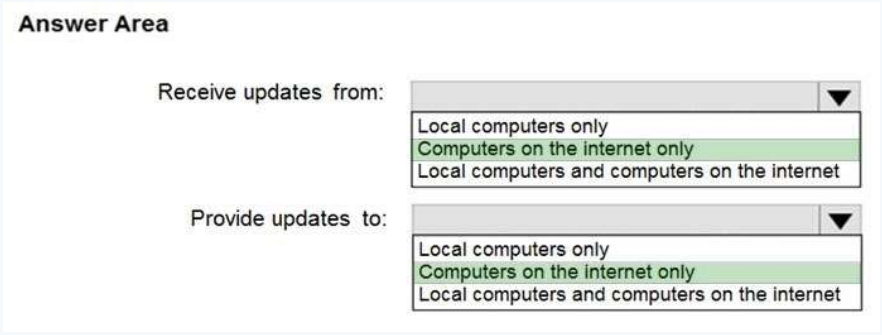
From which computers will Computer1 will receive updates and to which computers will Computer1 provide updates? To answer, select the appropriate options in the answer area.

NOTE: Each correct selection is worth one point.

Hot Area:



Correct Answer:



Sh1rub10 Highly Voted 1 year, 2 months ago

Correct answer for me
Network profile setted to "Public" so device can't discover and can't be discovered from other network devices, only via internet

upvoted 6 times

RodrigoT 5 months, 1 week ago

I agree. Just tested on my PC. When I change to Public I'm unable to even discover other devices, and Windows Explorer gives me an error.

upvoted 2 times

Pleebb Highly Voted 1 year, 2 months ago

Correct answers below..

Received updates from: Computers on the internet only

Provide updates to: Local computers nd computers on the internet
upvoted 5 times

gladi 1 year, 2 months ago
Why? Can you explain it? thanks :)
upvoted 1 times

ExamStudy101 1 year, 2 months ago
I think the provided answer is correct. Why would you be able to provide updates to local computers when Public Network is more restrictive and says you won't fileshare to other computers on the LAN?
upvoted 11 times

MR_Eliot Most Recent 5 months ago
Correct Answer, if you don't believe do your own research.
Delivery Optimization FW (in) firewall rule is configured for all profile types.
So the answer is:
1. Local computers & internet computers
1. Local computers & internet computers
upvoted 1 times

moobdoob 8 months, 2 weeks ago
Provided answer is correct. NOTE: Public network profile
upvoted 2 times

daonga 1 year, 2 months ago
I don't understand this can someone explain? Seems the network is on is configured for public use and DO is configured for public & local delivery.
Shouldn't it be option 3 for both? What am I missing here?
upvoted 1 times

tf444 11 months, 2 weeks ago
The network profile is set to public, computer1 is not discoverable on the network.
upvoted 5 times

HOTSPOT -

You have a Microsoft 365 tenant named contoso.com that contains a group named ContosoUsers. All the users in contoso.com are members of ContosoUsers.

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

Name	Join type	Mobile device management (MDM)
Computer1	Azure Active Directory (Azure AD) - registered	Microsoft Intune
Computer2	Azure Active Directory (Azure AD) – joined	Microsoft Intune

Both Computer1 and Computer2 contain two apps named App1 and App2.

You configure an app protection policy named AppPolicy1 that has the following settings:

- Protected apps: App1
- Assignments: ContosoUsers
- Enrollment state: Without enrollment
- Windows Information Protection mode: Block

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

NOTE: Each correct selection is worth one point.

Hot Area:

Answer Area

Statements	Yes	No
On Computer1, a user can copy and paste data from App1 to App2.	○	○
On Computer2, a user can copy and paste data from App1 to App2.	○	○
Data created by App1 can be wiped selectively from Computer1.	○	○

Correct Answer:

Answer Area

Statements	Yes	No
On Computer1, a user can copy and paste data from App1 to App2.	○	○
On Computer2, a user can copy and paste data from App1 to App2.	○	○
Data created by App1 can be wiped selectively from Computer1.	○	○

Reference:

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

Goofer Highly Voted 10 months, 3 weeks ago

Protected app is App1
App protection policy
Intune polices go above App protection policies

N - Azure registered - App protection policy: Block
Y - Azure Joined - Intune Policy
Y - Azure registered - App1 can selectively wiped

App Protection policies are available for: iOS/iPadOS, Android and Windows 10 and later

upvoted 11 times

RodrigoT 5 months, 1 week ago

Wrong. Both devices are ENROLLED in Intune. In this case it doesn't matter if one is registered and the other is joined. When the policy is Enrollment state: Without enrollment, then is more restrictive and will always protect the app by MAM. The correct answers are N N Y.
Check the link:
https://docs.microsoft.com/en-us/mem/intune/apps/app-protection-policy

upvoted 5 times

pinklemonade Highly Voted 1 year, 1 month ago

Should be No, Yes, Yes
upvoted 6 times

raduM Most Recent 1 week, 2 days ago
with enrollment opr without enrollment means if it is enrolled in intune or not. So the app Protection policy will apply to both devices.
upvoted 1 times

raduM 3 weeks, 3 days ago
given answers are correct
upvoted 1 times

MR_Eliot 5 months ago
Both devices are MDM managed so they're enrolled in MDM management. Therefore the enrolled devices policy will apply.
So the correct answer should be: YES, YES, YES.
https://docs.microsoft.com/en-us/mem/intune/apps/app-protection-policies#target-app-protection-policies-based-on-device-management-state
upvoted 1 times

forummj 7 months, 3 weeks ago
The more I look at this I think Y, Y, Y, the question stipulates that the APP has been created "without enrollment" in mind. Both devices are enrolled in Intune, surely they wouldn't monitor App1 or App2?
upvoted 3 times

CARO54 9 months ago
Can you explain ? I don't understand the answer ...
upvoted 1 times

b3arb0yb1m 10 months, 1 week ago
Block
WIP looks for inappropriate data sharing practices and stops the user from completing the action. Blocked actions can include sharing info across non-corporate-protected apps, and sharing corporate data between other people and devices outside of your organization.

Sounds like N,Y,Y to me.
upvoted 4 times

R0b671 11 months ago
Answer appears correct.

No - App Protection Policy only applies to Android and iOS devices.
No - App Protection Policy only applies to Android and iOS devices.
Yes - Once documents are protected with a WIP policy, the protected data can be selectively wiped by an Intune administrator (Global administrator or an Intune Service administrator).

Source: https://docs.microsoft.com/en-us/mem/intune/apps/apps-selective-wipe
upvoted 4 times

Garito 7 months, 1 week ago
MAM-WE supports Windows 10 along with Android and iOS:

https://docs.microsoft.com/en-us/mem/intune/fundamentals/deployment-guide-enrollment-mamwe
upvoted 1 times

b3arb0yb1m 10 months, 1 week ago
Windows Information Protection (WIP) policies can be deployed without requiring MDM users to enroll their Windows 10 device. This configuration allows companies to protect their corporate documents based on the WIP configuration, while allowing the user to maintain management of their own Windows devices. Once documents are protected with a WIP policy, the protected data can be selectively wiped by an Intune administrator (Global administrator or an Intune Service administrator). By selecting the user and device, and sending a wipe request, all data that was protected via the WIP policy will become unusable. From the Intune in the portal, select Client app > App selective wipe.
upvoted 3 times

BieLey 11 months, 2 weeks ago
This should be:
Yes - App Protection Policy only applies to Android and iOS devices.
Yes - App Protection Policy only applies to Android and iOS devices.
No - You can't selectively wipe data only created by App1. You would wipe all company data on the device.
upvoted 3 times

Rick11221 11 months, 3 weeks ago
Answer is correct.
upvoted 2 times

auton 11 months, 3 weeks ago
Both laptops are enrolled in to MDM and they are targeted by a app protection policy that is ment for MDM-WE.

This is a all "No".
upvoted 1 times

daonga 1 year, 2 months ago
Can someone break this down? Does it not matter if device is registered/joined?
It seems the policy will only apply to devices that are not enrolled (registered) but I'm sure I am missing something
upvoted 4 times

Angarali 1 year, 1 month ago
Computer 1 is a personal device
upvoted 1 times

daonga 1 year, 1 month ago

But it's still enrolled into Intune. Shouldn't this all be NO because the policy is set to apply to un-enrolled devices??

upvoted 2 times

Davidchercm 1 year, 2 months ago

https://docs.microsoft.com/en-us/mem/intune/apps/mam-faq

upvoted 1 times

HOTSPOT -

You have devices that are not rooted enrolled in Microsoft Intune as shown in the following table.

Name	Platform	IP address
Device1	Windows	192.168.10.35
Device2	Android	10.10.10.40
Device3	Android	192.168.10.10

The devices are members of a group named Group1.

In Intune, you create a device compliance location that has the following configurations:

- Name: Network1
- IPv4 range: 192.168.0.0/16

In Intune, you create a device compliance policy for the Android platform. The policy has the following configurations:

- Name: Policy1
- Device health: Rooted devices: Block
- Locations: Location: Network1
- Mark device noncompliant: Immediately
- Assigned: Group1

The Intune device compliance policy has the following configurations:

- Mark devices with no compliance policy assigned as: Compliant
- Enhanced jailbreak detection: Enabled
- Compliance status validity period (days): 20

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 compliant.	○	○
Device2 is marked as compliant.	○	○
Device3 is marked as compliant.	○	○

Correct Answer:

Answer Area

Statements	Yes	No
Device1 is marked as compliant.	○	○
Device2 is marked as compliant.	○	○
Device3 is marked as compliant.	○	○

Reference:

https://docs.microsoft.com/en-us/intune/device-compliance-get-started

Mikey82 Highly Voted 1 year ago

D1 YES (no compliance policy applies to Windows device)
D2 YES (no compliance policy applies, as the policy applies to a different subnet)
D3 YES (Policy applies, but device is compliant as it is UNROOTED, and therefore will not be marked as noncompliant)

upvoted 23 times

Angarali 5 months, 2 weeks ago

The device compliance policy for the Android platform applies to Group1, which device 2 is part of. Due to device 2 not being as part of the device compliance location IP range, it will be marked as noncompliant, immediately.

Therefore the answer is Yes, No, Yes.

upvoted 6 times

Alexbz Highly Voted 1 year, 5 months ago

Supplied answers are correct.
D1: compliant because of " mark devices with no compliance policy assigned as compliant "
D2: Not compliant because of the IP subnet
D3 compliant OS is android and IP subnet is in Network 1 location

upvoted 21 times

tf444 11 months, 2 weeks ago

Mark devices with no compliance policy assigned as: Compliant!

upvoted 5 times

forExamCert2023 6 months, 3 weeks ago

True!
First come this: "Mark device NONCOMPLIANT: Immediately"
Then comes this: "Mark devices with NO COMPLIANCE policy assigned as: CompliANT"
So step two turns the "NONCOMPLIANT" to CompliANT. Sometimes overthinking makes things complicated while the answer is right in front of us.

upvoted 2 times

forExamCert2023 6 months, 3 weeks ago

Answer is Yes, Yes, Yes.

upvoted 2 times

Angarali 6 months, 2 weeks ago

"In Intune, you create a device compliance policy for the Android platform."

"Mark devices with no compliance policy assigned as: Compliant"

upvoted 2 times

raduM Most Recent 1 week, 2 days ago

ok how exactly do you set the compliance location and haow exactly to you put the network in the compliance policy? i am really trying to test this...
with this information i would go with yes yes yes as i have no idea if one of the devices is rooted or not

upvoted 1 times

Russ_A7x 2 months ago

YNY Device 2 is a part of group one so the compliance policy is applied and gets marked NC. If device 2 was not in group1 it would get marked as compliant.

upvoted 2 times

saminsweden 2 months, 2 weeks ago

It is not possible to create location based compliance policies for android today. This location based access control is now in AAD.

upvoted 2 times

Whatsamattr81 3 months, 2 weeks ago

Surely Y N Y... You deploy policies by group, not IP or a particular subnet. Just because the first android is not in Network one does not mean it wont get the policy - its in Group 1. All it means is that its in an untrusted subnet, which depending on how you handle it, will see it as non-compliant.

upvoted 2 times

WinryKate 4 months ago

I am so confused. What answer is correct, the given is different than the discussions which vary...

upvoted 1 times

silver_bullet666 3 months, 2 weeks ago

I believe the answer is Y Y Y.
My reasoning on the contentious second android device outside the network defined in the policy
Policy 1 defines a scope of Android OS and Network 1
The device that is not in Network 1 but is Android is marked as Compliant as no policy is assigned to the device, as per "Intune device compliance policy" settings, Mark devices with no compliance policy assigned as: Compliant

upvoted 1 times

silver_bullet666 2 months ago

New answer is YNY
" If the device isn't connected to any of the selected locations, it's considered not compliant" REF: https://docs.microsoft.com/en-us/mem/intune/protect/create-compliance-policy

upvoted 2 times

Bouncy 5 months, 3 weeks ago

YNY
D1 and D3 are obvious, D2 seems to be an issue here. But the policy is still being applied despite the device having a different subnet. While creating a location-based policy it clearly reads "A device is considered noncompliant when none of the locations specified below are met". It's not a filter to "apply a policy only if device is in location XYZ"

upvoted 2 times

MR_Eliot 5 months ago

I agree with this.

upvoted 1 times

moobdoob 8 months, 2 weeks ago

Answer is correct: YES, NO ,YES

upvoted 2 times

b3arb0yb1m 10 months, 1 week ago

From what I see, D1 and D3 are unrooted and therefore pass Policy1. D2 doesn't fall within the Policy1 scope because of the subnet and therefore, it is marked as compliant. Y, Y, Y.

Am I missing something?

upvoted 2 times

Anon1212 6 months, 4 weeks ago

This is Correct
upvoted 1 times

Percyles 1 year, 3 months ago
YES : windows 10 not affected by "network location " (only for android) so device has no policy and then marked a s compliance. (windows 10 device)
NO : IP adress of this device is not inside the requiered ip range location. (android device)
YES : IP adress of this device is inside the requiered ip range location. (android device)
upvoted 10 times

RodrigoT 5 months, 1 week ago
Perfect answer.
upvoted 1 times

Tomtom11 1 year, 4 months ago
Configure network locations - Supported by Android devices, you can configure network locations and then use those locations as a device compliance rule. This type of rule can flag a device as noncompliant when it's outside of or leaves a specified network. Before you can specify a Location rule, you must configure the network locations.
upvoted 4 times

Tomtom11 1 year, 4 months ago
Configure network locations - Supported by Android devices, you can configure network locations and then use those locations as a device compliance rule. This type of rule can flag a device as noncompliant when it's outside of or leaves a specified network. Before you can specify a Location rule, you must configure the network locations.
upvoted 3 times

GohanF2 1 year, 4 months ago
this is a tricky question. but , i will mark all the devices as compiant due that in the question says that i add "unrooted" devices to the cloud .... So, all the 3 devices are unrooted "specially the android devices" ... the policy for the android device doesnt have any effect due that it will apply only to "rooted" devices that are in network 1. so, the device that belongs to this network 1 is unrooted so this policy hasnt have any effect so... it will be marked as compliance.
its important to re-read the question many times
upvoted 2 times

hansetue 1 year, 5 months ago
Why is the Windows device compliant when it is an Android policy? even tough it fits the IP range.
upvoted 2 times

Testtest123 1 year, 5 months ago
Is this not
1 - No
2 - No
3 - Yes
Because the policy said 0/16 and device 1 is 35 at the end?
Can some one confirm or explain?
upvoted 1 times

1morenickname 1 year, 5 months ago
I'm not sure if you understand CIDR notation. The /16 at the end represents the subnet mask (255.255.0.0)
upvoted 3 times

dDadau 1 year, 1 month ago
Which results in what he said appart from a small mistakes
192.168.0.0 - 192.168.255.255 (including Network ID and Broadcast)
or
192.168.0.1 - 192.168.255.254 (excluding Network ID and Broadcoast)
upvoted 2 times

coleszczuk 1 year, 5 months ago
/16 is CIDR notation. 192.168.0.0/16 covers all IPs from 192.168.0.0 to 192.168.254.254
upvoted 4 times

Testtest123 1 year, 5 months ago
Thank you for the explenation.
upvoted 1 times

Question #50 *Topic 3*

You have an Azure Active Directory (Azure AD) tenant named adatum.com. The tenant contains Windows 10 devices that are enrolled in Microsoft Intune.
You create an Azure Log Analytics workspace and add the Update Compliance Solution to the workspace.
You need to create a custom device configuration profile that will enroll the Windows 10 devices in Update Compliance.
Which OMA-URI should you add to the profile?

A. ./Vendor/MSFT/DMClient/Provider/MS DM Server/Push

B. ./Vendor/MSFT/DMClient/Provider/MS DM Server/CommercialID

C. ./Vendor/MSFT/DMClient/Provider/MS DM Server/ManagementServerAddressList

D. ./Vendor/MSFT/DMClient/Provider/MS DM Server/Push/ChannelURI

Correct Answer: *B*
Deploy Commercial ID to Windows devices
Besides enabling Windows Telemetry, you will also need to configure the Commercial ID on all your Windows devices. For this we will use the following OMA-URI
(Open Mobile Alliance Uniform Resource Identifier) configuration:

Setting Name	Windows Analytics Commercial ID
Setting Description	Configuring commercial ID for Windows Analytics solutions
OMA-URI	./Vendor/MSFT/DMClient/Provider/MS DM Server/CommercialID
Data Type	String
Value	<your commercial ID>

Reference:
https://allthingscloud.blog/monitor-windows-10-updates-for-intune-mdm-enrolled-devices/

HOTSPOT -

You have 100 computers that run Windows 10. The computers are joined to Microsoft Azure Active Directory (Azure AD) and enrolled in Microsoft Intune.

You need to configure the following device restrictions:

- Block users from browsing to suspicious websites.
- Scan all scripts loaded into Microsoft Edge.

Which two settings should you configure in Device restrictions? To answer, select the appropriate settings in the answer area.

NOTE: Each correct selection is worth one point.

Hot Area:

Answer Area

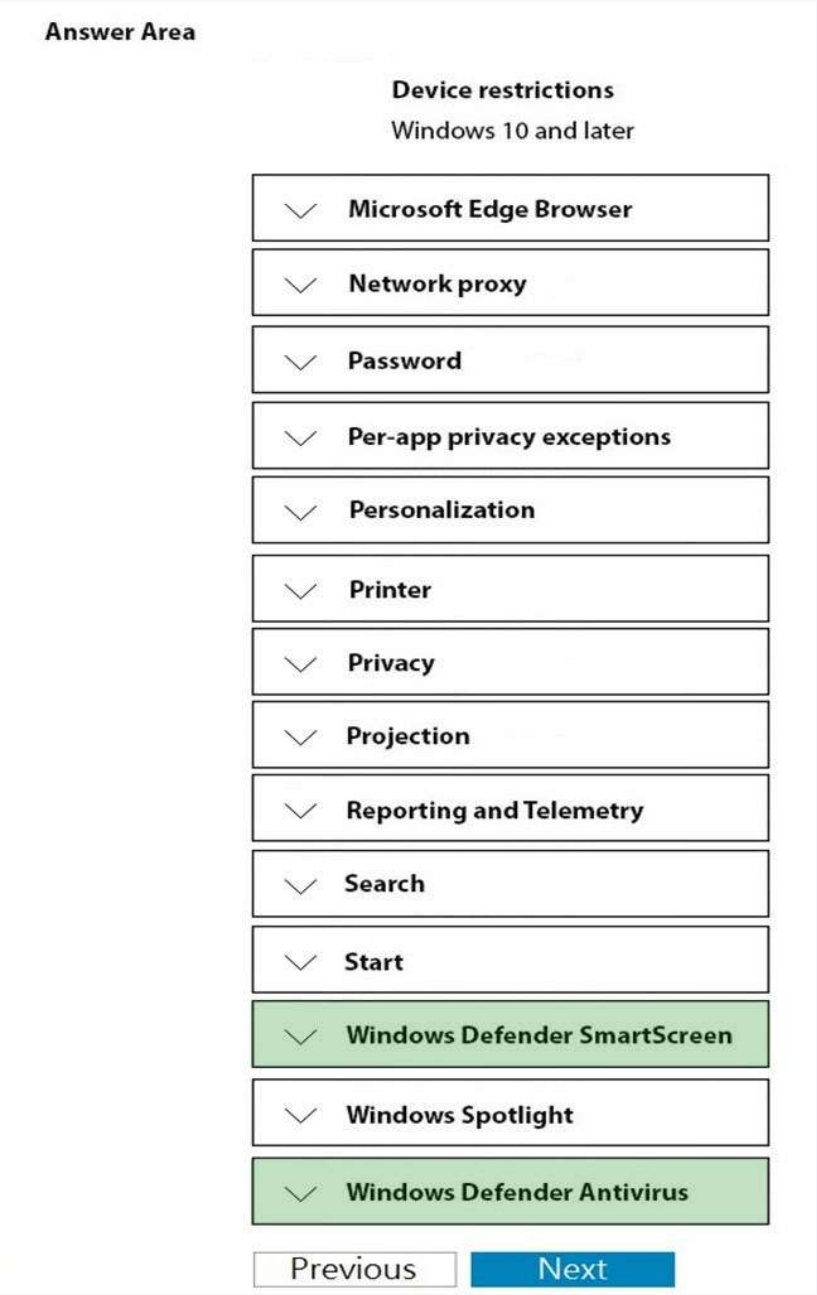
Device restrictions

Windows 10 and later

- Microsoft Edge Browser
- Network proxy
- Password
- Per-app privacy exceptions
- Personalization
- Printer
- Privacy
- Projection
- Reporting and Telemetry
- Search
- Start
- Windows Defender SmartScreen
- Windows Spotlight
- Windows Defender Antivirus

Previous Next

Correct Answer:



Box 1: Windows Defender SmartScreen

Block users from browsing to suspicious websites.

Microsoft Defender SmartScreen protects against phishing or malware websites and applications, and the downloading of potentially malicious files.

Microsoft Defender SmartScreen determines whether a site is potentially malicious

Box 2: Windows Defender Antivirus

Scan all scripts loaded into Microsoft Edge.

Reference:

https://docs.microsoft.com/en-us/windows/security/threat-protection/windows-defender-smartscreen/windows-defender-smartscreen-overview

lucadp010 Highly Voted 8 months, 2 weeks ago

Tested in my Endpoint Manager labs. Answer is correct.

upvoted 11 times

RodrigoT 5 months ago

Thank you for really testing.

upvoted 1 times

letters1234 Most Recent 7 months, 1 week ago

Not sure if this will still be asked as it's now default to have script scanning turned on by default

"Script scanning was a parity gap we had between Group Policy and MDM. Since this gap is now closed we are enforcing the enablement of script scanning (Windows Components\Microsoft Defender Antivirus\Real-time Protection\Turn on script-scanning)." Oct 2021

https://techcommunity.microsoft.com/t5/microsoft-security-baselines/windows-11-security-baseline/ba-p/2810772

upvoted 3 times

AVP_Riga 10 months, 3 weeks ago

Seems correct?! Any ideas?

upvoted 4 times

HOTSPOT -

You have computers that run Windows 10 as shown in the following table.

Name	Configuration
Computer1	Active Directory domain-joined
Computer2	Microsoft Azure Active Directory (Azure AD) –joined
Computer3	Hybrid Microsoft Azure Active Directory (Azure AD)-joined

Computer2 and Computer3 are enrolled in Microsoft Intune.

In a Group Policy object (GPO) linked to the domain, you enable the Computer Configuration/Administrative Templates/Windows Components/Search/Allow Cortana setting.

In an Intune device configuration profile that is assigned to an Azure Active Directory group that includes Computer2 and Computer3, you configure the following:

⇨ Device/Vendor/MSFT/Policy/Config/ControlPolicyConflict/MDMWinsOverGP to a value of 1

Experience/AllowCortana to a value of 0.

▪

Each of the following statement, 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 can use Cortana for each.	○	○
Computer2 can use Cortana for search.	○	○
Computer3 can use Cortana for search.	○	○

Correct Answer:

Answer Area

Statements	Yes	No
Computer1 can use Cortana for each.	○	○
Computer2 can use Cortana for search.	○	○
Computer3 can use Cortana for search.	○	○

Reference:

https://blogs.technet.microsoft.com/cbernier/2018/04/02/windows-10-group-policy-vs-intune-mdm-policy-who-wins/

junior6995 3 weeks, 2 days ago

Answer looks right

Computer 1 not linked to Intune = Can use Cortana
Computer 2 is Intune only = Cannot use Cortana
Computer 3 is hybrid but as the we set the value of "MDMWinsOverGP" to 1, Intune wins over GPO = Cannot use Cortana

upvoted 2 times

Question #53 *Topic 3*

Your company plans to deploy Windows 10 to devices that will be configured for English use and other devices that will be configured for Korean use.
You need to create a single multivariant provisioning package for the planned devices.
You create the provisioning package.
What should you do next to add the language settings to the package?

A. Modify the Customizations.xml file.

B. Create a file named Languages.xml that contains a header for Korean.

C. Modify the .ppkg file.

D. Create a file named Languages.xml that contains a header for English.

Correct Answer: *A*
Follow these steps to create a provisioning package with multivariant capabilities.
1. Build a provisioning package and configure the customizations you want to apply during certain conditions.
2. After you've configured the settings, save the project.
3. Open the project folder and copy the customizations.xml file to any local location.
4. Use an XML or text editor to open the customizations.xml file.
5. Edit the customizations.xml file to create a Targets section to describe the conditions that will handle your multivariant settings.
6. In the customizations.xml file, create a Variant section for the settings you need to customize.
7. Save the updated customizations.xml file and note the path to this updated file. You will need the path as one of the values for the next step.
8. Use the Windows Configuration Designer command-line interface to create a provisioning package using the updated customizations.xml.
Reference:
https://docs.microsoft.com/en-us/windows/configuration/provisioning-packages/provisioning-multivariant

Anthony_2770 Highly Voted 1 year, 8 months ago
Answer is Correct.
Refer to the supplied reference
upvoted 16 times

Perycles Highly Voted 1 year, 3 months ago
answer is correct.
upvoted 6 times

shaolin_monk Most Recent 2 months ago
A: Is correct, supplied link is correct.
https://docs.microsoft.com/en-us/windows/configuration/provisioning-packages/provisioning-multivariant
upvoted 1 times

b3arb0yb1m 9 months, 2 weeks ago
A. Modify the Customizations.xml file.
upvoted 5 times

Question #54 *Topic 3*

Your network contains an Active Directory domain that is synced to Microsoft Azure Active Directory (Azure AD).
You have a Microsoft 365 subscription.
You create a conditional access policy for Microsoft Exchange Online.
You need to configure the policy to prevent access to Exchange Online unless a user is connecting from a device that is hybrid Azure AD-joined.
Which settings should you configure?

A. Locations

B. Device platforms

C. Sign-in risk

D. Device state

Correct Answer: *D*
The device state condition was used to exclude devices that are hybrid Azure AD joined and/or devices marked as compliant with a Microsoft Intune compliance policy from an organization's Conditional Access policies.
Reference:
https://docs.microsoft.com/en-us/azure/active-directory/conditional-access/conditions#device-state

Perycles Highly Voted 1 year, 3 months ago
"Device state" : Control user access when the device the user is signing-in from is not "Hybrid Azure AD joined" or "marked as compliant" : answer is correct.

https://docs.microsoft.com/fr-fr/azure/active-directory/conditional-access/concept-conditional-access-conditions#device-state-preview
upvoted 9 times

RodrigoT 5 months, 1 week ago
And in English:
https://docs.microsoft.com/en-us/azure/active-directory/conditional-access/concept-conditional-access-conditions#device-state-preview
upvoted 2 times

shaolin_monk Most Recent 2 months ago
D: Device State.
"The device state condition was used to exclude devices that are hybrid Azure AD joined and/or devices marked as compliant with a Microsoft Intune compliance policy from an organization's Conditional Access policies."
upvoted 1 times

Brent0n 6 months, 3 weeks ago
This setting has been depricated:

Customers should use Filter for devices condition in Conditional Access to satisfy scenarios, previously achieved using device state (preview) condition.
https://docs.microsoft.com/en-us/azure/active-directory/conditional-access/concept-conditional-access-conditions#device-state-preview
upvoted 3 times

MR_Eliot 5 months ago
Above is true.
upvoted 1 times

b3arb0yb1m 9 months, 1 week ago
D. Device state
upvoted 2 times

sifa 1 year, 4 months ago
D is the correct answer.
upvoted 4 times

Question #55 *Topic 3*

You have 200 computers that run Windows 10. The computers are joined to Microsoft Azure Active Directory (Azure AD) and enrolled in Microsoft Intune.
You redirect Windows known folders to Microsoft OneDrive for Business.
Which folder will be included in the redirection?

A. Saved Games

B. Documents

C. Music

D. Downloads

E. Favorites

F. AppData

G. Videos

Correct Answer: *B*
There are two primary advantages of moving or redirecting Windows known folders (Desktop, Documents, Pictures, Screenshots, and Camera Roll) to Microsoft
OneDrive for the users in your domain:
Your users can continue using the folders they're familiar with. They don't have to change their daily work habits to save files to OneDrive.
Saving files to OneDrive backs up your users' data in the cloud and gives them access to their files from any device.
Reference:
https://docs.microsoft.com/en-us/onedrive/redirect-known-folders

Technik Highly Voted 1 year, 5 months ago
Desktop, Documents, Pictures, Screenshots, and Camera Roll are known folders
upvoted 22 times

RodrigoT 5 months ago
They use the word "redirection" just to confuse us.
upvoted 1 times

Anna_Peters Highly Voted 1 year, 5 months ago
Yes.Answer is correct.
upvoted 7 times

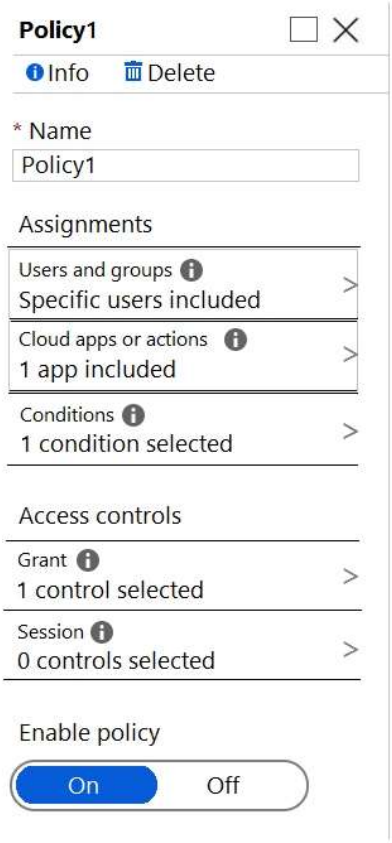
Perycles Most Recent 1 year, 3 months ago
B only.
upvoted 5 times

sifa 1 year, 4 months ago
B is correct.
upvoted 4 times

Question #56 *Topic 3*

You have a Microsoft 365 subscription.

You have a conditional access policy that requires multi-factor authentication (MFA) for users in a group name Sales when the users sign in from a trusted location. The policy is configured as shown in the exhibit. (Click the Exhibit tab.)



You create a compliance policy.

You need to ensure that the users are authenticated only if they are using a compliant device.

What should you configure in the conditional access policy?

A. a condition

B. a session control

C. a cloud app

D. a grant control

Correct Answer: *A*

The device state condition can be used to exclude devices that are hybrid Azure AD joined and/or devices marked as compliant with a Microsoft Intune compliance policy from an organization's Conditional Access policies.

Device state is located on the Condition tab.

Reference:

https://docs.microsoft.com/en-us/azure/active-directory/conditional-access/concept-conditional-access-conditions#device-state

RajeeMark Highly Voted 1 year, 4 months ago

D. "Grant - Grant Access - Require device to be marked as compliant".

upvoted 18 times

RodrigoT 5 months, 1 week ago

And what scares me the most is that you were upvoted 17 times even giving a wrong answer.
I tested in my tenant: Create a conditional Access policy > Conditions > Locations > Configure: Yes > "All trusted locations" or "Selected locations". You simply can NOT chose locations in any other setting.
Of course you have to first create you Named locations on Azure portal to be able to choose them after.
First step:
https://docs.microsoft.com/en-us/azure/active-directory/conditional-access/location-condition#location-condition-configuration
Second step (this question):
https://docs.microsoft.com/en-us/azure/active-directory/conditional-access/concept-conditional-access-conditions

upvoted 4 times

51007 4 months ago

I think you are confused. The Cond. access policy given to us already the trusted location requirement configured under 'conditions'- one selected. The diagram doesnt show it, but I can see in my tenant. Then the 1 control selected under Access controls/Grant is(probably) MFA. This is all based on the first paragraph and diagram giving us the known state of the cond. access policy.

Then we create a new comp. policy. And we need to go into the existing Cond. Access policy to make sure the Cond Access policy will require compliance. Grant-->MFA would already be checked. We need to add Grant-->Require Device Compliance.

upvoted 7 times

Perycles Highly Voted 1 year, 3 months ago

D is correct : "Require device to be marked as compliant" enabled in 'Grant' options

upvoted 14 times

RodrigoT 5 months ago

And where in that setting do you read "trusted location"? It's simply impossible. It's not there. It's in "Condition". I TESTED in my tenant.

upvoted 1 times

TonySuccess Most Recent 3 days, 9 hours ago

Selected Answer: B

1 Million % B, please sort this one out Mods.

upvoted 1 times

Jnorris 1 month, 1 week ago

Selected Answer: A

After reviewing other source materials since it requires location AND compliance I believe A is the correct answer.

upvoted 1 times

Vernon_max22 2 months, 2 weeks ago

Selected Answer: D

The answer is D. The policy shown in the diagram is already configured. The language they use “you HAVE a conditional access policy that requires mfa...” they aren’t asking you to set a location. They are asking you to create a policy that requires devices to be marked compliant.

upvoted 1 times

Whatsamattr81 3 months, 2 weeks ago

"You need to ensure that the users are authenticated only if they are using a compliant device." - That's Grant, condition is just to get it to be marked compliant, grant is a gatekeeper for that.

upvoted 1 times

AzureLearner01 3 months, 3 weeks ago

In my opinion this question isn‘t asking for any location based configurations, it is asking about implementing the compliant devices in this Policy. „You create a compliance policy.
You need to ensure that the users are authenticated only if they are using a compliant device.“ In the meantime there are 2 valid methods for an implementation. First method is in Conditions -> Filter for devices -> Include filtered devices in policy -> Rule syntax device.isCompliant -eq true.
Second method which is maybe the „native“ one is under Grant -> Grant Access -> Reqire device to be marked as compliant. Maybe the second one is the Microsoft way of accomplishing this goal, so i think D is a valid solution.

upvoted 2 times

Gabry96 3 months, 3 weeks ago

Deprecated https://docs.microsoft.com/en-us/azure/active-directory/conditional-access/concept-conditional-access-conditions#device-state-deprecated

upvoted 1 times

Gabry96 3 months, 3 weeks ago

Customers should use the Filter for devices condition in the Conditional Access policy, to satisfy scenarios previously achieved using device state (preview) condition. In section: "Conditions"

upvoted 1 times

Garito 7 months, 1 week ago

Selected Answer: D

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

Require device to be marked as compliant (Microsoft Intune)

upvoted 4 times

RodrigoT 5 months, 1 week ago

And where is the trusted location in this setting? Answer is A my friend. I tested in my tenant.

upvoted 1 times

Bouncy 7 months, 1 week ago

Selected Answer: D

D (vote distribution is still 50-50 between D and A hence this comment)

upvoted 2 times

chewitt 7 months, 2 weeks ago

Selected Answer: D

Tested in tenant answer is D

upvoted 3 times

RodrigoT 5 months, 1 week ago

And that is how to fail on an exam! The question states clearly that the users must "sign in from a trusted location". You are confusing with the end where it says "using a compliant device". Compliant with the location!
I tested in my tenant: Create a conditional Access policy > Conditions > Locations > Configure: Yes > "All trusted locations" or "Selected locations". You simply can NOT use locations in any other way.

upvoted 2 times

Alvaroll 8 months ago

In fact, we can control compliance state in both places.
Now we have to use "FIlter for devices" instead of "Device State" because is being deprecated.

https://docs.microsoft.com/en-us/azure/active-directory/conditional-access/concept-condition-filters-for-devices
upvoted 2 times

lucadp010 8 months, 1 week ago

Selected Answer: D

D.
Grant --> Grant Access --> Require device to be marked as compliant
upvoted 2 times

IykeP 8 months, 2 weeks ago

Selected Answer: A

A is the correct Answer, TESTED!!!
upvoted 4 times

lucadp010 8 months, 1 week ago

What did you test it?
Absolutely D, Grant --> Grant Access --> Require device to be marked as compliant
upvoted 1 times

RodrigoT 5 months, 1 week ago

Wrong dude, it's impossible to chose a trusted location in Grant. IykeP is 100% right.
upvoted 1 times

moobdoob 8 months, 2 weeks ago

Selected Answer: D

CORRECT ANSWER: D
upvoted 2 times

jibutoms 1 year, 3 months ago

A is correct. "All Trusted location" has to be added in Locations under conditions. As per this condition, grant controls can prompt MFA
upvoted 4 times

Cabanna94 1 year, 2 months ago

I think (based off of Policy1 in the the exhibit) that the location is already configured under "condition" which is a place you can require MFA as well . The question is ultimately asking how to ensure the users are using compliant devices. That requirement can be configured under "Grant". I would go with D.

Info on Grants: https://docs.microsoft.com/en-us/azure/active-directory/conditional-access/concept-conditional-access-grant

Info on Locations under Conditions:
https://docs.microsoft.com/en-us/azure/active-directory/conditional-access/location-condition
upvoted 4 times

bertik 1 year, 4 months ago

I think its D >
In every MS article I have had found, compliance is under the "Grand" section.

https://docs.microsoft.com/en-us/microsoft-365/security/office-365-security/identity-access-policies?view=o365-worldwide#require-compliant-pcs-and-mobile-devices
upvoted 2 times

Jimbob77 1 year, 4 months ago

If I had this question in the exam I would go with A: a condition
But the Grant control can Block/Grant based on one/all of these conditions:
- MFA
- Require device to be compliant
- Require Hybrid AD join
https://docs.microsoft.com/en-us/azure/active-directory/conditional-access/require-managed-devices
Not sure who has the correct answer here ...
upvoted 1 times

Question #57 *Topic 3*

You have an Azure Active Directory (Azure AD) tenant that contains a user named User1. User1 has the devices shown in the following table.

Name	Operating system	Version	Join type	Mobile device management (MDM)
Device1	Windows	10.0.18362.0	Azure AD registered	*None*
Device2	Windows	10.0.18362.30	Azure AD registered	Microsoft Intune
Device3	Windows	10.0.18362.0	Azure AD joined	*None*
Device4	Windows	10.0.18362.30	Azure AD joined	Microsoft Intune

Enterprise State Roaming is configured for User1.

User1 signs in to Device4 and changes the desktop.

You need to identify on which devices User1 will have a changed desktop.

Which devices should you identify?

A. Device1, Device2, Device3, and Device4

B. Device4 only

C. Device2, Device3, and Device4 only

D. Device2 and Device4 only

E. Device3 and Device4 only

Correct Answer: *E*

The requirements of Enterprise State Roaming are:

- Windows 10, with the latest updates, and a minimum Version 1511 (OS Build 10586 or later) is installed on the device.
- The device is Azure AD joined or hybrid Azure AD joined.
- Ensure that Enterprise State Roaming is enabled for the tenant in Azure AD.

The user is assigned an Azure Active Directory Premium license.

-
- The device must be restarted and the user must sign in again to access Enterprise State Roaming features.

Reference:

https://docs.microsoft.com/en-us/azure/active-directory/devices/enterprise-state-roaming-troubleshooting

Jana08 Highly Voted 1 year, 2 months ago

Answer is E. Device3 and Device4 Only.

Microsoft state in the key capabilities of Azure AD joined devices: "Enterprise State Roaming across devices"

Microsoft do not state this in the key capabilities of Azure AD registered Devices. I have provided links to both pages below to support this. Check the "Key Capabilites" in the table in the references provided.

Sources:
Azure AD Joined: https://docs.microsoft.com/en-us/azure/active-directory/devices/concept-azure-ad-join

Azure AD Registered: https://docs.microsoft.com/en-us/azure/active-directory/devices/concept-azure-ad-register

upvoted 12 times

Jana08 1 year, 2 months ago

Microsoft seem to be very inconsistent with their documentation regarding this. I have now found the following statement on a Microsoft document regarding ESR troubleshooting:

"Enterprise State Roaming requires the device to be registered with Azure AD."

https://docs.microsoft.com/en-us/azure/active-directory/devices/enterprise-state-roaming-troubleshooting#:~:text=Verify%20the%20device,Client%20is%20registered

upvoted 2 times

RodrigoT 5 months ago

You're right the documentation is very confusing. But on your link if you keep reading, on the point 3, it says: "For expected output, the AzureAdJoined field value should be “YES”.

upvoted 2 times

Merma Highly Voted 1 year, 5 months ago

We need more discussion on this topic. I can't find anything about Intune and ESR. Being Azure AD joined, (not registered) seems to be the key. It seems Azure AD registered (employee owned) devices are not included in ESR. Other thoughts or reference links?
From what I can find E. Device3 and Device4 only seems to be the correct answer.
https://docs.microsoft.com/en-us/azure/active-directory/devices/enterprise-state-roaming-windows-settings-reference
https://docs.microsoft.com/en-us/answers/questions/33891/difference-between-azure-ad-registered-azure-ad-jo.html

upvoted 11 times

JeremyBearimy7 1 year, 4 months ago

I searched far and wide but I can't really find a lot of resources on wether devices should be Azure AD joined or registered.
One of the things I could find was:
The first thing you need to do when troubleshooting Enterprise State Roaming is check your configuration. This includes ensuring that Windows 10 has the latest updates installed, check that the device which is having issues is Azure AD joined, and as we've just seen, you'll need to ensure that you've enabled Enterprise State Roaming in the Azure AD admin center.
Source: https://www.linkedin.com/learning/windows-10-troubleshooting-cloud-integration/azure-ad-enterprise-state-roaming
This source seems to suggest you need Azure AD joined devices so i'm inclined to agree with answer D as well.

upvoted 1 times

gotrekk Most Recent 1 month, 2 weeks ago

Selected Answer: E

ESR required a joined device

upvoted 1 times

MR_Eliot 5 months ago

Selected Answer: A

A is the correct answer. I have tested this in my lab.
Enterprise Roaming will work as long as you're logged on with your Microsoft account.

upvoted 3 times

Cisco 5 months ago

I am going with E based on this comment:

Verify sync, and the “Sync your settings” settings page

After joining your Windows 10 or newer PC to a domain that is configured to allow Enterprise State Roaming, sign on with your work account. Go to Settings > Accounts > Sync Your Settings and confirm that sync and the individual settings are on, and that the top of the settings page indicates that you are syncing with your work account

It clearly says after"JOINING" your Windows 10 or newer PC.
https://docs.microsoft.com/en-us/azure/active-directory/devices/enterprise-state-roaming-troubleshooting#preliminary-steps-for-troubleshooting

upvoted 1 times

defrey 8 months, 3 weeks ago

hmmm, ESR works for both registered & joined devices..I will say all devices

upvoted 2 times

RodrigoT 5 months, 1 week ago

Wrong. You set this on Azure, not Endpoint) > Devices | Enterprise State Roaming.
Answer is E.

upvoted 1 times

jorlloen 1 year, 1 month ago

Copy and paste from Official documentation for MD-101: "Enterprise State Roaming syncs settings across Azure AD joined devices and provides users with the same experience across their devices".
And from this link https://docs.microsoft.com/en-us/azure/active-directory/devices/enterprise-state-roaming-troubleshooting you can see :
"2. The device is Azure AD joined or hybrid Azure AD joined. For more information, see how to get a device under the control of Azure AD"

For me the correct answer is E.

upvoted 7 times

ercluff 1 year, 2 months ago

Check out contrasting articles from Microsoft: This one - https://docs.microsoft.com/en-us/azure/active-directory/devices/concept-azure-ad-register does not show that registered devices can use Enterprise State Roaming. While this one - https://docs.microsoft.com/en-us/azure/active-directory/devices/concept-azure-ad-join does show that. Also, this one -https://docs.microsoft.com/en-us/azure/active-directory/devices/concept-azure-ad-join-hybrid shows devices that are hybrid AAD joined can utilize Enterprise State Roaming. Therefore only Joined and Hybrid-Joined, not merely Registered devices, will benefit from the ESR feature.

upvoted 1 times

ercluff 1 year, 2 months ago

I would answer E.

upvoted 1 times

Angarali 1 year, 2 months ago

Answer is correct, all devices.

https://docs.microsoft.com/en-us/azure/active-directory/devices/enterprise-state-roaming-enable

upvoted 1 times

Whatsamattr81 3 months, 2 weeks ago

Cant see anywhere on that link that mentions 'registered'... Registered = BYOD, Joined = Full Fat Experience. That article mentions Joined or Hybrid Joined only. Makes the logical answer E.

upvoted 1 times

Perycles 1 year, 3 months ago

3 and 4 only. On Registered devices, unable to logon with Azure AD users.

upvoted 10 times

RajeeMark 1 year, 4 months ago

If you sign in to an Azure AD PC that is either registered or joined, the PC will download your settings from Azure when enterprise roaming is enabled on an other device signed in with the same user.

upvoted 2 times

Jimbob77 1 year, 4 months ago

I would go with answer E: Devices 3 and 4
They're Azure AD joined so User1 would authenticate when they login. The Azure Registered devices could be BYOD, local login account and 'not syncing' (they're not referenced below).
https://docs.microsoft.com/en-us/azure/active-directory/devices/enterprise-state-roaming-enable#view-per-user-device-sync-status
For a Windows 10 device to use the Enterprise State Roaming service, the device must authenticate using an Azure AD identity. For devices that are joined to Azure AD, the user's primary sign-in identity is their Azure AD identity, so no additional configuration is required. For devices that use on-premises Active Directory, the IT admin must Configure hybrid Azure Active Directory joined devices.

upvoted 2 times

Jimbob77 1 year, 4 months ago

Changing to Answer: A (all of them)
"Verify the device registration status.
Enterprise State Roaming requires the device to be registered with Azure AD. .. "
From the URL they provided (oops):
https://docs.microsoft.com/en-us/azure/active-directory/devices/enterprise-state-roaming-troubleshooting

upvoted 1 times

Prianishnikov 1 year ago

No, if you correct read this article, you can see - The device is Azure AD joined or hybrid Azure AD joined on https://docs.microsoft.com/en-us/azure/active-directory/devices/enterprise-state-roaming-troubleshooting#preliminary-steps-for-troubleshooting

upvoted 1 times

Malfureeon 1 year, 4 months ago

Given answer is correct. Even if a device is registered to Azure, that is enough for ESR.

upvoted 1 times

Danohav 1 year, 4 months ago

This one is really confusing :/
Based on the info here (check Key capabilities):
https://docs.microsoft.com/en-us/azure/active-directory/devices/concept-azure-ad-register
https://docs.microsoft.com/en-us/azure/active-directory/devices/concept-azure-ad-register
Enterprise State Roaming across devices is only a key capability of AAD joined devices.

However here:
https://docs.microsoft.com/en-us/azure/active-directory/devices/concept-azure-ad-join-hybrid it states that:
"If your environment has an on-premises AD footprint and you also want benefit from the capabilities provided by Azure Active Directory, you can implement hybrid Azure AD joined devices. These devices, are devices that are joined to your on-premises Active Directory and registered with your Azure Active Directory."
And is Enterprise State Roaming across devices capable.

upvoted 1 times

Tiit 1 year, 4 months ago

Should be A - "Enterprise State Roaming is a feature for Windows 10 users that are using a device which is Azure AD device registered (either AAD joined or hybrid joined)."

upvoted 3 times

jeff198807 1 year, 4 months ago

correct awnser is A

upvoted 1 times

GohanF2 1 year, 5 months ago

the answer is correct but the question still needs more information . it should have said that the user as a premium azure active directory license.
How do Microsoft account and Azure AD Enterprise State Roaming interoperability work?
In the November 2015 or later releases of Windows 10, Enterprise State Roaming is only supported for a single account at a time. If you sign in to Windows by using a work or school Azure AD account, all data will sync via Azure AD. If you sign in to Windows by using a personal Microsoft account, all data will sync via the Microsoft account. Universal appdata will roam using only the primary sign-in account on the device, and it will roam only if the app's license is owned by the primary account. Universal appdata for the apps owned by any secondary accounts will not be synced.
https://docs.microsoft.com/en-us/azure/active-directory/devices/enterprise-state-roaming-faqs

upvoted 2 times

Question #58 *Topic 3*

You have an Azure Active Directory (Azure AD) tenant named adatum.com that contains two computers named Computer1 and Computer2. The computers run
Windows 10 and are members of a group named GroupA.
The tenant contains a user named User1 that is a member of a group named Group1.
You need to ensure that if User1 changes the desktop background on Computer1, the new desktop background will appear when User1 signs in to Computer2.
What should you do?

A. Create a device configuration profile for Windows 10 and configure the Shared multi-user device settings. Assign the profile to Group1.

B. Create a device configuration profile for Windows 10 and configure the Shared multi-user device settings. Assign the profile to GroupA.

C. From the Azure Active Directory admin center, enable Enterprise State Roaming for Group1.

D. From the Azure Active Directory admin center, enable Enterprise State Roaming for GroupA.

Correct Answer: *C*
Enterprise State Roaming provides users with a unified experience across their Windows devices and reduces the time needed for configuring a new device.
Reference:
https://docs.microsoft.com/en-us/azure/active-directory/devices/enterprise-state-roaming-enable

lijk_manson Highly Voted 12 months ago
This one will be C
upvoted 16 times

RodrigoT 5 months, 1 week ago
Exactly! It's one user and two computers, not multi-user, for goodness sake.
upvoted 1 times

GazzMann Highly Voted 11 months, 1 week ago
I think C is the current answer.
upvoted 11 times

TonySuccess Most Recent 2 weeks, 2 days ago
Selected Answer: C
C for real.
upvoted 1 times

Brent0n 6 months, 3 weeks ago
I bet the answers are on a dart board and picked at random.
upvoted 2 times

RodrigoT 5 months, 1 week ago
I ask the moderators that I am paying as a contributor: please correct the huge amount of wrong answers. Thank you.
upvoted 1 times

4Shawsy 7 months, 3 weeks ago
Selected Answer: C
Defo C
upvoted 3 times

Djaboloke 8 months ago
Selected Answer: C
C for sure
upvoted 2 times

mayleni 8 months, 2 weeks ago
Selected Answer: C
Letter C for sureeee
upvoted 3 times

lucadp010 8 months, 2 weeks ago
Selected Answer: C
C for sure! Stop incorrect answes!
upvoted 2 times

moobdoob 8 months, 2 weeks ago
Correct answer: C
upvoted 2 times

IykeP 8 months, 3 weeks ago
Selected Answer: C

The Correct answer is C. I've had enough of all these incorrect Answers.
upvoted 10 times

SirTreebeard 8 months, 3 weeks ago
Pretty sure its on purpose. Which is why I am glad for these discussions.
upvoted 2 times

defrey 8 months, 3 weeks ago
C all the way...
upvoted 2 times

Goofer 10 months, 3 weeks ago
C. From the Azure Active Directory admin center, enable Enterprise State Roaming for Group1.
upvoted 5 times

ANDREVOX 11 months, 3 weeks ago
User 1 using Computer 1 and 2, thus 1 user using 2 computers not Multiple Users using 1 computer.
A is for multiple users using one device.

ESR is applied (enabled) to (for) a user or a Group of users, thus correct answer = C
upvoted 8 times

Question #59 *Topic 3*

You have a Microsoft 365 tenant that contains the devices shown in the following table.

Name	Platform	(Azure Active Directory) Azure AD join type	Managed by using Microsoft Intune
Device1	Windows 10	Joined	Yes
Device2	Android	Registered	Yes
Device3	iOS	**None**	Yes
Device4	Windows 10	**None**	No
Device5	iPadOS	Registered	No

You need to assign app protection settings to the devices.

What is the minimum number of app protection policies required?

A. 1

B. 2

C. 3

D. 4

E. 5

Correct Answer: *B*

One for Android, and one for iOS/iPadOS.

When you create an app protection policy for iOS/iPadOS and Android apps, you follow a modern Intune process flow that results in a new app protection policy.

Create an iOS/iPadOS or Android app protection policy.

1. Sign in to the Microsoft Endpoint Manager admin center.
2. Select Apps > App protection policies. This selection opens the App protection policies details, where you create new policies and edit existing policies.
3. Select Create policy and select either iOS/iPadOS or Android. The Create policy pane is displayed.
4. Etc.

Reference:

https://docs.microsoft.com/en-us/mem/intune/apps/app-protection-policies

lijk_manson Highly Voted 12 months ago

This need to be C. 3

upvoted 13 times

lijk_manson 10 months, 2 weeks ago

No this one is 4, Windows 10 needs 2 with and without enrollmend

upvoted 4 times

RodrigoT 5 months, 1 week ago

You're wrong my friend, for Windows 10 just chose "without enrollment" and it will work on any Win10 device because is applied to the app by MAM. Answer is C.3.

upvoted 1 times

raduM 1 week, 2 days ago

false. you need 2

upvoted 1 times

CARO54 Highly Voted 9 months ago

Just tested : 4 Application protection policy
- 1 for Android
- 1 for iOS/iPad
- 2 for Windows - with enrollment and without enrollment

upvoted 6 times

RodrigoT 5 months, 1 week ago

You don't need to create 2 policies for Windows 10. Just chose "without enrollment" and you are good to go.

upvoted 1 times

ZiOoi Most Recent 10 hours, 37 minutes ago

Selected Answer: C

1 for android, ios, windows each.

upvoted 1 times

Bukaj 3 days, 6 hours ago

I think i need to take some Crazy pills for some Answers...

upvoted 1 times

AVR31 5 months, 1 week ago

Selected Answer: B

One policy is needed for the mobile OSes (Android and iOS) and one for Windows. The fact the the device is managed by Inune or not is irellevant for the newest iteration of Intune.

upvoted 1 times

rj_client 6 months, 3 weeks ago

I think its 2 because WIP is never mentioned.

App protection policies for iOS/iPadOS and Android apps
When you create an app protection policy for iOS/iPadOS and Android apps, you follow a modern Intune process flow that results in a new app protection policy. For information about creating app protection policies for Windows apps, see Create and deploy Windows Information Protection (WIP) policy with Intune.

upvoted 3 times

Garito 7 months, 1 week ago

Selected Answer: D

Earlier Comment: I checked it in the endpoint manager. Apps --> App Protection Policies --> Create Policy
The options "with enrollment" and "without enrollment" are only available for Windows. iOS and iPadOS are in the same policy.
That is why i still take D - 4

upvoted 2 times

RodrigoT 5 months, 1 week ago

The "minimum" is 3. Just chose without enrollment and the app will be protected.

upvoted 2 times

4Shawsy 7 months, 3 weeks ago

Selected Answer: B

I say the answer is correct B as AppProtection is only available for Android / iOS. Even though there is a W10 option in AppProtection it actually creates WIP profiles not AppProtection.

upvoted 2 times

Angarali 6 months, 2 weeks ago

https://docs.microsoft.com/en-us/microsoft-365/admin/devices/protection-settings-for-windows-10-devices?view=o365-worldwide

upvoted 1 times

mayleni 8 months, 2 weeks ago

Selected Answer: D

D.
4 policies because you need 1 for W10 without enrollment
1 W10 enrolled
1 android
1 ipados an ios

upvoted 4 times

lucadp010 8 months, 2 weeks ago

Selected Answer: D

D.
One for Windows 10 with enrollment
One for Windows 10 without enrollment
One for Andorid (you can't set with or without enrollment)
One for iOS/iPadOS (you can't set with or without enrollment)

upvoted 3 times

moobdoob 8 months, 2 weeks ago

NOTE:
Windows 10 joined and NONE.

Therefore the answer is 4, as there needs to be 2 separate policies for Windows 10. One with and without enrollment.

upvoted 1 times

moobdoob 8 months, 2 weeks ago

Right answer: 4

upvoted 1 times

IykeP 8 months, 3 weeks ago

Selected Answer: C

App protection policies can apply to apps running on devices that may or may not be managed by Intune. So therefore, 1 policy for Windows 10, 1 for Android and 1 for iOS/iPADOS.

upvoted 1 times

ercluff 9 months ago

Only two policies are needed since only Android and iOS/iPadOS platforms are served by MAM app protection policies. Windows and macOS can be served by Windows Information Protection policies. Reference: https://docs.microsoft.com/en-us/mem/intune/apps/app-management#app-management-capabilities-by-platform (Superscript1 on the Windows column for 'Protect company data in apps with app protection policies' states: “Consider using Windows Information Protection to protect apps on devices that run Windows 10/11.”) Also, the column for MacOS has a NO on this item.

upvoted 2 times

J2daizzo412 9 months, 4 weeks ago

Isn't this 2? App protection policies apply to android and iOS. WIP applies to windows and isn't mentioned.

upvoted 3 times

Webleyboy 11 months ago

NOV-05-2021 | The question is about App Protection Policy.
*App protection policies for iOS/iPadOS and Android apps.

So Answer B: 2 is correct. Android en iOS only. Not Windows.
Reference:
https://docs.microsoft.com/en-us/mem/intune/apps/app-protection-policies
upvoted 3 times

Goofer 10 months, 3 weeks ago
When you creat an Application protection policy you can select:
1. iOS/iPadOS
2. Android
3. Windows 10 and later
Answer C: 3 is correct
upvoted 2 times

anzer123 11 months, 1 week ago
The answer is C
1 policy for the Windows devices
1 Policy for android
1 policy for iPadOS/iOS
upvoted 5 times

Question #60 *Topic 3*

You have following types of devices enrolled in Microsoft Intune:

- Windows 10
- Android
- iOS

For which types of devices can you create VPN profiles in Microsoft Endpoint Manager?

A. Windows 10 only

B. Windows 10 and Android only

C. Windows 10 and iOS only

D. Windows 10, Android, and iOS

E. Android and iOS only

Correct Answer: *D*
You can create VPN profiles for Android, Android Enterprise, iOS/iPadOS, macOS, Windows 10 and later, and Windows 8.1 devices.
Reference:
https://docs.microsoft.com/en-us/mem/intune/configuration/vpn-settings-android

examkiller321 Highly Voted 11 months, 2 weeks ago
Correct, you can create profiles for Windows, Android, iOS.
upvoted 10 times

examkiller321 11 months, 2 weeks ago
Sources
Windows: https://docs.microsoft.com/en-us/mem/intune/configuration/vpn-settings-windows-10
Android: https://docs.microsoft.com/en-us/mem/intune/configuration/vpn-settings-android
iOS/iPadOS: https://docs.microsoft.com/en-us/mem/intune/configuration/vpn-settings-ios
upvoted 5 times

RodrigoT 5 months, 1 week ago
Right, tested on my tenant.
upvoted 2 times

TonySuccess Most Recent 2 weeks, 2 days ago
Selected Answer: D
D fo sho
upvoted 1 times

HOTSPOT -

You have a Microsoft 365 tenant that uses Microsoft Intune to manage the devices shown in the following table.

Name	Platform
Device1	Windows 10
Device2	Android device administrator
Device3	Android Enterprise
Device4	iOS
Device5	iPadOS

You need to deploy a compliance solution that meets the following requirements:

- Marks the devices as Not Compliant if they do not meet compliance policies
- Remotely locks noncompliant devices

What is the minimum number of compliance policies required, and which devices support the remote lock action? To answer, select the appropriate options in the answer area.

NOTE: Each correct selection is worth one point.

Hot Area:

Answer Area

Minimum number of compliance policies required: [▼]
- 1
- 2
- 3
- 4
- 5

Devices that support the remote lock action: [▼]
- Device1 only
- Device2 and Device3 only
- Device4 and Device5 only
- Device2, Device3, Device4, and Device5
- Device1, Device2, Device3, Device4, and Device5

Correct Answer:

Answer Area

Minimum number of compliance policies required: [▼]
- 1
- 2
- 3
- 4
- 5

Devices that support the remote lock action: [▼]
- Device1 only
- Device2 and Device3 only
- Device4 and Device5 only
- Device2, Device3, Device4, and Device5
- Device1, Device2, Device3, Device4, and Device5

Box 1: 4 -

Windows, Android Enterprise, Android, and one for iOS/iPAD.

Box 2: Device2, Device3, Device4, and Device5

Remote lock is supported for the following platforms:

Android -

Android Enterprise kiosk devices

Android Enterprise work profile devices

Android Enterprise fully managed devices

Android Enterprise corporate-owned with work profile devices

iOS

macOS

Reference:

https://docs.microsoft.com/en-us/mem/intune/remote-actions/device-remote-lock

blueninja Highly Voted 12 months ago

Minimum number of policies: 4 (ios/ipad OS is one category in intune)
Remote lock: Device 2,3,4,5

https://docs.microsoft.com/en-us/mem/intune/protect/create-compliance-policy#create-the-policy

https://docs.microsoft.com/en-us/mem/intune/protect/actions-for-noncompliance#available-actions-for-noncompliance

upvoted 29 times

encxorblood 10 months, 2 weeks ago

Correct.

upvoted 2 times

Garito 7 months, 1 week ago

2nd.
Key here is Android Device Administrator is listed as supported for remote lock function.

upvoted 1 times

R0b671 Highly Voted 1 year ago

Answer (please correct me if Im wrong)...

Minimum number of policies: 4 - one for Android device administrator, one for Android enterprise, one for iOS/iPadOS, one for Windows 10.
Devices that support remote lock action: Device 3,4,5

Remote lock is supported for the following platforms:

Android
Android Enterprise kiosk devices
Android Enterprise work profile devices
Android Enterprise fully managed devices
Android Enterprise corporate-owned with work profile devices
iOS
macOS

Source: https://docs.microsoft.com/en-us/mem/intune/remote-actions/device-remote-lock

upvoted 9 times

FrancisLai 10 months, 3 weeks ago

Wrong, blueninja provided answer is correct.

upvoted 2 times

RodrigoT 5 months, 1 week ago

The only one that can't be locked is Windows 10.

upvoted 2 times

RodrigoT 4 months, 4 weeks ago

Android device administrator also supports lock:
https://docs.microsoft.com/en-us/mem/intune/protect/actions-for-noncompliance#available-actions-for-noncompliance

upvoted 1 times

Question #62 *Topic 3*

You have a Microsoft 365 tenant that contains the devices shown in the following table.

Name	Member of
Device1	Group1
Device2	Group1
Device3	Group1

The devices are managed by using Microsoft Intune.
You create a compliance policy named Policy1 and assign Policy1 to Group1. Policy1 is configured to mark a device as Compliant only if the device security settings match the settings specified in the policy.
You discover that devices that are not members of Group1 are shown as Compliant.
You need to ensure that only devices that are assigned a compliance policy can be shown as Compliant. All other devices must be shown as Not compliant.
What should you do?

A. From Endpoint security, configure the Conditional access settings.

B. From Device compliance, configure the Compliance policy settings.

C. From Policy1, modify the actions for noncompliance.

D. From Tenant administration, modify the Diagnostic settings.

Correct Answer: *B*
There are two parts to compliance policies in Intune:
Compliance policy settings ג€" Tenant-wide settings that are like a built-in compliance policy that every device receives. Compliance policy settings set a baseline for how compliance policy works in your Intune environment, including whether devices that haven't received any device compliance policies are compliant or noncompliant.
Device compliance policy ג€" Platform-specific rules you configure and deploy to groups of users or devices. These rules define requirements for devices, like minimum operating systems or the use of disk encryption. Devices must meet these rules to be considered compliant.
Reference:
https://docs.microsoft.com/en-us/mem/intune/protect/device-compliance-get-started

examkiller321 Highly Voted 11 months, 2 weeks ago
Correct
upvoted 5 times

TonySuccess Most Recent 2 weeks, 2 days ago
Selected Answer: B
B for real
upvoted 1 times

letters1234 7 months, 1 week ago
Endpoint security > Device compliance > Compliance policy settings.
"Mark devices with no compliance policy assigned as" .....
upvoted 2 times

AVP_Riga 10 months, 3 weeks ago
I think you'll see something like how to mark devices without policy assigned...
upvoted 1 times

Question #63 *Topic 3*

Your network contains an Active Directory domain. The domain contains 5,000 computers that run Windows 10.
All users use Roaming User Profiles.
Some users report that it takes a long time to sign in to the computers.
You discover that the users have user profiles that are larger than 1 GB.
You need to reduce the amount of time it takes for the users to sign in.
What should you configure?

A. Folder Redirection by using a Group Policy Object (GPO)

B. Sync your settings in the Settings app

C. Delivery Optimization in the Settings app

D. Microsoft User Experience Virtualization (UE-V) by using PowerShell

Correct Answer: *A*
Folder Redirection and Offline Files are used together to redirect the path of local folders (such as the Documents folder) to a network location, while caching the contents locally for increased speed and availability. Roaming User Profiles is used to redirect a user profile to a network location.
Reference:
https://docs.microsoft.com/en-us/windows-server/storage/folder-redirection/folder-redirection-rup-overview

lijk_manson Highly Voted 12 months ago
This one will be A

I think UE-V will still sync 1GB of data, with "redirection" login or logoff process wil not sync any data only where it can be found
upvoted 8 times

blueninja 12 months ago
Makes sense. A.

https://helgeklein.com/blog/how-to-reduce-the-size-of-roaming-profiles/
upvoted 4 times

Moderator Most Recent 6 months, 1 week ago
Selected Answer: A
A seems like the best answer here indeed.
upvoted 1 times

4Shawsy 7 months, 3 weeks ago
Selected Answer: D
UE-V is a modern alternative to Roaming Profiles so I'm going with D
upvoted 3 times

RodrigoT 5 months, 1 week ago
I just dealt with this problem in my company. Some users have huge profiles, 3 or 4GB. It took 20 or 30 minutes just to sign in. I solved this with A. Folder Redirection. Now it takes seconds.
UE-V is just for settings, not files. It wont solve the problem.
upvoted 4 times

forExamCert2023 6 months, 3 weeks ago
Okay, that is exactly why lijk_manson said the solution should not be Roaming: It takes a lot to sync. A is the answer.
upvoted 3 times

moobdoob 8 months, 2 weeks ago
Selected Answer: A
Correct answer A: Folder redirection
upvoted 4 times

moobdoob 8 months, 2 weeks ago
A seems to be the correct answer here.
upvoted 1 times

ANDREVOX 11 months, 2 weeks ago
UE-V = Customizable Windows settings include Microsoft Store appearance, language, background picture, font size, and accent colors. Customizable application settings include language, appearance, behavior, and user interface options thus, UE-V will capture user-customized Windows and application settings and store them on a centrally managed network file share, not user profile Data.

Folder Redirection, Offline Files, and Roaming User Profiles = Administrators can use Folder Redirection, Offline Files, and Roaming User Profiles to centralize storage for user data and settings and to provide users with the ability to access their data while offline or in the event of a network or server outage..

Correct answer is A - Folder Redirection.

https://docs.microsoft.com/en-us/windows-server/storage/folder-redirection/folder-redirection-rup-overview

upvoted 2 times

Souffke 11 months, 3 weeks ago

D seems to be correct if you want to speed up combined with roaming profiles.

https://social.technet.microsoft.com/Forums/en-US/0d530a62-7f24-4dd8-972e-fbfa04bf58e0/roaming-profile-vs-uev-user-experience-virtualization?forum=mdopuev

upvoted 2 times

Rick11221 10 months, 2 weeks ago

Microsoft User Experience Virtualization (UE-V) is settings not data

upvoted 4 times

Question #64 *Topic 3*

You have a Microsoft 365 tenant that contains the objects shown in the following table.

Name	Type
Admin1	User
Group1	Microsoft 365 group
Group2	Distribution group
Group3	Mail-enabled security group
Group4	Security group

You are creating a compliance policy named Compliance1.

Which objects can you specify in Compliance1 as additional recipients of noncompliance notifications?

A. Group1, Group2, Group3, Group4, and Admin1

B. Group1, Group2, Group3, and Group4 only

C. Group3, Group4, and Admin1 only

D. Group1, Group2, and Group3 only

E. Group3 and Group4 only

Correct Answer: *D*

Need email address to specify additional recipients of noncompliance notification.

Security groups have no email address.

	Microsoft 365 Groups	Distribution groups	Security groups	Mail-enabled security groups	Shared mailboxes	Dynamic distribution groups
Mail-enabled	Yes	Yes	No	Yes	Yes	Yes

Reference:

https://docs.microsoft.com/en-us/microsoft-365/admin/create-groups/compare-groups?view=o365-worldwide

HOTSPOT -

You have a workgroup computer named Computer1 that runs Windows 10 and has the users shown in the following table.

Name	Member of
User1	Group1
User2	Group2
User3	Group3

Group1 is a member of Group3.

You are creating a file named Kiosk.xml that specifies a lockdown profile for a multi-app kiosk.

Kiosk.xml contains the following section.

```
<Configs>
  <Config>
    <UserGroup Type="LocalGroup" Name="Group3" />
    <DefaultProfile Id="{9A2A490F-10F6-4764-974A-43B19E722C23}"/>
  </Config>
</Configs>
```

You apply Kiosk.xml to Computer1.

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 lockdown profile applies to User1.	○	○
The lockdown profile applies to User2.	○	○
The lockdown profile applies to User3.	○	○

Correct Answer:

Answer Area

Statements	Yes	No
The lockdown profile applies to User1.	○	●
The lockdown profile applies to User2.	○	●
The lockdown profile applies to User3.	●	○

Box 1: No -

The lockdown profile only applies to the specified group, not to the nested group.

Box 2: No -

Box 3: Yes -

Reference:

https://docs.microsoft.com/en-us/windows/configuration/lock-down-windows-10-to-specific-apps#config-for-group-accounts

Alexbz Highly Voted 1 year, 5 months ago

Answer is correct.
From the supplied like: Group accounts are specified using <UserGroup>. Nested groups are not supported. For example, if user A is member of Group 1, Group 1 is member of Group 2, and Group 2 is used in <Config/>, user A will not have the kiosk experience.

upvoted 26 times

ANDREVOX Highly Voted 11 months, 3 weeks ago

Please read the Microsoft Documents - Nested groups are not supported.
https://docs.microsoft.com/en-us/azure/active-directory/conditional-access/concept-conditional-access-users-groups

upvoted 7 times

SKK1986 Most Recent 1 month, 2 weeks ago

Nested local group is not supported as far as Windows 7 and Windows 2008 Servers are concerned (see link below). Though the computer is Windows 10, I could not locate a documentation that explicitly mentions nested local groups are supported in Windows 10. So I believe the answers are correct.

https://docs.microsoft.com/en-us/previous-versions/windows/it-pro/windows-7/ee681621(v=ws.10)?redirectedfrom=MSDN
upvoted 1 times

N0peasaurus 2 months, 4 weeks ago
Nested Groups Are Supported
https://docs.microsoft.com/en-us/azure/active-directory/conditional-access/concept-conditional-access-users-groups

"sers and groups
Allows targeting of specific sets of users. For example, organizations can select a group that contains all members of the HR department when an HR app is selected as the cloud app. A group can be any type of group in Azure AD, including dynamic or assigned security and distribution groups. Policy will be applied to nested users and groups."
upvoted 1 times

handsofthelp 9 months, 3 weeks ago
Is correct.
NO. User 1 is member of Group 1 and this of Group 2. Nested group are not supported.
upvoted 1 times

Testtest123 1 year, 5 months ago
The giving answer is correct, this only applies to Group 3, so user 3.
upvoted 2 times

petir 1 year, 5 months ago
I believe its yes no yes. user1 is part of group1 and group1 is part of group3 which the lockdown profile applies to.
upvoted 1 times

larry_cse20 1 year, 5 months ago
that's what I'm thinking also, so why NNY?
upvoted 1 times

larry_cse20 1 year, 5 months ago
Config for group accounts

The answer is correct, see the explanation from the link. Group accounts are specified using <UserGroup>. Nested groups are not supported. For example, if user A is member of Group 1, Group 1 is member of Group 2, and Group 2 is used in <Config/>, user A will not have the kiosk experience.
upvoted 9 times

HOTSPOT -

Your network contains an Active Directory domain named contoso.com that syncs to Azure Active Directory (Azure AD). The domain contains the users shown in the following table.

Name	Source	User profile path
User1	Windows Active Directory	\\Server1.contoso.com\users\User1
User2	Azure Active Directory	*Not applicable*

Enterprise State Roaming is enabled for User2.

You have the computers shown in the following table.

Name	Operating system	Joined to
Computer1	Windows 10	Azure AD tenant
Computer2	Windows 8.1	On-premises Active Directory domain
Computer3	Windows 10	Azure AD tenant

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 modifies his desktop icons on Computer1, the changes will be available when the user signs in to Computer2.	○	○
If User1 modifies his desktop icons on Computer1, the changes will be available when the user signs in to Computer3.	○	○
If User2 modifies his desktop icons on Computer1, the changes will be available when the user signs in to Computer3.	○	○

Correct Answer:

Answer Area

Statements	Yes	No
If User1 modifies his desktop icons on Computer1, the changes will be available when the user signs in to Computer2.	○	○
If User1 modifies his desktop icons on Computer1, the changes will be available when the user signs in to Computer3.	○	○
If User2 modifies his desktop icons on Computer1, the changes will be available when the user signs in to Computer3.	○	○

The requirements of Enterprise State Roaming are:

- Windows 10, with the latest updates, and a minimum Version 1511 (OS Build 10586 or later) is installed on the device.
- The device is Azure AD joined or hybrid Azure AD joined.
- Ensure that Enterprise State Roaming is enabled for the tenant in Azure AD.
- The user is assigned an Azure Active Directory Premium license.
- The device must be restarted and the user must sign in again to access Enterprise State Roaming features.

Box 1: No -

Computer2 runs Windows 8.1.

Enterprise State Roaming requires Windows 10, with the latest updates, and a minimum Version 1511 (OS Build 10586).

Also, Enterprise State Roaming is enabled for User2, not for User1.

Box 2: No -

The device must be Azure AD joined or hybrid Azure AD joined.

Your network contains an Active Directory domain named contoso.com that syncs to Azure Active Directory (Azure AD), in other words, a hybrid Azure AD.

Also, Enterprise State Roaming is enabled for User2, not for User1.

Box 3: Yes -

Reference:

https://docs.microsoft.com/en-us/azure/active-directory/devices/enterprise-state-roaming-troubleshooting

Nome2025 Highly Voted 1 year, 3 months ago

Answer is correct. NO NO YES

upvoted 24 times

RodrigoT 5 months, 1 week ago

NO- Because Computer 2 is Windows 8.1, different systems.
YES- Because both PCs are Windows 10 and User 1 has his profile path on a network share.
YES- Because ESR applies here.

upvoted 2 times

MitchF 2 months, 1 week ago

ESR is disabled for User1, so modifications can't follow the user.
Answers can only be:
No – ESR disabled for this user1
No – ESR disabled for this user1
Yes – ESR enabled for this user2

upvoted 1 times

MitchF 2 months, 1 week ago

Also, the devices (or the OS) have nothing to do with ESR.

"Enterprise State Roaming lets users securely synchronize user and application settings data to the cloud. **This means they'll have the same experience no matter which Windows device they sign into.**For example, if you replace one of their Microsoft Managed Desktop devices (e.g., Windows 8.1) with a new device (e.g., Windows 10), it will look and behave exactly the same as the last one.

https://docs.microsoft.com/en-us/managed-desktop/get-started/enterprise-state-roaming

upvoted 1 times

MitchF 2 months, 1 week ago

Need to fix my explanation. ESR is for Windows 10 or newer, but the results don't change:
No – ESR disabled for this user1
No – ESR disabled for this user1; Also Windows 8.1 doesn't work with ESR.
Yes – ESR enabled for this user2

upvoted 1 times

MitchF 2 months, 1 week ago

Source:
https://docs.microsoft.com/en-us/azure/active-directory/devices/enterprise-state-roaming-enable

upvoted 1 times

Technik Highly Voted 1 year, 4 months ago

Although entreprise roaming is only enabled for user 2, user 1 does have a roaming profile, because of the network path. I think the answer should be Yes, Yes, Yes.

Does anyone agree?

upvoted 8 times

camro675 1 month, 1 week ago

I agree. Everyone seems to be getting caught up on ESR when that only applies to User2 which is only relevant for box 3.

upvoted 1 times

pogap64757 8 months ago

Roaming profiles generally do not work between different versions of Windows and the AAD joined Computers (1 and 3) have no knowledge of the on-prem AD infrastructure since they are only aware of the AAD tenant (cloud)
Just my thought

upvoted 5 times

moobdoob Most Recent 8 months, 2 weeks ago

Answer is correct, NO NO YES.

upvoted 2 times

moobdoob 8 months, 2 weeks ago

Correct answer is no no yes

upvoted 3 times

Anon1212 8 months, 4 weeks ago

NNY as it does not say any other user other than User2 has Enterprise Roaming.

upvoted 1 times

afhelton 1 year ago

I personally feel the answers are No, Yes, Yes.

1 - No: User1's profile is a roaming profile. We can tell by looking at the User Profile Path. However, Windows 8 machines lack roaming profile compatibility with other versions of windows as indicated in this link: https://support.microsoft.com/en-us/topic/incompatibility-between-windows-8-roaming-user-profiles-and-roaming-profiles-in-other-versions-of-windows-994c2a2b-ad21-60da-e9ac-a0149513956a

2 - Yes: Both machines are W10 machines, so no issues with roaming profile compatibility.

3 - Yes. ESR is a W10 feature. Both PCs are W10. ESR is enabled on User2. Check. Check. Check.

upvoted 6 times

Sironin 1 year ago

NYY. This is the correct answer. Additional information on roaming profile versioning is here: https://docs.microsoft.com/en-us/troubleshoot/windows-server/user-profiles-and-logon/roaming-user-profiles-versioning

upvoted 2 times

jorlloen 1 year ago

I think that ESR not synchronize desktop icons, as you can see in https://docs.microsoft.com/en-us/azure/active-directory/devices/enterprise-state-roaming-faqs
Theme, which includes features such as desktop theme and taskbar settings.
Internet Explorer settings, including recently opened tabs and favorites.
Microsoft Edge browser settings, such as favorites and reading list.
Passwords, including Internet passwords, Wi-Fi profiles, and others.
Language preferences, which include settings for keyboard layouts, system language, date and time, and more.
Ease of access features, such as high-contrast theme, Narrator, and Magnifier.
Other Windows settings, such as mouse settings.

So, the correct answer for me is:
Y: because Roaming Profile is set for user1.
Y: because Roaming Profile is set for user1.
N: because ESR not syncs desktop icons and User2 doesn't have roaming profile

upvoted 2 times

Alvaroll 8 months, 1 week ago

N,N,N
As you said, ESR not syncronize desktop icons, only a roaming profile does. In order to a roaming profile take effect, computers has to be On-Premises AD Join.

On-Premises --> GPO, SCCM (System Center Configuration Manager)
Azure AD --> Intune
Both: Co-Management

Co-Management <> Hybrid (On-Prem + AzureAD)

upvoted 5 times

silver_bullet666 3 months, 1 week ago

the link for what ESR syncs is here: https://docs.microsoft.com/en-us/azure/active-directory/devices/enterprise-state-roaming-windows-settings-reference

upvoted 1 times

jorlloen 1 year ago

sorry I correct my answer :
N: because cannot use the same profile with accross differents windows versions
Y: because Roaming Profile is set for user1.
N: because ESR not syncs desktop icons and User2 doesn't have roaming profile

upvoted 4 times

51007 4 months ago

I was going to agree- N,Y,N for the same reasons as you..
But what's hanging me up is how pc1 and pc3 are 'joined to AZAD'.. but does that mean in ADDITION to on-prem AD? If so, shouldnt it say 'hybrid'? Are they only joined to AZAD and PC2 is only joined to on-prem AD? I think we should only assume what is explicitly stated. And i see at least one other question, 3-40 which specifically says active-directory joined, hybrid joined, or azure ad joined..

I think that just bc in this question we have 'An AD domain that syncs to AD' does not necessarily mean that all users are joined to both.. Someone *please* correct me here if im wrong.

If pc1 and pc2 are only joined to AZAD which seems to be the case... then the on-prem source of the profile path, along with ESR not enabled for User1.. would suggest that U1 cannot roam between PC1 and PC3..

I've been at this question for an hour and I think im going NO NO NO on this one.

upvoted 2 times

tpcwndr 1 month, 2 weeks ago

I'm going with NO NO NO aswell;

NO - No roaming compatibility between W10 and W8.1
NO - Computer 1 and 3 are Azure AD joined, roaming profiles will not apply.
NO - ESR doesn't synchronize desktop icons.

upvoted 1 times

jorlloen 1 year ago

But if modify icons it means change options on Desktop icon settings, .. the answers proposed are OK, ERS syncs Desktop configurations. It's crazy :-((N,N,Y)

upvoted 1 times

Richmawdsley 1 year, 3 months ago

My take on this is:
NO - Win10 > Win8.1 - Differing profile versions, not going to work.
YES - Roaming profiles enabled on both to a central server, both Win10, Yes. ESR does not matter here. Just because these devices are AzureAD joined does not mean they can't see the central server.
YES - All checks out, yes it is.

upvoted 2 times

Perycles 1 year, 3 months ago

YES : user 1 as roaming profile - computer are Azure AD hybrid joined. Login on computer 2 will sync the settings.
YES ;
YES

upvoted 1 times

pinklemonade 1 year, 1 month ago

Should be only within the local not online

upvoted 1 times

ExamStudy101 1 year, 2 months ago

It doesn't say user 1 has a roaming profile

upvoted 3 times

Malfureeon 1 year, 4 months ago

Technik I tend to agree with you. I would have liked more information on this question. Is it just me or does Microsoft tests seem to be designed to be intentionally confusing?

upvoted 3 times

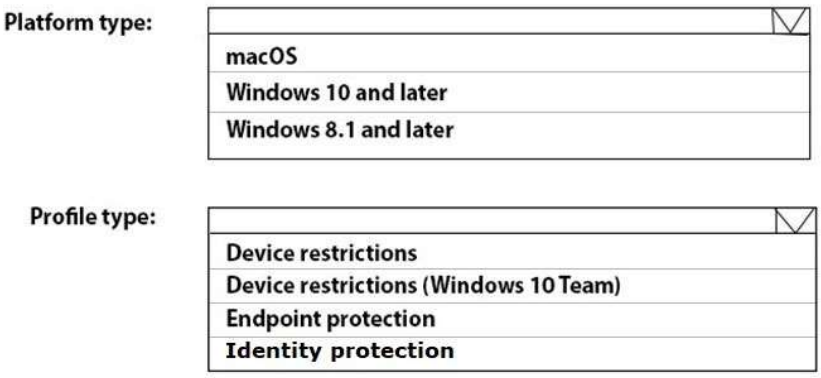
Wilf32 1 year, 4 months ago

I came to the same answer as was given. i cannot confirm 100% if it correct but it is what i would Answer.

upvoted 2 times

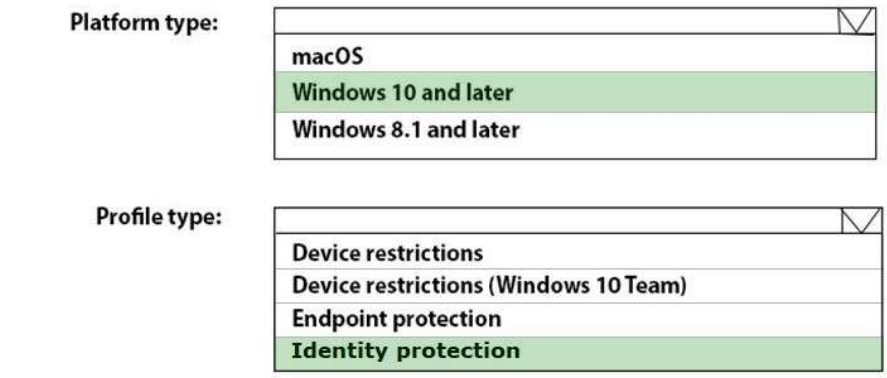
HOTSPOT -
Your company has computers that run Windows 8.1, Windows 10, or macOS.
The company uses Microsoft Intune to manage the computers.
You need to create a device configuration profile to configure Windows Hello for Business on the computers that support it.
Which platform type and profile type should you use? To answer, select the appropriate options in the answer area.
NOTE: Each correct selection is worth one point.
Hot Area:

Answer Area



Correct Answer:

Answer Area



Box 1: Windows 10 and later -
Windows Hello for Business is a method for signing in to Windows devices by replacing passwords, smart cards, and virtual smart cards. Intune includes built-in settings so Administrators can configure and use Windows Hello for Business. For example, you can use these settings to:
- Enable Windows Hello for Business for devices and users
- Set device PIN requirements, including a minimum or maximum PIN length
- Allow gestures, such as a fingerprint, that users can (or can't use) to sign in to devices

Box 2: Identity protection -

Create the device profile -
1. Sign in to the Microsoft Endpoint Manager admin center.
2. Select Devices > Configuration profiles > Create profile.
3. Enter the following properties:
4. Platform: Select Windows 10 and later.
5. Profile: Select Templates > Identity protection.
6. Etc
Reference:
https://docs.microsoft.com/en-us/mem/intune/protect/identity-protection-configure

moobdoob 8 months, 2 weeks ago
Windows 10 and later & Identity Protection

upvoted 2 times

Moderator 8 months, 4 weeks ago

Correct answers given.

Platform type: Windows 10 and later (the feature applies to devices running Windows 10 and 11).
Profile type: Identity protection.

upvoted 4 times

mikl 9 months, 1 week ago

True, but you can also make it from Settings Catalog (Preview)

upvoted 1 times

hawkens 9 months, 2 weeks ago

Correct!

upvoted 1 times

BAbdalla 11 months, 1 week ago

Seems correct

upvoted 4 times

Question #68 *Topic 3*

Note: This question is part of a series of questions that present the same scenario. Each question in the series contains a unique solution that might meet the stated goals. Some question sets might have more than one correct solution, while others might not have a correct solution.
After you answer a question in this section, you will NOT be able to return to it. As a result, these questions will not appear in the review screen.
You have an Azure Directory group named Group1 that contains Windows 10 Enterprise devices and Windows 10 Pro devices.
From Microsoft Intune, you create a device configuration profile named Profile1.
You need to ensure that Profile1 applies to only the Windows 10 Enterprise devices in Group1.
Solution: You create an Azure Active Directory group that contains only the Windows 10 Enterprise devices. You assign Profile1 to the new group.
Does this meet the goal?

A. Yes

B. No

Correct Answer: *B*
Instead: You configure an applicability rule for Profile1. You assign Profile1 to Group1.
Note: Applicability rules allow administrators to target devices in a group that meet specific criteria. For example, you create a device restrictions profile that applies to the All Windows 10/11 devices group. And, you only want the profile assigned to devices running Windows Enterprise.
To do this task, create an applicability rule.
Reference:
https://docs.microsoft.com/en-us/mem/intune/configuration/device-profile-create

CvdK Highly Voted 1 year, 10 months ago
Answer = A
Assigning a profile to a group means that only the devices in the group apply the profile settings. This can be filtered further by applying applicability rules but creating applicability rules is optional.
In this case the group that the profile was assigned to contains only the intended target devices, so the goal is met (even without applying applicability rules).
However creating a new group was unnecessary, instead the original group could have been used with applicability rules. But both options work equaly well to meet the goal.
upvoted 25 times

Anthony_2770 1 year, 8 months ago
Valid point.
Voting for A
upvoted 2 times

Anthony_2770 1 year, 7 months ago
I am changing my answer to No.
"You need to ensure that Profile1 applies to only the Windows 10 Enterprise devices in Group1." If you create a new group and apply Profile1 to it then you are not applying Profile1 to Group1 but to a new group.
upvoted 11 times

b33droid 1 year, 5 months ago
It doesn't say that you need to apply the profile to group 1 but only to Win 10 Entreprise devices wich are in group 1. So if your new group is a static group and you target "Group 1" as member then you use applicability rules to target windows 10 in this new group as CVdK said it's fine
upvoted 3 times

Layer8 1 year, 4 months ago
only problem is that if there are ever any more W10 Ent machines added to group 1, then the configuration profile no longer applies to all the machines you intend it to.
upvoted 5 times

raduM Most Recent 1 month, 3 weeks ago
i would go with yes here. Why not?
upvoted 1 times

jaroti2116 2 months, 2 weeks ago
Dynamic Profile
upvoted 1 times

Alejack 3 months ago
Solution states: You create an Azure Active Directory group that contains only the Windows 10 Enterprise devices. You assign Profile1 to the new group.
A is the correct answer.
upvoted 2 times

MR_Eliot 5 months ago
Selected Answer: A
Does this meet the goal? Yes, it does!
upvoted 2 times

Angarali 5 months, 2 weeks ago

Selected Answer: B

https://docs.microsoft.com/en-us/mem/intune/configuration/device-profile-create

upvoted 1 times

morito 7 months, 3 weeks ago

Selected Answer: A

I believe the correct answer here is yes, even though its quite confusing. Working strictly according to the question, you'd have to assign it to the group, and apply an applicability rule, ensuring that you only catch the devies in the group and further scope it to only match all Windows 10 Enterprise Versions. A good compromise is to simply create a new group with all the devices you want to target.

upvoted 1 times

PiPe 7 months, 4 weeks ago

Selected Answer: B

Applicability rules is obviously what they're asking for. Hence the question states that you need to ensure that Profile1 applies to only the Win10 Ent devices <IN GROUP 1>.
Creating a new group works of course, but that's not what the question is asking. So the answer is B.

upvoted 2 times

ken2ut 4 months, 1 week ago

Umm the question literally states "Does this meet the goal?". Well it sure hell does.
A is the answer

upvoted 2 times

mayleni 8 months, 2 weeks ago

Selected Answer: B

with a new group you can achieve the goal but you need to extra admin work.... so i vote B

upvoted 1 times

jcgm1990 3 months ago

question here does not state minimum work, read carefully, it states if it meats the goal

upvoted 1 times

IykeP 8 months, 3 weeks ago

Selected Answer: B

This is a tricky question. From Microsoft Intune, you create a device configuration profile named Profile1.
You need to ensure that Profile1 applies to only the Windows 10 Enterprise devices in Group1.

Since you are already in Microsoft Intune, with less Admin effort, the best thing will be to use "Applicability rules".

upvoted 1 times

morito 7 months, 3 weeks ago

I disagree with this. Using Applicability rules will scope the deployment to all Windows 10 Enterprise Devices Enrolled in Intune, however the question specifically wants it assigned to all Windows Enterprise devices in a specific group.

upvoted 1 times

IykeP 8 months, 3 weeks ago

Selected Answer: A

Correct Answer is A

upvoted 1 times

Mage7 11 months, 1 week ago

To much assumtions WHAT/IF...
I'll write important parts - will not write garbage information - stated as it is:

We have:
"Azure Directory group ... Group1 ... contains Windows 10 Enterprise devices and Windows 10 Pro devices"
So we have Pro and Enterprise devices in Group1.

Goal:
"... ensure ... Profile1 applies to only the Windows 10 Enterprise devices in Group1."
We want to apply Profile1 to Enterprise devices only.

Solution:
"... create an Azure Active Directory group that contains only the Windows 10 Enterprise devices. You assign Profile1 to the new group."

QUESTIONS (not sure):
Only question I have (from the "Solution") from which you want make different assumptions:
I assume that created group contains only the Windows 10 Enterprise Devices FROM THE GROUP1?

Answer should be A?
Why do you thing answer A would not me the goal?

upvoted 1 times

HellRaver80 11 months ago

"'You assign Profile1 to the new group." So not to group1

upvoted 1 times

tf444 11 months, 2 weeks ago

duh, who answers these Qs?

upvoted 1 times

PersoDaniels 1 year, 3 months ago

B. No

https://docs.microsoft.com/en-us/mem/intune/configuration/device-profile-create#applicability-rules
upvoted 2 times

jibutoms 1 year, 3 months ago
Answer is No. The right way is to use the "Applicability Rules" while you create profiles
upvoted 2 times

Perycles 1 year, 3 months ago
OSTYPE in dynamic group only allow "Windows" word. Nothing about Edition.
so the answer is NO.
upvoted 2 times

techh3ad 1 year, 6 months ago
Applicability Rules for OS and versions, Assignments for Devices and Users Groups. Is that a good way to remember it?
upvoted 1 times

Question #69 *Topic 3*

Note: This question is part of a series of questions that present the same scenario. Each question in the series contains a unique solution that might meet the stated goals. Some question sets might have more than one correct solution, while others might not have a correct solution.
After you answer a question in this section, you will NOT be able to return to it. As a result, these questions will not appear in the review screen.
You have an Azure Directory group named Group1 that contains Windows 10 Enterprise devices and Windows 10 Pro devices.
From Microsoft Intune, you create a device configuration profile named Profile1.
You need to ensure that Profile1 applies to only the Windows 10 Enterprise devices in Group1.
Solution: You create a scope tag, and then you add the scope tag to the Windows 10 Enterprise devices. You edit the settings of Profile1.
Does this meet the goal?

A. Yes

B. No

Correct Answer: *B*
Instead: You configure an applicability rule for Profile1. You assign Profile1 to Group1.
Note: Applicability rules allow administrators to target devices in a group that meet specific criteria. For example, you create a device restrictions profile that applies to the All Windows 10/11 devices group. And, you only want the profile assigned to devices running Windows Enterprise.
To do this task, create an applicability rule.
Reference:
https://docs.microsoft.com/en-us/mem/intune/configuration/device-profile-create

Anthony_2770 Highly Voted 1 year, 8 months ago
When you create or update a profile, you can also add scope tags and applicability rules to the profile.
Scope tags are a great way to filter profiles to specific groups, such as US-NC IT Team or JohnGlenn_ITDepartment. Use RBAC and scope tags for distributed IT has more information.
On Windows 10 devices, you can add applicability rules so the profile only applies to a specific OS version or a specific Windows edition. Applicability rules has more information.
Applicability rules is the better concept in this scenario but the question is does scope tags meet this goal. Applicability rules more clearly define the operating system filter that you need in this scenario and this is what you need to be using.
Voting for No.
upvoted 14 times

Anthony_2770 1 year, 7 months ago
Additionally :
Use Intune scope tags to provide administrative users with a filtered a view to securable objects. Scope tags are filtering option provided in Intune to ease the admin jobs.
So in this question the Scope tags are not used in the way that they are intended to be used. So again No.
upvoted 3 times

MR_Eliot Most Recent 5 months ago
Selected Answer: B
Correct.
upvoted 1 times

BLYBOI 1 year, 4 months ago
Answer is No.

Use scope tags or applicability rules
When you create or update a profile, you can also add scope tags and applicability rules to the profile.

Scope tags are a great way to filter profiles to specific groups, such as US-NC IT Team or JohnGlenn_ITDepartment.

On Windows 10 devices, you can add applicability rules so the profile only applies to a specific OS version or a specific Windows edition. Applicability rules has more information.
upvoted 2 times

petir 1 year, 5 months ago
This is such a confusing ass question. If you edit the settings you can add a scope tag to the configuration profile. so I think Yes but also.... I edited the settings but wtf did I do?
upvoted 1 times

Moorebid 1 year, 4 months ago
The answer is No because scope tags have no effect on applying the device profile; scope tags are only used for limiting view access to objects in Intune.
upvoted 6 times

vinnyct 1 year, 10 months ago
It's No

it's Applicability rules you have to use when you create a profile 1

Applicability rules allow administrators to target devices in a group that meet specific criteria. For example, you create a device restrictions profile that applies to the All Windows 10 devices group. And, you only want the profile assigned to devices running Windows 10 Enterprise.

https://docs.microsoft.com/en-us/mem/intune/configuration/device-profile-create
upvoted 3 times

Timmi 1 year, 8 months ago
the question is if "scope tags" meet the goal, nt if there is a better way
upvoted 1 times

DJM 1 year, 10 months ago
Yes - create a scope tag called e.g. ENT and apply to enterprise devices. Only the devices both in the group and containing the ENT scope tag will be in scope to receive the policy.
upvoted 3 times

gchristina 1 year, 5 months ago
I could agree but aren't we missing the part that the profile should be assigned to the group (in conjunction with the editing of the settings (adding scope)). So this would be a 'no'?
upvoted 4 times

silver_bullet666 3 months, 1 week ago
My answer is No.
Reading on the usage of Scope Tags, their usage appears to be for an IT admin to be able to manage objects that have the scope tags they have access to. It is not used as a filtering mechanism for the applicable devices the policy may apply to.
Applying the scope tag to the profile would mean any Admin with access to this scope tag would then be able to manage the profile.
upvoted 1 times

Question #70 *Topic 3*

Note: This question is part of a series of questions that present the same scenario. Each question in the series contains a unique solution that might meet the stated goals. Some question sets might have more than one correct solution, while others might not have a correct solution.
After you answer a question in this section, you will NOT be able to return to it. As a result, these questions will not appear in the review screen.
You have an Azure Directory group named Group1 that contains Windows 10 Enterprise devices and Windows 10 Pro devices.
From Microsoft Intune, you create a device configuration profile named Profile1.
You need to ensure that Profile1 applies to only the Windows 10 Enterprise devices in Group1.
Solution: You configure an applicability rule for Profile1. You assign Profile1 to Group1.
Does this meet the goal?

A. Yes

B. No

Correct Answer: *A*
Applicability rules allow administrators to target devices in a group that meet specific criteria. For example, you create a device restrictions profile that applies to the All Windows 10/11 devices group. And, you only want the profile assigned to devices running Windows Enterprise.
To do this task, create an applicability rule.
Reference:
https://docs.microsoft.com/en-us/mem/intune/configuration/device-profile-create

vinnyct Highly Voted 1 year, 10 months ago
It's Yes

it's Applicability rules you have to use when you create a profile 1

Applicability rules allow administrators to target devices in a group that meet specific criteria. For example, you create a device restrictions profile that applies to the All Windows 10 devices group. And, you only want the profile assigned to devices running Windows 10 Enterprise.

https://docs.microsoft.com/en-us/mem/intune/configuration/device-profile-create
upvoted 13 times

junior6995 Most Recent 3 weeks, 2 days ago
as of now (September 2022) While creating or editing a Configuration profile I don't see the option "Applicability rules", only assignments, probably this question is outdated.
upvoted 2 times

Goofer 10 months, 3 weeks ago
When you create an Applicability Rule you can choose:
- OS version (buildnumber)
- OS edition (options:)
- Windows 10/11 Education
- Windows 10/11 Education
- Windows 10/11 Professional
- Windows 10/11 Eneterprice
- etc.

Answer = Yes
upvoted 2 times

Perycles 1 year, 3 months ago
Yes, Finally :) this is the good one (no dynamic group or TAG seen in previous questions).
upvoted 4 times

BLYBOI 1 year, 4 months ago
Correct
upvoted 2 times

vinnyct 1 year, 10 months ago
sorry ignore my previous comment
upvoted 2 times

vinnyct 1 year, 10 months ago
It's Yes

It's No

it's Applicability rules you have to use when you create a profile 1

Applicability rules allow administrators to target devices in a group that meet specific criteria. For example, you create a device restrictions profile that applies to the All Windows 10 devices group. And, you only want the profile assigned to devices running Windows 10 Enterprise.

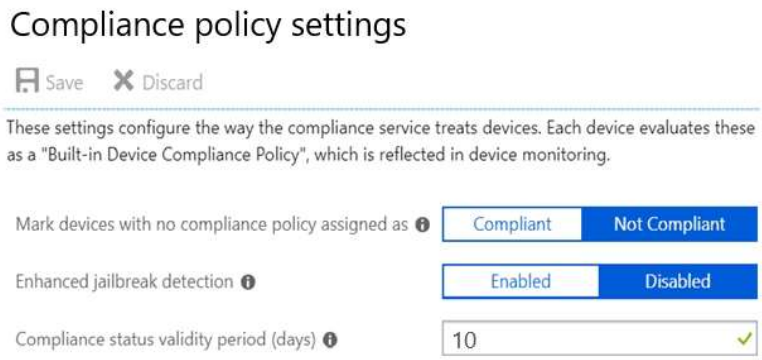
https://docs.microsoft.com/en-us/mem/intune/configuration/device-profile-create
upvoted 1 times

HOTSPOT -

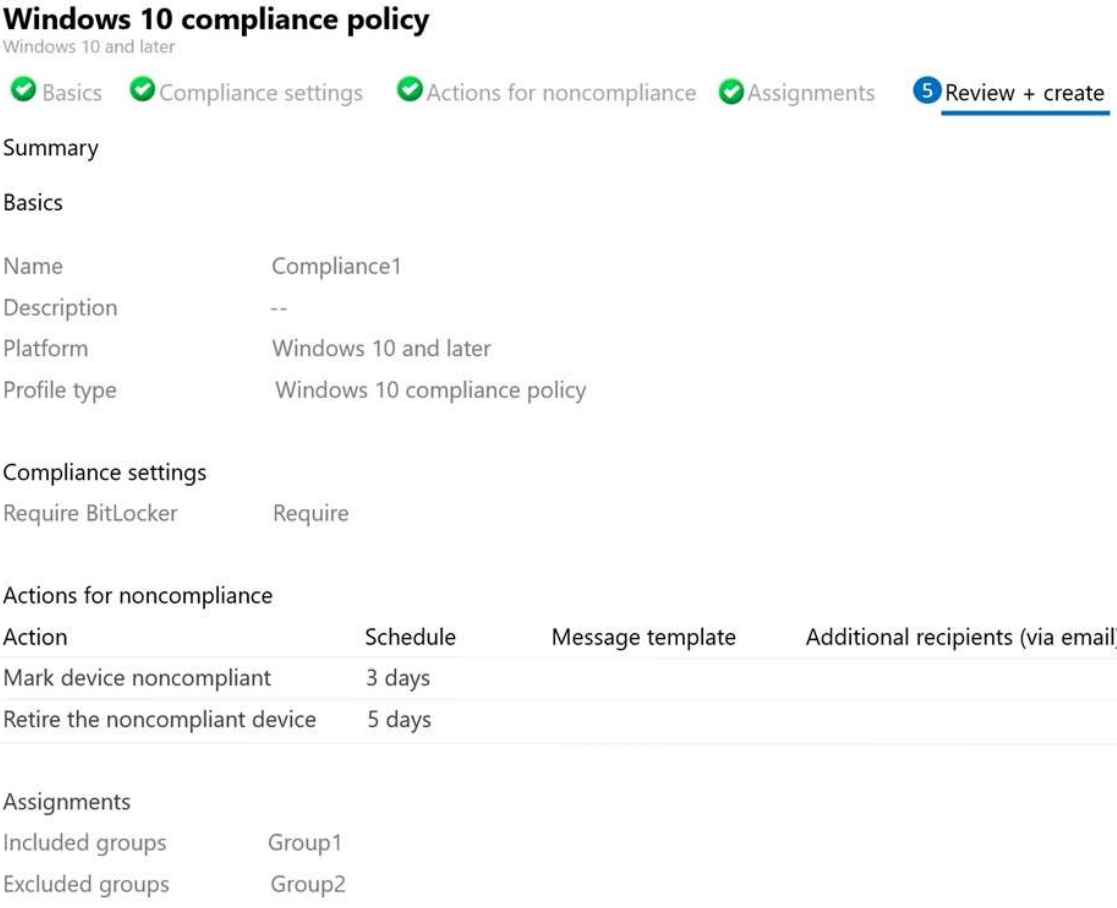
You have two Windows 10 devices enrolled in Microsoft Intune as shown in the following table.

Name	BitLocker Drive Encryption (BitLocker)	Member of
Device1	Enabled	Group2
Device2	Disabled	Group1

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



On August 1, you create a compliance policy 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
Device1 is marked as compliant on August 4.	◯	◯
Device1 is marked as compliant on August 2.	◯	◯
Device2 is retired on August 6.	◯	◯

Correct Answer:

Answer Area

Statements	Yes	No
Device1 is marked as compliant on August 4.	○	◉
Device1 is marked as compliant on August 2.	◉	○
Device2 is retired on August 6.	○	◉

Box 1: No -
Device1 belongs to Group2. Group2 has not been assigned a compliance policy. Devices with no compliance policy assigned as Not Compliant. Device1 gets a 3 day grace period, but at August 4 is it marked as Non-compliant.

Box 2: Yes -
Device1 belongs to Group2. Group2 has not been assigned a compliance policy. Devices with no compliance policy assigned as Not Compliant. Device1 gets a 3 day grace period, so at August 2 it is compliant.

Box 3: No -
Device2 has BitLocker Disabled. The Windows 10 compliance policy applies to Group1 which includes Device1. At August 4 Device is marked noncompliant. 5 days later, at August 9th it is retired.
Note:
* Retire the noncompliant device: This action removes all company data off the device and removes the device from Intune management.
* By default, each compliance policy includes the action for noncompliance of Mark device noncompliant with a schedule of zero days (0). The result of this default is when Intune detects a device isn't compliant, Intune immediately marks the device as noncompliant.
By configuring Actions for noncompliance you gain flexibility to decide what to do about noncompliant devices, and when to do it. For example, you might choose to not block the device immediately, and give the user a grace period to become compliant.
Compliance status validity period (days):
Specify a period in which devices must successfully report on all their received compliance policies. If a device fails to report its compliance status for a policy before the validity period expires, the device is treated as noncompliant.
Reference:
https://docs.microsoft.com/en-us/mem/intune/protect/device-compliance-get-started https://docs.microsoft.com/en-us/mem/intune/protect/actions-for-noncompliance

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.

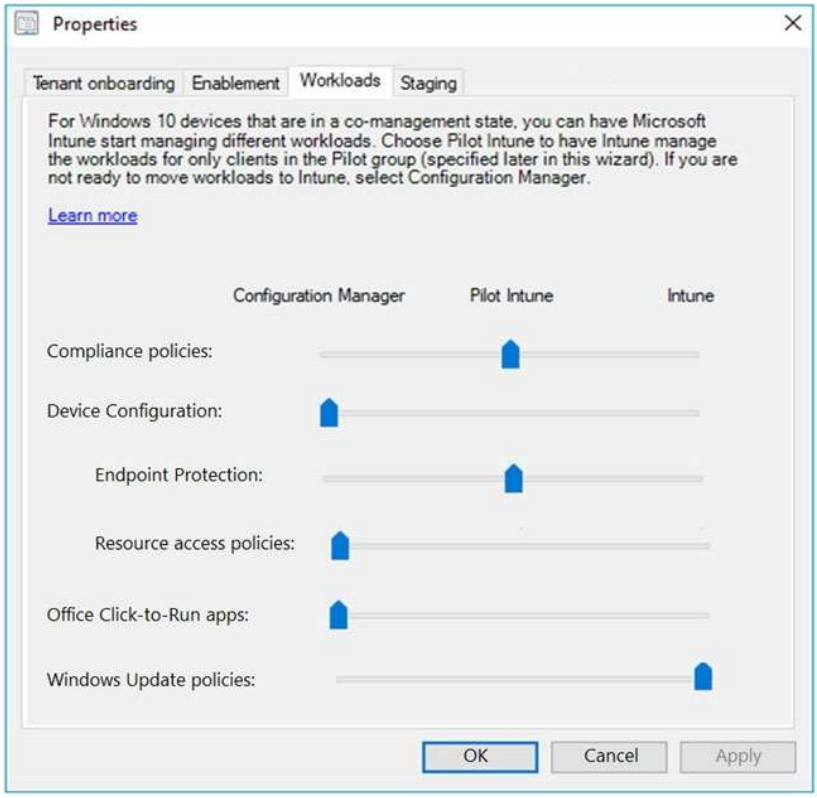
You have the Windows 10 devices shown in the following table.

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.	○	○

Correct 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.	○	○

Box 1: No -

The Pilot Group does not include Device1.

Box 2: Yes -

Box 3: Yes -

The Pilot Group includes Device3.
Reference:
https://docs.microsoft.com/en-us/mem/configmgr/comanage/how-to-enable

TonySuccess 2 weeks, 2 days ago
Can anyone explain why answer 2 is YES?
upvoted 1 times

bensrayan 2 weeks, 1 day ago
I think because device 1 is not in the collection 2, so it won't be managed by intune but by MECM instead
upvoted 2 times

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

Correct 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**

Box 1: Device 1, Device2, Device 3, and Device 4

Supported Windows versions include Windows 8.1 and Windows 10

Other supported operating systems

Android -

iOS

Linux -

macOS

Box 2: Device configuration profile, device compliance policy, and conditional access policy

We need all three policies.
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.
Reference:
https://docs.microsoft.com/en-us/microsoft-365/security/defender-endpoint/minimum-requirements https://docs.microsoft.com/en-us/mem/intune/protect/advanced-threat-protection#onboard-devices-by-using-a-configuration-profile

jenraed 5 days ago
Looks right according to the reference links.
upvoted 1 times

Question #74 *Topic 3*

Your on-premises network contains a database server and is accessible by using a VPN server.
You have a Microsoft 365 tenant.
You manage devices by using Microsoft Endpoint Manager.
You have an application named App1 that is deployed to every computer enrolled in Microsoft Intune. Each computer has a VPN profile assigned.
You need to ensure that App1 can access only the database server. App1 must be prevented from accessing other resources on the on-premises network.
What should you modify in the VPN profile?

A. Proxy

B. Network traffic rules

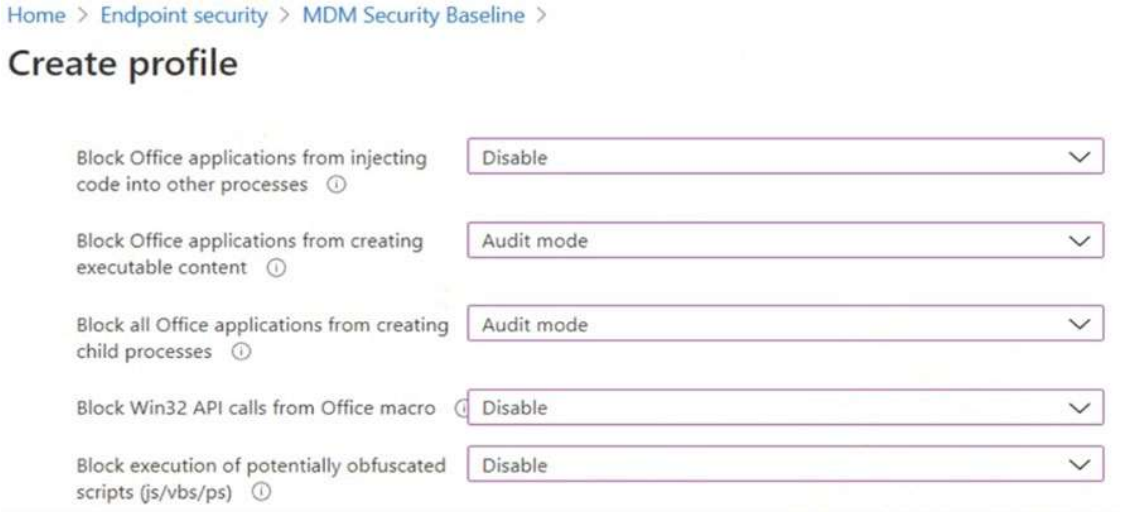
C. DNS Settings

D. Conditional Access

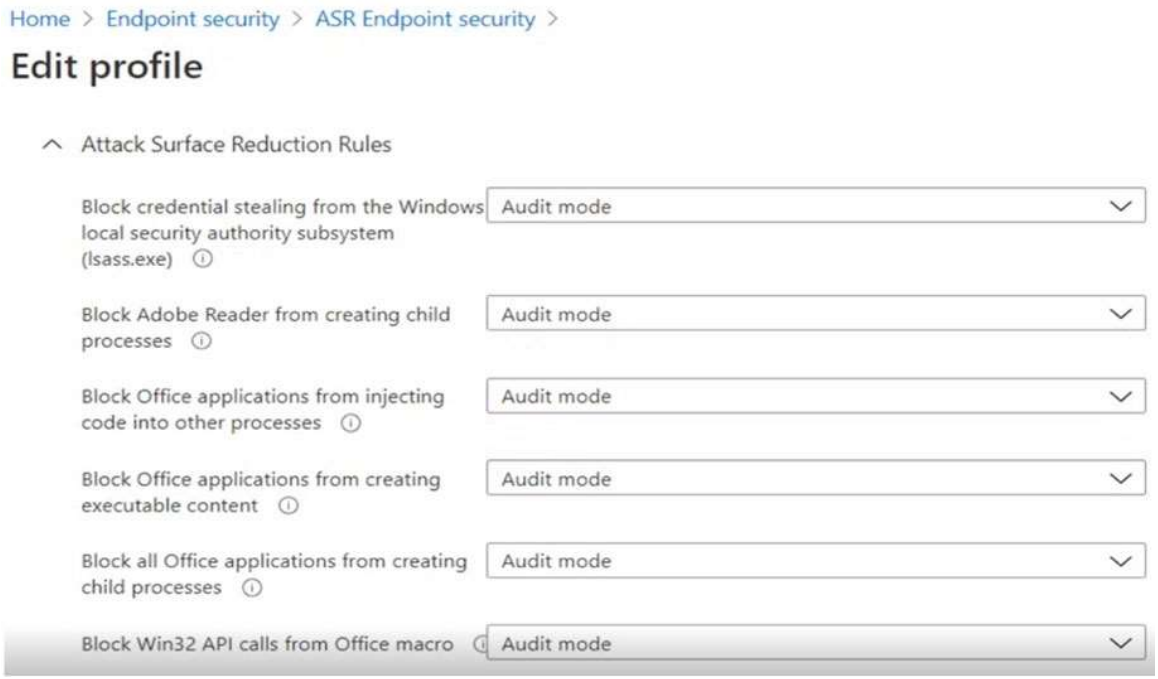
Correct Answer: *B*
You can use an Azure network security group to filter network traffic to and from Azure resources in an Azure virtual network. A network security group contains security rules that allow or deny inbound network traffic to, or outbound network traffic from, several types of Azure resources. For each rule, you can specify source and destination, port, and protocol.
A network security group contains zero, or as many rules as desired, within Azure subscription limits.
Reference:
https://docs.microsoft.com/en-us/azure/virtual-network/network-security-groups-overview

HOTSPOT -

You have the MDM Security Baseline profile shown in the MDM exhibit. (Click the MDM tab.)



You have the ASR Endpoint Security profile shown in the ASR exhibit. (Click the ASR tab.)



You plan to deploy both profiles to devices enrolled in Microsoft Intune.

You need to identify how the following settings will be configured on the devices:

- Block Office applications from creating executable content
- Block Win32 API calls from Office macro

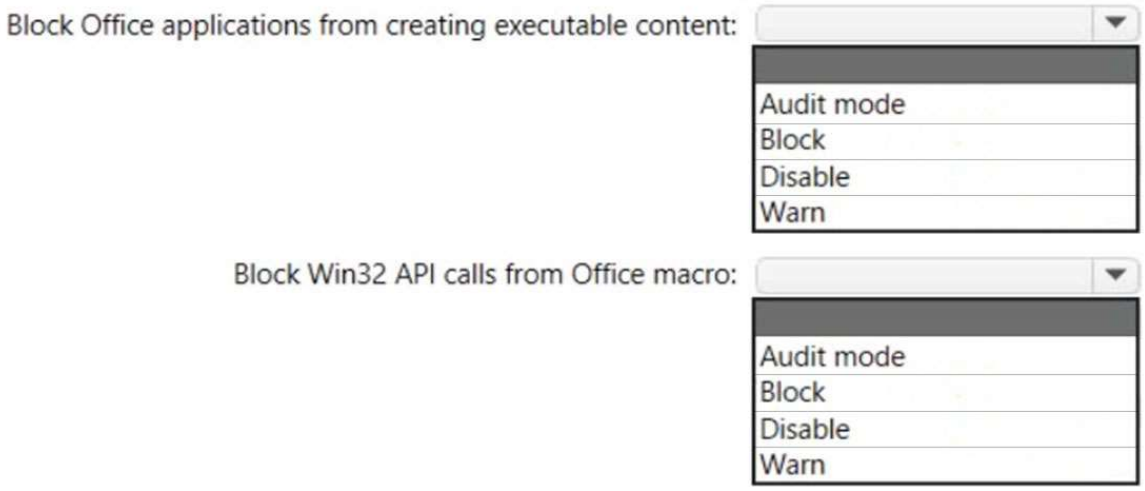
Currently, the settings are disabled locally on each device.

What are the effective settings on the devices? To answer, select the appropriate options in the answer area.

NOTE: Each correct selection is worth one point.

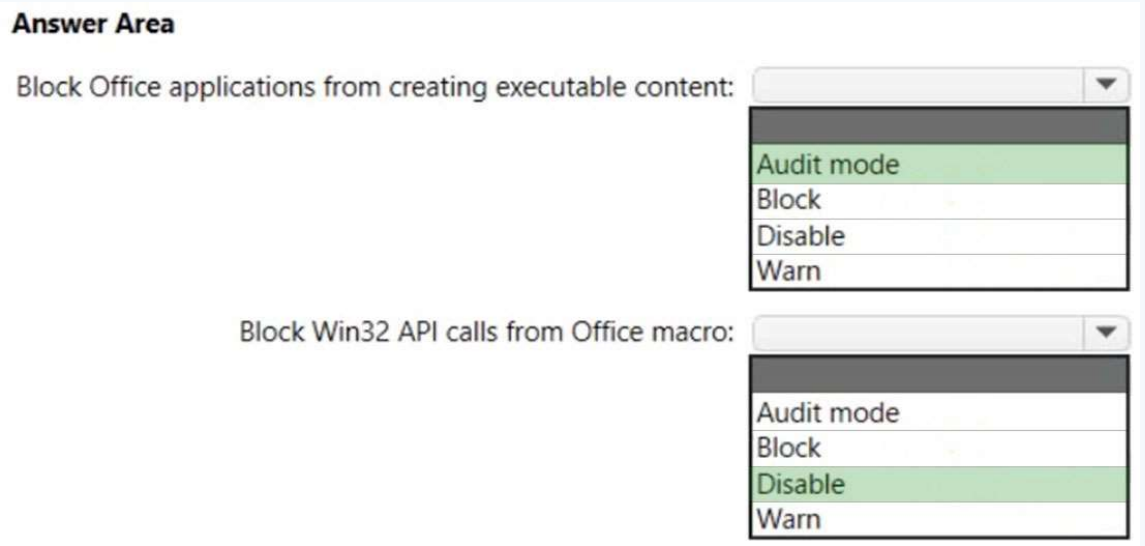
Hot Area:

Answer Area



Correct Answer:

Answer Area



Box 1: Audit mode -

According to the ASR Endpoint Security profile and to the MDM Security Baseline profile

, Block Office applications from creating executable content is set to Audit mode.

Box 2: Disable -

Block Win32 API calls from Office macro: According to MDM Security Baseline profile it is set to disable. According to the ASR Endpoint Security profile it is set to

Audit mode.

The profiles are merged. The Baseline profile overrides the Endpoint Security profile.

Note:

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.

Attack surface reduction rule merge behavior is as follows:

Endpoint security > Security baselines > Microsoft Defender for Endpoint Baseline > Attack Surface Reduction Rules.

MDM Security Baseline profile ASR Endpoint Security profile.

Reference:

https://docs.microsoft.com/en-us/mem/intune/protect/endpoint-security-asr-policy

junior6995 3 weeks ago

Is it too easy or I missed something?

upvoted 1 times

HOTSPOT -

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

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

MFA has a trusted IP address range of 123.30.20.0/24.

You have the Azure AD named locations shown in the following table.

Name	IP address range	Trusted
Location1	64.10.10.0/24	Yes
Location2	210.77.11.0/24	No

You create a Conditional Access policy that has the following settings:

⇨ Name: CAPolicy1

⇨ Assignments

- Users or workload identities
- Include: Group1
- Cloud apps or actions: App1

⇨ Conditions

- Locations
- Include: All trusted locations

⇨ Access controls

- Grant access
- Require multi-factor authentication

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 connects to App1 from a device that has an IP address of 210.77.11.10, the user will be prompted for MFA.	○	○
If User1 connects to App1 from a device that has an IP address of 64.10.10.15, the user will be prompted for MFA.	○	○
If User2 connects to App1 from a device that has an IP address of 123.30.20.10, the user will be prompted for MFA.	○	○

Correct Answer:

Answer Area

Statements	Yes	No
If User1 connects to App1 from a device that has an IP address of 210.77.11.10, the user will be prompted for MFA.	○	○
If User1 connects to App1 from a device that has an IP address of 64.10.10.15, the user will be prompted for MFA.	○	○
If User2 connects to App1 from a device that has an IP address of 123.30.20.10, the user will be prompted for MFA.	○	○

Box 1: Yes -

Location2 is not trusted.

Box 2: No -

Location1 is trusted.

Box 3:No -

MFA IP range is also trusted.

Reference:

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

TonySuccess 2 weeks, 2 days ago

Why won't user 2 be prompted for MFA in answer 3? They are not in a trusted location.

upvoted 1 times

TonySuccess 2 weeks, 2 days ago

Yes they are: MFA has a trusted IP address range of 123.30.20.0/24.

Missed that hehe.

upvoted 1 times

Mnguyen0503 3 weeks, 6 days ago

I feel like it should be N N N

User 1 MFA is disabled. That should override the Conditional Access Rule. So he won't be prompted for 2FA anywhere. Please correct me if I'm wrong

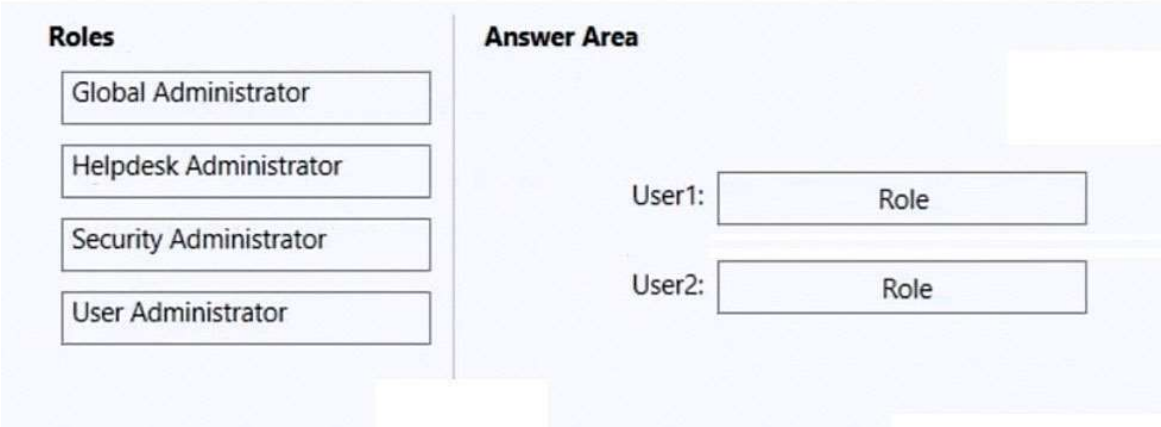
upvoted 1 times

tecnicosoffshoretech 3 weeks, 2 days ago

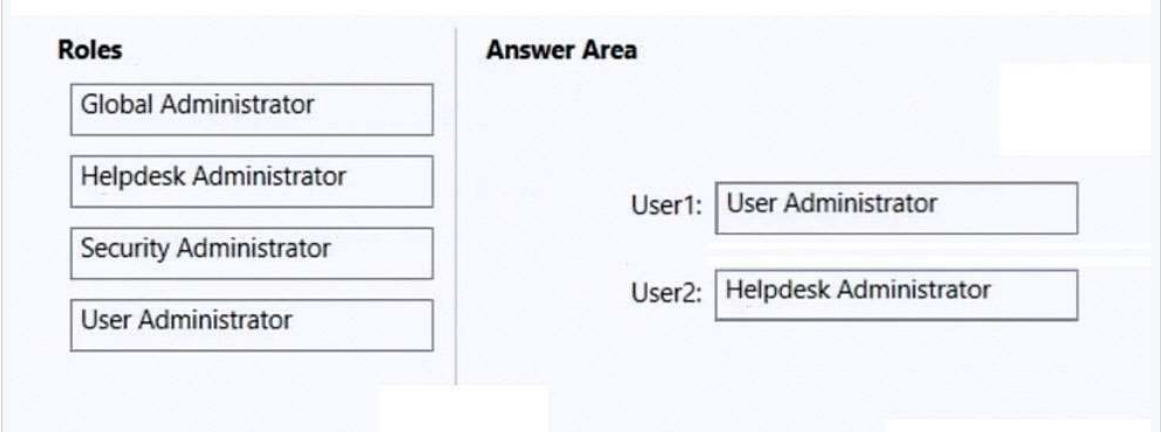
i think you are wrong. MFA for user 1 is disabled but he will be requested to register to MFA as soon as she tries to connect from the untrusted network

upvoted 2 times

DRAG DROP -
You have a Microsoft 365 subscription that contains two users named User1 and User2.
You need to ensure that the users can perform the following tasks:
User1 must be able to create groups and manage users.
▪
⇨ User2 must be able to reset passwords for nonadministrative users.
The solution must use the principle of least privilege.
Which role should you assign to each user? To answer, drag the appropriate roles to the correct users. Each role 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:



Correct Answer:



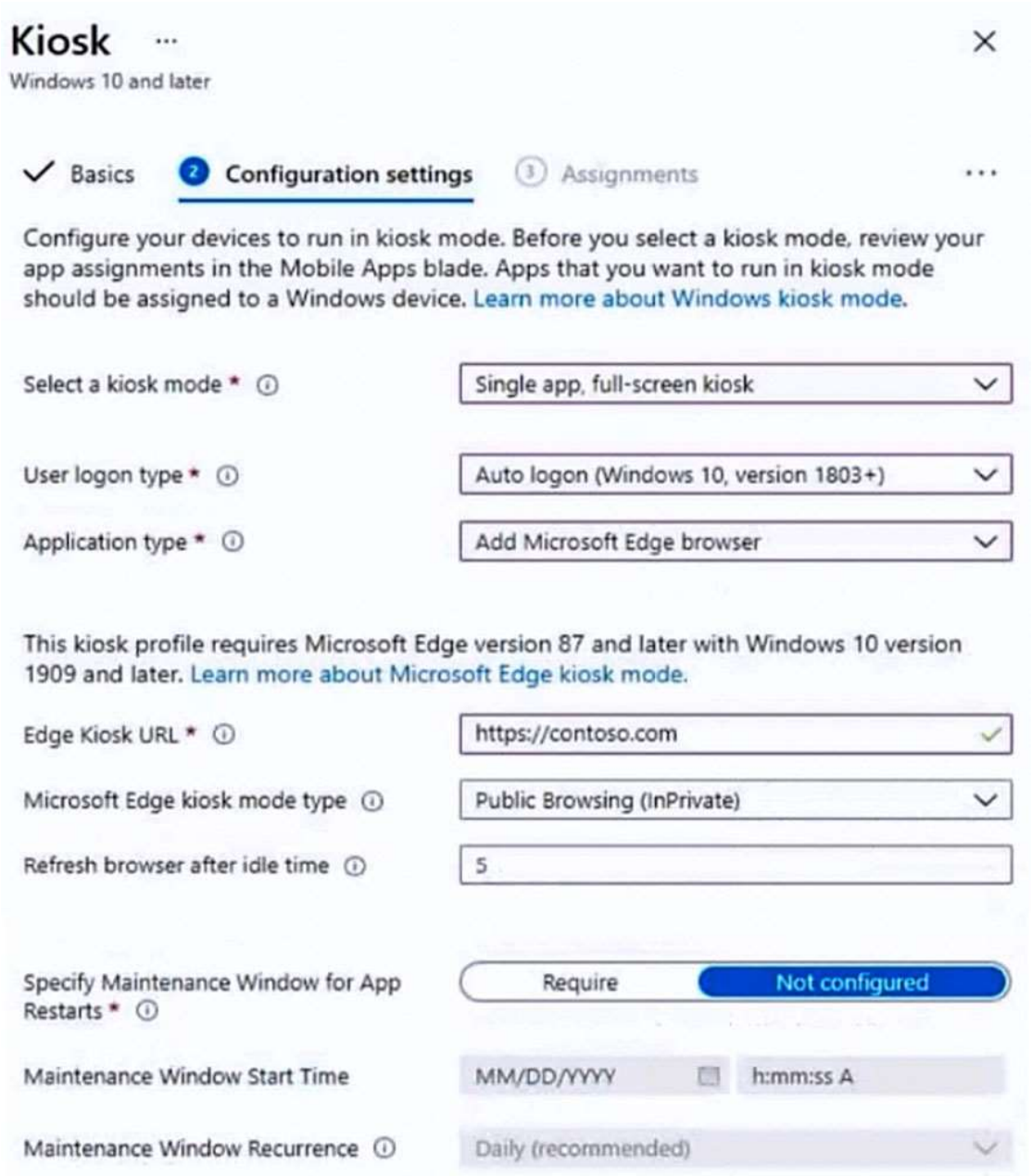
Box 1: User Administrator -

User admin -
Assign the user admin role to users who you want to access and manage user password resets and manage users and groups. They can also open and manage support requests to Microsoft support.

Box 2: Helpdesk Administrator -
Assign the Helpdesk admin role to users who want to reset passwords, force users to sign out for any security issues. They can also open and manage support requests to Microsoft support. The Helpdesk admin can only help non-admin users and users assigned these roles: Directory reader, Guest inviter, Helpdesk admin, Message center reader, and Reports reader.
Reference:
https://docs.microsoft.com/en-us/microsoft-365/admin/add-users/admin-roles-page

HOTSPOT -

You have the device configuration profile 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.

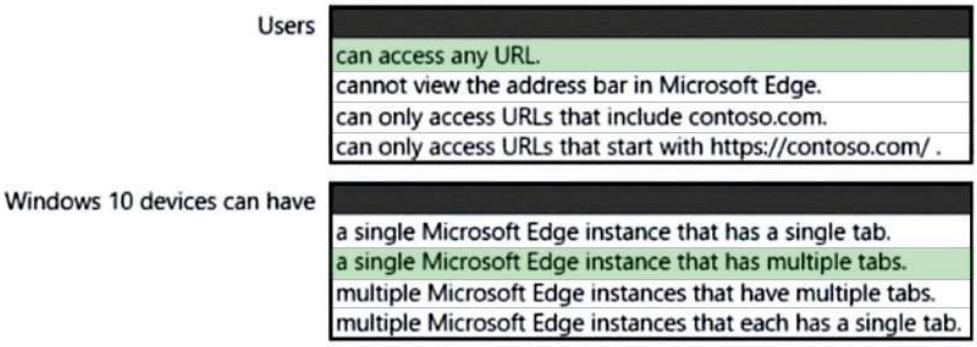
Hot Area:

Answer Area

Users	can access any URL. cannot view the address bar in Microsoft Edge. can only access URLs that include contoso.com. can only access URLs that start with https://contoso.com/ .
Windows 10 devices can have	a single Microsoft Edge instance that has a single tab. a single Microsoft Edge instance that has multiple tabs. multiple Microsoft Edge instances that have multiple tabs. multiple Microsoft Edge instances that each has a single tab.

Correct Answer:

Answer Area



Box 1: can access any URL.

Public Browsing (InPrivate): Runs a limited multi-tab version of Microsoft Edge. Users can browse publicly, or end their browsing session.

Box 2: a single Microsoft Edge instance that has multiple tabs

Single app, full-screen kiosk runs only one app on the device, such as a web browser or Store app.

Reference:

https://docs.microsoft.com/en-us/mem/intune/configuration/kiosk-settings-windows

Question #79 *Topic 3*

You have a Microsoft 365 subscription.
You plan to use Conditional Access policies.
You need to identify which scenarios the policies will support.
Which two scenarios should you identify? Each correct answer presents a complete solution.
NOTE: Each correct selection is worth one point.

A. Enforce multi-factor authentication (MFA) when users access a Microsoft Office 365 service.

B. Force users to renew an expired SSL certificate.

C. Force users to update Windows Defender definition files before they sign in to Microsoft Office 365.

D. Block users from using legacy authentication when signing in to Microsoft Exchange Online.

E. Force users to install the latest Windows and Microsoft Office updates before they sign in to Office 365.

Correct Answer: *AD*
A: Conditional Access allows administrators to control what Office 365 apps users can gain access to based on if they pass/fail certain conditions. These conditions are enforced by building a policy (or multiple policies) to control how users access your Office 365 resources.
Cloud Apps- What apps do you want to control? Conditional Access does not need to apply to all of Office 365, you can be more granular and just control access to specific apps λ€" E.g. Exchange Online.
Access can be allowed to Office 365 with the following conditions:
* Require multi-factor authentication λ€" User is allowed in but will need to complete additional security to log in.
* Etc.
D: The easiest way to block legacy authentication across your entire organization is by configuring a Conditional Access policy that applies specifically to legacy authentication clients and blocks access.
Reference:
https://docs.microsoft.com/en-us/azure/active-directory/conditional-access/block-legacy-authenticationhttps://docs.microsoft.com/en-us/azure/active- directory/conditional-access/block-legacy-authentication

TonySuccess 2 weeks, 2 days ago
Selected Answer: AD
Correct answers.
upvoted 1 times

HOTSPOT -

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

Name	Platform	Encryption	Secure Boot	Member of
Device1	Windows 10	Yes	No	Group1
Device2	Windows 10	No	Yes	Group2
Device3	Android	No	*Not applicable*	Group3

Intune includes the device compliance policies shown in the following table.

Name	Platform	Encryption	Secure Boot
Policy1	Windows 10	Not configured	Not configured
Policy2	Windows 10	Not configured	Required
Policy3	Windows 10	Required	Required
Policy4	Android	Not configured	*Not applicable*

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

Name	Assigned to
Policy1	Group1
Policy2	Group1, Group2
Policy3	Group3
Policy4	Group3

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

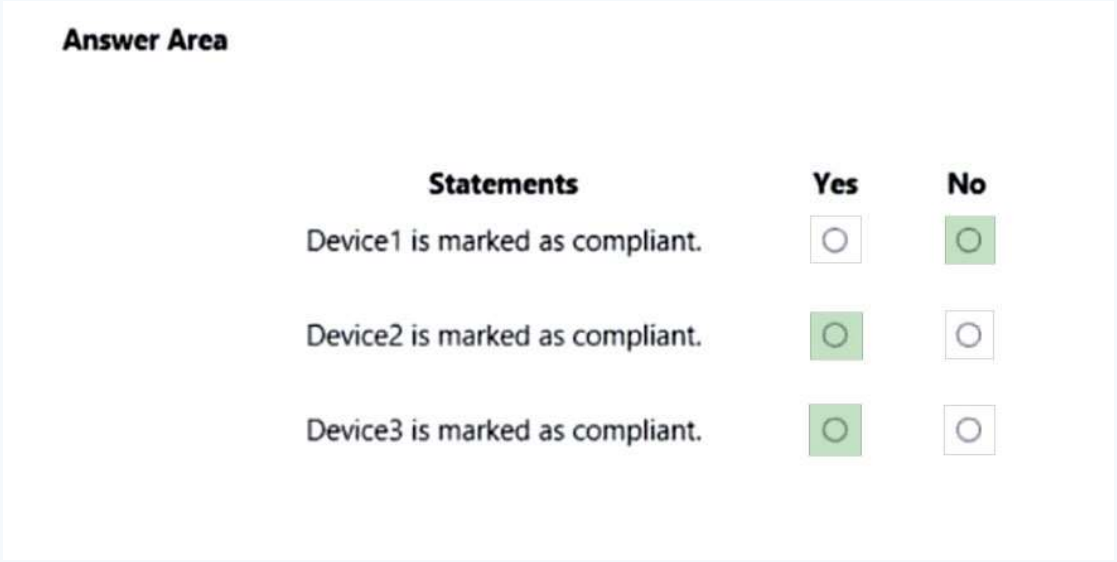
NOTE: Each correct selection is worth one point.

Hot Area:

Answer Area

Statements	Yes	No
Device1 is marked as compliant.	○	○
Device2 is marked as compliant.	○	○
Device3 is marked as compliant.	○	○

Correct Answer:



Box 1: No -
Device1 is in Group1. Policy1 is assigned to Group1. Policy2 is also assigned to Group1. Device1 is compliant to Policy1, but not compliant to Policy2 (fails on
Secure Boot).
By default, each device compliance policy includes the action to mark a device as noncompliant if it fails to meet a policy rule.

Box 2: Yes -
Device2 is in Group2. Policy2 is assigned to Group2. Device2 is compliant to Policy2 (Secure boot met).

Box 3: Yes -
Device3 is in Group 3. Policy3 and Policy4 are assigned to Group3. Policy3 is for Windows 10 so it is disregarded. Device3 is compliant to Policy4.
Reference:
https://docs.microsoft.com/en-us/mem/intune/protect/device-compliance-get-started

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

Name	Location type	Configuration
Location1	IP ranges	40.77.182.32/27
Location2	Countries (IP)	Canada
Location3	IP ranges	2a01:111::/32
Location4	Countries (IP)	Australia Include unknown countries/regions
Location5	Countries (GPS)	United States

You need to create a Conditional Access policy that will have a condition to include only trusted locations.
Which two named locations can be marked as trusted? Each correct answer presents a complete solution.
NOTE: Each correct selection is worth one point.

A. Location1

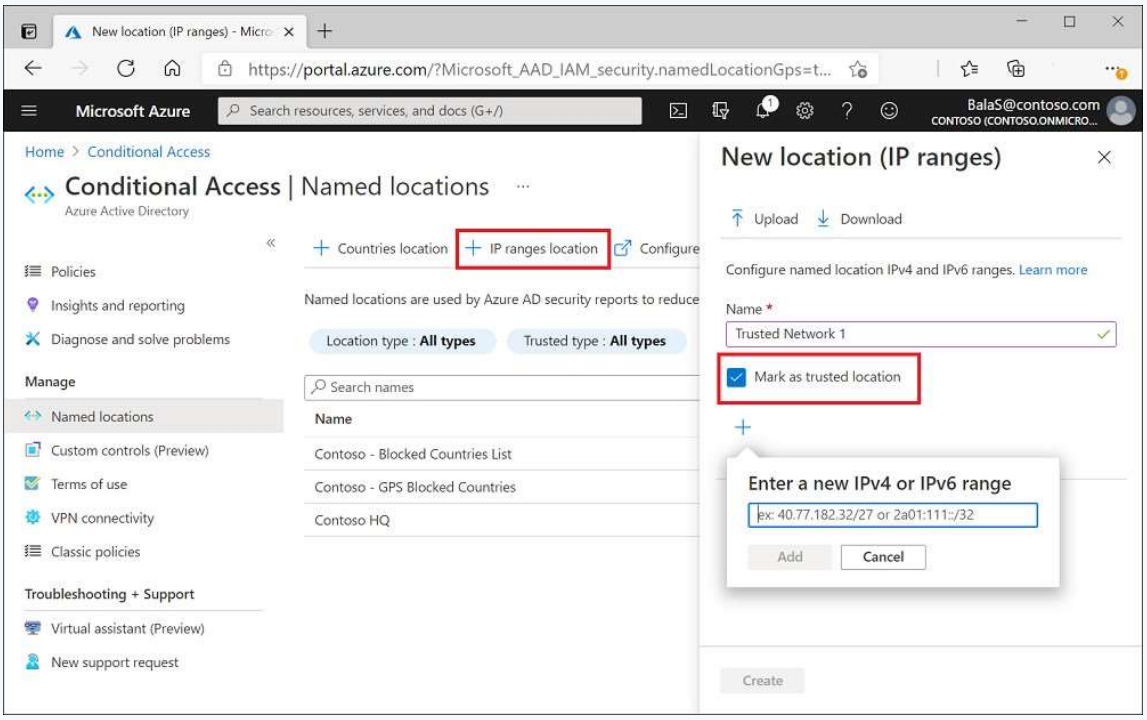
B. Location2

C. Location3

D. Location4

E. Location5

Correct Answer: *AC*
Trusted locations -
Administrators can name locations defined by IP address ranges to be trusted named locations
A: An IPv4 named location can be marked as trusted.



C: An IPv6 named location can be marked as trusted.
Reference:
https://docs.microsoft.com/en-us/azure/active-directory/conditional-access/location-condition

Question #82 *Topic 3*

You have a Microsoft 365 subscription,
You need provide a user the ability to disable Security defaults and create Conditional Access policies. The solution must use the principle of least privilege.
Which role should you assign to the user?

A. Global Administrator

B. Conditional Access Administrator

C. Security Administrator

D. Intune Administrator

Correct Answer: *B*
To enable or disable security defaults in your directory, sign in to theλ€‰Azure portalλ€‰as a security administrator, Conditional Access administrator, or global administrator.
Note: Conditional Access Administrator
Users with this role have the ability to manage Azure Active Directory Conditional Access settings.
Reference:
https://docs.microsoft.com/en-us/azure/active-directory/fundamentals/concept-fundamentals-security-defaults

bensrayan 2 weeks, 1 day ago
Correct !
Conditional Access administrator can disable security default:
https://learn.microsoft.com/en-us/azure/active-directory/fundamentals/concept-fundamentals-security-defaults
upvoted 2 times

Question #83 *Topic 3*

HOTSPOT -

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

You plan to create a Conditional Access policy to block users that have a high sign-in risk level.

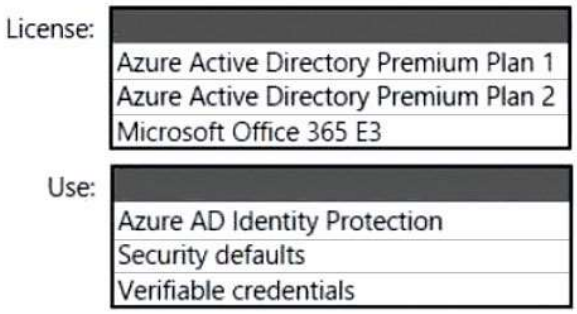
You need to identify the required license, and what to use to identify the sign-in risk level. The solution must minimize costs.

To answer, select the appropriate options in the answer area.

NOTE: Each correct selection is worth one point.

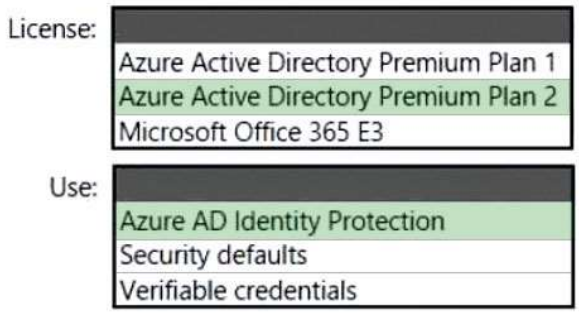
Hot Area:

Answer Area



Correct Answer:

Answer Area



Box 1: Azure AD Premium Plan 2 -

You will need an Azure AD Premium P1 license to get access to the Microsoft Office 365 conditional access policy feature.

However, need Azure AD Premium Plan 2 to sign-in risk.

Box 2: Azure AD Identity Protection

A sign-in risk represents the probability that a given authentication request isn't authorized by the identity owner. Organizations with Azure AD Premium P2 licenses can create Conditional Access policies incorporating Azure AD Identity Protection sign-in risk detections.

Reference:

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

https://blog.mydock365.com/what-is-conditional-access-in-microsoft-365

bensrayan 2 weeks, 1 day ago

Seems to be correct , look on the License requirements in this link :
https://learn.microsoft.com/en-us/azure/active-directory/identity-protection/overview-identity-protection

upvoted 1 times

Topic 4 - Question Set 4

Question #1 *Topic 4*

You have 200 computers that run Windows 10. The computers are joined to Microsoft Azure Active Directory (Azure AD) and enrolled in Microsoft Intune.
You need to ensure that only applications that you explicitly allow can run on the computers.
What should you use?

A. Microsoft Defender Credential Guard

B. Microsoft Defender Exploit Guard

C. Microsoft Defender Application Guard

D. Microsoft Defender Application Control

Correct Answer: *D*
Application control can help mitigate these types of security threats by restricting the applications that users are allowed to run and the code that runs in the
System Core (kernel). Application control policies can also block unsigned scripts and MSIs, and restrict Windows PowerShell to run in Constrained Language
Mode.
Reference:
https://docs.microsoft.com/en-us/windows/security/threat-protection/windows-defender-application-control/windows-defender-application-control

Arndog Highly Voted 1 year, 5 months ago
D is the answer
upvoted 19 times

Jimbob77 1 year, 4 months ago
Windows Defender Application Control
WDAC was introduced with Windows 10 and allows organizations to control which drivers and applications are allowed to run on their Windows 10 clients
https://docs.microsoft.com/en-us/windows/security/threat-protection/windows-defender-application-control/wdac-and-applocker-overview
this would support the correct answer to be: D
upvoted 5 times

CVT24 1 year, 4 months ago
Man who comes up with the answer to these questions?
D is clearly the answer
Windows Defender Application Control restricts the applications that users can run. Application Control only allows trusted apps to be used. This stops hackers accessing the system through compromised apps.
upvoted 4 times

raduM Most Recent 1 month, 2 weeks ago
d is correct
upvoted 1 times

ZahiLevi 4 months, 2 weeks ago
Selected Answer: D
D is the answer
Application Control is a software-based security layer that enforces an explicit list of software that is allowed to run on a PC. On its own
https://docs.microsoft.com/en-us/mem/configmgr/protect/deploy-use/use-device-guard-with-configuration-manager
upvoted 4 times

moobdoob 8 months, 2 weeks ago
Application control is correct.
upvoted 3 times

jibutoms 1 year, 3 months ago
Answer is D: The reference in the answer is given as https://docs.microsoft.com/en-us/windows/security/threat-protection/device-guard/introduction-to-device-guard-virtualization-based-security-and-windows- defender-application-control .
upvoted 1 times

Ouianonymous 1 year, 4 months ago
"Note that prior to Windows 10, version 1709, Windows Defender Application Control was known as configurable code integrity (CCI). WDAC was also one of the features which comprised the now-defunct term 'Device Guard"
upvoted 2 times

Layer8 1 year, 4 months ago
D, Application Guard is protections for Microsoft Edge specifically i believe
upvoted 3 times

JurFur 1 year, 4 months ago
This should be indeed be D. Windows Defender Application Control.
upvoted 4 times

Question #2 *Topic 4*

Note: This question is part of a series of questions that present the same scenario. Each question in the series contains a unique solution that might meet the stated goals. Some question sets might have more than one correct solution, while others might not have a correct solution.
After you answer a question in this section, you will NOT be able to return to it. As a result, these questions will not appear in the review screen.
Your company has several Windows 10 devices that are enrolled in Microsoft Intune.
You deploy a new computer named Computer1 that runs Windows 10 and is in a workgroup.
You need to enroll Computer1 in Intune.
Solution: From Computer1, you sign in to https://portal.manage.microsoft.com and use the Devices tab.
Does this meet the goal?

A. Yes

B. No

Correct Answer: *B*
Use MDM enrolment.
MDM only enrollment lets users enroll an existing Workgroup, Active Directory, or Azure Active directory joined PC into Intune. Users enroll from Settings on the existing Windows PC.
Reference:
https://docs.microsoft.com/en-us/mem/intune/enrollment/windows-enrollment-methods

thecomodor Highly Voted 1 year, 7 months ago
This should be Yes. You can sign in to https://portal.manage.microsoft.com with your Azure Ad account and access company apps and enroll the device in Intune
upvoted 14 times

Mr01z0 Highly Voted 1 year, 6 months ago
This should be Yes, the question is only stating that the device needs to be registered in intune.

This approach is valid for registering a windows 10 device with intune. Auto enrollment has to be enabled (Azure premium P1). The device will be registered in Intune as a personally owned windows 10 device.

When you login to the company portal website you will have the option to add a device, then you will be redirected to the settings blade to Accounts -> Access Work or School from there you can enroll your device with company credentials.

It is maybe not what you want for a large company rollout, but nonetheless it's a valid way to add devices to intune.

https://docs.microsoft.com/en-us/mem/intune/enrollment/windows-enrollment-methods#user-self-enrollment-in-intune
upvoted 8 times

AzureLearner01 Most Recent 5 months ago
These Questions and the provided answer are sometimes make you go crazy. Result from my Lab - freshly installed Windows 10 Enterprise VM, which was in the default Workgroup not domain-joined or Azure joined nor Azure registred. Went to the URL portal.manage.microsoft.com and logged in. Choosed devices and it promted again for Credentials. Checked after a few minutes in Azure->Yourtenant->Devices->Testdevice. Device is Azure AD Registred and MDM Microsoft Intune enrolled. Answer should be yes in my opinion. Grateful for feedback!
upvoted 3 times

MR_Eliot 5 months ago
Selected Answer: A
Just tested this. Answer should be Yes.
upvoted 3 times

Angarali 5 months, 2 weeks ago
The answer is No.

https://docs.microsoft.com/en-us/mem/intune/enrollment/windows-enrollment-methods
upvoted 1 times

Kifla 6 months, 1 week ago
If you follow that link you get to page that says the following:
"Getting this device managed might let you access other company resources available to you, such as email and documents. Go to Devices to get started."
And when you click Devices you can enroll this device in Intune. A is correct answer.
upvoted 1 times

forummj 8 months, 2 weeks ago
Personally, looking at how this is done, the fundamental point is "Devices tab" you don't use that to enroll a device, this is done from the Home tab of the company portal. So, I'm sticking with No as my answer.
upvoted 5 times

BrentOn 6 months, 3 weeks ago
I've personally looked at how this is done. gone to https://portal.manage.microsoft.com. You can definitely add devices (enroll) from the Devices tab.
upvoted 1 times

Rednevi 10 months, 1 week ago

Selected Answer: A

The Company Portal apps, Company Portal website, and Intune app on Android are where users access company data and can do common tasks. Common task may include enrolling devices, installing apps, and locating information (such as for assistance from your IT department).

https://docs.microsoft.com/en-us/mem/intune/apps/company-portal-app

upvoted 3 times

Goofer 10 months, 3 weeks ago

You need first import the Hardware Hash in Intune to deploy the device.

upvoted 3 times

NZS 5 months ago

No, hardware hash is for Autopilot

upvoted 1 times

[Removed] 11 months, 3 weeks ago

I just tested it and my device is only Azure AD registered, not Intune enrolled... I vote for B...

upvoted 1 times

[Removed] 11 months, 1 week ago

It's confusing... I change to Yes, because of https://docs.microsoft.com/en-us/troubleshoot/mem/intune/enroll-devices-in-intune-tip#7 "Provide the following instructions to users so that they can use your company's management portal for enrollment: In a web browser, go to portal.manage.microsoft.com. ...." I believe in MS Docs, not in me =P

upvoted 2 times

akah34 1 year, 3 months ago

The answer is YES.

upvoted 3 times

akah34 1 year, 3 months ago

The URL opens the company portal website. Users can use the website to search for apps, install them, and view, edit, add, and remove their registered devices. Windows 10 is supported by different types of devices (including desktop, smartphone, and tablet). The registration steps are the same on all devices. On a Windows 10 computer that is part of a workgroup, you can download the free Company Portal app from the Microsoft Store or use the web to register your device for device management through Microsoft Intune. Alternatively, you can use the "Access work or school account" page in the "Accounts" area of the Settings app to register your Windows 10 device. If your computer is part of an Active Directory domain (AD DS), the integration can also take place automatically as part of the synchronization using Azure AD Connect.

upvoted 1 times

Tomtom11 1 year, 3 months ago

I tried this with a E3 Licence. And Intune enrollment on//all user.
The device is AD registered in Azure and not enrolled in Intune

upvoted 2 times

Tomtom11 1 year, 5 months ago

Correct my lost post. I have joined to Azure AD put not reg to Intune?

upvoted 2 times

Tomtom11 1 year, 5 months ago

The answer is Yes. I just did it

upvoted 3 times

Question #3 *Topic 4*

Note: This question is part of a series of questions that present the same scenario. Each question in the series contains a unique solution that might meet the stated goals. Some question sets might have more than one correct solution, while others might not have a correct solution.
After you answer a question in this section, you will NOT be able to return to it. As a result, these questions will not appear in the review screen.
Your company has several Windows 10 devices that are enrolled in Microsoft Intune.
You deploy a new computer named Computer1 that runs Windows 10 and is in a workgroup.
You need to enroll Computer1 in Intune.
Solution: You install the Company Portal app on Computer1 and use the Devices tab from the app.
Does this meet the goal?

A. Yes

B. No

Correct Answer: *B*
Use MDM enrolment.
MDM only enrollment lets users enroll an existing Workgroup, Active Directory, or Azure Active directory joined PC into Intune. Users enroll from Settings on the existing Windows PC.
Reference:
https://docs.microsoft.com/en-us/mem/intune/enrollment/windows-enrollment-methods

DJM Highly Voted 1 year, 10 months ago
Company portal method only registers devices with AAD, not joins them. It is designed for end-users connecting personal/BYOD devices and not for administrators to deploy PCs. https://docs.microsoft.com/en-us/mem/intune/enrollment/windows-enrollment-methods
upvoted 18 times

Anthony_2770 1 year, 8 months ago
Agree.
DJM has offerred decisive comments to both MD-101 and MD-100. Excellent contribution
upvoted 7 times

john909 10 months, 4 weeks ago
Yes, this does enroll the device to intune:

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

"Bring your own device (BYOD): Users enroll their personally owned devices by downloading and installing the Company Portal App
This process:
Registers the device with Azure Active Directory to gain access to corporate resource like email.
Enrolls the device in Intune as a personal owned device (BYOD). If an administrator has configured Auto enrollment (available with Azure AD premium subscriptions), the user only has to enter their credentials once. Otherwise, they'll have to enroll separately through MDM only enrollment and reenter their credentials."
upvoted 5 times

Timmi 1 year, 8 months ago
Questions says: "You need to enroll Computer1 in Intune."

According to your link this registers the device in AAD and enrolls to Intune. So this does meet the goal.

Answer: Yes
upvoted 9 times

Angarali 5 months, 2 weeks ago
I would also support this, the answer is Yes

https://docs.microsoft.com/en-us/mem/intune/user-help/enroll-windows-10-device
upvoted 1 times

LordCaine 1 year ago
Incorrect: Use Intune Company Portal to enroll devices running on Windows 10, version 1607 and later. The answer should be yes.
https://docs.microsoft.com/en-us/mem/intune/user-help/enroll-windows-10-device
upvoted 4 times

AzureLearner01 5 months ago
Disagree, yes the device is Azure registred but also Microsoft Intune enrolled after this approach. So answer is no - verified in my lab
upvoted 2 times

RodrigoT 5 months ago
If the device is enrolled then the answer is A. Yes. Check the link:

https://docs.microsoft.com/en-us/mem/intune/user-help/enroll-windows-10-device

There is also a video and several screenshots showing how to use the Company Portal app.
upvoted 1 times

RodrigoT 5 months ago

I guess they answered No just because when you install the app for the first time and open it you are unable to use the Devices tab. I have to sign in first. Only then you will have the Devices tab available. Tested on two computers. One was already registered and the other was brand new.

upvoted 3 times

Cisco Most Recent 5 months ago

I find this question fairly confusing as there seems to be articles indicating yes and no for the company portal. To see for myself I enrolled my device into Azure and made certain there was no trace of it in Intune. Later on when I had some more spare time I downloaded the Company Portal App and I have no enrolled my test device into intune, so for me its a yes. I didnt need to do anything with the devices tab though, not sure what that bits about.

upvoted 1 times

Cisco 5 months ago

Is it marked wrong because the device is not already enrolled in Azure? In my case I enrolled it in Azure and then enrolled in intune afterwards using the portal app. So the app does indeed enroll it in Intune but it its not already in Azure it wouldnt.

upvoted 2 times

AzureLearner01 5 months ago

Verified in my lab - Windows 10 Device, freshly installed, worgroup, downloaded Company Portal App from the Store, went to Devices and logged in with Work or School Account. Device was afterwards registred in Azure AD an MDM Microsoft Intune enrolled.

upvoted 2 times

lykeP 8 months, 3 weeks ago

A is the correct answer.
Company Portal App This process:
Registers the device with Azure Active Directory to gain access to corporate resource like email.
Enrolls the device in Intune as a personal owned device (BYOD). If an administrator has configured Auto enrollment (available with Azure AD premium subscriptions), the user only has to enter their credentials once. Otherwise, they'll have to enroll separately through MDM only enrollment and reenter their credentials.

upvoted 1 times

lykeP 8 months, 3 weeks ago

Selected Answer: A

A is the correct answer.
Company Portal App This process:
Registers the device with Azure Active Directory to gain access to corporate resource like email.
Enrolls the device in Intune as a personal owned device (BYOD). If an administrator has configured Auto enrollment (available with Azure AD premium subscriptions), the user only has to enter their credentials once. Otherwise, they'll have to enroll separately through MDM only enrollment and reenter their credentials.

upvoted 2 times

Rednevi 10 months, 1 week ago

Voting A:

The Company Portal apps, Company Portal website, and Intune app on Android are where users access company data and can do common tasks. Common task may include enrolling devices, installing apps, and locating information (such as for assistance from your IT department).

https://docs.microsoft.com/en-us/mem/intune/apps/company-portal-app

upvoted 2 times

Pleebb 1 year, 3 months ago

when launching Company Portal the prompts are not always available. Prompts are configured to show or not show. But Company Portal must be configured to will allow user to enroll device. Device tab will work, if there is no prompt.

upvoted 1 times

ThomasDehottay 1 year, 3 months ago

I think it would be yes if the question was asking whether we can enroll this device as a "BYOD" device. But here I think the question is asking implicitly whether an administrator can enroll a device with this method. In an enterprise environment, that's not the method that should be used.
The question is a bit confusing for me...

upvoted 1 times

Perycles 1 year, 3 months ago

answer is YES

upvoted 1 times

Perycles 1 year, 3 months ago

NOOOOOOO - using "account settings" or "company Portal" , register in AAD , it's sure BUT nothing says that auto enrollement option is enabled to push the device into intune !!!!

upvoted 2 times

b33droid 1 year, 5 months ago

Answer is "No",because out of enrollment consideration, the solution isn't correct because you can't use the Device tab without sign-in previously.

"Solution: You install the Company Portal app on Computer1 and use the Devices tab from the app."

upvoted 2 times

Wilf32 1 year, 5 months ago

From the video in this link on a Microsoft page i would say the answer is YES.

https://docs.microsoft.com/en-us/mem/intune/user-help/enroll-windows-10-device

upvoted 1 times

techh3ad 1 year, 6 months ago

Although this answer is not correct because you don't go to the Devices tab. After you register into AAD, you have to click on the yellow warning on the Home screen of the app that says "This device hasn't been set up for corporate use yet..." and follow the prompts to enroll into InTune.

upvoted 4 times

techh3ad 1 year, 6 months ago

The Company Portal app allows the user account and device to register with AAD, and can enroll the device into Intune.

https://docs.microsoft.com/en-us/mem/intune/user-help/enroll-windows-10-device

upvoted 3 times

miry117 1 year, 7 months ago

The answer is NO.
A new (non-existing) Windows 10 device that is in workgroup and has a local user installs company portal and uses the devices tab. The result will be an Azure AD Registered device without MDM, therefore not enrolled in Intune.
Tested in a real environment.

upvoted 4 times

j0eyv 1 year, 10 months ago

I should say Yes to.

upvoted 2 times

PatTOM 1 year, 11 months ago

Answer should be yes.
https://docs.microsoft.com/bg-bg/mem/intune/user-help/enroll-windows-10-device

upvoted 3 times

goran 1 year, 11 months ago

why the answer is No? from the setting we can enroll the windows to MDM

upvoted 2 times

Question #4 *Topic 4*

Note: This question is part of a series of questions that present the same scenario. Each question in the series contains a unique solution that might meet the stated goals. Some question sets might have more than one correct solution, while others might not have a correct solution.
After you answer a question in this section, you will NOT be able to return to it. As a result, these questions will not appear in the review screen.
Your company has several Windows 10 devices that are enrolled in Microsoft Intune.
You deploy a new computer named Computer1 that runs Windows 10 and is in a workgroup.
You need to enroll Computer1 in Intune.
Solution: From the Settings app on Computer1, you use the Connect to work or school account settings.
Does this meet the goal?

A. Yes

B. No

Correct Answer: *B*
Use MDM enrolment.
MDM only enrollment lets users enroll an existing Workgroup, Active Directory, or Azure Active directory joined PC into Intune. Users enroll from Settings on the existing Windows PC.
Reference:
https://docs.microsoft.com/en-us/mem/intune/enrollment/windows-enrollment-methods

marz Highly Voted 1 year, 7 months ago
I'm going for No. This joins the device to AAD but does not enroll in Intune beause no auto enrollment has been configured.
upvoted 15 times

Perycles 1 year, 3 months ago
totally exact ! nothing says that auto enrollement is enabled.
upvoted 4 times

RodrigoT 5 months, 1 week ago
If your tenant is not configured for auto-enrollment, you just have to go through the enrollment flow a second time to connect your device to MDM. Anyway is always using the settings app. The right answer is YES.
https://docs.microsoft.com/en-us/windows/client-management/mdm/mdm-enrollment-of-windows-devices#connect-personally-owned-devices
Check point 5, the third paragraph.
upvoted 4 times

Anthony_2770 1 year, 7 months ago
I agree
upvoted 5 times

Angarali 5 months, 2 weeks ago
I agree with you.

https://docs.microsoft.com/en-us/mem/intune/enrollment/windows-enrollment-methods
upvoted 1 times

RodrigoT 5 months ago
Your own link says: "Users enroll from Settings on the existing Windows PC". You don't need autoenrollment configured. If your tenant is not configured for auto-enrollment, you just have to go through the enrollment flow a second time to connect your device to MDM. The right answer is YES. Check the link, point 5, the third paragraph:

https://docs.microsoft.com/en-us/windows/client-management/mdm/mdm-enrollment-of-windows-devices#connect-personally-owned-devices
upvoted 3 times

LordCaine 1 year ago
This should be incorrect, it used to work but the latest versions use the company portal as described here:
Use Intune Company Portal to enroll devices running on Windows 10, version 1607 and later.
Enroll devices running Windows 10, version 1511 and earlier. Company Portal doesn't support these versions, so setup is done in the Settings app.

https://docs.microsoft.com/en-us/mem/intune/user-help/enroll-windows-10-device
upvoted 4 times

AzureLearner01 Most Recent 5 months ago
I would choose yes, tried this in my lab and it also registred my device in azure ad and enrolled it in intune.
upvoted 2 times

defrey 8 months, 3 weeks ago
Is YES ". Once you've set up Intune, users enroll Windows devices by signing in with their work or school account.
"
https://docs.microsoft.com/en-us/mem/intune/enrollment/windows-enroll
upvoted 2 times

Garito 7 months, 1 week ago
So in essence the answer is B No because the question does not mention 'once intune is setup with auto-enroll'

upvoted 1 times

RodrigoT 5 months, 1 week ago

Not necessarily. If your tenant is not configured for auto-enrollment, you will have to go through the enrollment flow a second time to connect your device to MDM. Anyway is always using the settings app. The right answer is YES.
https://docs.microsoft.com/en-us/windows/client-management/mdm/mdm-enrollment-of-windows-devices#connect-personally-owned-devices
Check point 5, the third paragraph.

upvoted 1 times

DogeZaemon 11 months, 1 week ago

Answer is Yes
https://docs.microsoft.com/en-us/windows/client-management/mdm/mdm-enrollment-of-windows-devices
-> Connect to MDM on a desktop (enrolling in device management)

upvoted 2 times

Heimdallr 1 year, 3 months ago

I would say yes and no to other this type questions - In order to enroll to Intune device needs to be Azure AD Joined or registered at least. If device is in WORKGROUP it literally is denied access to Intune as it is not in Azure AD. Work or School actually allows you to join Azure AD, which is the first step to Intune registration. This isn't specified but I would say yes, in case the auto enroll devices that are in Azure AD is turned on

upvoted 2 times

Perycles 1 year, 3 months ago

Finally yes. Mdm only enrollement is possible wish string options.https://docs.microsoft.com/en-us/mem/intune/enrollment/windows-enrollment-methods#user-self-enrollment-in-intune

upvoted 2 times

Tomtom11 1 year, 3 months ago

Enroll in MDM only
If you want to enroll a Windows device using this method, use the following procedure: 1. Enable Windows Automatic Enrollment for either all users or for an appropriate group to
whom the designated account (which you use in step 6) belongs.
2. Sign in to your Windows 10 computer and open Settings.
3. Click Accounts.
4. Select the Access Work Or School tab.
5. On the Access Work Or School tab, click Enroll Only In Device Management.
6. In the Microsoft Account window, enter the organizational email account.

upvoted 1 times

Ediddy 1 year, 4 months ago

I think this makes it YES
Azure Active Directory (Azure AD) Join - Joins the device with Azure Active Directory and enables users to sign in to Windows with their Azure AD credentials. If Auto Enrollment is enabled, the device is automatically enrolled in Intune. The benefit of auto enrollment is a single-step process for the user. Otherwise, they'll have to enroll separately through MDM only enrollment and reenter their credentials. Users enroll this way either during initial Windows OOBE or from Settings. The device is marked as a corporate owned device in Intune.

upvoted 1 times

Ediddy 1 year, 4 months ago

I take this back. The computer is in a workgroup. The answer is NO.

upvoted 2 times

ramankatoch 1 year, 5 months ago

The correct answer is A verified from the MS FTE

upvoted 1 times

techh3ad 1 year, 6 months ago

Yes. This is doable. In Windows 10 1607 and later, you can enroll a device from System > Accounts > Access work or school > Connect.

https://docs.microsoft.com/en-us/mem/intune/user-help/enroll-windows-10-device

upvoted 3 times

Mr01z0 1 year, 6 months ago

This should be Yes, the question is only stating that the device needs to be registered in intune.

This approach is valid for registering a windows 10 device with intune. Auto enrollment has to be enabled (Azure premium P1). The device will be registered in Intune as a personally owned windows 10 device.

When you login to the company portal website you will have the option to add a device, then you will be redirected to the settings blade to Accounts -> Access Work or School from there you can enroll your device with company credentials.

It is maybe not what you want for a large company rollout, but nonetheless it's a valid way to add devices to intune.

https://docs.microsoft.com/en-us/mem/intune/enrollment/windows-enrollment-methods#user-self-enrollment-in-intune

upvoted 1 times

DJM 1 year, 10 months ago

No, this is valid for a user enrolling their device but not for an admin to deploy as per the question https://docs.microsoft.com/en-us/mem/intune/enrollment/windows-enrollment-methods

upvoted 4 times

CvdK 1 year, 10 months ago

Nowhere in the questions does it state that you are an Admin deploying the device. You might as well be the user.

upvoted 3 times

vinnyct 1 year, 9 months ago

It says " you deploy a computer" then it asks to enrol computer1 which means you are an IT Engineer instead of an end-user. I believe that an end-user does not deploy and enrol by own their device

upvoted 1 times

DergX 1 year, 7 months ago

Enroll in device management is a separate link on the same screen as connect to work or school. Tricky question but has nothing to do with being an Admin. If computer was AAD joined then yes connecting to work would also enroll but it specifically said workgroup so that's ruled out.

upvoted 1 times

JJSikma 2 years ago

No
This would Join the device, not Enrol it

upvoted 3 times

loganharris 2 years ago

Since computer is in a workgroup you must use MDM. From link provided
"MDM only enrollment lets users enroll an existing Workgroup, Active Directory, or Azure Active directory joined PC into Intune. Users enroll from Settings on the existing Windows PC. This method isn't recommended because it doesn't register the device into Azure Active Directory. It also prevents the use of features such as Conditional Access."

upvoted 3 times

CvdK 1 year, 10 months ago

Although this s not the required option for workgroup PC's. It is true that this will enroll the PC into intune. It may not be the best option to use, but the only goal in the question is to enroll it into intune. So the goal is met. Answer A.

upvoted 2 times

Cliffh 2 years ago

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

upvoted 1 times

marz 1 year, 7 months ago

This would imply auto enrollment to be set up which is not mentioned. Computer is in a workgroup so cannot be added to the auto enrollment profile.

upvoted 1 times

mlleremallqui 2 years, 1 month ago

Yes
https://docs.microsoft.com/es-es/azure/active-directory/user-help/user-help-join-device-on-network

upvoted 3 times

loganharris 2 years ago

This would be true if the computer were not in a workgroup

upvoted 2 times

ExamStudy101 1 year, 2 months ago

"MDM only enrollment lets users enroll an existing Workgroup, Active Directory, or Azure Active directory joined PC into Intune. Users enroll from Settings on the existing Windows PC. This method isn't recommended because it doesn't register the device into Azure Active Directory. It also prevents the use of features such as Conditional Access."

upvoted 1 times

HOTSPOT -

You have a Microsoft 365 subscription.

You plan to enroll devices in Microsoft Endpoint Manager that have the platforms and versions shown in the following table.

Platform	Version
Android	8, 9
iOS	11, 12

You need to configure device enrollment to meet the following requirements:

- Ensure that only devices that have approved platforms and versions can enroll in Endpoint Manager.
- Ensure that devices are added to Microsoft Azure Active Directory (Azure AD) groups based on a selection made by users during the enrollment.

Which device enrollment setting should you configure for each requirement? To answer, select the appropriate options in the answer area.

NOTE: Each correct selection is worth one point.

Hot Area:

Answer Area

Ensure that only devices that have approved platforms and versions can enroll in Endpoint Manager:

- Android enrollment
- Apple enrollment
- Corporate device identifiers
- Device categories
- Enrollment restrictions
- Windows enrollment

Ensure that devices are added to Azure AD groups based on a selection made by users during enrollment:

- Android enrollment
- Apple enrollment
- Corporate device identifiers
- Device categories
- Enrollment restrictions
- Windows enrollment

Correct Answer:

Answer Area

Ensure that only devices that have approved platforms and versions can enroll in Endpoint Manager:

- Android enrollment
- Apple enrollment
- Corporate device identifiers
- Device categories
- **Enrollment restrictions**
- Windows enrollment

Ensure that devices are added to Azure AD groups based on a selection made by users during enrollment:

- Android enrollment
- Apple enrollment
- Corporate device identifiers
- **Device categories**
- Enrollment restrictions
- Windows enrollment

Box 1: Enrollment restrictions -

As an Intune administrator, you can create and manage enrollment restrictions that define what devices can enroll into management with Intune, including the:

- Number of devices.
- Operating systems and versions.

Box 2: Device categories -

To make managing devices easier, you can use Microsoft Intune device categories to automatically add devices to groups based on categories that you define.

Device categories use the following workflow:

- Create categories that users can choose from when they enroll their device.
- When users of iOS/iPadOS and Android devices enroll a device, they must choose a category from the list of categories you configured. To assign a category to a Windows device, users must use the Company Portal website.
- You can then deploy policies and apps to these groups.

👉 You can create any device categories you want. For example:
- Point-of-sale device
- Demonstration device
- Sales
- Accounting
- Manager

Reference:
https://docs.microsoft.com/en-us/mem/intune/enrollment/enrollment-restrictions-set https://docs.microsoft.com/en-us/mem/intune/enrollment/device-group-mapping

Perycles Highly Voted 1 year, 3 months ago

Correct

upvoted 7 times

RodrigoT 5 months, 1 week ago

Enrollment resttrictions:
https://docs.microsoft.com/en-us/mem/intune/enrollment/enrollment-restrictions-set#create-a-device-platform-restriction
Device categories:
https://docs.microsoft.com/en-us/mem/intune/enrollment/device-group-mapping

upvoted 4 times

Moderator Most Recent 7 months ago

Yep, seems right.

upvoted 2 times

HOTSPOT -
Your company has 1,000 Windows 10 devices that are enrolled in Windows Analytics.
You need to view the following information:
⇨ The number of devices that are vulnerable to Spectre and Meltdown vulnerabilities
⇨ The number of devices that have Windows Defender real-time protection turned off
Which Windows Analytics solutions should you use? To answer, select the appropriate options in the answer area.
NOTE: Each correct selection is worth one point.
Hot Area:

Correct Answer:

Box 1: Device Health -

Driver health -
App health (outside of a deployment plan)
Frequently crashing devices or driver-induced crashes

Windows sign-in health -

Windows Information Protection -

Support for Windows Server -

Box 2: Device Health -
Incorrect:
* Update Compliance
Support for Windows Update for Business

Delivery Optimization insights -
Support for Windows 10 long-term servicing channel (LTSC)

Windows Insider reports -

Windows Defender status -
* Upgrade Readiness
Internet Explorer Site Discovery data
Microsoft 365 Apps add-in insights (now available in Configuration Manager)

Feedback Hub insights -
Reference:
https://docs.microsoft.com/en-us/mem/configmgr/desktop-analytics/faq

Adilh99 6 months, 3 weeks ago
If only all of the questions were as easy as this :)
upvoted 4 times

thuba_TD 2 weeks, 2 days ago
if only
upvoted 1 times

Merma 1 year, 4 months ago
You can apply the following filters to limit the list of alerts and get a more focused view.
Risk level
Exposure level
OS Platform
Health state
https://docs.microsoft.com/en-us/microsoft-365/security/defender-endpoint/machines-view-overview?view=o365-worldwide
https://docs.microsoft.com/en-us/microsoft-365/security/defender-endpoint/machine-reports?view=o365-worldwide
upvoted 3 times

Question #7 *Topic 4*

Your network contains an on-premises Active Directory domain named contoso.com that syncs to Azure Active Directory (Azure AD).

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

Name	Active Directory	Endpoint Configuration Manager agent	Microsoft Intune	Azure AD
Device1	Joined	Not installed	Enrolled	Registered
Device2	Not joined	Installed	Enrolled	Registered
Device3	Not joined	Not installed	Enrolled	Joined
Device4	Joined	Installed	Not enrolled	Registered
Device5	Not joined	Installed	Not enrolled	Joined
Device6	Joined	Installed	Enrolled	Joined

You need to ensure that you can use co-management to manage all the Windows 10 devices.

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

NOTE: Each correct selection is worth one point.

A. Join Device 1, Device2, and Device4 to Azure AD.

B. Unjoin Device3, Device5, and Device6 from Azure AD, and then register the devices in Azure AD.

C. Enroll Device4 and Device5 in Intune.

D. Join Device2, Device3, and Device5 to the domain.

E. Install the Endpoint Configuration Manager agent on Device1 and Device3.

Correct Answer: *CE*

Co-management enables you to concurrently manage Windows 10 devices by using both Configuration Manager and Microsoft Intune.

Co-management requires Configuration Manager version 1710 or later and enrollment in Microsoft Intune.

Windows 10 devices must be hybrid Azure AD joined.

Reference:

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

Alexbz Highly Voted 1 year, 5 months ago

Correct.
There are two main paths to reach to co-management:
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.
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.

upvoted 12 times

Perycles Highly Voted 1 year, 3 months ago

Correct

upvoted 6 times

thuba_TD Most Recent 2 weeks, 2 days ago

Selected Answer: CE

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

upvoted 1 times

Cisco 5 months ago

Seems partially correct, dont the devices have to be Joined to Azure AD not just registered?

upvoted 1 times

BrentOn 6 months, 3 weeks ago

So easy it feels like a trick.

upvoted 3 times

Wilf32 1 year, 5 months ago

Answer seems correct to me

upvoted 4 times

Question #8 *Topic 4*

Note: This question is part of a series of questions that present the same scenario. Each question in the series contains a unique solution that might meet the stated goals. Some question sets might have more than one correct solution, while others might not have a correct solution.
After you answer a question in this section, you will NOT be able to return to it. As a result, these questions will not appear in the review screen.
Your company has an Azure Active Directory (Azure AD) tenant named contoso.com that contains several Windows 10 devices.
When you join new Windows 10 devices to contoso.com, users are prompted to set up a four-digit pin.
You need to ensure that the users are prompted to set up a six-digit pin when they join the Windows 10 devices to contoso.com.
Solution: From the Azure Active Directory admin center, you modify the User settings and the Device settings.
Does this meet the goal?

A. Yes

B. No

Correct Answer: *B*
Instead, from the Azure Active Directory admin center, you configure automatic mobile device management (MDM) enrollment. From the Endpoint Management admin center, you configure the Windows Hello for Business enrollment options.
Reference:
https://docs.microsoft.com/en-us/intune/protect/windows-hello

Perycles Highly Voted 1 year, 3 months ago
Correct
upvoted 6 times

Moderator Most Recent 8 months, 1 week ago
Selected Answer: B
Correct answer is No (B).
This can't be done under User Settings and/or Device Settings.
upvoted 1 times

john909 10 months, 4 weeks ago
Really? Where can this be found?

The solution I found is in endpoint.microsoft.com > Devices > Enroll Devices > Windows enrollment > Windows Hello ...

Copied from another comment:
"From the Device Management or Endpoint Manager Admin Center, go to Devices, then Enroll Devices.

From there
Select Windows enrollment, then select Windows Hello for Business.

Enable Windows Hello then set minimum PIN length."
upvoted 1 times

Question #9 *Topic 4*

Your network contains an Active Directory domain named contoso.com. The domain contains computers that run Windows 10 and are joined to the domain.
The domain is synced to Microsoft Azure Active Directory (Azure AD).
You create an Azure Log Analytics workspace and deploy the Device Health solution.
You need to enroll the computers in Windows Analytics.
Which Group Policy setting should you configure?

A. Specify intranet Microsoft update service location

B. Allow Telemetry

C. Configure the Commercial ID

D. Connected User Experiences and Telemetry

Correct Answer: *C*
Microsoft uses a unique commercial ID to map information from user computers to your Azure workspace. Copy your commercial ID key from any of the Windows
Analytics solutions you have added to your Windows Portal, and then deploy it to user computers.
Reference:
https://docs.microsoft.com/en-us/windows/deployment/update/windows-analytics-get-started

Merma Highly Voted 1 year, 4 months ago
C. is correct.
A CommercialID is a globally-unique identifier assigned to a specific Log Analytics workspace. The CommercialID is copied to an MDM or Group Policy and is used to identify devices in your environment.
To find your CommercialID within Azure:
Navigate to the Solutions tab for your workspace, and then select the WaaSUpdateInsights solution.
From there, select the Update Compliance Settings page on the navbar.
Your CommercialID is available in the settings page.
https://docs.microsoft.com/en-us/windows/deployment/update/update-compliance-get-started
upvoted 7 times

Poncho25 Most Recent 1 year, 5 months ago
The answer is both B & C. Both are required for Windows Analytics to work: https://www.petervanderwoude.nl/post/the-different-ways-of-enrolling-devices-in-windows-analytics/
upvoted 3 times

daonga 1 year, 2 months ago
Believe that Telemetry is enabled by default, so when presented with such a question the answer would be C because B is presumed to already be enabled (unless the question directly specifies Telemetry is disabled)
upvoted 7 times

RodrigoT 5 months ago
Required diagnostic data, previously labeled as Basic is the default setting for current releases of Windows, Windows 10, version 1903. Check the link:

https://docs.microsoft.com/en-us/windows/privacy/configure-windows-diagnostic-data-in-your-organization#required-diagnostic-data
upvoted 2 times

marz 1 year, 7 months ago
https://www.petervanderwoude.nl/post/the-different-ways-of-enrolling-devices-in-windows-analytics/
upvoted 3 times

h3nk13 2 years, 7 months ago
Correct. https://gpsearch.azurewebsites.net/#13551
upvoted 4 times

Question #10 *Topic 4*

DRAG DROP -

You use the Antimalware Assessment solution in Microsoft Azure Log Analytics.

From the Protection Status dashboard, you discover the computers shown in the following table.

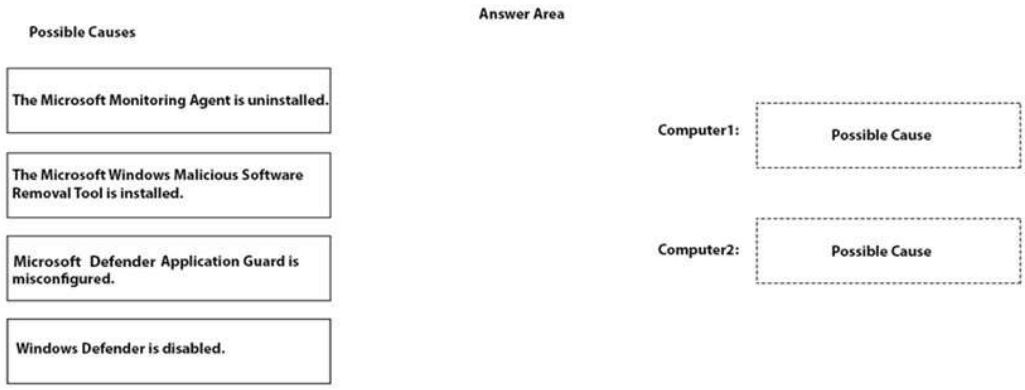
Name	Issue
Computer1	No real time protection
Computer2	Not reporting

You verify that both computers are connected to the network and running.

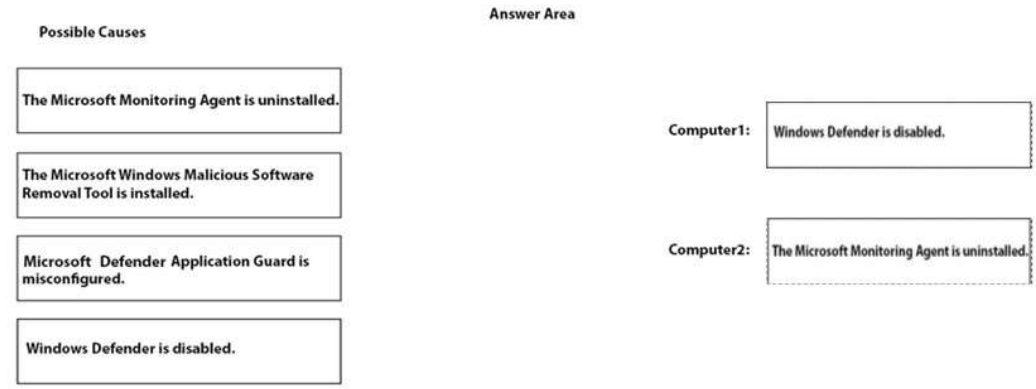
What is a possible cause of the issue on each computer? To answer, drag the appropriate causes to the correct computers. Each cause may be used once, more than once, or not at all. You may need to drag the split bar between panes or scroll to view content.

NOTE: Each correct selection is worth one point.

Select and Place:



Correct Answer:



Reference:

https://docs.microsoft.com/ga-ie/azure/security-center/security-center-install-endpoint-protection

josekast Highly Voted 2 years, 3 months ago

Computer 1: Windows Defender is disabled.
Computer 2: The MMA is uninstalled.

upvoted 66 times

RodrigoT 5 months ago

I agree. Application Guard is for Edge. It has nothing to do with Log Analytics.

upvoted 2 times

pkryan21 Highly Voted 2 years, 9 months ago

Windows Analytics needs client to have an agent (MMA)

upvoted 5 times

DUSHIWORLD 2 years, 7 months ago

not reporting means that the malware is installed but not reporting the answers are correct.

upvoted 4 times

h3nk13 2 years, 7 months ago

not reporting means telemetry is disabled or MMA not installed. Why Application Guard?

upvoted 11 times

wilmatic81 2 years, 4 months ago

yes I agree, Application Guard has nothing to do with Antimalware Assessment, turning it on is optional.

upvoted 1 times

musiman 2 years, 2 months ago

Answer A is: the agent is uninstalled. So, it was installed first but now it's uninstalled. That would be the cause why the computer isn't reporting anymore. The answer should be, that the agent was uninstalled.

upvoted 1 times

moobdoob Most Recent 8 months, 2 weeks ago

1. Defender disabled
2. MMA is uninstalled

upvoted 3 times

mbn 10 months, 1 week ago

appears to be a variation on questions 32 and 33 of topic1; given answers are identical

upvoted 1 times

cubalondon 1 year, 7 months ago

I agree with Josekast
Computer 1: Windows Defender is disabled.
Computer 2: The MMA is uninstalled.

upvoted 3 times

Mendel 3 years ago

https://docs.microsoft.com/en-us/azure/security-center/security-center-install-endpoint-protection

upvoted 1 times

Question #11 *Topic 4*

You have a shared computer that runs Windows 10.

The computer is infected with a virus.

You discover that a malicious TTF font was used to compromise the computer.

You need to prevent this type of threat from affecting the computer in the future.

What should you use?

A. Microsoft Defender Exploit Guard

B. Microsoft Defender Application Guard

C. Microsoft Defender Credential Guard

D. Microsoft Defender System Guard

E. Microsoft Defender SmartScreen

Correct Answer: *A*

Exploit protection helps protect against malware that uses exploits to infect devices and spread. Exploit protection consists of many mitigations that can be applied to either the operating system or individual apps.

Reference:

https://docs.microsoft.com/en-us/windows/security/threat-protection/microsoft-defender-atp/exploit-protection

Perycles Highly Voted 1 year, 3 months ago

Correct

upvoted 5 times

RodrigoT Most Recent 5 months ago

Selected Answer: A

Answer is correct. Got it on a KAPLAN practice exam.

upvoted 1 times

letters1234 7 months, 1 week ago

Block untrusted fonts
-Prevents loading any GDI-based fonts not installed in the system fonts directory, notably fonts from the web.
-App-level only
https://docs.microsoft.com/en-us/microsoft-365/security/defender-endpoint/customize-exploit-protection?view=o365-worldwide

upvoted 3 times

DRAG DROP -

Your company has a Microsoft Azure Active Directory (Azure AD) tenant.

The company uses Microsoft Intune to manage iOS, Android, and Windows 10 devices.

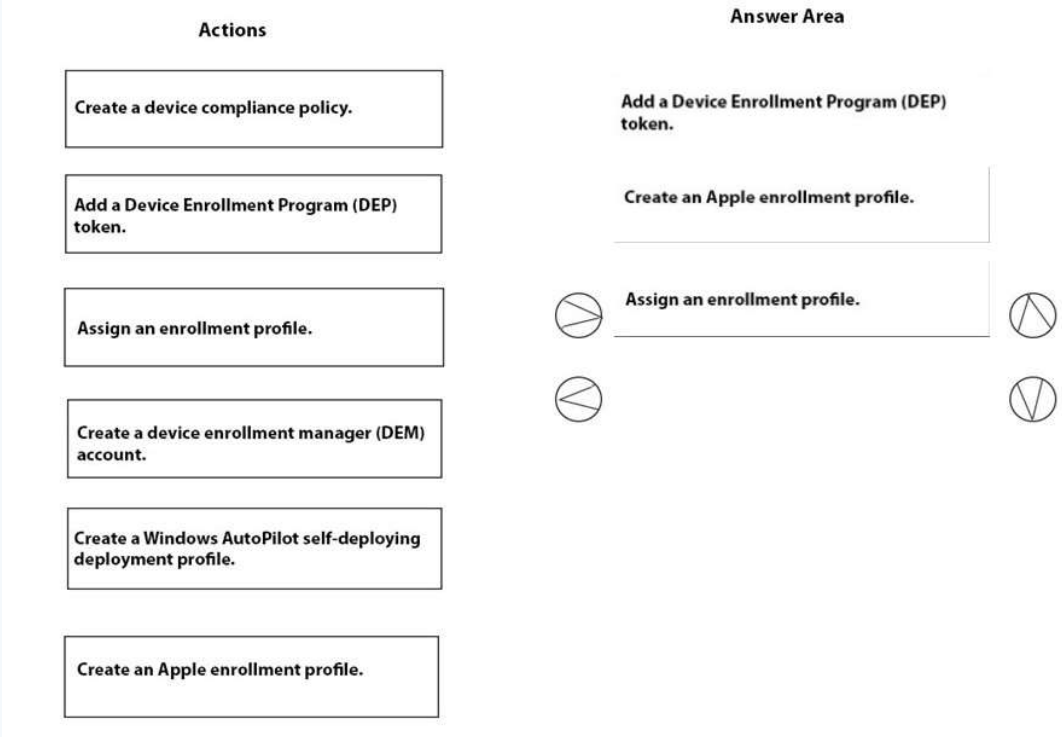
The company plans to purchase 1,000 iOS devices. Each device will be assigned to a specific user.

You need to ensure that the new iOS devices are enrolled automatically in Intune when the assigned user signs in for the first time.

Which three actions should you perform in sequence? To answer, move the appropriate actions from the list of actions to the answer area and arrange them in the correct order.

Select and Place:

Correct Answer:



Step 1: Add a Device Enrollment (DEP) token.

Get an Apple Automated Device Enrollment token.

Before you can enroll iOS/iPadOS devices with ADE, you need an ADE token (.p7m) file from Apple. This token lets Intune sync information about ADE devices that your corporation owns. It also allows Intune to upload enrollment profiles to Apple and to assign devices to those

profiles.
Step 2: Create an Apple enrollment profile.
You can create an enrollment profile for ADE devices. A device enrollment profile defines the settings applied to a group of devices during enrollment. There's a limit of 1,000 enrollment profiles per ADE token.
Step 3: Assign an enrollment profile
Assign an enrollment profile to devices.
Before devices can be enrolled, you need to assign an enrollment program profile to them.
Reference:
https://docs.microsoft.com/en-us/intune/device-enrollment-program-enroll-ios

Hester Highly Voted 2 years, 4 months ago
"Device Enrollment Program" is now called "Automated Device Enrollment" (ADE).
upvoted 23 times

vinnyct Highly Voted 1 year, 9 months ago
DEP
Create a profile
Assigned the profile
upvoted 14 times

Question #13 *Topic 4*

Your network contains an Active Directory domain. The functional level of the forest and the domain is Windows Server 2012 R2.
The domain contains 500 computers that run Windows 10. All the computers are managed by using Microsoft System Center 2012 R2 Configuration Manager.
You need to enable co-management.
What should you do first?

A. Deploy the Microsoft Intune client.

B. Raise the forest functional level.

C. Upgrade Configuration Manager to Current Branch.

D. Raise the domain functional level.

Correct Answer: *C*
Microsoft System Center 2012 R2 is quite old.
Co-management requires Configuration Manager version 1710 or later.
Reference:
https://docs.microsoft.com/en-us/sccm/comanage/overview#prerequisites

tonytones Highly Voted 1 year, 4 months ago
"Co-management requires Configuration Manager version 1710 or later."

My mans is still on 2012, boy needs to update
upvoted 27 times

vm007 Highly Voted 2 years, 6 months ago
Co-management enables you to concurrently manage Windows 10 devices by using both Configuration Manager and Microsoft Intune. It lets you cloud-attach your existing investment in Configuration Manager by adding new functionality.
Windows 10 device has the Configuration Manager client and is enrolled to Intune, you get the benefits of both services.
https://docs.microsoft.com/en-us/configmgr/comanage/overview#prerequisites
upvoted 5 times

BLYBOI Most Recent 1 year, 4 months ago
I think A is the answer:

Paths to co-management
There are two main paths to reach to co-management:

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.

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.
upvoted 2 times

raduM 1 month, 2 weeks ago
how do you deploy the intune client?
upvoted 1 times

RodrigoT 5 months ago
Maybe later, but FIRST is C.
upvoted 2 times

Harrysa 1 year, 5 months ago
cant find anything on current branch in the doc
upvoted 1 times

Question #14 *Topic 4*

HOTSPOT -

Your company uses Microsoft Intune to manage Windows 10, Android, and iOS devices.

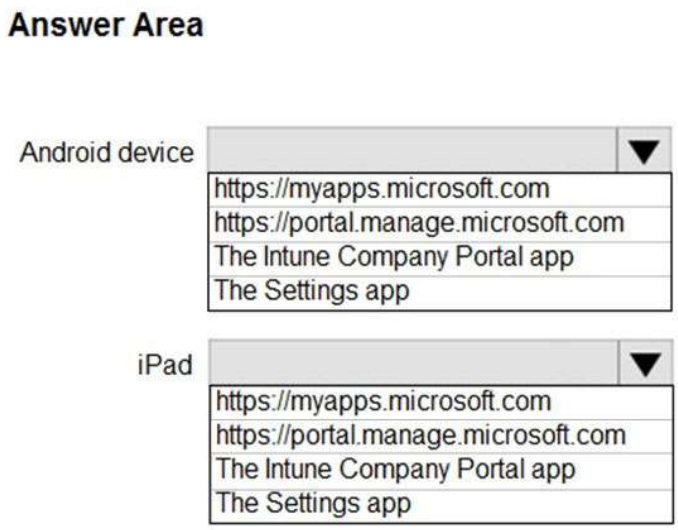
Several users purchase new iPads and Android devices.

You need to tell the users how to enroll their device in Intune.

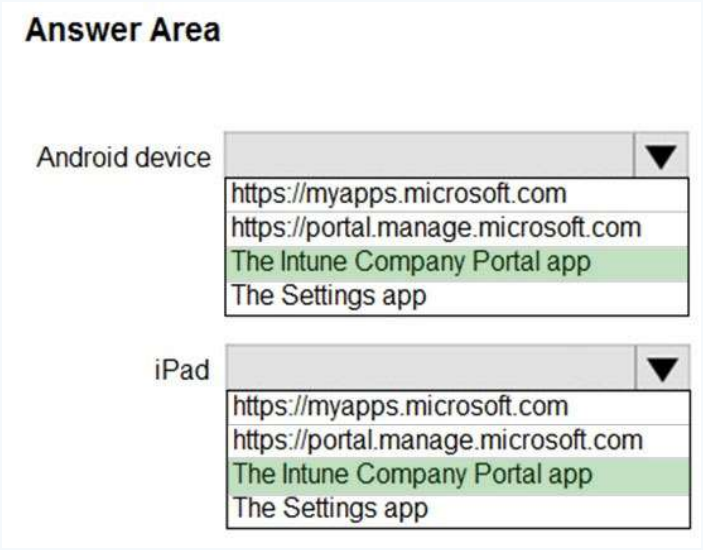
What should you instruct the users to use for each device? To answer, select the appropriate options in the answer area.

NOTE: Each correct selection is worth one point.

Hot Area:



Correct Answer:



The Intune Company Portal app is used to enroll Android, iOS, macOS, and Windows devices

Reference:

https://docs.microsoft.com/en-us/intune-user-help/enroll-device-android-company-portal https://docs.microsoft.com/en-us/intune-user-help/enroll-your-device-in-intune-ios https://docs.microsoft.com/en-us/intune-user-help/enroll-your-device-in-intune-macos-cp

chrisvit Highly Voted 1 year, 3 months ago

Both answers are correct
https://docs.microsoft.com/en-us/mem/intune/user-help/enroll-device-android-company-portal
https://docs.microsoft.com/en-us/mem/intune/user-help/enroll-your-device-in-intune-ios

upvoted 14 times

john909 10 months, 4 weeks ago

thank you

upvoted 4 times

moobdoob Most Recent 8 months, 2 weeks ago

Very good!

upvoted 2 times

HOTSPOT -

Your company has a Microsoft Azure Active Directory (Azure AD) tenant and computers that run Windows 10.

The company uses Microsoft Intune to manage the computers.

The Azure AD tenant has the users shown in the following table.

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

The device type restrictions in Intune 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

User3 is a device enrollment manager (DEM) in Intune.

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 Windows device in Intune.	○	○
User2 can enroll a Windows device in Intune.	○	○
User3 can enroll an iOS device in Intune.	○	○

Correct Answer:

Answer Area

Statements	Yes	No
User1 can enroll a Windows device in Intune.	○	●
User2 can enroll a Windows device in Intune.	●	○
User3 can enroll an iOS device in Intune.	○	●

Box 1: No -

User1 is part of Group1 which only allows enrollment of Android, iOS devices (NOT Windows devices)

Box 2: Yes -

User2 is part of Group1 and Group2 but Group2 has Priority 2 which is higher priority than Group 1, so only Policy2 applies. Policy2 allows enrollment of Windows devices

Box 3: No -

User3 is not part of any group and is therefore in "All users"

The "All users" Device Restriction Types only allow Android and Windows (MDM) but not iOS.

Reference:

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

JasiJay Highly Voted 2 years, 9 months ago

This Should be No, Yes, No

Policy 1 - Priority 1 (Andriod, IOS, Windows) Applied to None
Policy 2 - Priority 2 (Windows) Applied to Group 2
Policy 3 - Priority 3 (Android) Applied to Group 1

User 1 is in G1, so they cannot enroll Windows devices.

User 2 is in both G1 & G2, G2 has P2 with a Pri.2 which means, even though they are in G1, G1 has a pri.3, so P3 will not apply

User 3 Is not a member of any group so the Default will apply. Policy 1 is assigned to NONE, default is assigned to All users, therefore they can NOT enroll iOS as default is only Android & Win.

upvoted 56 times

sasstu 2 years, 8 months ago

I think it is No, Yes, Yes because User3 is a Device Enrollment Manager

upvoted 16 times

DJM 1 year, 10 months ago

JasiJay is correct, the DEM user in the example does not have any specific policy to allow it to enrol all devices, so it will get the default profile which does not allow iOS. A DEM user does not circumvent the device type restrictions

Tested in a lab and confirmed

upvoted 15 times

RodrigoT 5 months, 1 week ago

Thank you for testing. And here is a link for studying:
https://docs.microsoft.com/en-us/mem/intune/enrollment/enrollment-restrictions-set#change-restriction-priority

upvoted 2 times

th11 Highly Voted 2 years, 5 months ago

It is:
User 1 - NO
User 2 - YES
User 3 - YES (DEM)

upvoted 17 times

DJM 1 year, 10 months ago

Sorry this is incorrect, I tested this in a lab, the DEM account has no specific group giving it permissions to allow devices, meaning it will get the default restrictions which prevent the DEM user from enrolling an iOS device.

Again I tested this myself it is 100% NO, YES, NO

upvoted 27 times

RodrigoT 5 months ago

Thank you for really testing.

upvoted 2 times

TonySuccess Most Recent 2 weeks, 2 days ago

N,Y,N.

upvoted 1 times

moobdoob 8 months, 2 weeks ago

Great success!

upvoted 1 times

uns_uns 1 year, 3 months ago

STATEMENT1: User1 can enroll a Windows device in Intune > NO
User1 is part of Group1 which only allows enrollment of Android, iOS devices (NOT Windows devices)
STATEMENT2: User2 can enroll a Windows device in Intune > YES
User2 is part of 2x Groups (Group1 & Group2) but Group2 = Priority 2 which is higher priority than Group 1 = Priority 3, so only Priority 2 = Policy2 applies
Policy2 allows enrollment of Windows devices (and also happens to have the highest priority)
STATEMENT3: User3 can enroll an iOS device in Intune > NO
User3 is not part of any created group and therefore ends up in "All users"
The "All users" Device Restriction Types only allow Android, Windows (MDM) and not iOS
I would make an assumption that if "All Users" has "No iOS Device Type" enrollments allowed, then even DEM accounts could not enroll them (would not make sense if thought as a security admin)

upvoted 2 times

Tomtom11 1 year, 4 months ago

Priority is used when a user exists in multiple groups that are assigned restrictions. Users are subject only to the highest priority restriction assigned to a group that they are in. For example, Joe is in group A assigned to priority 5 restrictions and also in group B assigned to priority 2 restrictions. Joe is subject only to the priority 2 restrictions.

upvoted 1 times

BLYBOI 1 year, 4 months ago

No Yes No

User 3 is DEM and cannot enroll IOS devices.

upvoted 2 times

geoffC 1 year, 5 months ago

I think DEM just has a higher limit to the number of devices, here the defalult rule does not include IOS so No, Yes , No

upvoted 5 times

sakthivelesec 1 year, 5 months ago

Restrictions with a higher priority always overwrite the default restriction or the ones with a lower priority.
Given answer is right. NO NO YES(DEM)

upvoted 2 times

Tomtom11 1 year, 5 months ago

A device must comply with the highest priority enrollment restrictions assigned to its user.

User2 is in two groups

User2 can enroll Windows as is in Group 2
User2 can enroll Android and IOS as is in Group 1
upvoted 1 times

cubalondon 1 year, 7 months ago
User 1 - Group 1 - (Android & iOS) - Answer NO
User 2 - Group 1 and group 2 - (Group 1 allow Android & iOS) + group 2 allow Windows OS)- Answer Yes
User 3 - is a device enrollment manager (DEM) - Answer Yes - Can enrol up to 1000 devices, the only restrictions are:
* DEM user accounts cannot use Apple Volume Purchase Program (VPP) apps with Apple VPP user licenses because of per-user Apple ID requirements for app management.
* DEM accounts cannot be used when enrolling devices via Apple's Automated Device Enrollment (ADE).
* Devices can install VPP apps if they have Apple VPP device licenses.
* Enrolling Android Enterprise fully managed devices with DEM accounts isn't supported.
upvoted 1 times

stromnessian 1 year, 7 months ago
Answer 3 is NO. Device TYPE restrictions do apply to DEM accounts. Tested in lab environment.
upvoted 3 times

lucidgreen 1 year, 8 months ago
DEM just means the user can enroll large numbers of devices.
You can also restrict who can enroll devices but that is not covered here.
If each user can enroll devices, then:
User1: member of Group 1 & All Users can enroll Android, iOS and Windows devices.
Yes.

User2/Group 1&2/All Users can enroll Windows, Android and iOS devices.
Yes.

User3 is the DEM, so group membership is irrelevant.
Yes.

The gotcha wasn't whether the other 2 could enroll devices. It was whether 3 could and the fact that all three users are members of All Users.
upvoted 3 times

BLYBOI 1 year, 10 months ago
Change enrollment restriction priority

Priority is used when a user exists in multiple groups that are assigned restrictions. Users are subject only to the highest priority restriction assigned to a group that they are in. For example, Joe is in group A assigned to priority 5 restrictions and also in group B assigned to priority 2 restrictions. Joe is subject only to the priority 2 restrictions.

When you create a restriction, it's added to the list just above the default.

Device enrollment includes default restrictions for both device type and device limit restrictions. These two restrictions apply to all users unless they're overridden by higher-priority restrictions.
upvoted 1 times

j0eyv 1 year, 10 months ago
Ok, so it is NO, YES, NO. But what would be the correct answer in the real exam? Is it the once this site shows that are OK or is it something else? Looks like the answer on this site is very often wrong?
upvoted 2 times

DJM 1 year, 10 months ago
In my experience, use this as guide to the exam content and test it yourself (it's free...) as you can see in many of the comments above, you'll always get conflicting opinions. In this case, the DEM user permissions do not override the device type restrictions, it's those minor details that catch you out on these questions..

G'luck.
upvoted 2 times

Darisha 2 years, 1 month ago
Was intrigued so I tested this in test lab environment by the all settings provided, finally result is as expected
No
Yes
No
upvoted 10 times

Mr01z0 1 year, 6 months ago
User1 No because group1 only has Android and iOS allowed
User2 Yes because Policy2 has a higher priority than policy3
User3 No because All users only have Android and Windows, the fact it's a DEM user only matters for Windows deployments.
upvoted 2 times

josekast 2 years, 3 months ago
It is:
User 1 - NO
User 2 - YES
User 3 - YES (DEM)
upvoted 7 times

DJM 1 year, 10 months ago
This is not correct, the DEM user does not get extra permissions over the device type restrictions, they have no specific restrictions set so will by default get the default policy which does not allow them to enrol an iOS device.

Tested in a lab, and confirmed.
upvoted 4 times

densyo 1 year, 4 months ago

You are correct DJM. In addition to this:
DEM accounts cannot be used when enrolling devices via Apple's Automated Device Enrollment (ADE)
https://docs.microsoft.com/en-us/mem/intune/enrollment/device-enrollment-manager-enroll

upvoted 1 times

Adhishree 2 years, 4 months ago

So whats the final conclusion guys? user 3 - yes I think the DEM can enroll, User 2 yes --As they are part of group 2 which allows platform Windows MDM. User 1 - No as allowed platform is only android and IOS for G1.

upvoted 3 times

Question #16 *Topic 4*

HOTSPOT -

Your network contains an Active Directory domain. Active Directory is synced with Microsoft Azure Active Directory (Azure AD).

There are 500 Active Directory domain-joined computers that run Windows 10 and are enrolled in Microsoft Intune.

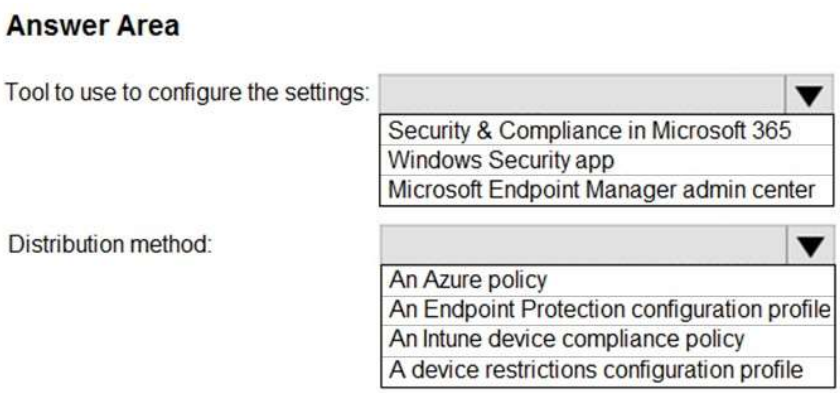
You plan to implement Microsoft Defender Exploit Guard.

You need to create a custom Microsoft Defender Exploit Guard policy, and then distribute the policy to all the computers.

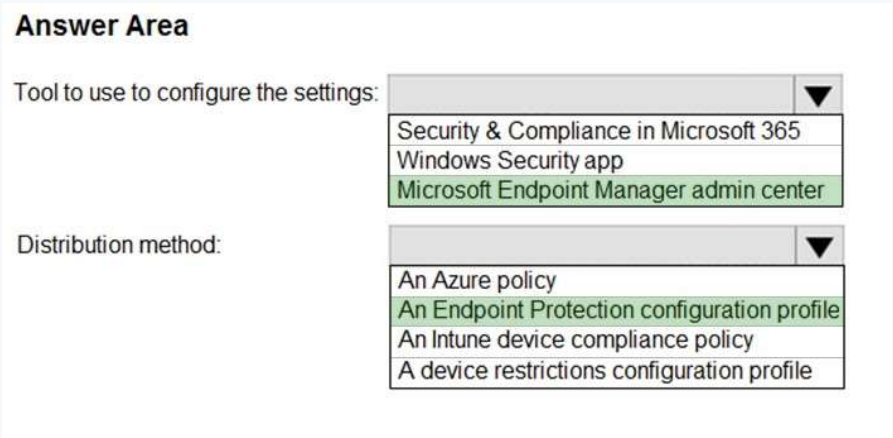
What should you do? To answer, select the appropriate options in the answer area.

NOTE: Each correct selection is worth one point.

Hot Area:



Correct Answer:



Reference:

https://docs.microsoft.com/en-us/windows/security/threat-protection/microsoft-defender-atp/import-export-exploit-protection-emet-xml#manage-or-deploy-a- configuration https://docs.microsoft.com/en-us/intune/endpoint-protection-windows-10

https://docs.microsoft.com/en-us/windows/security/threat-protection/microsoft-defender-atp/enable-exploit-protection

Mujja Highly Voted 1 year, 3 months ago

App to configure settings should be the Security app.

Microsoft Defender Security Center UI: In the Microsoft Defender Security Center, click on App & browser control and then scroll to the bottom of the resulting screen to find Exploit Protection. First, use the System settings and Program settings tabs to configure mitigation settings. Then, find the Export settings link at the bottom of the screen to export an XML representation of them

MEM config profile > endpoint protection > exploit protection only allow distribution.

upvoted 13 times

99redeyeflight 7 months, 2 weeks ago

i believe this is only needed for "Exploit Protection" (one of 4 parts of Exploit Guard). The others being Network filtering, Controlled folder access, and Attack Surface reduction (these 3 can still be configured in the Intune Endpoint protection config policy. the questions doesn't specify "exploit protection", just "exploit guard" policy

upvoted 4 times

BrentOn 6 months, 3 weeks ago

Agree this is about Defender exploit Guard, not exploit protection which you use a custom xml which is obtained through the Windows security Centre
Answer should be:
Tool to use to Configure Settings: Microsoft Endpoint Manager Admin Centre
Distribution Method: An Endpoint Protection Configuration Profile.

upvoted 3 times

RodrigoT Highly Voted 5 months, 1 week ago

The answer provided is correct. TESTED in my tenant. "This is the way" ;-)

upvoted 7 times

MR_Eliot 5 months ago

this is correct.

upvoted 2 times

AzureLearner01 Most Recent 3 months, 3 weeks ago

There are 2 Questions of this kind, both have the identical requirements, only the suggested answers are different. In one of the questions you deploy via GPO and in the Other via Intune. But you can choose in both Questions the Security App to Configure the settings, so i go with Security App. For sure you can configure all Exploit Guard features with an Device Configuration Profile (Device Restriction) except Exploit Protection, but you have this answer only in this question

upvoted 1 times

Garito 7 months, 1 week ago

Above answer is correct.

Windows Security App is technically right, if you are doing it locally on an endpoint - the scenario clearly states to apply and distribute across multiple devices - therefore it is MEM admin center and Endpoint Protection Profile.

upvoted 3 times

jage01 7 months, 2 weeks ago

Many features from the Enhanced Mitigation Experience Toolkit (EMET) are included in exploit protection.
You can enable each mitigation separately by using any of these methods:
* Windows Security app
* Microsoft Intune
* Mobile Device Management (MDM)
* Microsoft Endpoint Configuration Manager
* Group Policy
* PowerShell

https://docs.microsoft.com/en-us/microsoft-365/security/defender-endpoint/enable-exploit-protection?view=o365-worldwide#windows-security-app

Intune
Endpoint Protection Configuration Profile

upvoted 1 times

Perycles 1 year, 3 months ago

correct

upvoted 4 times

ExamStudy101 1 year, 2 months ago

Mujja is correct

upvoted 2 times

Question #17 *Topic 4*

HOTSPOT -

Your company has computers that run Windows 10 and are Microsoft Azure Active Directory (Azure AD)-joined.

The company purchases an Azure subscription.

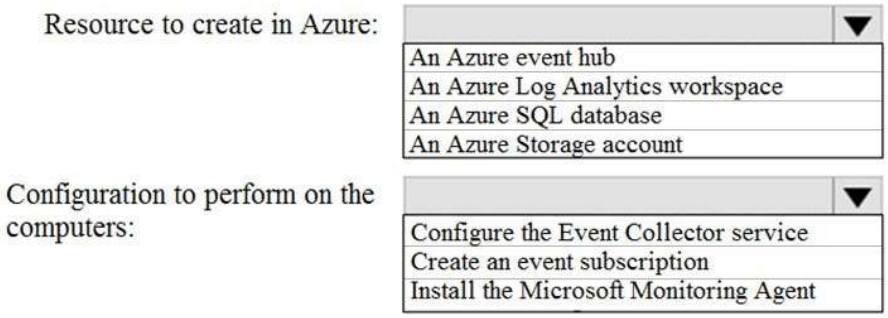
You need to collect Windows events from the Windows 10 computers in Azure. The solution must enable you to create alerts based on the collected events.

What should you create in Azure and what should you configure on the computers? To answer, select the appropriate options in the answer area.

NOTE: Each correct selection is worth one point.

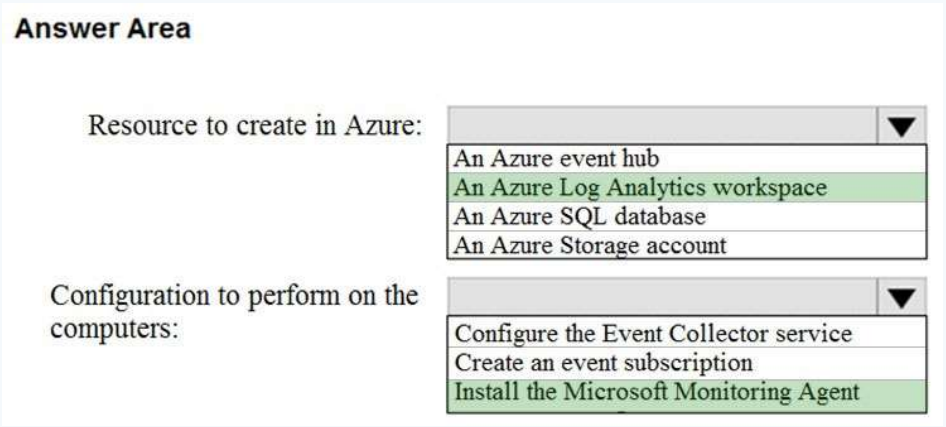
Hot Area:

Answer Area



Correct Answer:

Answer Area



The Azure Log Analytics agent collects telemetry from Windows and Linux virtual machines in any cloud, on-premises machines, and those monitored by System

Center Operations Manager and sends collected data to your Log Analytics workspace in Azure Monitor.

Reference:

https://docs.microsoft.com/en-us/azure/azure-monitor/platform/log-analytics-agent

daonga Highly Voted 1 year, 2 months ago

1: Azure Log Analytics workspace
2: Install MMA

upvoted 15 times

RodrigoT 5 months, 1 week ago

Answer valid until August 31, 2024. Then you will have to migrate from MMA to AMA.
From:
https://docs.microsoft.com/en-us/azure/azure-monitor/agents/agent-windows
To:
https://docs.microsoft.com/en-us/azure/azure-monitor/agents/azure-monitor-agent-migration

upvoted 2 times

Question #18 *Topic 4*

You have a public computer named Public1 that runs Windows 10.
Users use Public1 to browse the internet by using Microsoft Edge.
You need to view events associated with website phishing attacks on Public1.
Which Event Viewer log should you view?

A. Applications and Services Logs > Microsoft\Windows > DeviceGuard > Operational

B. Applications and Services Logs > Microsoft > Windows > Security-Mitigations > User Mode

C. Applications and Services Logs > Microsoft > Windows > SmartScreen > Debug

D. Applications and Services Logs > Microsoft > Windows > Microsoft Defender > Operational

Correct Answer: *C*
Viewing Windows event logs for Microsoft Defender SmartScreen.
Microsoft Defender SmartScreen events appear in the Microsoft-Windows-SmartScreen/Debug log, in the Event Viewer.
Reference:
https://docs.microsoft.com/en-us/windows/security/threat-protection/microsoft-defender-smartscreen/microsoft-defender-smartscreen-overview#viewing-windows- event-logs-for-microsoft-defender-smartscreen

Timmi Highly Voted 1 year, 8 months ago
looks correct from reference.

note: No SmartScreen events will be logged when using Microsoft Edge version 77 or later.

so maybe soon legacy
upvoted 9 times

RodrigoT 5 months, 1 week ago
Source:
https://docs.microsoft.com/en-us/windows/security/threat-protection/microsoft-defender-smartscreen/microsoft-defender-smartscreen-overview#viewing-microsoft-defender-smartscreen-anti-phishing-events
upvoted 1 times

Anna_Peters Highly Voted 1 year, 4 months ago
Yes,Answer is correct for Edge.
upvoted 7 times

Question #19 *Topic 4*

You have a hybrid Microsoft Azure Active Directory (Azure AD) tenant, a Microsoft System Center Configuration Manager (Current Branch) environment, and a
Microsoft 365 subscription.
You have computers that run Windows 10 as shown in the following table.

Name	Managed by Configuration Manager	Domain membership
Computer1	Yes	Active Directory-joined
Computer2	Yes	Hybrid Azure AD-joined
Computer3	Yes	Azure AD-joined

You plan to use Microsoft 365 Device Management.
Which computers support co-management by Configuration Manager and Device Management?

A. Computer3 only

B. Computer1 and Computer2 only

C. Computer2 only

D. Computer1, Computer2, and Computer3

Correct Answer: *D*
Paths to co-management -
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.
Reference:
https://docs.microsoft.com/en-us/mem/configmgr/comanage/overview

grakara Highly Voted 1 year, 4 months ago
From the reference given:

"Windows 10 devices must be connected to Azure AD. They can be either of the following types:
1.) Hybrid Azure AD-joined, where the device is joined to your on-premises Active Directory and registered with your Azure Active Directory.
2.) Azure AD-joined only. (This type is sometimes referred to as "cloud domain-joined")

Computer 1 will first need to be joined to AAD or registered to AAD.

If Computer1 does get registered or joined to the AAD it does support co-management. But not in the state it is in now. Thus if I would get this question I would answer:

Computer 2 and 3, if that option is not available I would go option D.
upvoted 8 times

Harrysa Highly Voted 1 year, 5 months ago
The answer choices here look incorrect as you cannot select 2 & 3
upvoted 6 times

silver_bullet666 Most Recent 2 months, 2 weeks ago
Based on the fact the co-management requires Hybrid AzureAD-Joined or Azure AD-Joined, REF1, I would say only Computer2 and Computer3 can be co-managed, but seeing as that isn't an available answer, I would say only Computer2.
I think we can confidently say that Computer1 is excluded from ADConnect sync and will never be HybridAAD Joined unless ADConnect sync scope is changed, and therefore cannot be co-managed. REF2.

REF1: https://docs.microsoft.com/en-us/mem/configmgr/comanage/overview#azure-ad
REF2: https://docs.microsoft.com/en-us/azure/active-directory/devices/howto-hybrid-azure-ad-join
upvoted 1 times

Alejack 2 months, 4 weeks ago
For me answer B is correct, since the devices need to be AD joined to be completely manageable thru Config Manager. Once you add the computer account to be co managed it will be automatically registered in Azure an can be enrolled.
upvoted 1 times

Angarali 5 months, 2 weeks ago
Selected Answer: D
https://docs.microsoft.com/en-us/mem/configmgr/comanage/overview
upvoted 1 times

ANDREVOX 11 months, 2 weeks ago
The question states – "You PLAN" to use Microsoft 365 Device Management.
Which computers SUPPORT co-management by Configuration Manager and Device Management?

As it stands, none can currently be managed by Device management because the prerequisite is that Windows devices has the Configuration Manager client and is ENROLLED to INTUNE.

The question does not state if the devices are already enrolled to Intune but they all SUPPORT the function when properly configured...

I'll go with - D

upvoted 6 times

jorlloen 1 year, 1 month ago

I don't understand this type of questions... the correct answare, for me, will be Computer 2 and 3. I found this on web "Hybrid Azure AD join and co-management are two different things:
"
Co-management enables you to concurrently manage a Windows 10 device with both Configuration Manager and Intune. You install the Configuration Manager client and enroll the device to Intune. The device communicates with both services. Configuration Manager policy controls which workloads you switch to Intune as the management authority. Co-management requires that the device has a cloud identity. This identity can be either hybrid Azure AD join or Azure AD join only.

For an existing Configuration Manager client that's already joined to Active Directory, it needs to be hybrid joined before you enable co-management.

For new devices that are only cloud domain-joined with Azure AD, you can enable co-management right away. There's no requirement for hybrid Azure AD join for new co-managed devices.
"
https://docs.microsoft.com/en-us/mem/configmgr/comanage/faq

upvoted 3 times

tf444 11 months, 2 weeks ago

Tenant Attache:
Tenant Attach is simply a way to attach your ConfigMgr hierarchy to your tenant and leverage the capabilities available from the cloud, such as discovery cloud users and groups, synchronize Azure AD groups from a device collection and more.
Cloud Attach:is Configuration Manager only managed devices that show up in the cloud portal. ... Intune releases new functionality every month while Configuration Manager releases new functionality approximately every four months.

upvoted 1 times

angelize 1 year, 3 months ago

The question is "Which computers support co-management" The answer is D Computer 1, Computer2 and Computer 3. On this link https://docs.microsoft.com/en-us/mem/configmgr/comanage/overview under "Paths to co-mangement" you can read "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"
And as it says in the first sentence the enviroment already have Hybrd Azure AD.

You can read more about Hybrid AAD: https://docs.microsoft.com/en-us/mem/configmgr/comanage/quickstart-setup-hybrid-aad

upvoted 4 times

RodrigoT 5 months, 1 week ago

Exactly, support.

upvoted 1 times

Perycles 1 year, 3 months ago

normally only AAD and Azure Hybride AD. ADDS yes but need to but synchronise with Azure AD connector. SO a "little" D even if for me it's only computers 2 and 3 but this answer isn't present.

upvoted 4 times

BLYBOI 1 year, 4 months ago

Answer looks correct.

Enabling co-management itself doesn't require that you onboard your site with Azure AD.

upvoted 3 times

Harrysa 1 year, 5 months ago

Yes that is correct you need to setup Azure AD https://docs.microsoft.com/en-us/mem/configmgr/comanage/overview

upvoted 1 times

Arndog 1 year, 5 months ago

2 and 3 only. They need to be joined to Azure or Hybird

upvoted 3 times

Mujja 1 year, 3 months ago

2 and 3 only isn't an option, no idea what the person writing the question expects as the correct answer.

If I was sitting the exam, I would choose computer 2 only to be safe.

upvoted 3 times

Question #20 *Topic 4*

You have a computer named Computer1 that runs Windows 10.
Computer1 is used by a user named User1.
You need to ensure that when User1 opens websites from untrusted locations by using Microsoft Edge, Microsoft Edge runs in an isolated container.
What should you do first?

A. From Windows Features, turn on Microsoft Defender Application Guard.

B. From Windows Features, turn on Hyper-V Platform.

C. From Windows Security, configure the Virus & threat protection settings.

D. From Windows Security, configure the Device security settings.

Correct Answer: *A*
For Microsoft Edge, Application Guard helps to isolate enterprise-defined untrusted sites, protecting your company while your employees browse the Internet. As an enterprise administrator, you define what is among trusted web sites, cloud resources, and internal networks. Everything not on your list is considered untrusted. If an employee goes to an untrusted site through either Microsoft Edge or Internet Explorer, Microsoft Edge opens the site in an isolated Hyper-V- enabled container.
Reference:
https://docs.microsoft.com/en-us/windows/security/threat-protection/windows-defender-application-guard/wd-app-guard-overview
https://docs.microsoft.com/en-us/windows/security/threat-protection/windows-defender-application-guard/install-wd-app-guard

Jammer Highly Voted 1 year, 11 months ago
https://www.windowscentral.com/how-enable-application-guard-microsoft-edge-windows-10-april-2018-update Here is a working link
upvoted 7 times

Solaris2002 Most Recent 6 months, 2 weeks ago
I'm really confused, isn't Hyper-V required for Application Guard to function? Would it not make sense to make sure Hyper-V is enabled first?
upvoted 3 times

51007 4 months ago
Jammer's link, comments at bottom of page say your hardware must support Hyper-V but the feature needn't be enabled
upvoted 1 times

RodrigoT 5 months, 1 week ago
You read my mind. But, I would "first" try to enable Application Guard. If it wouldn't work "then" I would check if the Hyper-V features are installed.
upvoted 1 times

silver_bullet666 2 months, 2 weeks ago
Hardware virtualization is required to enable Application Guard, Hyper-V windows component is not; https://social.technet.microsoft.com/Forums/en-US/518aea48-fbd8-4cff-a3e9-344788a4a5b9/windows-defender-application-guard-does-hyper-v-needs-to-be-enabled-on-every-machine-in-enterprise
upvoted 1 times

Perycles 1 year, 3 months ago
correct : for informations : Microsoft Defender Application Guard can be installed directly from computer (ADD/ remove Program or with powershell command) and with Intune (profile configuration > templates > Endpoint Protection > Microsfoft Defender Application Guard > Application Guard = enabled for Edge)
upvoted 3 times

grakara 1 year, 4 months ago
Answer given is correct.
upvoted 1 times

techh3ad 1 year, 6 months ago
In Endpoint Manager portal (endpoint.microsoft.com), go to Devices > Configuration Profiles. Create a new Windows 10, Templates configuration profile, choose Endpoint protection, under Microsoft Defender Application Guard, the description for Application Guard says "If enabled for Edge, Application Guard opens unapproved sites in a Hyper-V virtualized browsing container"
upvoted 2 times

Question #21 *Topic 4*

You have computers that run Windows 10 and are managed by using Microsoft Intune.
Users store their files in a folder named D:\Folder1.
You need to ensure that only a trusted list of applications is granted write access to D:\Folder1.
What should you configure in the device configuration profile?

A. Microsoft Defender SmartScreen

B. Microsoft Defender Exploit Guard

C. Microsoft Defender Application Guard

D. Microsoft Defender Application Control

Correct Answer: *B*
The four components of Windows Defender Exploit Guard are:
* Controlled folder access: Protects sensitive data from ransomware by blocking untrusted processes from accessing your protected folders
* Attack Surface Reduction (ASR)
* Exploit protection
* Network protection
Reference:
https://www.microsoft.com/security/blog/2017/10/23/windows-defender-exploit-guard-reduce-the-attack-surface-against-next-generation-malware/

techh3ad Highly Voted 1 year, 6 months ago
Create a Windows 10 > Templates > Endpoint protection configuration policy in endpoint.microsoft.com. Under Microsoft Defender Exploit Guard, configure Controlled folder access.
upvoted 18 times

RodrigoT 5 months, 1 week ago
You're right. TESTED in my tenant.
https://docs.microsoft.com/en-us/microsoft-365/security/defender-endpoint/controlled-folders?view=o365-worldwide
upvoted 4 times

Perycles Most Recent 1 year, 3 months ago
correct
upvoted 3 times

sgarj 1 year, 7 months ago
https://docs.microsoft.com/en-us/windows/security/threat-protection/microsoft-defender-atp/enable-controlled-folders correct!
upvoted 2 times

Anthony_2770 1 year, 8 months ago
Notes from the supplied link:
Encryption of files by ransomware and other unauthorized apps means losing control of your data: documents, precious photos and videos, and other important files. For enterprises and small businesses, losing access to files can mean disrupted operations. Controlled folder access protects files by locking down critical folders, allowing only authorized apps to access files. Unauthorized apps, including malicious and suspicious executable files, DLLs, scripts, and others will be denied access even when they are running with the user's or administrator's privilege, which malware is often be able to secure.
upvoted 4 times

Anthony_2770 1 year, 8 months ago
Answer is correct
upvoted 4 times

Timmi 1 year, 8 months ago
looks correct from reference.

See: Controlled folder access
upvoted 2 times

Question #22 *Topic 4*

HOTSPOT -

Your company uses Microsoft Endpoint Configuration Manager and purchases a Microsoft 365 subscription.

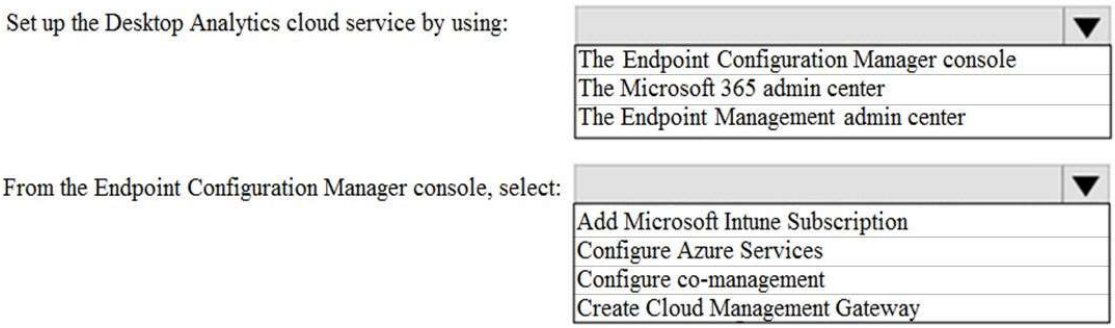
You need to set up Desktop Analytics.

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

NOTE: Each correct selection is worth one point.

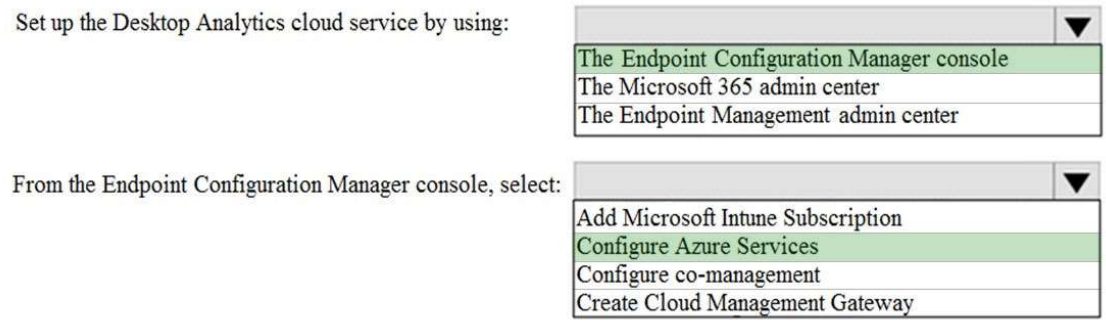
Hot Area:

Answer Area



Correct Answer:

Answer Area



Box 1: The Microsoft Endpoint Manager console

How to set up Desktop Analytics.

Use this procedure to sign in to Desktop Analytics and configure it in your subscription. This procedure is a one-time process to set up Desktop Analytics for your organization.

Initial onboarding -

1. Open the Desktop Analytics portal in the Microsoft Endpoint Manager admin center as a user with the Global Admin role. Select Start. Alternatively, on the
Configuration Manager console, go to the Software Library workspace, select the Desktop Analytics Servicing node, and select Plan deployments.
2. Etc.

Box 2: Configure Azure Services -

Use this procedure to connect Configuration Manager to Desktop Analytics, and configure device settings. This procedure is a one-time process to attach your hierarchy to the cloud service.

In the Configuration Manager console, go to the Administration workspace, expand Cloud Services, and select the Azure Services node. Select Configure Azure
Services in the ribbon.

Reference:

https://docs.microsoft.com/en-us/mem/configmgr/desktop-analytics/connect-configmgr https://docs.microsoft.com/en-us/mem/configmgr/desktop-analytics/set-up

ownydepowny Highly Voted 1 year, 1 month ago

Answer for the first question is in the second question

upvoted 18 times

[Removed] 6 months, 3 weeks ago

Easy to see if you know what you're looking for. ;)

upvoted 2 times

RodrigoT 5 months, 1 week ago

And the second from the link provided.

upvoted 1 times

Mujja Highly Voted 1 year, 3 months ago

Answer is what I guessed, so must be correct :)

upvoted 6 times

junior6995 Most Recent 2 weeks, 6 days ago

Desktop Analytics is deprecated

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

upvoted 1 times

PiPe 7 months, 3 weeks ago

https://docs.microsoft.com/en-us/mem/configmgr/desktop-analytics/set-up
"Open the Desktop Analytics portal in the Microsoft Endpoint Manager admin center as a user with the Global Admin role. Select Start. Alternatively, on the Configuration Manager console, go to the Software Library workspace, select the Desktop Analytics Servicing node, and select Plan deployments."
So I guess the answer to the first question could be either Microsoft Endpoint Manager admin center or the Configuration Manager console, I guess.

https://systemcenterdudes.com/sccm-desktop-analytics/
1) Navigate to Administration / Cloud Services / Azure Services.
2) Right-click Azure Services and click Configure Azure Services
3) Set a name and select Desktop Analytics, Click Next
...
So the answer to the 2nd question is obviously 'Configure Azure Services'

upvoted 4 times

Question #23 *Topic 4*

You need to enable Microsoft Defender Credential Guard on computers that run Windows 10.
What should you install on the computers?

A. Hyper-V

B. Microsoft Defender Application Guard

C. a guarded host

D. containers

Correct Answer: *A*
Microsoft Defender Credential Guard software requirements.
The Virtualization-based security requires:
64-bit CPU
CPU virtualization extensions plus extended page tables
Windows hypervisor (does not require Hyper-V Windows Feature to be installed)
Reference:
https://docs.microsoft.com/en-us/windows/security/identity-protection/credential-guard/credential-guard-requirements

Merma Highly Voted 1 year, 4 months ago
Windows Defender Credential Guard can be enabled either by using Group Policy, the registry, or the Hypervisor-Protected Code Integrity (HVCI) and Windows Defender Credential Guard hardware readiness tool. Windows Defender Credential Guard can also protect secrets in a Hyper-V virtual machine, just as it would on a physical machine. The same set of procedures used to enable Windows Defender Credential Guard on physical machines applies also to virtual machines.
Add the virtualization-based security features to an offline image by using DISM
Open an elevated command prompt.
Add the Hyper-V Hypervisor by running the following command:
dism /image:<WIM file name> /Enable-Feature /FeatureName:Microsoft-Hyper-V-Hypervisor /all
Add the Isolated User Mode feature by running the following command:
dism /image:<WIM file name> /Enable-Feature /FeatureName:IsolatedUserMode
https://docs.microsoft.com/en-us/windows/security/identity-protection/credential-guard/credential-guard-manage
upvoted 7 times

PiPe Highly Voted 7 months, 3 weeks ago
Selected Answer: A
https://docs.microsoft.com/en-us/windows/security/identity-protection/credential-guard/credential-guard-requirements#hardware-and-software-requirements
"Windows hypervisor (does NOT require Hyper-V Windows Feature to be installed)"

It used to be a requirement in legacy Win10 versions however:
https://docs.microsoft.com/en-us/windows/security/identity-protection/credential-guard/credential-guard-manage#add-the-virtualization-based-security-features
"Starting with Windows 10, version 1607 and Windows Server 2016, enabling Windows features to use virtualization-based security is not necessary and this step can be skipped.
If you are using Windows 10, version 1507 (RTM) or Windows 10, version 1511, Windows features have to be enabled to use virtualization-based security."

So I don't think you're gonna see this question on the exam anymore. If you do, select A. Hyper-V and party like it's 2015.
upvoted 7 times

RodrigoT 5 months, 1 week ago
It's still a requirement. TESTED on a Windows 10 Pro 21H2. You don't need to enable the "Hypervisor" feature, but you NEED at least the Hyper-V Services.
upvoted 3 times

Test99 Most Recent 1 year, 4 months ago
https://docs.microsoft.com/en-us/windows/security/identity-protection/credential-guard/credential-guard-manage
upvoted 4 times

Question #24 *Topic 4*

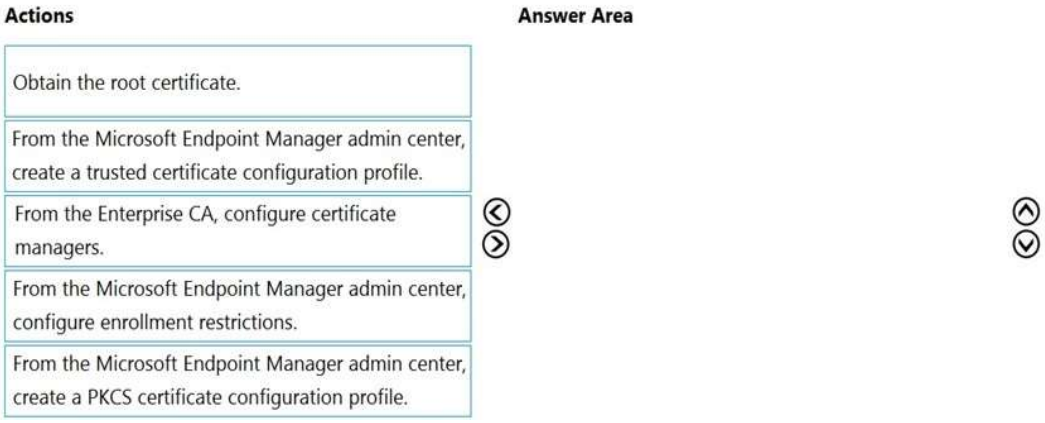
DRAG DROP -

You have a Microsoft Intune subscription that is configured to use a PFX certificate connector to an on-premises Enterprise certification authority (CA).

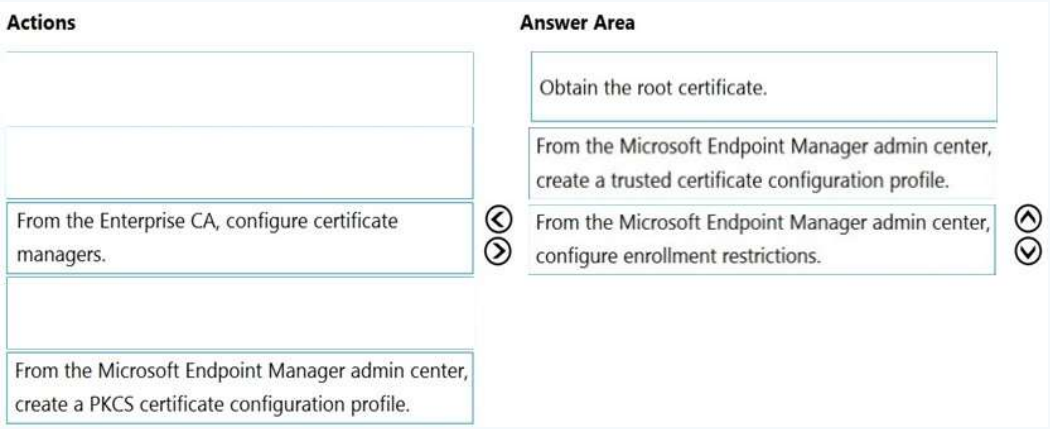
You need to use Intune to configure autoenrollment for Android devices by using public key pair (PKCS) certificates.

Which three actions should you perform in sequence? To answer, move the appropriate actions from the list of actions to the answer area and arrange them in the correct order.

Select and Place:



Correct Answer:



Step 1: Obtain the root certificate.

Export the root certificate from the Enterprise CA.

To authenticate a device with VPN, WiFi, or other resources, a device needs a root or intermediate CA certificate.

Step 2: From the Microsoft Endpoint Manager admin center, create a trusted certificate profile

Create a trusted certificate profile

1. Sign in to the Microsoft Endpoint Manager admin center.
2. Select and go to Devices > Configuration profiles > Create profile.
3. Enter the following properties:

Platform:

Profile: Select Trusted certificate. Or, select Templates > Trusted certificate.

Select Create.

4. Etc.

Step 3: From the Microsoft Endpoint Manager admin center, create a PKCS certificate profile

Create a PKCS certificate profile

1. Sign in to the Microsoft Endpoint Manager admin center.
2. Select and go to Devices > Configuration profiles > Create profile.
3. Enter the following properties:

Platform:

Profile: Select PKCS certificate. Or, select Templates > PKCS certificate.

Select Create.

4. Etc.

Reference:

https://docs.microsoft.com/en-us/mem/intune/protect/certificates-pfx-configure

Bradobrey Highly Voted 1 year, 4 months ago

it looks like 1.Obtain 2.Create a trusted certificate profile 3.Create a PKCS certificate profile

upvoted 20 times

Perycles 1 year, 3 months ago

agree with you for answer 3.

upvoted 5 times

PiPe 7 months, 3 weeks ago

Agreed
1) Obtain the root certificate
https://docs.microsoft.com/en-us/mem/intune/protect/certificates-pfx-configure#export-the-root-certificate-from-the-enterprise-ca
2) From the Microsoft Endpoint Manager admin center, create a trusted certificate configuration profile
https://docs.microsoft.com/en-us/mem/intune/protect/certificates-pfx-configure#create-a-trusted-certificate-profile
3) From the Microsoft Endpoint Manager admin center, create a PKCS certificate configuration profile
https://docs.microsoft.com/en-us/mem/intune/protect/certificates-pfx-configure#create-a-pkcs-certificate-profile

upvoted 3 times

RodrigoT Most Recent 5 months, 1 week ago

On the link provided there is nothing about enrollment restrictions. The steps are:
1-Obtain the root certificate (from the Enterprise CA)
2-From MEM admin center Create a trusted certificate profile
3-From MEM admin center Create a PKCS certificate profile

upvoted 3 times

Question #25 *Topic 4*

HOTSPOT -

You have a Microsoft 365 tenant that uses Microsoft Intune to manage personal and corporate devices. The tenant contains three Windows 10 devices as shown in the following exhibit.

Name	Enabled	OS	Version	Join Type	Owner	MDM	Compliant
LON-CL2	Yes	Windows	10.0.17763.615	Azure AD registered	User2	Microsoft Intune	Yes
LON-CL4	Yes	Windows	10.0.17763.107	Azure AD joined	User1	Microsoft Intune	Yes

How will Intune classify each device after the devices are enrolled in Intune automatically? To answer, select the appropriate options in the answer area.

NOTE: Each correct selection is worth one point.

Hot Area:

Answer Area

Identified by Intune as a personal device:

- LON-CL2 only
- LON-CL4 only
- Both LON-CL2 and LON-CL4
- Neither LON-CL2 or LON-CL4

Identified by Intune as a corporate device:

- LON-CL2 only
- LON-CL4 only
- Both LON-CL2 and LON-CL4
- Neither LON-CL2 or LON-CL4

Correct Answer:

Answer Area

Identified by Intune as a personal device:

- LON-CL2 only
- LON-CL4 only
- Both LON-CL2 and LON-CL4
- Neither LON-CL2 or LON-CL4

Identified by Intune as a corporate device:

- LON-CL2 only
- LON-CL4 only
- Both LON-CL2 and LON-CL4
- Neither LON-CL2 or LON-CL4

Reference:

https://docs.microsoft.com/en-us/azure/active-directory/devices/concept-azure-ad-join https://docs.microsoft.com/en-us/azure/active-directory/devices/concept-azure-ad-register

Perycles Highly Voted 1 year, 3 months ago

i like this question :) so easy.

upvoted 16 times

tf444 11 months, 2 weeks ago

Stupid? Lol

upvoted 2 times

PiPe 7 months, 3 weeks ago

I'm still struggling to find the third Windows 10 device they're referring to in this question ;-)

upvoted 6 times

daonga Highly Voted 1 year, 2 months ago

AAD Registered = BYOD
AAD Joined = Corporate

upvoted 12 times

moobdoob Most Recent 8 months, 2 weeks ago

Great success!

upvoted 1 times

grakara 1 year, 4 months ago

I believe the answer is correct, Devices that are AAD Joined are identified as corporate-owned and devices that are registered to AAD are identified as personal.

https://docs.microsoft.com/en-us/azure/active-directory/devices/overview
upvoted 10 times

Question #26 *Topic 4*

You have computers that run Windows 10 and are joined to Azure Active Directory (Azure AD).
All users sign in to the computers by using their Azure AD account.
Enterprise State Roaming is enabled.
From the Settings app, a user named User1 adds a Microsoft account.
Which account will be used for the Synchronizing Windows setting?

A. the work account only

B. the Microsoft account only

C. both the Microsoft account and the work account

Correct Answer: *A*
What account is used for settings sync?
In Windows 8.1, settings sync always used consumer Microsoft accounts. Enterprise users had the ability to connect a Microsoft account to their Active Directory domain account to gain access to settings sync. In Windows 10, this connected Microsoft account functionality is being replaced with a primary/secondary account framework.
The primary account is defined as the account used to sign in to Windows. This can be a Microsoft account, an Azure Active Directory (Azure AD) account, an on- premises Active Directory account, or a local account. In addition to the primary account, Windows 10 users can add one or more secondary cloud accounts to their device. A secondary account is generally a Microsoft account, an Azure AD account, or some other account such as Gmail or Facebook. These secondary accounts provide access to additional services such as single sign-on and the Windows Store, but they aren't capable of powering settings sync.
Reference:
https://docs.microsoft.com/en-us/azure/active-directory/devices/enterprise-state-roaming-faqs

Jana08 Highly Voted 1 year, 3 months ago
Link provided by admin is broken:

In the November 2015 or later releases of Windows 10, Enterprise State Roaming is only supported for a single account at a time. If you sign in to Windows by using a work or school Azure AD account, all data will sync via Azure AD. If you sign in to Windows by using a personal Microsoft account, all data will sync via the Microsoft account. Universal appdata will roam using only the primary sign-in account on the device, and it will roam only if the app's license is owned by the primary account. Universal appdata for the apps owned by any secondary accounts will not be synced.

https://docs.microsoft.com/en-us/azure/active-directory/devices/enterprise-state-roaming-faqs#:~:text=How%20do%20Microsoft,not%20be%20synced.
upvoted 7 times

Angarali Highly Voted 1 year, 1 month ago
A. the work account only
upvoted 6 times

horoshi64 Most Recent 5 months, 1 week ago
For a Windows 10 or newer device to use the Enterprise State Roaming service, the device must authenticate using an Azure AD identity

https://docs.microsoft.com/en-us/azure/active-directory/devices/enterprise-state-roaming-enable

A. The Work Account only
upvoted 1 times

moobdoob 8 months, 2 weeks ago
Great success!
upvoted 3 times

Question #27 *Topic 4*

Your network contains an Active Directory domain. The domain contains 100 computers that run Windows 10.
You need to prevent users and apps from accessing dangerous websites.
What should you configure?

A. Microsoft Defender Application Control

B. Microsoft Defender Exploit Guard

C. Microsoft Defender Application Guard

D. Microsoft Defender Firewall

Correct Answer: *B*
Network protection, a part of Microsoft Defender Exploit Guard, helps to prevent employees from using any application to access dangerous domains that may host phishing scams, exploits, and other malicious content on the internet.
Reference:
https://docs.microsoft.com/en-us/microsoft-365/security/defender-endpoint/enable-network-protection?view=o365-worldwide

hawkens Highly Voted 9 months, 2 weeks ago
Exploid Guard! https://admx.help/?Category=Windows_10_2016&Policy=Microsoft.Policies.WindowsDefender::ExploitGuard_EnableNetworkProtection
upvoted 6 times

PiPe 7 months, 3 weeks ago
That's it indeed. Exploit Guard for sure!
upvoted 2 times

Moderator Most Recent 6 months, 1 week ago
Selected Answer: B
Tough one, both Exploit Guard and Application Guard seem to be able to do the job.
Most info I could gather point to the Exploit Guard, so I'd go for that.
upvoted 1 times

letters1234 7 months, 1 week ago
Selected Answer: B
Not application specific and can be used to protect non-Microsoft applications.
upvoted 1 times

tf444 11 months, 2 weeks ago
APPLICATION GUARD!
upvoted 1 times

RodrigoT 5 months, 1 week ago
Application Guard only runs Edge in a virtual container. It doesn't prevent users and APPS from accessing dangerous websites.
You need Exploit Guard > Network filtering
Check the link:
https://docs.microsoft.com/en-us/microsoft-365/security/defender-endpoint/network-protection?view=o365-worldwide
upvoted 2 times

Saph69 1 year, 2 months ago
Just re-read the question "You need to prevent users and apps from accessing dangerous websites." since it says "users and apps" i agree that it should be exploit guard.
My bad...
upvoted 3 times

Saph69 1 year, 2 months ago
I believe this should be application Guard.
"What is Application Guard and how does it work?
For Microsoft Edge, Application Guard helps to isolate enterprise-defined untrusted sites, protecting your company while your employees browse the Internet."

https://docs.microsoft.com/en-us/windows/security/threat-protection/microsoft-defender-application-guard/md-app-guard-overview
upvoted 1 times

daonga 1 year, 1 month ago
Yes but that is for MS Edge only. The question says "users and apps" so need to consider other browsers, etc
upvoted 3 times

forummj 8 months, 1 week ago
From the same article as above. I believe it's Application Guard. It prevents access to/from untrusted sites for both users and applications.

"For Microsoft Office, Application Guard helps prevents untrusted Word, PowerPoint and Excel files from accessing trusted resources. Application Guard opens untrusted files in an isolated Hyper-V-enabled container. "
upvoted 3 times

letters1234 7 months, 1 week ago

"For Microsoft Office" - How does that protect Chrome, Firefox, Vivaldi etc?
upvoted 1 times

sgarj 1 year, 2 months ago
Correct!
upvoted 1 times

Question #28 *Topic 4*

You have a Microsoft Intune subscription associated to an Azure Active Directory (Azure AD) tenant named contoso.com.
Users use one of the following three suffixes when they sign in to the tenant: us.contoso.com, eu.contoso.com, or contoso.com.
You need to ensure that the users are NOT required to specify the mobile device management (MDM) enrollment URL as part of the enrollment process. The solution must minimize the number of changes.
Which DNS records do you need?

A. three TXT records

B. one CNAME record only

C. one TXT record only

D. three CNAME records

Correct Answer: *D*
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.
If the company uses more than one UPN suffix, you need to create one CNAME for each domain name and point each one to EnterpriseEnrollment- s.manage.microsoft.com. For example, users at Contoso use the following formats as their email/UPN: name@contoso.com name@us.contoso.com name@eu.contoso.com
Reference:
https://docs.microsoft.com/en-us/mem/intune/enrollment/windows-enroll#simplify-windows-enrollment-without-azure-ad-premium

moobdoob 8 months, 2 weeks ago
Good ansa
upvoted 2 times

lykeP 8 months, 3 weeks ago
Selected Answer: D
If the company uses more than one UPN suffix, you need to create one CNAME for each domain name and point each one to EnterpriseEnrollment-s.manage.microsoft.com.
upvoted 4 times

badguytoo 1 year, 1 month ago
If the company uses more than one UPN suffix, you need to create one CNAME for each domain name and point each one to EnterpriseEnrollment-s.manage.microsoft.com.
upvoted 3 times

daonga 1 year, 2 months ago
Can someone explain why they need the 3 CNAME? If they are all enrolling into the same domain, what is the point of needing a CNAME for each suffix of the domain?
upvoted 1 times

Redrock2063 1 year, 1 month ago
The question tell you: "Users use one of the following three suffixes when they sign in to the tenant: us.contoso.com, eu.contoso.com, or contoso.com"

You need a CNAME reference for each domain.
upvoted 4 times

RodrigoT 5 months, 1 week ago
Check the link provided. Under Step 1 read carefully the third paragraph.
upvoted 1 times

Question #29 *Topic 4*

Note: This question is part of a series of questions that present the same scenario. Each question in the series contains a unique solution that might meet the stated goals. Some question sets might have more than one correct solution, while others might not have a correct solution.
After you answer a question in this section, you will NOT be able to return to it. As a result, these questions will not appear in the review screen.
Your company has several Windows 10 devices that are enrolled in Microsoft Intune.
You deploy a new computer named Computer1 that runs Windows 10 and is in a workgroup.
You need to enroll Computer1 in Intune.
Solution: From Computer1, you sign in to https://endpoint.microsoft.com and use the Windows enrollment blade.
Does this meet the goal?

A. Yes

B. No

Correct Answer: *B*
Use MDM enrolment.
MDM only enrollment lets users enroll an existing Workgroup, Active Directory, or Azure Active directory joined PC into Intune. Users enroll from Settings on the existing Windows PC.
Reference:
https://docs.microsoft.com/en-us/mem/intune/enrollment/windows-enrollment-methods

Dong1999 Highly Voted 1 year, 2 months ago
B is Correct
upvoted 5 times

letters1234 Most Recent 7 months, 1 week ago
Selected Answer: B
Workgroup is a non domain AAD/AD device and needs to be joined to the workplace first. As ercluff mentioned, you need to: Use built in Windows Setting menu (Accounts > Access Work or School > Enroll Only in Device Management.
upvoted 1 times

defrey 8 months, 3 weeks ago
I m so confused by " is in a workgroup." Can anyone explain?
upvoted 1 times

[Removed] 6 months, 3 weeks ago
A workgroup is an ancient way of sharing access to files and printers between different computers (no mobile devices :-). Workgroups have certain severe limitations (e.g. no centralized user identity management) and in business settings it isn't used (much) anymore. A domain (AD) or a cloud tenant (Azure AD) is a better way to achieve the same results (and much more).
upvoted 1 times

ercluff 8 months, 3 weeks ago
This one poses the same question as questions 9,10, and 11 of this same question set 4, with a different proposed solution. Just the same, the answer is no. Using an answer from question #9: "Use built in Windows Setting menu (Accounts > Access Work or School > Enroll Only in Device Management. MDM only enrollment lets users enroll an existing Workgroup, Active Directory, or Azure Active directory joined PC into Intune. Users enroll from Settings on the existing Windows PC.
Reference:
https://docs.microsoft.com/en-us/mem/intune/enrollment/windows-enrollment-methods
upvoted 2 times

Question #30 *Topic 4*

HOTSPOT -

Your network contains an Active Directory domain. Active Directory is synced with Microsoft Azure Active Directory (Azure AD).

There are 500 Active Directory domain-joined computers that run Windows 10 and are enrolled in Microsoft Intune.

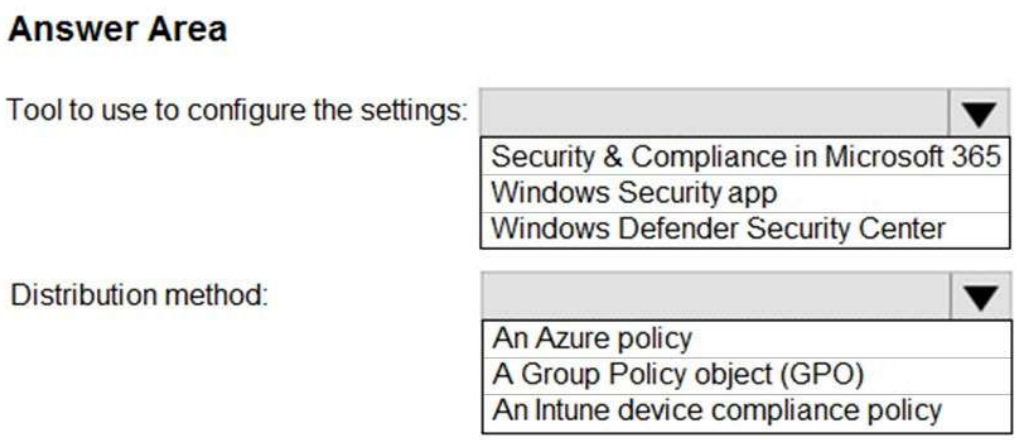
You plan to implement Microsoft Defender Exploit Guard.

You need to create a custom Microsoft Defender Exploit Guard policy, and then distribute the policy to all the computers.

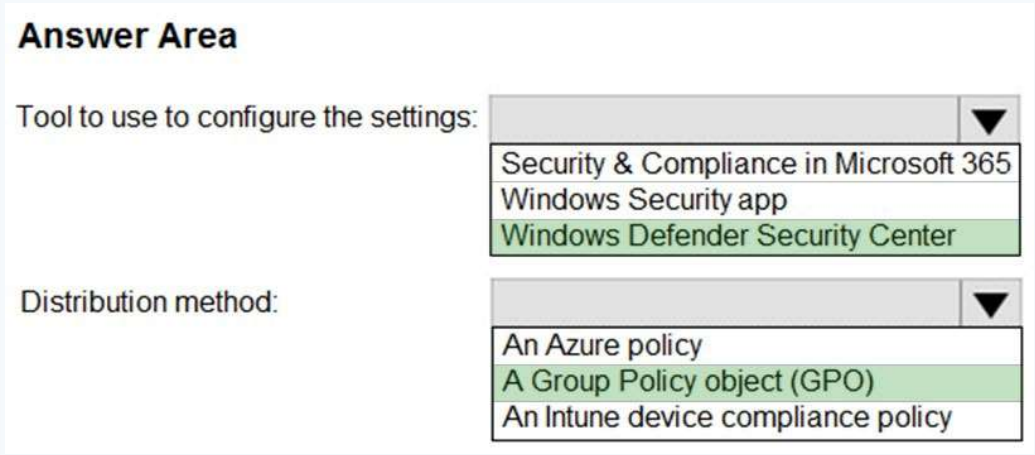
What should you do? To answer, select the appropriate options in the answer area.

NOTE: Each correct selection is worth one point.

Hot Area:



Correct Answer:



Reference:

https://docs.microsoft.com/en-us/windows/security/threat-protection/microsoft-defender-atp/exploit-protection

bertik Highly Voted 1 year, 3 months ago

I would said :

Tool : Windows Security app
Method : GPO

https://docs.microsoft.com/en-us/microsoft-365/security/defender-endpoint/import-export-exploit-protection-emet-xml?view=o365-worldwide

upvoted 15 times

PiPe 7 months, 3 weeks ago

Agreed

upvoted 1 times

RodrigoT 5 months, 1 week ago

I also agree. There is no possible way to create the settings using Microsoft Defender Security Center. The link bellow says:
"You use the Windows Security app or PowerShell to create a set of mitigations (known as a configuration). You can then export this configuration as an XML file and share it with multiple devices on your network. Then, they all have the same set of mitigation settings."
https://docs.microsoft.com/en-us/microsoft-365/security/defender-endpoint/import-export-exploit-protection-emet-xml?view=o365-worldwide

Since you are on-premises environment and the other 2 options are wrong, you should use GPO do deploy the policies using the XML created.

upvoted 1 times

RodrigoT 5 months ago

https://docs.microsoft.com/en-us/microsoft-365/security/defender-endpoint/enable-exploit-protection?view=o365-worldwide
You can enable each mitigation separately by using any of these methods:

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

In the scenario of this question we are using GPO. On the previous page Question #16 we used the Intune method.

upvoted 2 times

Mujja Highly Voted 1 year, 3 months ago

Distribution method is obvious, GPO, as none of the others are correct.

So an exported XML from the Windows Security App, added to GPO
Windows Defender Exploit Guard > Exploit Protection > Use a common set of exploit protection settings > Browse to XML

upvoted 5 times

silver_bullet666 Most Recent 2 months ago

We are configuring Exploit Guard, not Exploit Protection (one component of Exploit Guard).
Exporting XML from Windows settings is only for Exploit Protection.
I have a feeling that this question means to say we are configuring Exploit Protection rather than Exploit Guard.
see this breakdown of Exploit Guard components, https://www.microsoft.com/security/blog/2017/10/23/windows-defender-exploit-guard-reduce-the-attack-surface-against-next-generation-malware/

upvoted 1 times

jage01 7 months, 2 weeks ago

Tool : Windows Security app
Method : GPO

Manyfeatures from the Enhanced Mitigation Experience Toolkit (EMET) are included in exploit protection.
You can enable each mitigation separately by using any of these methods:
* Windows Security app
* Microsoft Intune
* Mobile Device Management (MDM)
* Microsoft Endpoint Configuration Manager
* Group Policy
* PowerShell

https://docs.microsoft.com/en-us/microsoft-365/security/defender-endpoint/enable-exploit-protection?view=o365-worldwide#windows-security-app

upvoted 1 times

jibutoms 1 year, 3 months ago

This should be:
Windows Security App : "App & Browser control" --> Exploit protection --> Export setting XML
Endpoint Security policy : Exploit protection, Import the XML

upvoted 4 times

Question #31 *Topic 4*

You have 100 devices that run Windows 10 and are joined to Microsoft Azure Active Directory (Azure AD).
You need to prevent users from joining their home computer to Azure AD.
What should you do?

A. From the Device enrollment blade in the Intune admin center, modify the Enrollment restriction settings.

B. From the Devices blade in the Azure Active Directory admin center, modify the Device settings.

C. From the Device enrollment blade in the Intune admin center, modify the Device enrollment manages settings.

D. From the Mobility (MDM and MAM) blade in the Azure Active Directory admin center, modify the Microsoft Intune enrollment settings.

Correct Answer: *A*
As an Intune administrator, you can create and manage enrollment restrictions that define what devices can enroll into management with Intune, including the:
Number of devices.
Operating systems and versions.
You can create multiple restrictions and apply them to different user groups. You can set the priority order for your different restrictions.
Create a device type restriction
1. Sign in to the Microsoft Endpoint Manager admin center > Devices > Enroll Devices > Enrollment restrictions > Create restriction > Device type restriction.
2. Etc.
Reference:
https://docs.microsoft.com/en-us/intune/enrollment-restrictions-set

asdffail99 Highly Voted 2 years, 9 months ago
I believe this is A.
Wouldn't you set the enrollment restrictions to block personally owned devices - https://docs.microsoft.com/en-us/intune/enrollment/enrollment-restrictions-set#blocking-personal-windows-devices
upvoted 34 times

JasiJay 2 years, 9 months ago
asdffail99 - I stand corrected, thank you for pointing that out!
upvoted 9 times

ExamStudy101 1 year, 2 months ago
When you enroll a device in Intune, doesn't that register it? Intune is configured so that when users sign in to a device with their work credentials they are automatically 'enrolled' and have access to Azure AD. The device is now registered to Azure AD and not joined. To stop someone from joining you have to configure this in Azure AD
upvoted 2 times

FlailingLimbs 1 year, 3 months ago
This is correct.

Answer cannot be B - because if "Users may join devices to Azure AD" was selected, that would also include corporate devices, which by inference still need to be joined to Azure AD.

A very subtly worded Microsoft-style question ;)
upvoted 4 times

ExamStudy101 1 year, 2 months ago
That isn't inferred at all. It states you already have the 100 computers in your environment which suggest they're already joined.
upvoted 2 times

RodrigoT 5 months, 1 week ago
Why not B? Just go with B and select only the IT group guys to join the devices. Since JOIN is a one time procedure it's not a huge load of extra work, and it's an admin job, as you can see on the next question. Using A would apparently work but it would also block registering and enrolling at least personal devices. Using B you can solve both.
upvoted 2 times

RodrigoT 5 months ago
I WROTE to Microsoft and their OFFICIAL answer is B. Check my thread here:

https://github.com/MicrosoftDocs/azure-docs/issues/92026
Block personally-owned devices from join Azure AD.
upvoted 6 times

hitten_za Highly Voted 2 years, 3 months ago
Question states you need to prevent the user from joining Azure AD not enrolling a device. You can set the "Users may join devices to Azure AD" setting to NONE or scope it to a group to achieve this. So the answer would be B.

If the question had mentioned Intune then I would agree with A but at no point does it do so.
upvoted 13 times

RodrigoT 5 months, 1 week ago

To solve this I would go with B and select only the IT group guys to join the devices. Since join is a one time procedure it's not a huge load of extra work. Using A would apparently also work but it would also block registering that is not requested. Using B you can solve both.
The most incredible part is that there is NOWHERE on Microsoft documentation that even mention this: how to just block personally-owned devices to be JOINED to Azure AD. Believe me, I searched a lot.
upvoted 1 times

TonySuccess Most Recent 2 weeks, 2 days ago

Selected Answer: B

B Correct.
upvoted 1 times

raduM 1 month ago

answer is a Enrolment device platform restrictions now
upvoted 1 times

BenCook 2 months ago

I believe it's A.
The question specifically asks about blocking their home computers. The Intune device platform restriction has a specific setting called "Personally owned devices - Block" which makes me think this is the answer MS are looking for.
upvoted 1 times

skalolaz 2 months, 3 weeks ago

I would say A.
Create restriction --> Platform settings --> Personaly owned devices --> block.
upvoted 1 times

IM77 2 months, 3 weeks ago

The answer is "A".
"Use device platform restrictions to restrict enrollment by device platform and OS version. You can also use platform restrictions to block personally-owned devices from enrolling. "
https://docs.microsoft.com/en-us/mem/intune/enrollment/enrollment-restrictions-set
upvoted 1 times

AVR31 5 months ago

Selected Answer: B

B is the correct answer. This is not about registering to Intune but joining Azure AD.
upvoted 1 times

Moderator 8 months ago

Selected Answer: B

B seems to be right indeed
upvoted 2 times

moobdoob 8 months, 2 weeks ago

Good answer! :)
upvoted 1 times

forummj 1 year, 2 months ago

I would suggest it's B, unless the question is wrongly worded. Enrollment Restrictions are for Enrolling, not Joining.

This forum post shows the page and the option to disallow users to use the join function.

https://serverfault.com/questions/893881/how-to-restrict-device-join-in-azure-ad/894208
upvoted 2 times

forummj 1 year, 2 months ago

Moreover, look at the next question. #3 of Topic 3. It poses the exact same question in a different way, and Enrollment Restrictions aren't an option.
upvoted 1 times

Perycles 1 year, 3 months ago

C and D are Wrong.
B could be correct but the question is "prevent user from JOIN" not "Register" : "device settings" under Azure AD just allow to prevent user to register.
A is correct : i created a "enrollement Restriction" under intune > select "Personnaly owned" = BLOCK for Windows (MDM) , apllied to to group, started a byod computer. try to join AAD using Account settings > recieved the message " failed to authenticate". So it's the solution

Correct answer is A
upvoted 4 times

ExamStudy101 1 year, 2 months ago

The setting says "prevent users from joining" it doesn't say register like you're suggesting. Makes me think it's B
upvoted 2 times

Angarali 5 months, 2 weeks ago

If the question said register, then it'll be done via AAD. I agree with answer A.
upvoted 1 times

[Removed] 6 months, 3 weeks ago

Thanks that made it clear to me! It is confusing that you would manage access to AAD join via Intune MDM (and not the Azure portal). But that indeed turns out to be the case. In AAD admin center you can only configure which users may join (whatever sort of) devices, there's no differentiation possible between corporate and personally owned devices there.
upvoted 1 times

Maas76 1 year, 5 months ago

I have it as A....https://docs.microsoft.com/en-us/intune/enrollment-restrictions-set

upvoted 1 times

Tomtom11 1 year, 5 months ago

Answer B is correct

upvoted 1 times

DJHASH786 1 year, 6 months ago

Its B, just checked on Azure AD, under Device Settings you have the option "User may join Devices to Azure AD" Options to select All, Selected or NONE..

upvoted 1 times

[Removed] 6 months, 3 weeks ago

True, but you can't differentiate between corporate devices (allowed) and personal ones (not allowed) in that setting. And you do want people to be able to join their corporate devices. So that rules out B as an answer.

upvoted 2 times

miry117 1 year, 7 months ago

B is correct.
https://docs.microsoft.com/es-es/azure/active-directory/devices/device-management-azure-portal#configure-device-settings
There is no mention of MDM in the question.

upvoted 2 times

mfalkjunk 1 year, 8 months ago

There is a difference between "Joining" a device to Azure and "Registering" a device.

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

"Devices that are Azure AD registered are typically personally owned or mobile devices, and are signed in with a personal Microsoft account or another local account."

"Devices that are Azure AD joined are owned by an organization, and are signed in with an Azure AD account belonging to that organization. They exist only in the cloud."

To block personal devices from "joining" to Azure AD, you go to Microsoft Endpoint Manager admin center > devices > enrollment restrictions > create restriction > device type restriction > then designate BLOCK for personal devices.

This will prevent personal devices from being "Joined" to Azure AD.
https://docs.microsoft.com/en-us/mem/intune/enrollment/enrollment-restrictions-set

upvoted 5 times

lucidgreen 1 year, 8 months ago

Agreed. Back before all Intune stuff was in Endpoint Manager, these settings were in Intune. Everything is now in Endpoint Manager. You might as well consider Intune as defunct.

upvoted 1 times

mfalkjunk 1 year, 7 months ago

Balena, I believe you are correct:

https://docs.microsoft.com/en-us/azure/active-directory/devices/device-management-azure-portal#configure-device-settings

https://social.technet.microsoft.com/Forums/en-US/149b399e-ccf3-4631-bfaa-7a1cff1a1ab2/block-users-from-azure-ad-joining-their-windows-10-device?forum=microsoftintuneprod#:~:text=In%20Azure%20AD%20console%2C%20you,from%20joining%20devices%20into%20AAD.

I will go with B.

upvoted 1 times

Balena 1 year, 7 months ago

In my understanding, Enrollment restriction in Endpoint is about MDM enrollment. There is no word about AZAD joining or registering. Further, they talk about "their home computer". One would suppose that every other device would be corporate owned and as such not user enrolled (enrollment manager?). I go with B.

upvoted 2 times

Question #32 *Topic 4*

Your company has a Microsoft 365 subscription.
A new user named Admin1 is responsible for deploying Windows 10 to computers and joining the computers to Microsoft Azure Active Directory (Azure AD).
Admin1 successfully joins computers to Azure AD.
Several days later, Admin1 receives the following error message: `This user is not authorized to enroll. You can try to do this again or contact your system administrator with the error code (0x801c0003).`
You need to ensure that Admin1 can join computers to Azure AD and follow the principle of least privilege.
What should you do?

A. Assign the Global administrator role to Admin1.

B. Modify the Device settings in Azure AD.

C. Assign the Cloud device administrator role to Admin1.

D. Modify the User settings in Azure AD.

Correct Answer: *B*
If you have rights to manage devices in Intune, you can manage devices for which mobile device management is listed as Microsoft Intune. If the device isn't enrolled with Microsoft Intune, the Manage option won't be available.
Note: Enable or disable an Azure AD device
There are two ways to enable or disable devices:
The toolbar on the All devices page, after you select one or more devices.
The toolbar, after you drill down for a specific device.
Reference:
https://docs.microsoft.com/en-us/azure/active-directory/devices/device-management-azure-portal

rbrink2001 Highly Voted 1 year, 3 months ago
Seeing this:
This user is not allowed to enroll.

Error 0x801c0003: "This user is not allowed to enroll. You can try again or contact your system administrator with the error code 801c0003."

Cause: The Users may join devices to Azure AD setting is set to None. It prevents new users from joining their devices to Azure AD. Therefore Intune enrollment fails.
Resolution

Sign in to the Azure portal as administrator.
Go to Azure Active Directory > Devices > Device Settings.
Set Users may join devices to Azure AD to All.
Enroll the device again.
leads me to believe that the answer is B
https://docs.microsoft.com/en-us/troubleshoot/mem/intune/troubleshoot-windows-enrollment-errors
upvoted 14 times

tf444 11 months, 2 weeks ago
It says Admin1 joins the computer to Azure AD, a couple of days later he/she receives the error message.
It has to do with the number of devices Admin1 can enroll.
upvoted 7 times

Pleebb Highly Voted 1 year, 2 months ago
Modify the Device settings in Azure AD.

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. If a user reaches this quota, they are not be able to add additional devices until one or more of the existing devices are removed. The default value is 50. You can increase the value up to 100 and if you enter a value above 100, Azure AD will set it to 100. You can also use Unlimited value to enforce no limit other than existing quota limits.

https://docs.microsoft.com/en-us/azure/active-directory/devices/device-management-azure-portal
upvoted 10 times

MR_Eliot Most Recent 5 months ago
B seems correct to me. Assuming the administrator is the one who is enrolling devices to azure we can put him in a group and assign that group in Azure > Device Settings.
upvoted 2 times

chapinoli 8 months, 1 week ago
The cause
The person receives the error, because he or she has reached the limit of maximum allowed devices to Azure AD Join.

By default, Azure Active Directory enforces a limit of 20 devices for any user object to join. It even enforces this limit on privileged users, like users with the Global Admin role (Admin1)

https://dirteam.com/sander/2018/03/20/knowledgebase-you-receive-error-801c0003-when-you-try-to-azure-ad-join-a-device-during-the-out-of-the-box-experience-oobe/

upvoted 1 times

Goofer 10 months, 3 weeks ago

increase the device enrollment limit under devices enrollment restriction

upvoted 3 times

tf444 11 months, 2 weeks ago

https://systemcenterdudes.com/intune-error-0x801c003-this-user-is-not-authorized-to-enroll/

upvoted 3 times

AdamMSConfig 1 year, 2 months ago

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

upvoted 1 times

Perycles 1 year, 3 months ago

B is correct, it's possible to increase the number here : Maximum number of device per user. and it can be also done under intune (under Enrollement restriction > Device limit restriction)

upvoted 4 times

NetY2K 1 year, 3 months ago

The given answer I correct. I checked it myself. In AAD you go to Devices>Device settings> Maximum number of devices per user and choose the number you want to set.

upvoted 3 times

JeremyBearimy7 1 year, 4 months ago

I don't think the options you are given are very useful if you want to apply the principle of least privilige.
Microsoft gives the solution to increase the device limit in Endpoint through Devices > Enrollment restrictions > Default (under Device limit restrictions) > Properties > Edit (next to Device limit) > increase the Device limit (maximum 15)> Review + Save.
Source: https://docs.microsoft.com/en-us/troubleshoot/mem/intune/troubleshoot-windows-enrollment-errors
The only problem is that it gives all users the same limit to register devices.
Wouldn't a device enrollment manager account be the better option (so modify the user)?

upvoted 3 times

Merma 1 year, 4 months ago

Wouldn't C. Assign the Cloud device administrator role to Admin1. be the correct answer?

upvoted 1 times

bertik 1 year, 4 months ago

No. Cloud device administrator doesn't have permissions to create devices, only enable, disable and delete.
https://docs.microsoft.com/en-us/azure/active-directory/roles/permissions-reference#cloud-device-administrator

So I think answer should be D as Layer8 stated.

upvoted 2 times

Layer8 1 year, 4 months ago

the question led me to believe that the user had maxed out their total # of enrollments (15). isn't the goal to modify the user so they can continue to enroll?

upvoted 3 times

Layer8 1 year, 4 months ago

I suppose the suggested answer would work, but that would allow for all users to add more than the default number of devices.

upvoted 3 times

Question #33 *Topic 4*

Your network contains an Active Directory domain named contoso.com. The domain contains computers that run Windows 10 and are joined to the domain.
The domain is synced to Microsoft Azure Active Directory (Azure AD).
You create an Azure Log Analytics workspace and deploy the Update Compliance solution.
You need to enroll the computers in the Update Compliance solution.
Which Group Policy setting should you configure?

A. Specify intranet Microsoft update service location

B. Allow Telemetry

C. Configure the Commercial ID

D. Connected User Experiences and Telemetry

Correct Answer: *C*
Microsoft uses a unique commercial ID to map information from user computers to your Azure workspace. Copy your commercial ID key from any of the Windows
Analytics solutions you have added to your Windows Portal, and then deploy it to user computers.
Reference:
https://docs.microsoft.com/en-us/windows/deployment/update/update-compliance-get-started

Perycles Highly Voted 1 year, 3 months ago
C is ok but in fact, telemetry must be enabled to allow diagnostic.
upvoted 6 times

bertik 1 year, 3 months ago
I think it's C.
Telemetry is enabled by default (you can configure only how much data you are sending, or disable in Enterprise SKU). No need to allow.
upvoted 4 times

letters1234 Most Recent 7 months, 1 week ago
Selected Answer: C
C is correct as you need to configure where the data will be sent, the Allow Telemetry is enabled by default when not configured.
upvoted 2 times

Merma 1 year, 4 months ago
From the provided link:
"A CommercialID is a globally-unique identifier assigned to a specific Log Analytics workspace. The CommercialID is copied to an MDM or Group Policy and is used to identify devices in your environment.
To find your CommercialID within Azure:
Navigate to the Solutions tab for your workspace, and then select the WaaSUpdateInsights solution.
From there, select the Update Compliance Settings page on the navbar.
Your CommercialID is available in the settings page."
upvoted 1 times

Question #34 *Topic 4*

You have an Azure Active Directory (Azure AD) tenant and 100 Windows 10 devices that are Azure AD joined and managed by using Microsoft Intune.
You need to configure Microsoft Defender Firewall and Microsoft Defender Antivirus on the devices. The solution must minimize administrative effort.
Which two actions should you perform? Each correct answer presents part of the solution.
NOTE: Each correct selection is worth one point.

A. To configure Microsoft Defender Antivirus, create a device configuration profile and configure the Endpoint protection settings.

B. To configure Microsoft Defender Firewall, create a device configuration profile and configure the Device restrictions settings.

C. To configure Microsoft Defender Firewall, create a Group Policy Object (GPO) and configure Windows Defender Firewall with Advanced Security.

D. To configure Microsoft Defender Antivirus, create a Group Policy Object (GPO) and configure Windows Defender Antivirus settings.

E. To configure Microsoft Defender Antivirus, create a device configuration profile and configure the Device restrictions settings.

F. To configure Microsoft Defender Firewall, create a device configuration profile and configure the Endpoint protection settings.

Correct Answer: *EF*
F: With Intune, you can use device configuration profiles to manage common endpoint protection security features on devices, including:
- Firewall
- BitLocker
- Allowing and blocking apps
- Microsoft Defender and encryption

Reference:
https://docs.microsoft.com/en-us/mem/intune/protect/endpoint-protection-configure https://docs.microsoft.com/en-us/mem/intune/protect/endpoint-security-policy#create-an-endpoint-security-policy

j0eyv Highly Voted 1 year, 10 months ago
Defender AV is in Device Restrictions.
Defender FW is in Endpoint Restrictions.

E/F!
upvoted 27 times

FlailingLimbs 1 year, 3 months ago
Correct. Just tested and confirmed.
upvoted 9 times

RodrigoT 5 months, 1 week ago
E. F. I tested in my tenant too. However I don't understand with Microsoft sees Antivirus under Device Restrictions. It doesn't make any sense. For me it should be also under Endpoint Protection.
upvoted 2 times

Lomak Highly Voted 2 years, 1 month ago
it is NOT a Device Restriction profile.
AV/Firewall both exist in the Endpoint Protection profile
Answer : A, F
upvoted 14 times

Cliffh 2 years ago
true:
https://docs.microsoft.com/en-us/mem/intune/protect/endpoint-protection-windows-10
upvoted 1 times

Nail 1 year, 11 months ago
No, they are right, E and F. I'm looking at it right now in Intune. AV is in Device Restrictions, Firewall is in Endpoint Protection.
upvoted 10 times

M0nster 1 year, 11 months ago
This litterly states that AV is in device restrictions. So E and F
upvoted 9 times

Solaris2002 6 months, 4 weeks ago
I do have to admit it is very dumb that Endpoint Protection does NOT include Defender AV. Microsoft is weird like that. but the answer is E and F.
upvoted 2 times

junior6995 Most Recent 2 weeks, 6 days ago
Outdated question - as of now, September 2022, both options sit under Endpoint Security (Firewall and Anti-virus)
upvoted 2 times

raduM 1 month, 2 weeks ago

Selected Answer: EF

e and f are the correct answers. no antivirus under endpoint protection

upvoted 1 times

MitchF 2 months, 1 week ago

The first figure in the Microsoft document (below) shows they are both under Endpoint Protection.
So the answer is correct (A & F are correct)

Source:
https://docs.microsoft.com/en-us/mem/intune/protect/endpoint-security-policy

upvoted 1 times

Kumargvm 7 months, 2 weeks ago

Selected Answer: EF

Answer is E & F
WD Firewall is in EndPoint Protection
WD Antivirus is in Device Restriction

upvoted 1 times

Solaris2002 7 months, 3 weeks ago

I have my Intune tenant open right now as I type this.
You COULD create Device Restrictions for Firewall and AV settings via Devices > Configuration Profiles > Create Profile >Device Restrictions

But it would appear to me the PROPER way to do this is to navigate to Endpoint Security> and then select either Antivirus or Firewall and create the policies from there.

To reiterate, AV IS IN Endpoint Security. I'd attach a screenshot if I could

The answer should therefore be A and F

upvoted 1 times

Solaris2002 7 months, 3 weeks ago

From https://docs.microsoft.com/en-us/mem/intune/protect/endpoint-protection-windows-10

"To configure Microsoft Defender Antivirus, see Windows device restrictions or use endpoint security Antivirus policy."

upvoted 1 times

lucadp010 8 months, 2 weeks ago

Selected Answer: EF

E.
F.
You can test it with a lab!

upvoted 1 times

IykeP 8 months, 2 weeks ago

Selected Answer: EF

E and F is the correct answer, just tested in intune now.

upvoted 2 times

moobdoob 8 months, 2 weeks ago

Selected Answer: AF

Correct answer: A F

upvoted 1 times

Pleebb 1 year, 3 months ago

A & F
"You can use Microsoft Endpoint Manager to configure Microsoft Defender Antivirus scans. Microsoft Intune and Configuration Manager are now part of Endpoint Manager."

https://docs.microsoft.com/en-us/microsoft-365/security/defender-endpoint/use-intune-config-manager-microsoft-defender-antivirus?view=o365-worldwide

upvoted 1 times

RajeeMark 1 year, 3 months ago

You can do both AV and FW in Endpoint Protection. You need to create this with least effort. Therefore A and F since it is the quickest way.

upvoted 1 times

Mujja 1 year, 3 months ago

The is no Defender AV in Endpoint protection

upvoted 1 times

Perycles 1 year, 3 months ago

E F are correct, just tested.

upvoted 5 times

Tomtom11 1 year, 3 months ago

Microsoft Defender Antivirus is in Device Restrictions

upvoted 2 times

leepae 1 year, 4 months ago

E and F

upvoted 3 times

Danohav 1 year, 4 months ago

E & F Correct - confirmed via:
https://docs.microsoft.com/en-us/mem/intune/configuration/device-restrictions-windows-10
> include only Defender AV

https://docs.microsoft.com/en-us/mem/intune/protect/endpoint-protection-windows-10?toc=/intune/configuration/toc.json&bc=/intune/configuration/breadcrumb/toc.json
> include only Defender FW

upvoted 3 times

Tiit 1 year, 4 months ago

A, F correct, because prerequisite is, that the solution must minimize administrative effort.
Yes - you can modify also device restrictions for antivirus, but this is "separate activity", it does not minimize :)
Just create a device configuration profile and configure the Endpoint protection settings for both: antivirus and firewall:
- Endpoint security profiles provide a concise, curated set of security templates including Firewall, BitLocker, Antivirus and more. Security baseline profiles are templates with pre-configured settings values recommended by security experts.

upvoted 1 times

Tiit 1 year, 4 months ago

Sry, Tested again - could not find Defender antivirus in Endpoint protection template, however it is in device restriction only. Forget my previous post - Right answer is E / F

upvoted 7 times

Question #35 *Topic 4*

Your network contains an Active Directory domain that is synced to Microsoft Azure Active Directory (Azure AD). The domain contains computers that run
Windows 10. The computers are enrolled in Microsoft Intune and Windows Analytics.
Your company protects documents by using Windows Information Protection (WIP).
You need to identify non-approved apps that attempt to open corporate documents.
What should you use?

A. the Device Health solution in Windows Analytics

B. Microsoft Cloud App Security

C. Intune Data Warehouse

D. the App protection status report in Intune

Correct Answer: *D*
The App learning report monitors your apps, not in policy, that attempt to access work data. You can identify these apps using the report and add them to your
WIP policies to avoid productivity disruption before fully enforcing WIP with ג€Blockג€ mode. Frequent monitoring of the report will help you continuously identify access attempts so you can update your policy accordingly.
Note: Access the WIP Learning reports
1. Sign in to the Microsoft Endpoint Manager admin center.
2. Select Apps > Monitor > App protection status > Reports.
Reference:
https://docs.microsoft.com/en-us/windows/security/information-protection/windows-information-protection/wip-learning

mfalkjunk Highly Voted 1 year, 7 months ago
It is now under:

Microsoft Endpoint Manager admin center > Apps > Monitor > App protection status
upvoted 17 times

RodrigoT 5 months, 1 week ago
April 2022 and is still there. Just tested. Follow the path above and then click on the cog Reports | App learning report for Windows Information Protection.
https://docs.microsoft.com/en-us/windows/security/information-protection/windows-information-protection/wip-learning
upvoted 2 times

BLYBOI Highly Voted 1 year, 10 months ago
Click Intune > Client apps > App protection status > Reports.
upvoted 6 times

Perycles Most Recent 1 year, 3 months ago
correct
upvoted 1 times

sakthivelesec 1 year, 5 months ago
App protection status report gives the report whether the app is protected with App Protection policy or not.
I have exported the report and could not find which non-corporate app tries to open the corporate document.
upvoted 1 times

RodrigoT 5 months, 1 week ago
Use App learning report to monitor your apps, not in policy, that attempt to access work data.
https://docs.microsoft.com/en-us/windows/security/information-protection/windows-information-protection/wip-learning
upvoted 2 times

HOTSPOT -

Your company uses Microsoft Defender for Endpoint. Microsoft Defender for Endpoint includes the device groups shown in the following table.

Rank	Name	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
5	Group5	Name starts with COMP
Last	Ungrouped machines (default)	*Not applicable*

You onboard a computer to Microsoft Defender for Endpoint as shown in the following exhibit.

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

NOTE: Each correct selection is worth one point.

Hot Area:

Answer Area

Computer1 will be a member of:
- Group3 only
- Group4 only
- Grou5 only
- Group3, Group4, and Group5 only

If you add the tag demo to Computer1, Computer1 will be a member of:
- Group1 only
- Group2 only
- Group1 and Group2 only
- Group1, Group2, Group3, Group4, and Group5

Correct Answer:

Answer Area

Computer1 will be a member of:
- Group3 only
- Group4 only
- Grou5 only
- Group3, Group4, and Group5 only

If you add the tag demo to Computer1, Computer1 will be a member of:
- Group1 only
- Group2 only
- Group1 and Group2 only
- Group1, Group2, Group3, Group4, and Group5

Reference:

https://docs.microsoft.com/en-us/microsoft-365/security/defender-endpoint/machine-groups?view=o365-worldwide#manage-device-groups

HellRaver80 Highly Voted 11 months, 1 week ago

If a device is also matched to other groups, it's added only to the highest ranked device group.

upvoted 14 times

AVR31 Most Recent 5 months ago

If the answer would be as presented, the ranking would have no meaning.
In any situation where multiple items can apply and there is a ranking system, the highest ranking item applies.

upvoted 1 times

blueninja 11 months, 4 weeks ago

Please correct if I am wrong:
1. Group 3 only
2. Group 2 only

https://docs.microsoft.com/en-us/microsoft-365/security/defender-endpoint/machine-groups?view=o365-worldwide#manage-device-groups

upvoted 4 times

blueninja 11 months, 3 weeks ago

Sorry, there was a typo. Please see correct one below:
1. Group 3 only
2. Group 1 only

upvoted 16 times

RodrigoT 5 months, 1 week ago

And we are paying contributor access to correct their answers.
https://docs.microsoft.com/en-us/microsoft-365/security/defender-endpoint/machine-groups?view=o365-worldwide

upvoted 2 times

[Removed] 11 months, 3 weeks ago

I agree.
"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. You can also edit and delete groups."

upvoted 6 times

[Removed] 11 months, 3 weeks ago

No wait.
1. Group 3 only
2. Group 1 only

upvoted 8 times

Question #37 *Topic 4*

Your company has computers that run Windows 10. The company uses Microsoft Intune to manage the computers.
You have an app protection policy for Microsoft Edge. You assign the policy to a group.
On a computer named Computer1, you open Microsoft Edge.
You need to verify whether Microsoft Edge on Computer1 is protected by the app protection policy.
Which column should you add in Task Manager?

A. Operating system context

B. UAC virtualization

C. Enterprise Context

D. Data Execution Prevention

Correct Answer: *C*
Use Task Manager to check the context of your apps while running in Windows Information Protection (WIP) to make sure that your organization's policies are applied and running correctly.
Viewing the Enterprise Context column in Task Manager.
You need to add the Enterprise Context column to the Details tab of the Task Manager.
Reference:
https://docs.microsoft.com/en-us/windows/security/information-protection/windows-information-protection/wip-app-enterprise-context
https://www.itpromentor.com/win10-mam-wip/

LordCaine Highly Voted 1 year ago
This was nowhere in the book. Full of nonsensical questions this exam.
upvoted 20 times

hasquaati 7 months, 1 week ago
I agree, there are many many questions not found in either the First Edition or Second Edition of the book. Its like the authors saying "Read this, but click on the link and read everything there".
upvoted 5 times

RodrigoT 5 months, 1 week ago
At least the answer was right this time.
upvoted 5 times

vinnyct Highly Voted 1 year, 10 months ago
Use Task Manager to check the context of your apps while running in Windows Information Protection (WIP) to make sure that your organization's policies are applied and running correctly.

Viewing the Enterprise Context column in Task Manager
You need to add the Enterprise Context column to the Details tab of the Task Manager.

Make sure that you have an active WIP policy deployed and turned on in your organization.

Open the Task Manager (taskmgr.exe), click the Details tab, right-click in the column heading area, and click Select Columns.

The Select columns box appears.
Scroll down and check the Enterprise Context option, and then click OK to close the box.

The Enterprise Context column should now be available in Task Manager
upvoted 11 times

letters1234 Most Recent 7 months, 1 week ago
Selected Answer: C
Answer is correct, see VinnyCT's response
upvoted 1 times

J2daizzo412 10 months ago
Answer C.
upvoted 4 times

Technik 1 year, 5 months ago
https://howtomanagedevices.com/windows-10/2738/windows-10-enterprise-context/
upvoted 4 times

Anthony_2770 1 year, 8 months ago
Review the Enterprise Context
The Enterprise Context column shows you what each app can do with your enterprise data:

Domain. Shows the employee's work domain (such as, corp.contoso.com). This app is considered work-related and can freely touch and open work data and resources.

Personal. Shows the text, Personal. This app is considered non-work-related and can't touch any work data or resources.

Exempt. Shows the text, Exempt. WIP policies don't apply to these apps (such as, system components).

Important
Enlightened apps can change between Work and Personal, depending on the data being touched. For example, Microsoft Word 2016 shows as Personal when an employee opens a personal letter, but changes to Work when that same employee opens the company financials.

upvoted 5 times

Anthony_2770 1 year, 8 months ago

This adds to vinnyct's comments.

upvoted 3 times

HOTSPOT -

You have 200 computers that run Windows 10. The computers are joined to Microsoft Azure Active Directory (Azure AD) and enrolled in Microsoft Intune.

You need to configure an Intune device configuration profile to meet the following requirements:

- Prevent Microsoft Office applications from launching child processes.
- Block users from transferring files over FTP.

Which two settings should you configure in Endpoint protection? To answer, select the appropriate settings in the answer area.

NOTE: Each correct selection is worth one point.

Hot Area:

Answer Area

Device restrictions

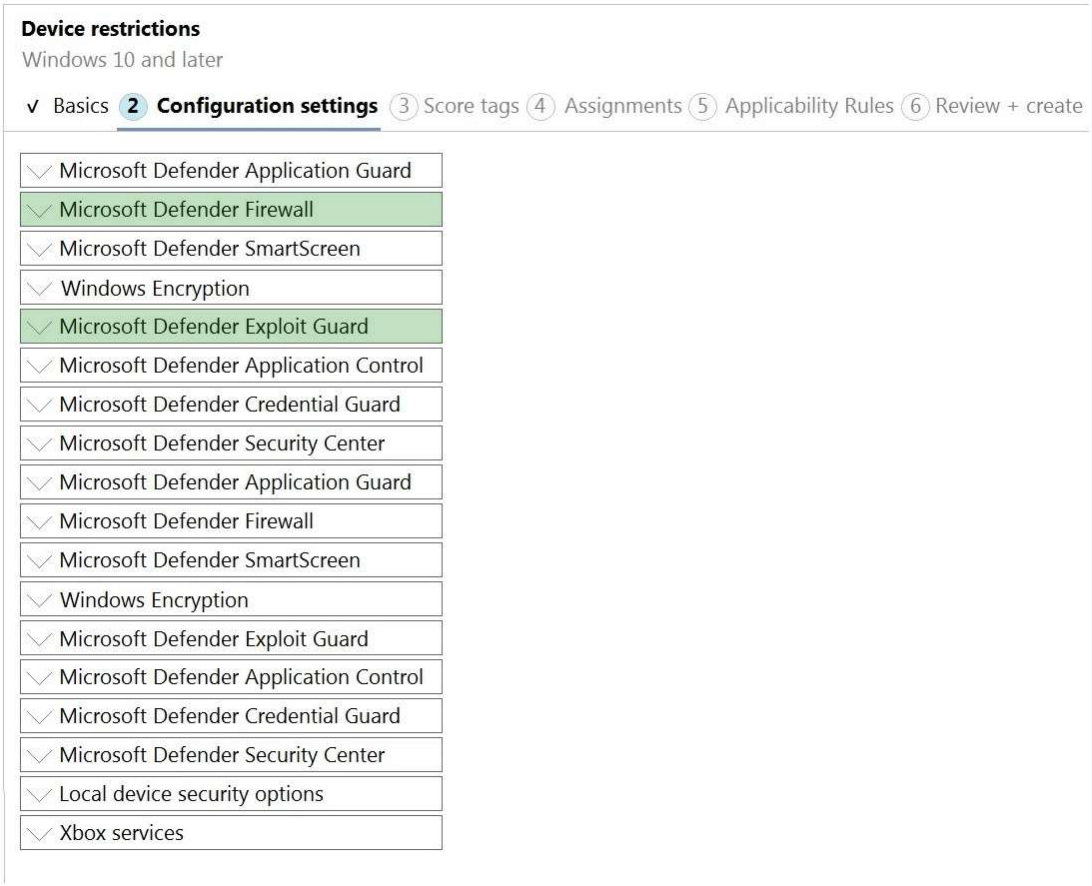
Windows 10 and later

✓ Basics (2) **Configuration settings** (3) Score tags (4) Assignments (5) Applicability Rules (6) Review + create

- Microsoft Defender Application Guard
- Microsoft Defender Firewall
- Microsoft Defender SmartScreen
- Windows Encryption
- Microsoft Defender Exploit Guard
- Microsoft Defender Application Control
- Microsoft Defender Credential Guard
- Microsoft Defender Security Center
- Microsoft Defender Application Guard
- Microsoft Defender Firewall
- Microsoft Defender SmartScreen
- Windows Encryption
- Microsoft Defender Exploit Guard
- Microsoft Defender Application Control
- Microsoft Defender Credential Guard
- Microsoft Defender Security Center
- Local device security options
- Xbox services

Correct Answer:

Answer Area



Box 1: Microsoft Defender Firewall

Block users from transferring files over FTP.

Microsoft Defender Firewall settings include MdmStore/Global/DisableStatefulFtp, which could be used to disable stateful FTP.

Box 2: Microsoft Defender Exploit Guard

Prevent Microsoft Office applications from launching child processes.

Attack surface reduction rules in the Microsoft Defender.

These rules include: Block all Office applications from creating child processes

Note: Attack surface reduction rule merge behavior is as follows:

Attack surface reduction rules from the following profiles are evaluated for each device the rules apply to:

Devices > Configuration policy > Endpoint protection profile > *Microsoft Defender Exploit Guard* > Attack Surface Reduction

Endpoint security > Attack surface reduction policy > Attack surface reduction rules

Endpoint security > Security baselines > Microsoft Defender for Endpoint Baseline > Attack Surface Reduction Rules.

Reference:

https://docs.microsoft.com/en-us/intune/endpoint-protection-windows-10

Moumouh07 Highly Voted 1 year ago

Correct

upvoted 7 times

[Removed] Most Recent 6 months, 3 weeks ago

Yes, Exploit Guard.
The required setting is under "Attack surface reduction". I just checked that.

upvoted 1 times

RodrigoT 5 months, 1 week ago

You're right my friend. I tested too in my tenant. And here is the link:
https://docs.microsoft.com/en-us/microsoft-365/security/defender-endpoint/attack-surface-reduction-rules-reference?view=o365-worldwide#block-all-office-applications-from-creating-child-processes

upvoted 1 times

RodrigoT 5 months, 1 week ago

I just don't understand why the picture is repeating items. The correct list is:
Microsoft Defender Application Guard
Microsoft Defender Firewall <----------
Microsoft Defender SmartScreen
Windows Encryption
Microsoft Defender Exploit Guard <--------
Microsoft Defender Application Control
Microsoft Defender Credential Guard
Microsoft Defender Security Center
Local device security options

Xbox services
User Rights

upvoted 1 times

Soufien1030 9 months, 3 weeks ago

I will go with
prevent M Office Apps from launching processes: Windows Defender Exploit Guard
https://www.microsoft.com/security/blog/2017/10/23/windows-defender-exploit-guard-reduce-the-attack-surface-against-next-generation-malware/
Block users transfering files over FTP: Microsoft Defender Firewall
https://docs.microsoft.com/en-us/mem/intune/protect/endpoint-protection-windows-10

upvoted 3 times

HOTSPOT -

You have a Microsoft 365 subscription.

You need to configure access to Microsoft Office 365 for unmanaged devices. The solution must meet the following requirements:

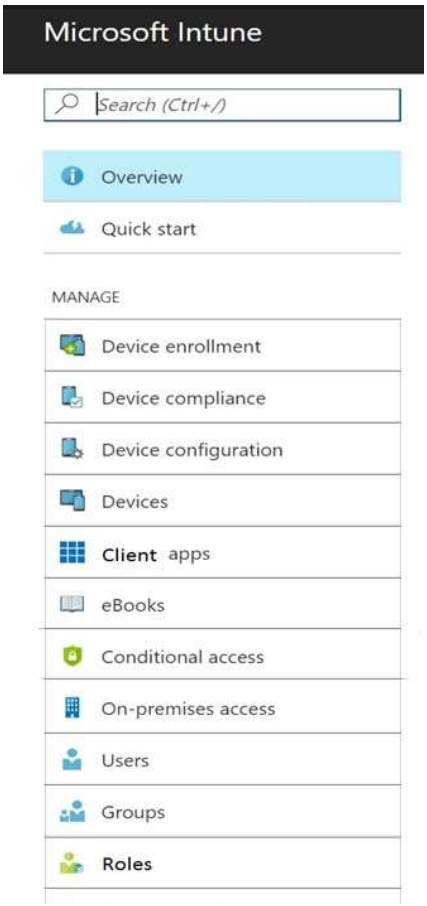
⇨ Allow only the Microsoft Intune Managed Browser to access Office 365 web interfaces.

⇨ Ensure that when users use the Intune Managed Browser to access Office 365 web interfaces, they can only copy data to applications that are managed by the company.

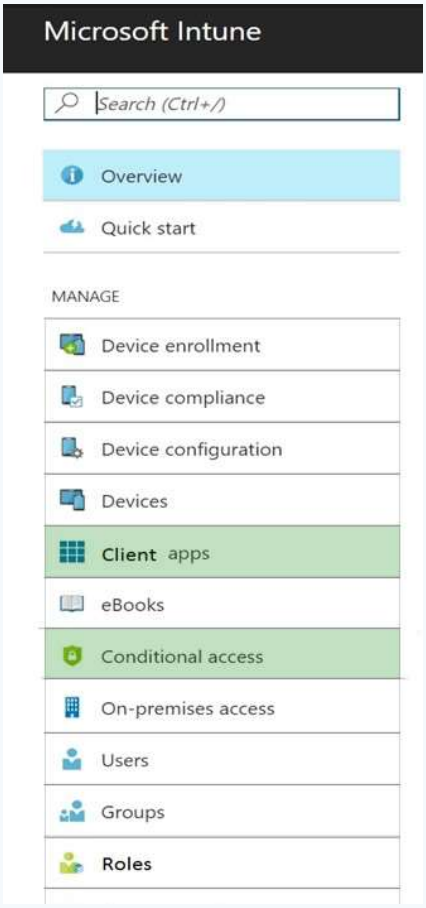
Which two settings should you configure from the Microsoft Intune blade? To answer, select the appropriate settings in the answer area.

NOTE: Each correct selection is worth one point.

Hot Area:



Correct Answer:



Box 1: Client -
Ensure that when users use the Intune Managed Browser to access Office 365 web interfaces, they can only copy data to applications that are managed by the company.

Box 2: Conditional Access -
Allow only the Microsoft Intune Managed Browser to access Office 365 web interfaces.
Organizations can use Azure AD Conditional Access policies to ensure that users can only access work or school content using Edge for iOS and Android. To do this, you will need a conditional access policy that targets all potential users. These policies are described in Conditional Access: Require approved client apps or app protection policy.
Reference:
https://docs.microsoft.com/en-us/intune/app-configuration-managed-browser#application-protection-policies-for-protected-browsers

minajahan Highly Voted 2 years, 5 months ago
I guess it should the other way round:
- Client Apps to restrict copy and paste
- Conditional Access to allow Edge to access O365
upvoted 19 times

RodrigoT 5 months, 1 week ago
April 2022 now. I would go to:
-Endpoint > Devices > Conditional Access | Policies > Conditions > Client apps > Browser
-Endpoint > Apps | App protection policies > Platform > Targeted Apps > Edge

https://docs.microsoft.com/en-us/azure/active-directory/conditional-access/concept-conditional-access-conditions#client-apps
upvoted 3 times

RodrigoT 5 months ago
Anyway, the answer provided is correct.
upvoted 1 times

techh3ad Highly Voted 1 year, 6 months ago
This question may be irrelevant. The Intune site has already moved to endpoint.microsoft.com and the blade options are different.
upvoted 9 times

LordCaine Most Recent 1 year ago
This question is irrelevant indeed its endpoint manager now
upvoted 5 times

Hester 2 years, 4 months ago
Intune Manager Browser has been retired: https://docs.microsoft.com/en-us/mem/intune/apps/app-configuration-managed-browser
upvoted 6 times

vm007 2 years, 7 months ago

1st.. set Clients Apps to allow Intune Manage apps
2nd...set the Conditional Access like copy & paste restriction
upvoted 3 times

Question #40 *Topic 4*

Your company implements Microsoft Azure Active Directory (Azure AD), Microsoft 365, Microsoft Intune, and Azure Information Protection.
The company's security policy states the following:
⇨ Personal devices do not need to be enrolled in Intune.
⇨ Users must authenticate by using a PIN before they can access corporate email data.
⇨ Users can use their personal iOS and Android devices to access corporate cloud services.
⇨ Users must be prevented from copying corporate email data to a cloud storage service other than Microsoft OneDrive for Business.
You need to configure a solution to enforce the security policy.
What should you create?

A. a data loss prevention (DLP) policy from the Microsoft 365 Compliance admin center

B. an insider risk management policy from the Microsoft 365 Compliance admin center

C. an app protection policy from the Endpoint Manager admin center

D. a device configuration profile from the Endpoint Manager admin center

Correct Answer: *C*
By implementing app-level policies, you can restrict access to company resources and keep data within the purview of your IT department.
Note: The important benefits of using App protection policies are the following:
Protecting your company data at the app level. Because mobile app management doesn't require device management, you can protect company data on both managed and unmanaged devices. The management is centered on the user identity, which removes the requirement for device management.
End-user productivity isn't affected and policies don't apply when using the app in a personal context. The policies are applied only in a work context, which gives you the ability to protect company data without touching personal data.
App protection policies makes sure that the app-layer protections are in place. For example, you can:
Require a PIN to open an app in a work context
Control the sharing of data between apps
Prevent the saving of company app data to a personal storage location
MDM, in addition to MAM, makes sure that the device is protected. For example, you can require a PIN to access the device, or you can deploy managed apps to the device. You can also deploy apps to devices through your MDM solution, to give you more control over app management.
Reference:
https://docs.microsoft.com/en-us/intune/app-protection-policy

Moderator 8 months ago
Selected Answer: C
Correctamundo! Just look at the reference provided :)
upvoted 3 times

moobdoob 8 months, 2 weeks ago
Very good!
upvoted 2 times

AVP_Riga 10 months, 2 weeks ago
Seems correct ☺
upvoted 4 times

Question #41 *Topic 4*

Note: This question is part of a series of questions that present the same scenario. Each question in the series contains a unique solution that might meet the stated goals. Some question sets might have more than one correct solution, while others might not have a correct solution.
After you answer a question in this section, you will NOT be able to return to it. As a result, these questions will not appear in the review screen.
Your company has an Azure Active Directory (Azure AD) tenant named contoso.com that contains several Windows 10 devices.
When you join new Windows 10 devices to contoso.com, users are prompted to set up a four-digit pin.
You need to ensure that the users are prompted to set up a six-digit pin when they join the Windows 10 devices to contoso.com.
Solution: From the Azure Active Directory admin center, you configure the Authentication methods.
Does this meet the goal?

A. Yes

B. No

Correct Answer: *B*
Instead, from the Azure Active Directory admin center, you configure automatic mobile device management (MDM) enrollment. From the Endpoint Management admin center, you configure the Windows Hello for Business enrollment options.
Reference:
https://docs.microsoft.com/en-us/intune/protect/windows-hello

techh3ad Highly Voted 1 year, 6 months ago
Correct. Set up Windows Hello for Business in Endpoint manager > Devices > Enroll devices > Windows enrollment > Windows Hello for Business. Set to Enabled and configure the minimum PIN length.
upvoted 6 times

techh3ad Most Recent 1 year, 6 months ago
Correct. Set up an Identity Protection device configuration profile and enable "Configure Windows Hello for Business and set the Minimum PIN length to the desired length.
upvoted 3 times

Question #42 *Topic 4*

Note: This question is part of a series of questions that present the same scenario. Each question in the series contains a unique solution that might meet the stated goals. Some question sets might have more than one correct solution, while others might not have a correct solution.
After you answer a question in this section, you will NOT be able to return to it. As a result, these questions will not appear in the review screen.
Your company has an Azure Active Directory (Azure AD) tenant named contoso.com that contains several Windows 10 devices.
When you join new Windows 10 devices to contoso.com, users are prompted to set up a four-digit pin.
You need to ensure that the users are prompted to set up a six-digit pin when they join the Windows 10 devices to contoso.com.
Solution: From the Azure Active Directory admin center, you configure automatic mobile device management (MDM) enrollment. From the Endpoint Manager admin center, you configure the Windows Hello for Business enrollment options.
Does this meet the goal?

A. Yes

B. No

Correct Answer: *A*
Hello for Business is an alternative sign-in method that uses Active Directory or an Azure Active Directory account to replace a password, smart card, or a virtual smart card. It lets you use a user gesture to sign in, instead of a password. A user gesture might be a PIN, biometric authentication such as Windows Hello, or an external device such as a fingerprint reader.
Intune integrates with Hello for Business in two ways:
➪ An Intune policy can be created under Device enrollment. This policy targets the entire organization (tenant-wide). It supports the Windows AutoPilot out-of- box-experience (OOBE) and is applied when a device enrolls.
➪ An identity protection profile can be created under Device configuration. This profile targets assigned users and devices, and is applied during check-in.
Reference:
https://docs.microsoft.com/en-us/intune/protect/windows-hello

john909 Highly Voted 10 months, 4 weeks ago
A is correct
upvoted 5 times

mrjeet Most Recent 3 months, 1 week ago
Correct answer!
upvoted 1 times

Question #43 *Topic 4*

You enable controlled folder access in audit mode for several computers that run Windows 10.
You need to review the events audited by controlled folder access.
Which Event Viewer log should you view?

A. Applications and Services\Microsoft\Windows\Windows Defender\Operational

B. Windows\Security

C. Applications and Services\Microsoft\Windows\Known Folders\Operational

Correct Answer: *A*
Review controlled folder access events in Windows Event Viewer
Controlled folder access events appear in Windows Event Viewer under Microsoft/Windows/Windows Defender/Operational folder.
Reference:
https://docs.microsoft.com/en-us/microsoft-365/security/defender-endpoint/evaluate-controlled-folder-access?view=o365-worldwide

SethuRam Highly Voted 11 months, 3 weeks ago
Now it has been moved to Intune > EndpointSecurity > Account protection. As on writing - 16th Oct 2021 it is in Preview
upvoted 11 times

RodrigoT 5 months, 1 week ago
April 2022. Still on Windows Event Viewer under Microsoft/Windows/Windows Defender/Operational
Source:
https://docs.microsoft.com/en-us/microsoft-365/security/defender-endpoint/evaluate-controlled-folder-access?view=o365-worldwide#review-controlled-folder-access-events-in-windows-event-viewer

Endpoint Account protection (Preview) policies help protect user credential by using technology such as Windows Hello for Business and Credential Guard. It has nothing to do with Event Viewer.
upvoted 2 times

letters1234 Most Recent 7 months, 1 week ago
Selected Answer: A
Controlled folder access events appear in Windows Event Viewer: Microsoft/Windows/Windows Defender/Operational folder.

Event ID Description
5007 Event when settings are changed
1124 Audited controlled folder access event
1123 Blocked controlled folder access event

https://docs.microsoft.com/en-us/microsoft-365/security/defender-endpoint/evaluate-controlled-folder-access?view=o365-worldwide
upvoted 2 times

HOTSPOT -

You have a Microsoft 365 tenant that uses Microsoft Intune.

From the Microsoft Endpoint Manager admin center, you plan to create a baseline to monitor the Startup score and the App reliability score of enrolled Windows

10 devices.

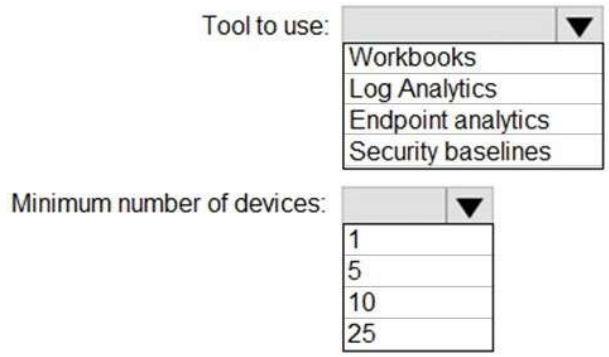
You need to identify which tool to use to create the baseline and the minimum number of devices required to create the baseline.

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

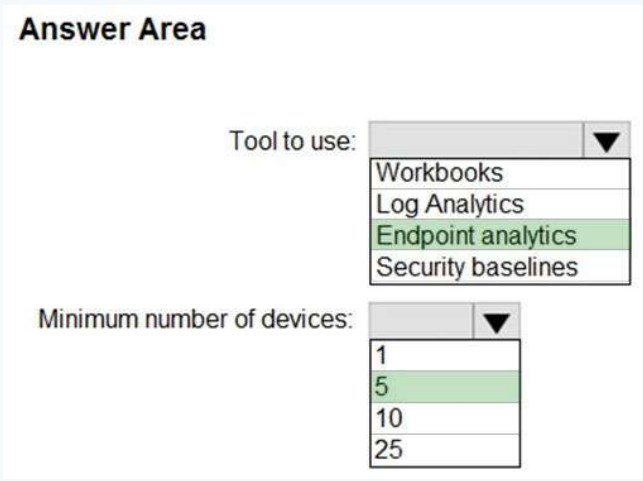
NOTE: Each correct selection is worth one point.

Hot Area:

Answer Area



Correct Answer:



Box 1: Endpoint analytics -

Endpoint analytics has the following three items are central to understanding each of the reports:

Scores -

Baselines -

Insights and recommendations -

Box 2: 5 -

A status of insufficient data means you don't have enough devices reporting to provide a meaningful score. Currently, at least five devices are required.

Reference:

https://docs.microsoft.com/en-us/mem/analytics/scores#understanding-scores

R0b671 Highly Voted 11 months ago

Minimum number of devices: 10

There also needs to be a minimum of 10 x Windows 10 devices enrolled into Intune (Azure AD joined or Co-managed/Hybrid joined) in your tenant before Endpoint Analytics will start to collect data, and it will take up to 72 hours (from experience) for the tenant to report on what it has found.

Source: https://iamitgeek.com/2021/08/23/microsoft-endpoint-analytics-overview/

upvoted 9 times

forExamCert2023 6 months, 3 weeks ago

five devices.
"A status of insufficient data means you don't have enough devices reporting to provide a meaningful score. Currently, at least five devices are required."
Ref: https://docs.microsoft.com/en-us/mem/analytics/scores#understanding-scores

upvoted 3 times

[Removed] 6 months, 3 weeks ago

I just checked this in Endpoint Manager (Reports>Endpoint Analytics>Settings>Baseline).
It clearly states, that 10 (TEN) devices are necessary to CREATE a baseline. (After that, it seems that 5 devices need to report to access the data, but that is not what the question is about!)

upvoted 1 times

RodrigoT 5 months, 1 week ago

I CHECKED in my tenant too. When you click on Reports > Endpoint analytics | Settings > Baseline it says 10 devices to CREATE a baseline. But on the link provided dated 04/05/2022, it says 5 devices to REPORT. Microsoft kills me. So, I vote:
-Endpoint Analytics
-10 (to create)

upvoted 2 times

lykeP Highly Voted 8 months, 2 weeks ago

1. Endpoint Analytics
2. Minimum number of Devices is 5

https://docs.microsoft.com/en-us/mem/analytics/enroll-intune#:~:text=We%20currently%20require%20at%20least%20five%20devices.

upvoted 7 times

learningmonkey Most Recent 7 months, 2 weeks ago

1. Endpoint Analytics
2. Minimum number of devices : 5

A status of insufficient data means you don't have enough devices reporting to provide a meaningful score. Currently, at least five devices are required.

https://docs.microsoft.com/en-us/mem/analytics/scores#understanding-scores

upvoted 2 times

RodrigoT 5 months, 1 week ago

Microsoft#understanting-the-documentation 5 to "report", 10 to "create".

upvoted 1 times

Moderator 8 months ago

Correct answer provided, look at the reference.

upvoted 1 times

RodrigoT 5 months, 1 week ago

Looking at the reference sometimes is not enough. Specially when it says 5 devices to "report", not to "create" a baseline. You have to TEST in your own test tenant. There you're not allowed to "create" a baseline if you don't have at minimum 10 devices.

upvoted 1 times

lucadp010 8 months, 2 weeks ago

Answer is correct.

upvoted 1 times

lucadp010 8 months, 2 weeks ago

https://docs.microsoft.com/en-us/mem/analytics/scores

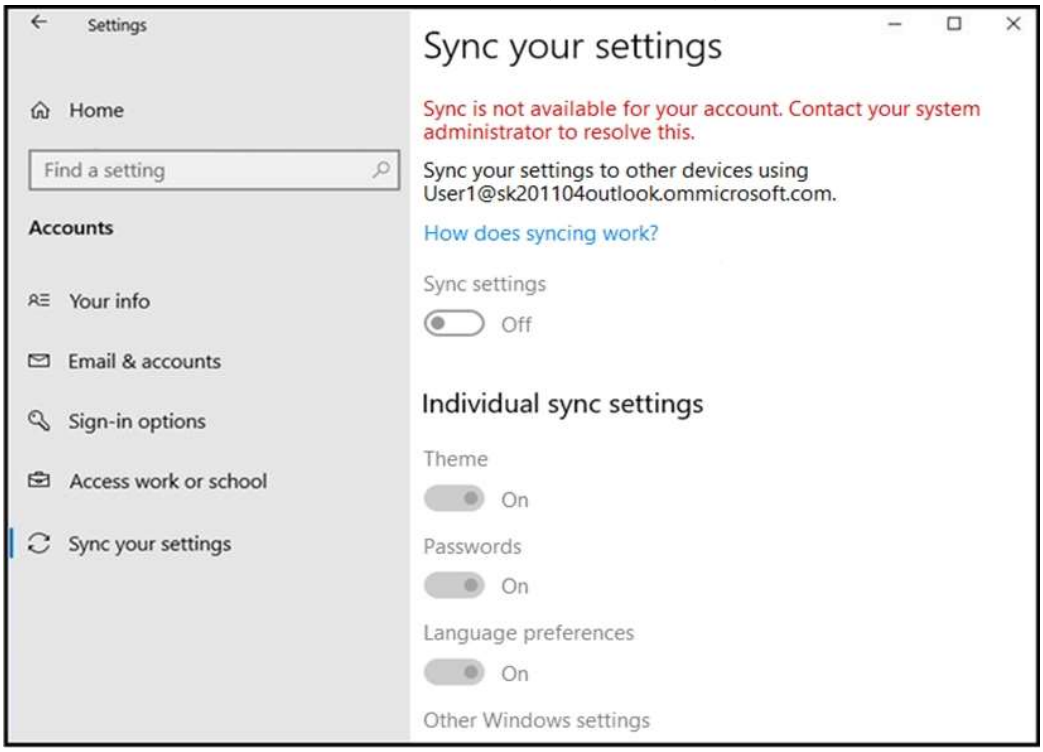
upvoted 2 times

Question #45 *Topic 4*

Your company has a Microsoft 365 tenant.

Users sign in to Windows 10 devices by using their Microsoft 365 account.

On a computer, you open Sync your settings as shown in the exhibit. (Click the Exhibit tab.)



You need to set Sync settings to On.

What should you do?

A. Enable User Experience Virtualization (UE-V).

B. Enable Windows Mobility Center.

C. Disable Windows Hello for Business.

D. Enable Enterprise State Roaming.

Correct Answer: *D*

Enterprise State Roaming provides users with a unified experience across their Windows devices and reduces the time needed for configuring a new device.

Enterprise State Roaming operates similar to the standard consumer settings sync that was first introduced in Windows 8.

Note: To enable Enterprise State Roaming

1. Sign in to the Azure portal.
2. Browse to Azure Active Directory > Devices > Enterprise State Roaming.
3. Select Users may sync settings and app data across devices.

Reference:

https://docs.microsoft.com/en-us/azure/active-directory/devices/enterprise-state-roaming-enable

john909 Highly Voted 10 months, 4 weeks ago

Seems correct

upvoted 6 times

Garito Most Recent 7 months, 1 week ago

D is the answer. I confirmed in lab.

upvoted 4 times

RodrigoT 5 months, 1 week ago

Thank you for really testing.

upvoted 1 times

RodrigoT 5 months ago

Here is a visible picture:
https://cdn.appuals.com/wp-content/uploads/2019/11/sync-is-not-available-for-your-account.png.webp
And here is the official answer:
https://answers.microsoft.com/en-us/msoffice/forum/all/settings-sync-is-not-available-for-your-account/87aabb9f-b637-45b5-9394-1cba100da4bf?auth=1

upvoted 1 times

HOTSPOT -

Your network contains an Active Directory domain. The domain contains the computers shown in the following table.

Name	Operating system
Computer1	Windows 10 Enterprise
Computer2	Windows 10 Pro
Computer3	Windows 10 Pro

Microsoft Defender Application Guard is installed on the computers.

Application Guard Group Policy settings are applied to the computers as shown in the following table.

Setting	State
Turn on Windows Defender Application Guard in Managed Mode	Enabled
Configure Windows Defender Application Guard clipboard settings	Enabled
Allow files to download and save to the host operating system from Windows Defender Application Guard	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
Computer1 can use Application Guard in Enterprise-managed mode.	○	○
Computer2 can copy clipboard settings from Microsoft Edge to Application Guard.	○	○
Computer3 can download files from Application Guard to the host operating system.	○	○

Correct Answer:

Answer Area

Statements	Yes	No
Computer1 can use Application Guard in Enterprise-managed mode.	○	○
Computer2 can copy clipboard settings from Microsoft Edge to Application Guard.	○	○
Computer3 can download files from Application Guard to the host operating system.	○	○

Reference:

https://docs.microsoft.com/en-us/windows/security/threat-protection/microsoft-defender-application-guard/configure-md-app-guard

tf444 Highly Voted 11 months, 2 weeks ago

Tested, Y, Y, N.

upvoted 6 times

RodrigoT 5 months, 1 week ago

Y- for Enterprise
Y- for Pro or Enterprise
N- for Pro

Answers provided are correct.

upvoted 1 times

RodrigoT 5 months ago

A more specific link:
https://docs.microsoft.com/en-us/windows/security/threat-protection/microsoft-defender-application-guard/configure-md-app-guard#application-specific-settings

upvoted 1 times

letters1234 Most Recent 7 months, 1 week ago

Windows 10 1803 is out of support - May 11th 2021. This question will possibly not be asked or will be Y Y Y.

upvoted 1 times

examkiller321 11 months, 3 weeks ago

Why not YYY?

upvoted 3 times

IcemanJim 10 months, 1 week ago

Allow files to download to host operating system Windows 10 Enterprise, 1803 or higher

upvoted 3 times

examkiller321 11 months, 2 weeks ago

Okay, I already know. "Allow files" only works in Windows 10 Enterpise, and in the scenario we have Windows 10 Pro. All answers are correct.

upvoted 2 times

Question #47 *Topic 4*

You have a Microsoft 365 tenant that contains the Windows 10 devices shown in the following table.

Name	Used by	Azure Active Directory (Azure AD) join type	Managed by using Microsoft Intune
Device1	User1	Joined	Yes
Device2	User1	Registered	Yes
Device3	User1	Joined	No

You enable Enterprise State Roaming.

You need to ensure that User1 can sync Windows settings across the devices.

What should you do?

A. Remove Device1 and Device2 from Intune.

B. Join Device2 to Azure AD.

C. Add a Microsoft account to each device.

D. Enroll Device3 in Intune.

Correct Answer: *B*

For a Windows 10 or newer device to use the Enterprise State Roaming service, the device must authenticate using an Azure AD identity. For devices that are joined to Azure AD, the user's primary sign-in identity is their Azure AD identity, so no other configuration is required.

Reference:

https://docs.microsoft.com/en-us/azure/active-directory/devices/enterprise-state-roaming-enable

auton Highly Voted 11 months, 3 weeks ago

I believe this is B) Join Device to AAD instead of enrolling the device in to Intune

upvoted 15 times

examkiller321 11 months, 2 weeks ago

You're right, the answer is B.

upvoted 5 times

BAbdalla 10 months, 4 weeks ago

So then Enterprise State Roaming wouldn't work on personal devices? In practice, personal devices appear as Registered rather than Joined in Azure AD. Could you explan, please? I think I missed something.

upvoted 3 times

IcemanJim 10 months, 1 week ago

This only works for a AAD joined device. Windows backup is the consumer equivalent to Enterprise State Roaming. Remember this is a AAD feature, it is nothing to do with Intune.

upvoted 6 times

MR_Eliot Most Recent 5 months ago

Selected Answer: B

B is correct. You need to enroll the device in Azure AD to use enterprise roaming feature.

upvoted 1 times

RodrigoT 5 months, 1 week ago

How can they answer D on a simple question like this? Moderator, please correct the answer provided.

upvoted 1 times

moobdoob 8 months, 2 weeks ago

Selected Answer: B

Answer is B

upvoted 4 times

IykeP 8 months, 2 weeks ago

Selected Answer: B

B is the correct Answer.

upvoted 4 times

ameli8222 8 months, 3 weeks ago

I agree with B

upvoted 3 times

hawkens 9 months, 2 weeks ago

Must be the version, but there is nog version stated in the question??

Enterprise State Roaming is a feature for Windows 10 users that are using a device which is Azure AD device registered (either AAD joined or hybrid joined). User gain the ability to securely synchronize their user and application settings data to the Microsoft cloud.

upvoted 1 times

FrancisLai 10 months, 2 weeks ago

Selected Answer: B

The device is Azure AD joined or hybrid Azure AD joined. For more information, see how to get a device under the control of Azure AD."
https://docs.microsoft.com/en-us/azure/active-directory/devices/enterprise-state-roaming-troubleshooting

upvoted 3 times

[Removed] 11 months, 2 weeks ago

A: Join Device2 to AzureAD
"The device is Azure AD joined or hybrid Azure AD joined. For more information, see how to get a device under the control of Azure AD."
https://docs.microsoft.com/en-us/azure/active-directory/devices/enterprise-state-roaming-troubleshooting

upvoted 3 times

[Removed] 11 months, 2 weeks ago

I mean B, not A, sorry

upvoted 3 times

Question #48 *Topic 4*

You use Microsoft Defender for Endpoint to protect computers that run Windows 10.
You need to assess the differences between the configuration of Microsoft Defender for Endpoint and the Microsoft-recommended configuration baseline.
Which tool should you use?

A. Microsoft Defender Security Center

B. Desktop Analytics

C. Microsoft Defender for Endpoint Power BI app

D. Microsoft Secure Score

Correct Answer: *D*
Following the Secure Score recommendations can protect your organization from threats.
Secure Score helps organizations:
⇨ Report on the current state of the organization's security posture.
⇨ Improve their security posture by providing discoverability, visibility, guidance, and control.
⇨ Compare with benchmarks and establish key performance indicators (KPIs).
Note: Products included in Secure Score
Currently there are recommendations for the following products:
⇨ Microsoft 365 (including Exchange Online)
⇨ Azure Active Directory
⇨ Microsoft Defender for Endpoint
⇨ Microsoft Defender for Identity
⇨ Defender for Cloud Apps
⇨ Microsoft Teams
⇨ Recommendations for other security products are coming soon. The recommendations won't cover all the attack surfaces associated with each product, but they're a good baseline.
Reference:
https://docs.microsoft.com/en-us/microsoft-365/security/defender/microsoft-secure-score?view=o365-worldwide

matelin Highly Voted 7 months, 1 week ago
Selected Answer: A
I'd say "A". Secure Score shows you the security state of the whole M365 tenant. MS Defender Security Center has the feature in question: https://docs.microsoft.com/en-us/microsoft-365/security/defender-endpoint/configure-machines-security-baseline?view=o365-worldwide#compare-the-microsoft-defender-for-endpoint-and-the-windows-intune-security-baselines
upvoted 6 times

RodrigoT 5 months, 1 week ago
Your link says exactly the opposite. Read again.
The correct answer is D.
upvoted 2 times

Anon1212 6 months, 3 weeks ago
Agreed^^
upvoted 1 times

DragonSlayer848 Most Recent 2 weeks, 1 day ago
Selected Answer: D
The documentation reads the following for Security Center:
https://docs.microsoft.com/en-us/microsoft-365/security/defender-endpoint/use?view=o365-worldwide
I say the answer is D
upvoted 1 times

Garito 7 months, 1 week ago
Documentation reads the following for Security Center:

https://docs.microsoft.com/en-us/microsoft-365/security/defender-endpoint/use?view=o365-worldwide

I say this is D
upvoted 1 times

TaboloDude 9 months, 2 weeks ago
The answer seems to be correct.
upvoted 2 times

Rick11221 9 months, 3 weeks ago
Group Policy Analytics?
upvoted 1 times

AVP_Riga 10 months, 3 weeks ago

Is it right? Anyone?
upvoted 1 times

Question #49 *Topic 4*

Note: This question is part of a series of questions that present the same scenario. Each question in the series contains a unique solution that might meet the stated goals. Some question sets might have more than one correct solution, while others might not have a correct solution.
After you answer a question in this section, you will NOT be able to return to it. As a result, these questions will not appear in the review screen.
Your company has an Azure Active Directory (Azure AD) tenant named contoso.com that contains several Windows 10 devices.
When you join new Windows 10 devices to contoso.com, users are prompted to set up a four-digit pin.
You need to ensure that the users are prompted to set up a six-digit pin when they join the Windows 10 devices to contoso.com.
Solution: From the Azure Active Directory admin center, you configure automatic mobile device management (MDM) enrollment. From the Endpoint Manager admin center, you create and assign a device restrictions profile.
Does this meet the goal?

A. Yes

B. No

Correct Answer: *B*
Instead, from the Azure Active Directory admin center, you configure automatic mobile device management (MDM) enrollment. From the Endpoint Management admin center, you configure the Windows Hello for Business enrollment options.
Reference:
https://docs.microsoft.com/en-us/intune/protect/windows-hello

Question #50 *Topic 4*

Your company has a Microsoft Azure Active Directory (Azure AD) tenant. All users in the company are licensed for Microsoft Intune.
You need to ensure that the users enroll their iOS device in Intune.
What should you configure first?

A. A Device Enrollment Program (DEP) token.

B. An Intune device configuration profile.

C. A Device enrollment manager (DEM) account.

D. An Apple MDM Push certificate.

Correct Answer: *D*
You need to create an Apple MDM push certificate and use it to manage Apple devices with Intune. The Apple MDM push certificate must be added to Endpoint
Manager, and must be active.
Reference:
https://docs.microsoft.com/en-us/mem/intune/enrollment/apple-mdm-push-certificate-get

wx78 Highly Voted 3 years, 1 month ago
Correct: D .
upvoted 25 times

lucidgreen 1 year, 7 months ago
You don't configure the Apple Push Cert. You use it to configure the DEP token. The question asks what you need to CONFIGURE first, not what you need.
upvoted 2 times

geoffC 1 year, 5 months ago
Click on Apple MDM Push certificate and at the top of the screen it says "Configure MDM Push Certificate"
upvoted 1 times

Mr01z0 1 year, 6 months ago
I have done this several times and I can tell you that:

It is literally impossible to configure an "Enrollment program tokens" before you configure "Configure MDM Push Certificate" (APN). The intune portal does not allow you to do that.

So the answer to this question is still to first configure an apple push cert (answer D) and after that you configure the enrollment program token.

Even then after configuring that, your apple devices themselves need to be registered as DEP/Autoenrollment in Apple Business Manager or Apple School Manager, this can be done either by buying the devices DEP enabled or adding them manually to DEP by using the Apple Configurator 2 software.

Then Devices also need to be assigned to an enrollment profile. After that, and also only from the Apple device setup wizard (Intune integrated or not) the users will be forced to enroll their devices.
upvoted 9 times

configmike 1 year, 6 months ago
On the iOS enrollment page, it literally says "Intune requires an Apple MDM Push certificate to manage Apple devices, and supports multiple enrollment methods. Set up the MDM push certificate to begin. Learn more."
upvoted 2 times

DJHASH786 1 year, 6 months ago
Thats literally what it asks for as soon as you click on Apple Devices ... so answer is D..
upvoted 3 times

zordss Highly Voted 2 years, 8 months ago
COrrect answer is A.
The very first step is to use the apple DEP portal to get a DEP token. Got this from CBT nuggets.
upvoted 15 times

RodrigoT 5 months, 1 week ago
And what scares me the most is that 15 guys upvoted you.
upvoted 6 times

[Removed] 6 months, 3 weeks ago
Unfortunately, this is not correct, see https://docs.microsoft.com/en-us/mem/intune/enrollment/ios-enroll
The Apple MDM push certificate is a requirement to set up the different enrollment methods, among them DEP (now called ADE).
upvoted 1 times

[Removed] 6 months, 3 weeks ago
So the correct answer is indeed D.
upvoted 1 times

trevderpy Most Recent 2 months, 3 weeks ago

Selected Answer: D

D is correct

upvoted 2 times

BLYBOI 1 year, 4 months ago

Before you can enroll iOS/iPadOS devices with ADE, you need an ADE token (.p7m) file from Apple.

upvoted 1 times

RodrigoT 5 months, 1 week ago

But FIRST you need a certificate.

upvoted 2 times

slaoui 1 year, 5 months ago

Push certificate is a prerequisite for DEP
https://docs.microsoft.com/en-us/mem/intune/enrollment/device-enrollment-program-enroll-ios#prerequisites

Answer is D

upvoted 1 times

Jeffoort 1 year, 6 months ago

Correct, D

https://docs.microsoft.com/nl-nl/mem/intune/enrollment/apple-mdm-push-certificate-get

upvoted 1 times

Kryan 1 year, 6 months ago

Based on the article below, i would lean towards: D
https://docs.microsoft.com/en-us/mem/intune/enrollment/ios-user-enrollment

upvoted 1 times

hawkens 1 year, 7 months ago

A prerequisites is a Apple MDM Push Certificate.

You need an Apple MDM push certificate to manage Apple devices with Intune.

upvoted 2 times

cubalondon 1 year, 7 months ago

you need to fill A Device Enrollment Program (DEP) token form, and upload it in order to get an apple push Certificate.

upvoted 3 times

Balena 1 year, 7 months ago

These are "their" IOS devices = BYOD. Therefor, you need to first addan Apple MDM push certificate. Check section "User and Device enrollment administrator tasks" of : https://docs.microsoft.com/en-us/mem/intune/fundamentals/deployment-guide-enrollment-ios-ipados#byod-user-and-device-enrollment

upvoted 2 times

Hamilcar 1 year, 7 months ago

First step: Create a New Push Certificate

upvoted 1 times

Vig 1 year, 7 months ago

Answer is D:

In article linked as reference:
Automatically enroll iOS/iPadOS devices by using Apple's Automated Device Enrollment
Prerequisites
Devices purchased in Apple's ADE
Mobile device management (MDM) authority
An Apple MDM push certificate

upvoted 1 times

lijk_manson 1 year, 7 months ago

Well look at this: https://vceguide.com/when-you-try-to-enroll-an-ios-device-in-intune-you-get-an-error-you-need-to-ensure-that-you-can-enroll-the-ios-device-in-intune/

upvoted 1 times

hawkens 1 year, 8 months ago

User and Device enrollment administrator tasks

This task list provides an overview. For more specific information, see Set up iOS/iPadOS and iPadOS User Enrollment.

Be sure your devices are supported.

Be sure the Apple MDM push certificate is added to Endpoint Manager, and is active. This certificate is required to enroll iOS/iPadOS devices. For more information, see Get an Apple MDM push certificate.

upvoted 1 times

romanticflower 1 year, 9 months ago

The push certificate is the bare minimum requirement. Without this the other options are not even available to configure (enrollment program tokens included).

upvoted 1 times

lucidgreen 1 year, 7 months ago

It's asking what you configure, not what you need. The DEP needs the Apple Push Cert in order to be configured.

upvoted 1 times

Baxter 1 year, 9 months ago

See question #12 for topic 3, further evidence that MS is looking for DEP token setup to be completed first

upvoted 1 times

kktamang 1 year, 9 months ago

Before you can enroll iOS/iPadOS devices with ADE, you need an ADE token (.p7m) file from Apple https://docs.microsoft.com/en-us/mem/intune/enrollment/device-enrollment-program-enroll-ios#get-an-apple-automated-device-enrollment-token . Answer is A.

upvoted 1 times

Question #51 *Topic 4*

You have the devices shown in the following table.

Name	Operating system	Domain member
Device1	Windows 8.1 Enterprise	Yes
Device2	Windows 10 Pro	No
Device3	Windows 10 Enterprise	Yes
Device4	Mac OS X	No

You plan to implement Microsoft Defender for Endpoint.

You need to identify which devices can be onboarded to Microsoft Defender for Endpoint.

What should you identify?

A. Device3 only

B. Device1, Device2, and Device3 only

C. Device1, Device2, Device3, and Device4

D. Device2 and Device3 only

E. Device2, Device3, and Device4 only

Correct Answer: *B*

All the operating systems are supported.

Note: You can onboard the following operating systems:

Windows 8.1 -
Windows 10, version 1607 or later

Windows 11 -

Windows Server 2012 R2 -

Windows Server 2016 -
Windows Server Semi-Annual Channel (SAC), version 1803 or later

Windows Server 2019 -

Windows Server 2022 -

Reference:

https://docs.microsoft.com/en-us/mem/configmgr/protect/deploy-use/defender-advanced-threat-protection#bkmk_os

AleDrinker 5 months, 1 week ago

B - all devices except for #4 MAX OS X

https://docs.microsoft.com/en-us/mem/configmgr/protect/deploy-use/defender-advanced-threat-protection#bkmk_os

Microsoft Defender for Endpoint

Article
02/22/2022
Supported client operating systems

You can onboard the following operating systems:

Windows 8.1
Windows 10, version 1607 or later
Windows 11
Windows Server 2012 R2
Windows Server 2016
Windows Server Semi-Annual Channel (SAC), version 1803 or later
Windows Server 2019
Windows Server 2022

upvoted 1 times

RodrigoT 5 months, 1 week ago

A correct answer and an excellent link. Thank you Examtopics.

upvoted 1 times

HOTSPOT -

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

Name	Member of
User1	Group1
User2	Group2

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

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

From Intune, you create and send a custom notification named Notification1 to Group1.

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

NOTE: Each correct selection is worth one point.

Hot Area:

Answer Area

Statements	Yes	No
User1 receives Notification1 on Device1.	○	○
User2 receives Notification1 on Device2.	○	○
User1 receives Notification1 on Device3.	○	○

Correct Answer:

Answer Area

Statements	Yes	No
User1 receives Notification1 on Device1.	○	○
User2 receives Notification1 on Device2.	○	○
User1 receives Notification1 on Device3.	○	○

Box 1: No -

Windows 10 devices cannot receive notifications.

Custom notifications can be visible on lock screens on both iOS/iPadOS and Android devices depending on device settings

Box 2: No -

User2 is in the wrong group. Only Group1 receives notifications.

Note: Sending a notification to a group will target only the users of that group; the notification will go to all iOS/iPadOS and Android devices enrolled by that user.

Box 3: Yes -

User1 is in the right group and Device3 has the right OS.

Reference:

https://docs.microsoft.com/en-us/mem/intune/remote-actions/custom-notifications

DragonSlayer848 2 weeks, 1 day ago

Wouldn't it be N N N? User1 is not a member of Group2, and Device3 is in Group2. User1 is a member of Group1.

upvoted 1 times

Suxi22 5 months, 1 week ago

N - Windows device
N - In a group with Users and Devices only Users will receive the notifications
Y - User1 in Group 1
Tested in Tennant under Intune>Tenant Administration > Custom Notification (it will say it at assignments)
https://docs.microsoft.com/en-us/mem/intune/remote-actions/custom-notifications

upvoted 1 times

AleDrinker 5 months, 1 week ago

N - Windows device
Y - Android and G1

N - G2
Send custom notifications in Intune

Article
01/13/2022

Use Microsoft Intune to send custom notifications to the users of managed iOS/iPadOS and Android devices.

upvoted 1 times

RodrigoT 5 months, 1 week ago

Correct.
N- Windows devices are not included
N- Group of devices are ignored when they include users.
Y- User1 is in Group1 and the device is IOS
From the link:
Use Microsoft Intune to send custom notifications to the users of managed iOS/iPadOS and Android devices. These messages appear as standard push notifications. Intune custom notifications aren't supported by macOS and Windows devices. When sending a notification to a group, messages target only the users in the group and are sent to each iOS/iPadOS or Android device that the user has registered. Devices in the group will be ignored when targeting the notification. But, you can send notifications to a single device.

upvoted 3 times

Question #53 *Topic 4*

You have a Microsoft Azure Log Analytics workplace that collects all the event logs from the computers at your company.
You have a computer named Computer1 than runs Windows 10. You need to view the events collected from Computer1.
Which query should you run in Log Analytics?

A. Event | where Computer = = "Computer1"

B. ETWEvent | where SourceSystem = = "Computer1"

C. ETWEvent | where Computer = = "Computer1"

D. Event | where SourceSystem = = "Computer1"

Correct Answer: *A*
Windows event records properties include:
Computer: Name of the computer that the event was collected from.
The following table provides different examples of log queries that retrieve Windows Event records.

Query	Description
Event	All Windows events.
Event | where EventLevelName == "error"	All Windows events with severity of error.
Event | summarize count() by Source	Count of Windows events by source.
Event | where EventLevelName == "error" | summarize count() by Source	Count of Windows error events by source.

Reference:
https://docs.microsoft.com/en-us/azure/azure-monitor/platform/data-sources-windows-events

Question #54 *Topic 4*

HOTSPOT -

A company named A.Datum Corporation uses Microsoft Endpoint Configuration Manager, Microsoft Intune, and Desktop Analytics.

A.Datum purchases a company named Contoso, Ltd. Contoso has devices that run the following operating systems:

- Windows 8.1
- Windows 10
- Android
- iOS

A.Datum plans to use Desktop Analytics to monitor the Contoso devices.

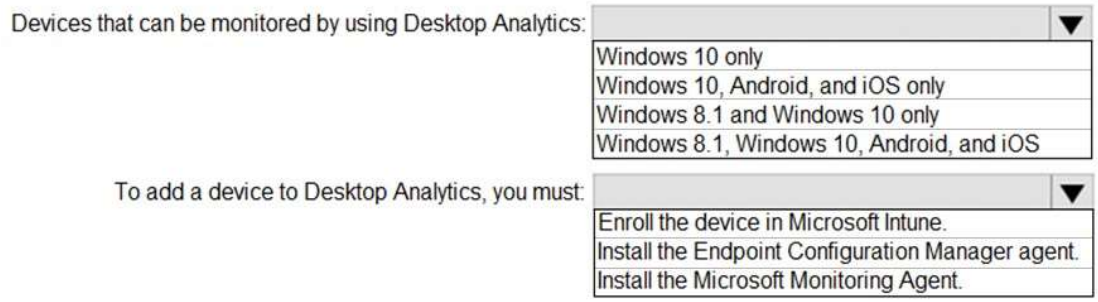
You need to identify which devices can be monitored by using Desktop Analytics and how to add the devices to Desktop Analytics.

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

NOTE: Each correct selection is worth one point.

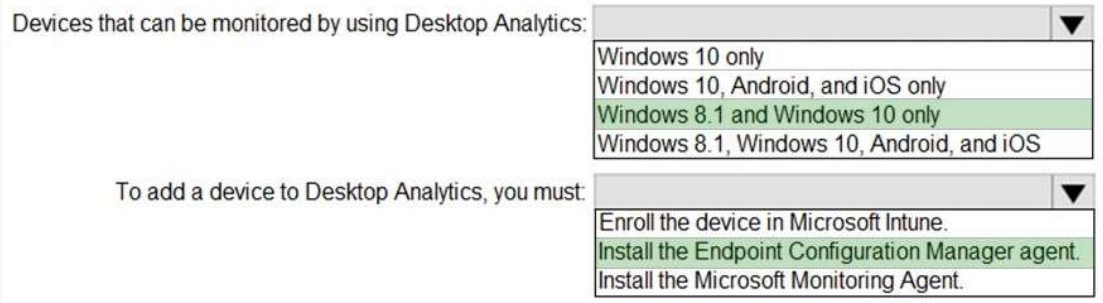
Hot Area:

Answer Area



Correct Answer:

Answer Area



Box 1: Windows 8.1 and Windows 10 only

Windows 7, Windows 8.1 and Windows 10 are supported.

Box 2: Install the Endpoint Configuration Manager agent.

Need to for the Windows 8.1 client.

Reference:

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

Wilf32 Highly Voted 1 year, 5 months ago

Answer seems to be correct after reading the link provided.

upvoted 9 times

Merma Most Recent 1 year, 4 months ago

Box 1: Windows 8.1 and Windows 10 only
Box 2: Enroll the device in Microsoft Intune
"Starting in Configuration Manager 1802, you don't need to install the Endpoint Protection agent (SCEPInstall) on Windows 10 devices."
https://docs.microsoft.com/en-us/mem/configmgr/protect/deploy-use/endpoint-protection-configure-client

upvoted 1 times

grakara 1 year, 4 months ago

"When you connect Configuration Manager to Desktop Analytics, you configure settings to enroll devices to Desktop Analytics."

Answer given is correct.

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

upvoted 5 times

Jimbob77 1 year, 3 months ago

Yep, thanks for the url grakara ..
Device enrollment
The Desktop Analytics service has no agents to install. Device enrollment requires configuring settings on the devices you want it to monitor. Configuration Manager provides an integrated experience for managing and deploying these settings to clients. For the best experience, use Configuration Manager.
upvoted 1 times

ExamStudy101 1 year, 2 months ago
For Windows 10 there is no agents to install. Not true if you're using Windows 8.1
upvoted 1 times

lahey69 1 year, 4 months ago
But if one of the PCs is W8.1 then surely configuration manager is required?
upvoted 2 times

ExamStudy101 1 year, 2 months ago
Except you have Windows 8.1 devices that will need the agent.
upvoted 1 times

Question #55 *Topic 4*

Your company uses Microsoft Intune to manage devices. You need to ensure that only Android devices that use Android work profiles can enroll in Intune.
Which two configurations should you perform in the device enrollment restrictions? Each correct answer presents part of the solution.
NOTE: Each correct selection is worth one point.

A. From Platform Settings, set Android Enterprise (work profile) to Allow.

B. From Platform Settings, set Android device administrator Personally Owned to Block.

C. From Platform Settings, set Android device administrator Personally Owned to Allow.

D. From Platform Settings, set Android device administrator to Block.

Correct Answer: *AB*
Once you have entered your corporate device indentifiers those devices are automatically enrolled as ג€Corporate Devicesג€. The next step is to block enrolment of personal devices. You can do this by navigating to Intune > Device Enrollment > Enrollment Restrictions.
Under Device Type Restrictions click on ג€Defaultג€ and then navigate to ג€Propertiesג€. Under properties click ג€Configure Platformsג€ and next to android change the selection from ג€allowג€ to ג€blockג€ for personally owned devices and click ok
Reference:
https://triplesixseven.com/block-personal-android-devices-from-enrolling-in-intune/

RodrigoT 5 months, 1 week ago
Answers correct.
-Android device administrator (legacy) doesn't have work profiles. Google is decreasing device administrator support in new Android releases. Actually since Android 10, device administrator is deprecated. Microsoft advise against enrolling new devices using the device administrator process and recommend that you migrate devices off of device administrator if the devices are going to update to Android 10.
https://docs.microsoft.com/en-us/mem/intune/enrollment/android-enroll-device-administrator
-Android Enterprise has a work profile. And they can be personally-owned or corporate-owned.
https://docs.microsoft.com/en-us/mem/intune/enrollment/android-enroll
upvoted 1 times

Question #56 *Topic 4*

QUESTION NO: 291 -
You have a Microsoft 365 E5 subscription and 25 Apple iPads.
You need to enroll the iPads in Microsoft Intune by using the Apple Configurator enrollment method.
What should you do first?

A. Upload a file that has the device identifiers for each iPad.

B. Modify the enrollment restrictions.

C. Configure an Apple MDM push certificate.

D. Add your user account as a device enrollment manager (DEM).

Correct Answer: *C*
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.
Reference:
https://docs.microsoft.com/en-us/mem/intune/enrollment/apple-mdm-push-certificate-get

RodrigoT 5 months, 1 week ago
Correct. It's the "first" thing to do.
upvoted 1 times

Question #57 *Topic 4*

HOTSPOT -
You have 1,000 computers that run Windows 10 and are members of an Active Directory domain.
You need to capture the event logs from the computers to Azure.
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

Azure service to provision:

- An Azure Storage account
- Azure Cosmos DB
- Azure SQL Database
- Log Analytics

Action to perform on the computers:

- Create a collector-initiated subscription
- Install the Microsoft Monitoring Agent
- Enroll in Microsoft Intune
- Register to Azure Active Directory (Azure AD)

Correct Answer:

Answer Area

Azure service to provision:

- An Azure Storage account
- Azure Cosmos DB
- Azure SQL Database
- **Log Analytics**

Action to perform on the computers:

- Create a collector-initiated subscription
- **Install the Microsoft Monitoring Agent**
- Enroll in Microsoft Intune
- Register to Azure Active Directory (Azure AD)

Box 1: Log Analytics -
Box 2: Install the Microsoft Monitoring Agent
Azure Monitor agent currently supports the following core functionality:
* Collect guest logs and metrics from any machine in Azure, in other clouds, or on-premises. Azure Arc-enabled servers are required for machines outside of
Azure.
* Centrally manage data collection configuration using data collection rules, and management configuration using Azure Resource Manager (ARM) templates or policies.
* Use Windows event filtering or multi-homing for Windows or Linux logs.
* Improved extension management.
Reference:
https://docs.microsoft.com/en-us/azure/azure-monitor/platform/agent-windows https://docs.microsoft.com/en-us/azure/azure-monitor/agents/azure-monitor-agent-migration

otondoj Highly Voted 1 year, 2 months ago
the given answer is correct
upvoted 8 times

RodrigoT 5 months, 1 week ago
I agree.
upvoted 3 times

moobdoob Most Recent 8 months, 2 weeks ago
Good answer.
upvoted 3 times

HOTSPOT -

You have a Microsoft 365 E5 subscription that contains 100 Windows 10 devices enrolled in Microsoft Intune.

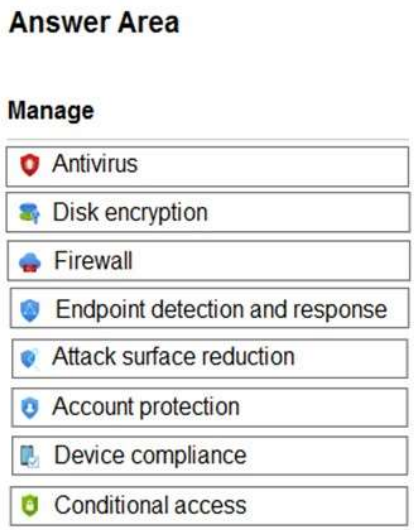
You need to create Endpoint security policies to meet the following requirements:

- Hide the Firewall & network protection area in the Windows Security app.
- Disable the provisioning of Windows Hello for Business on the devices.

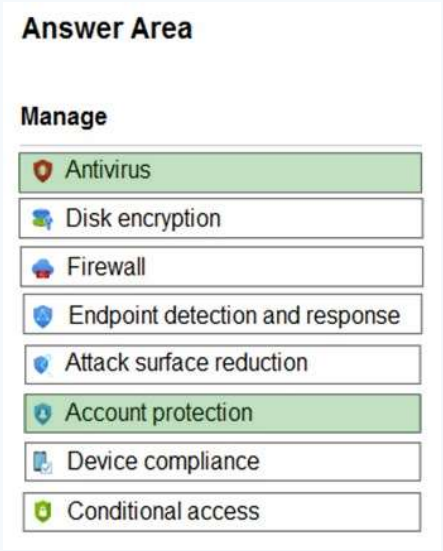
Which two policy types should you use? To answer, select the policies in the answer area.

NOTE: Each correct selection is worth one point.

Hot Area:



Correct Answer:



In the Antivirus policy settings, you can hide the Firewall and network protection area in the Windows Security app.

Windows Hello for Business settings are configured in Identity protection.

Reference:

https://docs.microsoft.com/en-us/mem/intune/protect/antivirus-security-experience-windows-settings https://docs.microsoft.com/en-us/mem/intune/protect/identity-protection-windows-settings

RodrigoT 5 months, 1 week ago

Correct answers and good links too. Good job. TESTED in my tenant. And the paths are:
Endpoint > Endpoint security | Antivirus + Create Policy > Windows 10, 11 and Server > Windows Security Experience > Create > Disable Network UI > Enable

Endpoint > Endpoint security | Account protection + Create Policy > Windows 10 and later > Account protection (preview) > Create > Block Windows Hello for Business > Enabled

upvoted 1 times

DRAG DROP -

You have 500 Windows 10 devices enrolled in Microsoft Intune.

You plan to use Exploit protection in Microsoft Endpoint Manager to enable the following system settings on the devices:

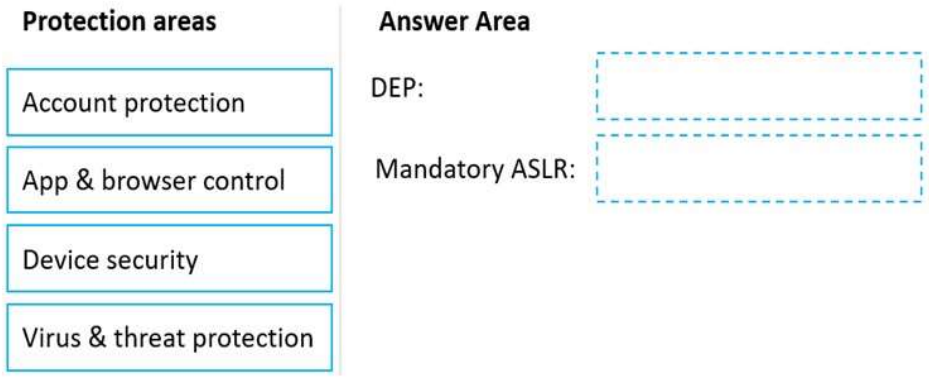
- Data Execution Prevention (DEP)
- Force randomization for images (Mandatory ASLR)

You need to configure a Windows 10 device that will be used to create a template file.

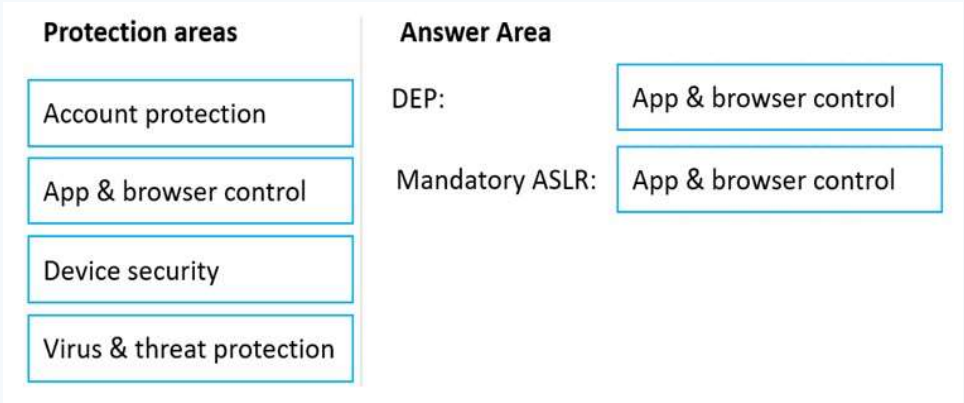
Which protection areas on the device should you configure in the Windows Security app before you create the template file? To answer, drag the appropriate protection areas to the correct settings. Each protection area may be used once, more than once, or not at all. You may need to drag the split bar between panes or scroll to view content.

NOTE: Each correct selection is worth one point.

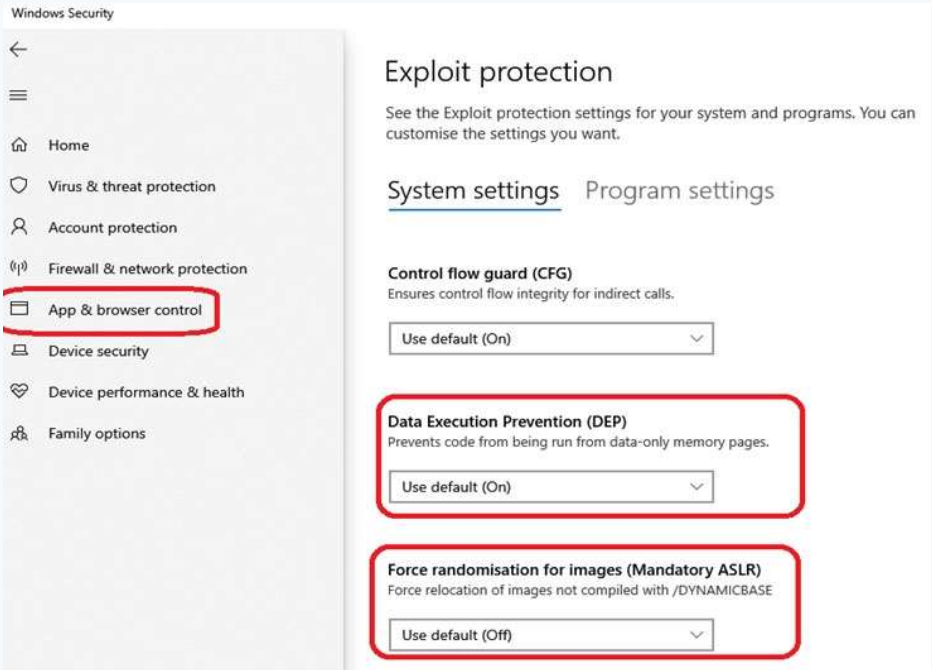
Select and Place:



Correct Answer:



Box 1: App & browser control -



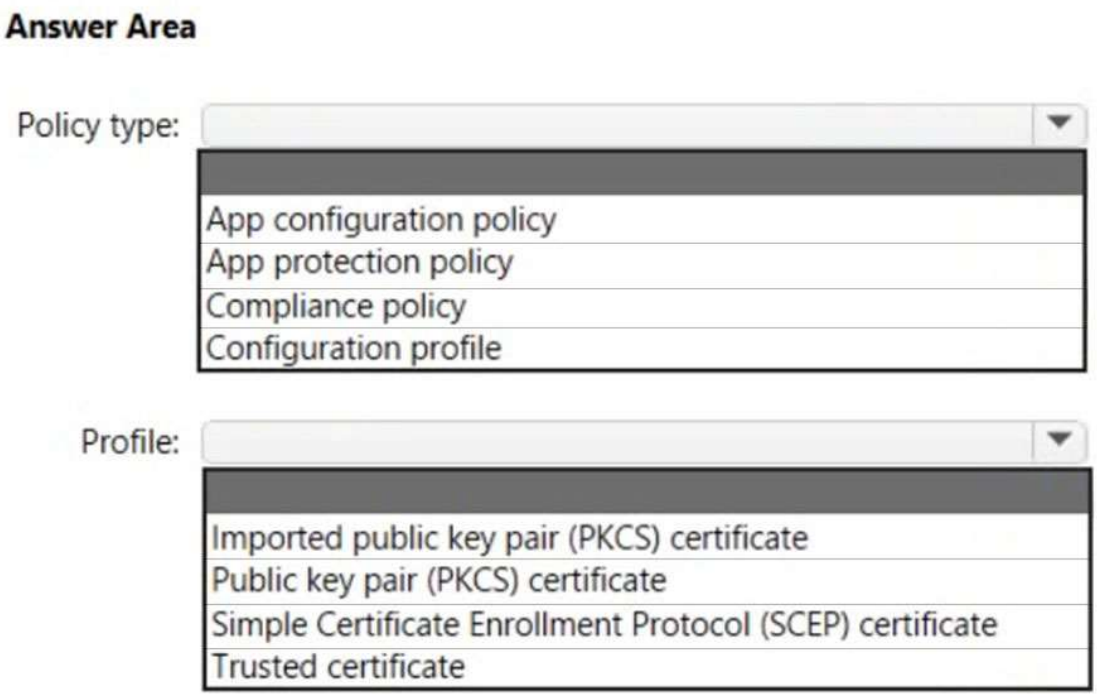
Note: Data Execution Prevention (DEP): This mitigation prevents code from being run from data-only memory pages.

Box 2: App & browser control -

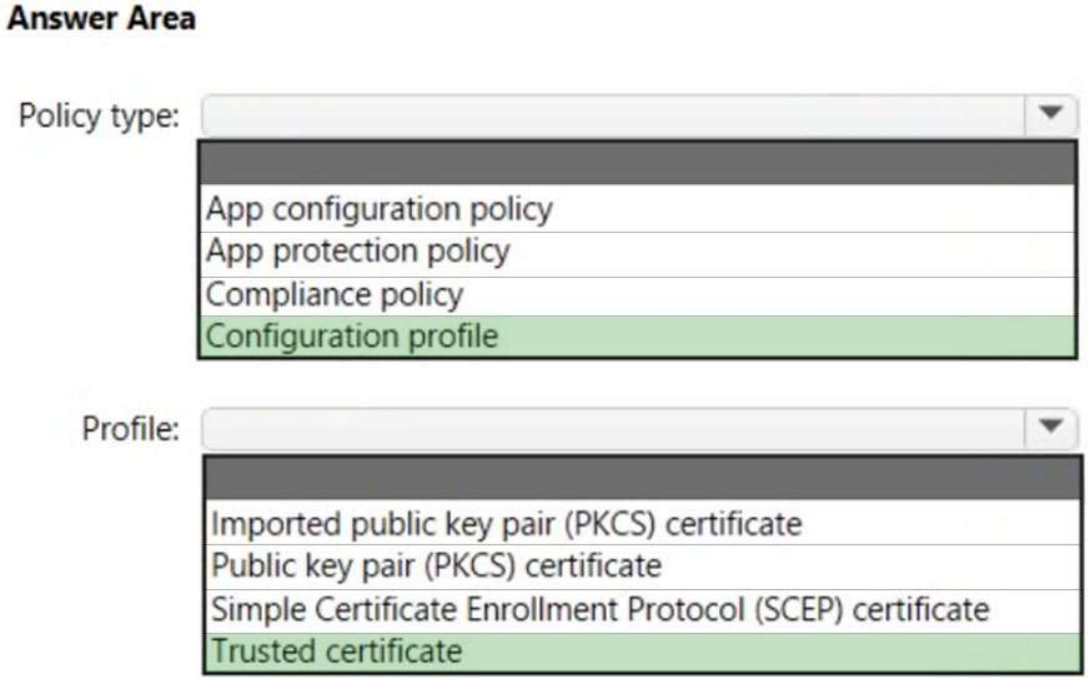
Force randomization for images (Mandatory ASLR). This mitigation forcibly relocates images not compiled with /DYNAMICBASE.
Reference:
https://support.microsoft.com/en-us/windows/app-browser-control-in-windows-security-8f68fb65-ebb4-3cfb-4bd7-ef0f376f3dc3

Question #60 *Topic 4*

HOTSPOT -
You have a Microsoft 365 tenant and an internal certification authority (CA).
You need to use Microsoft Intune to deploy the root CA certificate to managed devices.
Which type of Intune policy and profile should you use? To answer, select the appropriate options in the answer area.
NOTE: Each correct selection is worth one point.
Hot Area:



Correct Answer:



Box 1: Configuration profile -
Create a trusted certificate profile.

Box 2: Trusted certificate -
When using Intune to provision devices with certificates to access your corporate resources and network, use a trusted certificate profile to deploy the trusted root certificate to those devices. Trusted root certificates establish a trust from the device to your root or intermediate

(issuing) CA from which the other certificates are issued.
Reference:
https://docs.microsoft.com/en-us/mem/intune/protect/certificates-trusted-root

Question #61 *Topic 4*

You use Microsoft Intune and Intune Data Warehouse.
You need to create a device inventory report that includes the data stored in the data warehouse.
What should you use to create the report?

A. the Azure portal app

B. Endpoint analytics

C. the Company Portal app

D. Microsoft Power BI

Correct Answer: *D*
You can use the Power BI Compliance app to load interactive, dynamically generated reports for your Intune tenant. Additionally, you can load your tenant data in
Power BI using the OData link. Intune provides connection settings to your tenant so that you can view the following sample reports and charts related to:

Devices -

Enrollment -

App protection policy -

Compliance policy -

Device configuration profiles -

Software updates -

Device inventory logs -
Note: Load the data in Power BI using the OData link
With a client authenticated to Azure AD, the OData URL connects to the RESTful endpoint in the Data Warehouse API that exposes the data model to your reporting client. Follow these instructions to use Power BI Desktop to connect and create your own reports.
1. Sign in to the Microsoft Endpoint Manager admin center.
2. Select Reports > Intune Data warehouse > Data warehouse.
3. Retrieve the custom feed URL from the reporting blade, for example:
4. https://fef.{yourtenant}.manage.microsoft.com/ReportingService/DataWarehouseFEService/dates?api-version=v1.0
5. Open Power BI Desktop.
6. Choose File > Get Data. Select OData feed.
7. Choose Basic.
8. Type or paste the OData URL into the URL box.
9. Select OK.
10.If you have not authenticated to Azure AD for your tenant from the Power BI desktop client, type your credentials. To gain access to your data, you must authorize with Azure Active Directory (Azure AD) using OAuth 2.0.
11.Select Organizational account.
12.Type your username and password.
13.Select Sign In.
14.Select Connect.
15.Select Load.
Reference:
https://docs.microsoft.com/en-us/mem/intune/developer/reports-proc-get-a-link-powerbi

Question #62 *Topic 4*

Your company has devices enrolled in Microsoft Intune as shown in the following table.

Name	Platform
Device1	Windows 10
Device2	Android device administrator
Device3	iOS

In Microsoft Endpoint Manager, you define the company's network as a location named Location1.
Which devices can use network location-based compliance policies?

A. Device2 and Device3 only

B. Device2 only

C. Device1 and Device2 only

D. Device1 only

E. Device1, Device2, and Device3

Correct Answer: *E*
Intune supported operating systems
Intune supports devices running the following operating systems (OS): iOS

Android -

Windows -
macOS
Note: View the device compliance settings for the different device platforms:

Android device administrator -

Android Enterprise -
iOS
macOS
Windows Holographic for Business

Windows 8.1 and later -

Windows 10/11 -
Reference:
https://docs.microsoft.com/en-us/mem/intune/fundamentals/supported-devices-browsers https://docs.microsoft.com/en-us/mem/intune/protect/device-compliance-get-started

Question #63 *Topic 4*

HOTSPOT -

You have an Azure Active Directory Premium Plan 2 subscription that contains the users shown in the following table.

Name	Member of	Assigned license
User1	Group1	Enterprise Mobility + Security E5
User2	Group2	Enterprise Mobility + Security E5

You purchase the devices shown in the following table.

Name	Type
Device1	Windows 10
Device2	Android

You configure automatic mobile device management (MDM) and mobile application management (MAM) enrollment by using the following settings:

- MDM user scope: Group1
- MAM user scope: 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 enroll Device1 in Intune by using automatic enrollment.	○	○
User1 can enroll Device2 in Intune by using automatic enrollment.	○	○
User2 can enroll Device1 in Intune by using automatic enrollment.	○	○

Correct 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 Device1 in Intune by using automatic enrollment.	○	●

Reference:

https://docs.microsoft.com/en-us/mem/intune/enrollment/android-enroll https://powerautomate.microsoft.com/fr-fr/blog/mam-flow-mobile/

raduM 3 days, 11 hours ago

why can't user enroll device 2?

upvoted 1 times

HOTSPOT -

You have the on-premises servers shown in the following table.

Name	Description
DC1	Domain controller that runs Windows Server 2022
Server1	Standalone server that runs Windows Server 2022
Server2	Member server that runs Windows Server 2022 and has the Remote Access role installed
Server3	Member server that runs Windows Server 2019
Server4	Red Hat Enterprise Linux (RHEL) 8.4 server

You have a Microsoft 365 E5 subscription that contains Android and iOS devices. All the devices are managed by using Microsoft Intune.

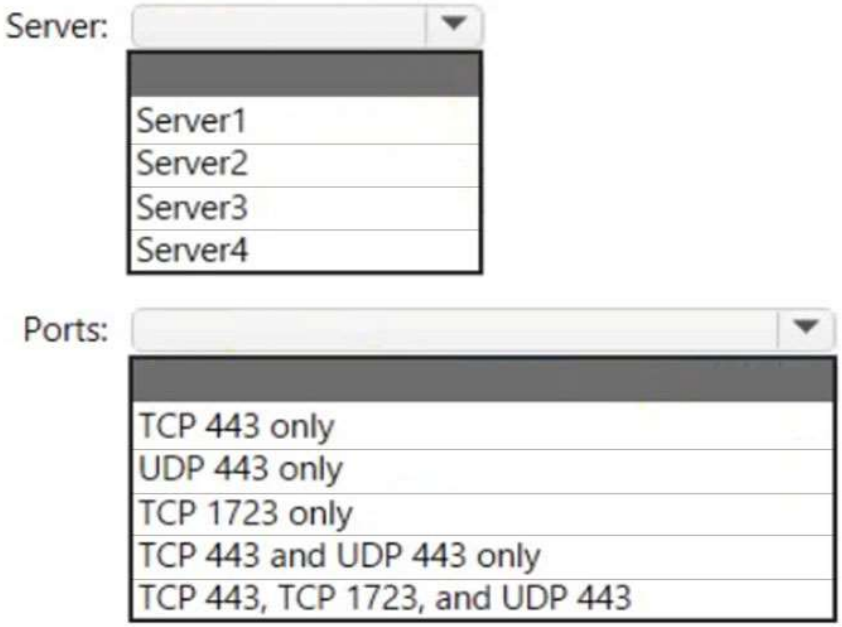
You need to implement Microsoft Tunnel for Intune. The solution must minimize the number of open firewall ports.

To which server can you deploy a Tunnel Gateway server, and which inbound ports should be allowed on the server to support Microsoft Tunnel connections? To answer, select the appropriate options in the answer area.

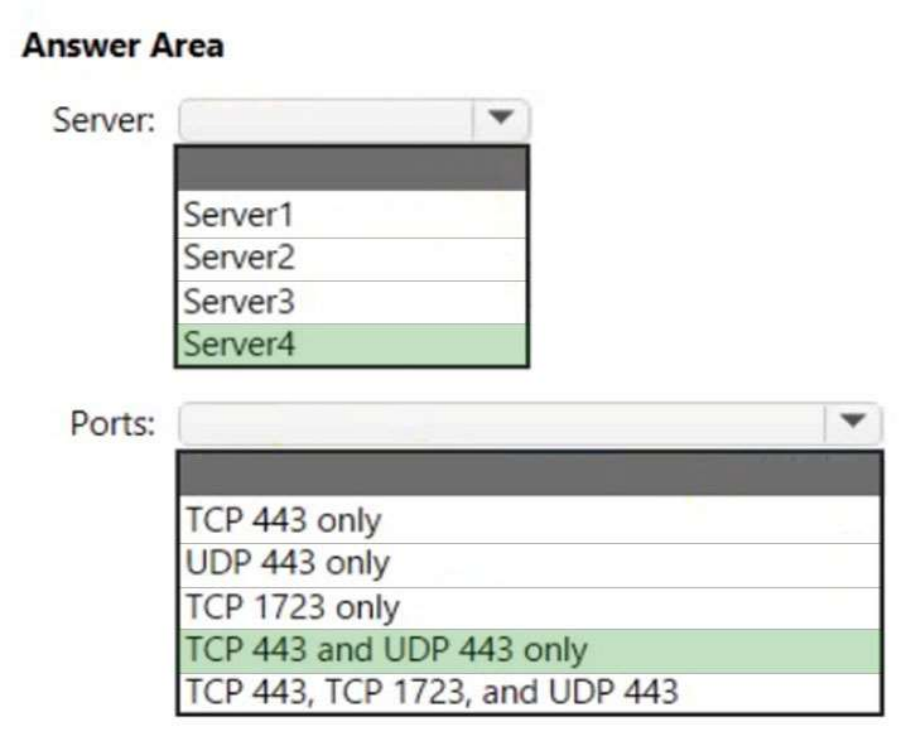
NOTE: Each correct selection is worth one point.

Hot Area:

Answer Area



Correct Answer:



Box 1: Server4 -
Microsoft Tunnel is a VPN gateway solution for Microsoft Intune that runs in a container on Linux and allows access to on-premises resources from iOS/iPadOS and Android Enterprise devices using modern authentication and Conditional Access.

Box 2: TCP 443 and UDP 443 only -
Some traffic goes to your public facing IP address for the Tunnel. The VPN channel will use TCP, TLS, UDP, and DTLS over port 443.
By default, port 443 is used for both TCP and UDP, but this can be customized via the Intune Server Configuration â€" Server port setting. If changing the default port (443) ensure your inbound firewall rules are adjusted to the custom port.

Question #65 *Topic 4*

You have a Microsoft 365 E5 subscription that contains 500 macOS devices enrolled in Microsoft Intune.
You need to ensure that you can apply Microsoft Defender for Endpoint antivirus policies to the macOS devices. The solution must minimize administrative effort.
What should you do?

A. From the Microsoft Endpoint Manager admin center, create a configuration profile.

B. From the Microsoft Endpoint Manager admin center, create a security baseline.

C. Onboard the macOS devices to the Microsoft 365 compliance center.

D. Install Defender for Endpoint on the macOS devices.

Correct Answer: *D*
Just install, and use Defender for Endpoint on Mac.
Reference:
https://docs.microsoft.com/en-us/microsoft-365/security/defender-endpoint/microsoft-defender-endpoint-mac

bensrayan 2 weeks ago
The given answer is correct :
https://learn.microsoft.com/en-us/mem/intune/protect/microsoft-tunnel-prerequisites
upvoted 1 times

bensrayan 2 weeks ago
Sorry this answer is for question 64..but i cant' delete it
upvoted 1 times

HOTSPOT -

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

Name	Platform
Device1	Windows 10
Device2	iOS

You plan to enroll the devices in Microsoft Intune.

How often will the compliance policy check-ins run after each device is enrolled in Intune? To answer, select the appropriate options in the answer area.

NOTE: Each correct selection is worth one point.

Hot Area:

Answer Area

Device1:

- Every 15 minutes for one hour, and then every eight hours
- Every five minutes for 15 minutes, then every 15 minutes for two hours, and then every eight hours
- Every three minutes for 15 minutes, then every 15 minutes for two hours, and then every eight hours

Device2:

- Every 15 minutes for one hour, and then every eight hours
- Every five minutes for 15 minutes, then every 15 minutes for two hours, and then every eight hours
- Every three minutes for 15 minutes, then every 15 minutes for two hours, and then every eight hours

Correct Answer:

Answer Area

Device1:

- Every 15 minutes for one hour, and then every eight hours
- Every five minutes for 15 minutes, then every 15 minutes for two hours, and then every eight hours
- **Every three minutes for 15 minutes, then every 15 minutes for two hours, and then every eight hours**

Device2:

- **Every 15 minutes for one hour, and then every eight hours**
- Every five minutes for 15 minutes, then every 15 minutes for two hours, and then every eight hours
- Every three minutes for 15 minutes, then every 15 minutes for two hours, and then every eight hours

Box 1: Every three minutes for 15 minutes, then every 15 minutes for two hours, and then around every eight hours

If devices recently enroll, then the compliance, non-compliance, and configuration check-in runs more frequently. The check-ins are estimated at:

Windows 10: Every 3 minutes for 15 minutes, then every 15 minutes for 2 hours, and then around every 8 hours

Platform	Frequency
iOS/iPadOS	Every 15 minutes for 1 hour, and then around every 8 hours
macOS	Every 15 minutes for 1 hour, and then around every 8 hours
Android	Every 3 minutes for 15 minutes, then every 15 minutes for 2 hours, and then around every 8 hours
Windows 10/11 PCs enrolled as devices	Every 3 minutes for 15 minutes, then every 15 minutes for 2 hours, and then around every 8 hours
Windows 8.1	Every 5 minutes for 15 minutes, then every 15 minutes for 2 hours, and then around every 8 hours

Box 2: Every 15 minutes for one hour, and then every eight hours iOS/iPadOS: Every 15 minutes for 1 hour, and then around every 8 hours
Reference:
https://docs.microsoft.com/en-us/mem/intune/configuration/device-profile-troubleshoot

bensrayan 2 weeks ago
correct
upvoted 1 times

HOTSPOT -

You have a Microsoft 365 E5 subscription that uses Microsoft Intune.

You need to ensure that users can only enroll devices that meet the following requirements:

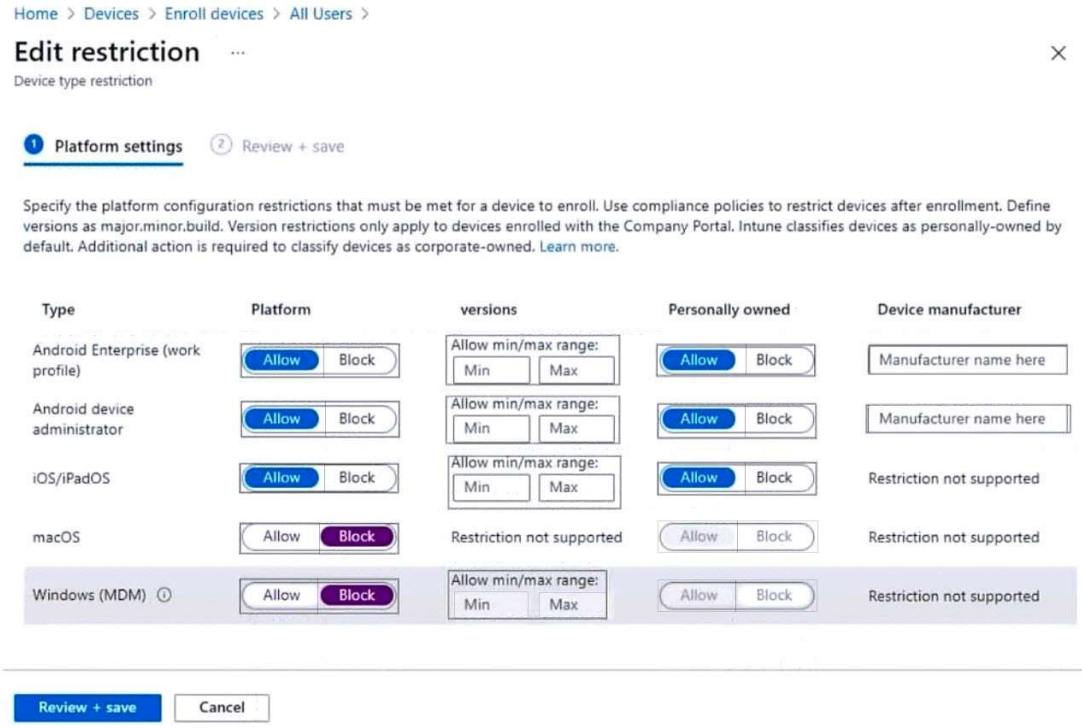
- Android devices that support the use of work profiles.
- iOS devices that run iOS 11.0 or later.

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

NOTE: Each correct selection is worth one point.

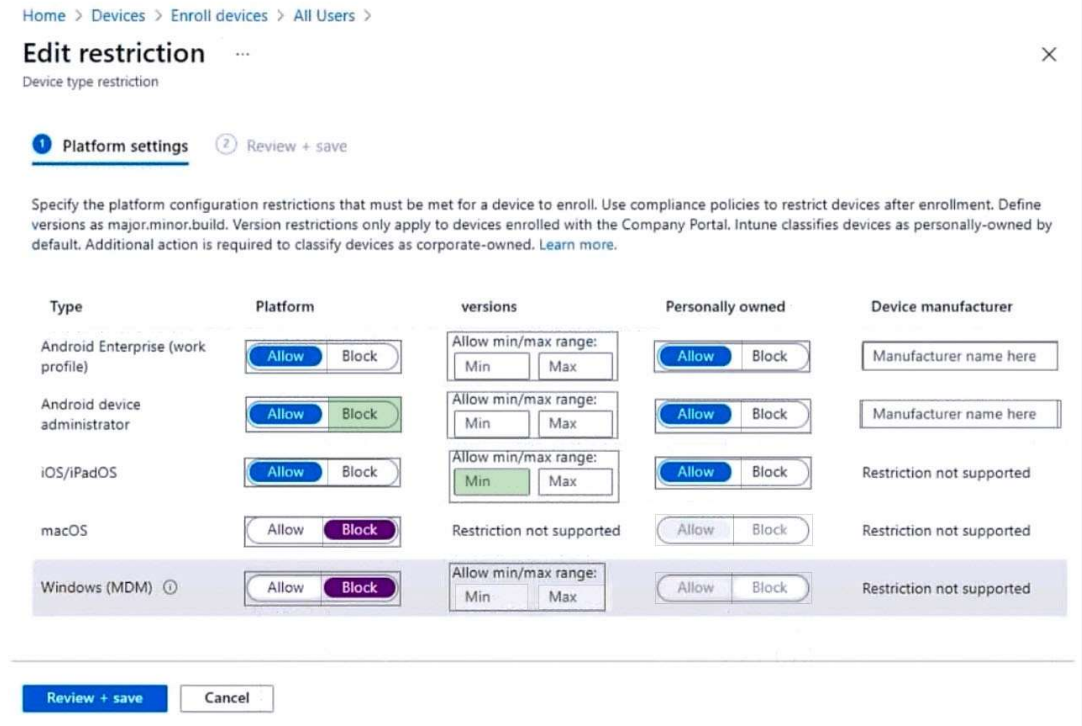
Hot Area:

Answer Area



Correct Answer:

Answer Area



Box 1: Android device administrator, Platform: Block

Restrict devices running on the following platforms:

Android device administrator -

Android Enterprise work profile -
iOS/iPadOS
macOS

Windows -
Note: If you allow both Android platforms for the same group, devices that support work profile will enroll with a work profile. Devices that don't support it will enroll on the Android device administrator platform. Neither work profile nor device administrator enrollment will work until you complete all prerequisites for Android enrollment.
Box 2: iOS/PadOS, Allow min/max Range: Min
Reference:
https://docs.microsoft.com/en-us/mem/intune/enrollment/enrollment-restrictions-set

Question #68 *Topic 4*

You have an Azure Active Directory (Azure AD) tenant named contoso.com.
You have a workgroup computer named Computer1 that runs Windows 10.
You need to add Computer1 to contoso.com.
What should you use?

A. the Settings app

B. Computer Management

C. netdom.exe

D. dsregcmd.exe

Correct Answer: *D*
If you want to manually join the computer to Azure AD, you can execute the dsregcmd /join command. This command should be run in SYSTEM context (using psexec for example) and will force an attempt to Azure AD.
Reference:
https://365bythijs.be/2019/11/02/troubleshooting-hybrid-azure-ad-join/

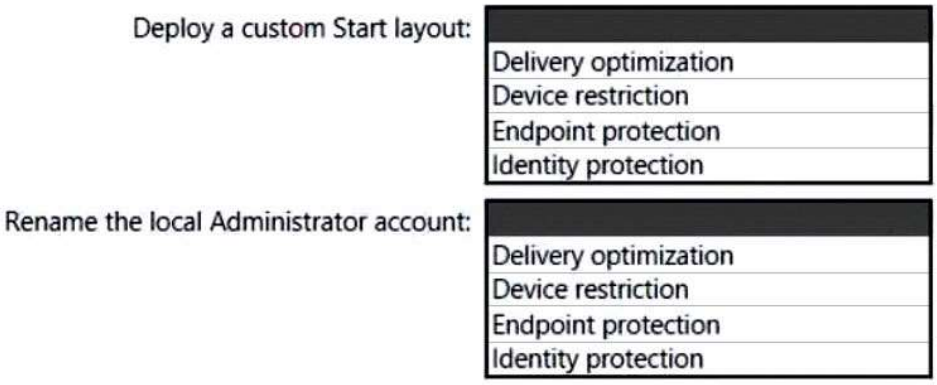
ManFlo1603 3 days, 11 hours ago
AAD and working group is not it Hybrid?
upvoted 1 times

raduM 5 days, 11 hours ago
i wopuld go with a as well
upvoted 1 times

Mnguyen0503 3 weeks, 5 days ago
Selected Answer: A
This question should be A using Settings -> Work or School account. All I can find for dsregcmd usage is normally in a hybrid environment, this PC is in workgroup. Correct me if I'm wrong.
upvoted 1 times

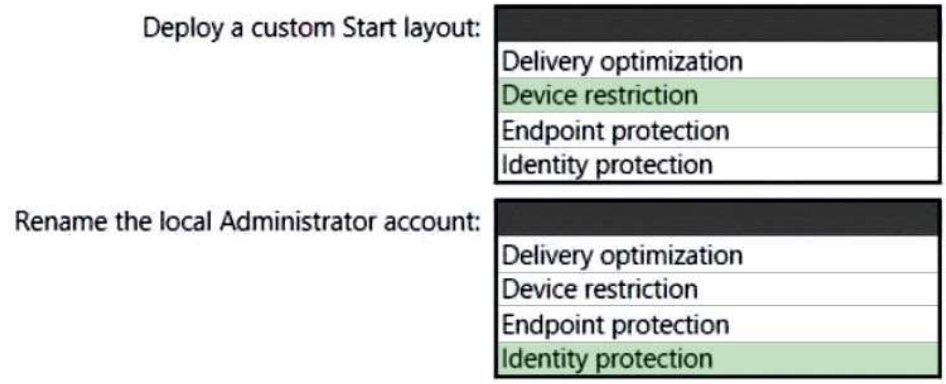
HOTSPOT -
You have a Microsoft 365 subscription that uses Microsoft Intune and contains 100 Windows 10 devices.
You need to create Intune configuration profiles to perform the following actions on the devices:
⇨ Deploy a custom Start layout.
⇨ Rename the local Administrator account.
Which profile template should you use for each action? To answer, select the appropriate options in the answer area.
NOTE: Each correct selection is worth one point.
Hot Area:

Answer Area



Correct Answer:

Answer Area



Box 1: Device restriction -
Customize Start Menu Custom & Taskbar
Here is a quick step-by-step guide to help you to deploy the prepared XML file. This Intune policy helps to customize the start menu and taskbar for Windows 10 devices.
Logon to Microsoft Endpoint Manager Portal.
Navigate to Devices -> Windows -> Configuration Profiles.
Select Platform -> Windows 10 and later.
Select Profile Type -> Template.
Search with ג€deviceג€ and select Device Restrictions.
Click on Create button.

Box 2: Identity protection -
Use an Identity protection profile to manage Windows Hello for Business on groups of devices in Microsoft Intune. Windows Hello for Business is a method for signing in to Windows devices by replacing passwords, smart cards, and virtual smart cards. Intune includes built-in settings so Administrators can configure and use Windows Hello for Business.
Incorrect:

* Delivery Optimization settings for your Windows devices to reduce bandwidth consumption when those devices download applications and updates. Configure
Delivery Optimization as part of your device configuration profiles.
* With Intune, you can use device configuration profiles to manage common Endpoint protection security features on devices, including:

Firewall -

BitLocker -

Allowing and blocking apps -
Microsoft Defender and encryption
For example, you can create an Endpoint protection profile that only allows macOS users to install apps from the Mac App Store. Or, enable Windows
SmartScreen when running apps on Windows 10/11 devices.
Reference:
https://www.anoopcnair.com/start-menu-taskbar-custom-layout-intune-cloudpc/ https://docs.microsoft.com/en-us/mem/intune/protect/identity-protection-configure

Mnguyen0503 3 weeks, 5 days ago
Answer to Q2 is Endpoint protection, under local device security
upvoted 2 times

bensrayan 2 weeks ago
agree : Q2 is Endpoint protection
upvoted 1 times

Question #70 *Topic 4*

HOTSPOT -

You have an Azure Active Directory (Azure AD) tenant named contoso.com that contains a user named User1. User1 has a user principal name (UPN) of user1

@contoso.com.

You join a Windows 10 device named Client1 to contoso.com.

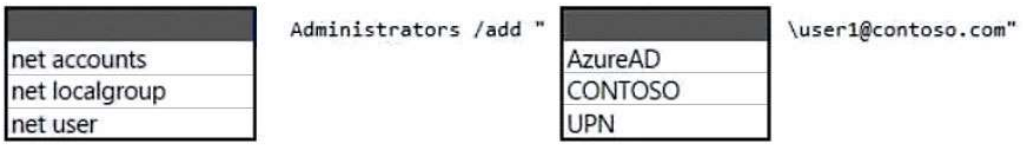
You need to add User1 to the local Administrators group of Client1.

How should you complete the command? To answer, select the appropriate options in the answer area.

NOTE: Each correct selection is worth one point.

Hot Area:

Answer Area



Correct Answer:

Answer Area

Box 1: net localgroup -

Add user to group from command line (CMD)

Windows provides command line utilities to manager user groups. In this post, learn how to use the command net localgroup to add user to a group from command prompt'

For example to add a user 'John' to administrators group, we can run the below command. net localgroup administrators John /add

Box 2: Contoso -

The domain of the user is Contoso.

Reference:

https://www.windows-commandline.com/add-user-to-group-from-command-line/

raduM 3 days, 11 hours ago

AzureAD shopuld be corect here

upvoted 1 times

bensrayan 2 weeks ago

- If your tenant users are synchronized from on-premises Active Directory, use net localgroup administrators /add "Contoso\username".
-- If your tenant users are created in Azure AD, use net localgroup administrators /add "AzureAD\UserUpn"
In our case , should be : net localgroup administrators /add "AzureAD\UserUpn"

upvoted 1 times

Mnguyen0503 3 weeks, 1 day ago

Box 2 answer should be AzureAD. It is well documented. CONTOSO would only be valid if this in on-premise AD.
https://docs.microsoft.com/en-us/azure/active-directory/devices/assign-local-admin

upvoted 2 times

TonySuccess 2 weeks, 2 days ago

This was also my thought process too.

upvoted 1 times

Question #71 *Topic 4*

You have a Microsoft 365 E5 subscription that contains 10 Android Enterprise devices. Each device has a corporate-owned work profile and is enrolled in
Microsoft Intune.
You need to configure the devices to run a single app in kiosk mode.
Which Configuration settings should you modify in the device restrictions profile?

A. General

B. Users and Accounts

C. System security

D. Device experience

Correct Answer: *D*
Device experience -
Use these settings to configure a kiosk-style experience on your dedicated devices, or to customize the home screen experiences on your fully managed devices.
You can configure devices to run one app, or run many apps. When a device is set with kiosk mode, only the apps you add are available.
Device experience, Enrollment profile type: Select an enrollment profile type to start configuring Microsoft Launcher or the Microsoft Managed Home Screen on your devices. Your options:
* Dedicated device, Kiosk mode, Single App
* etc.
Reference:
https://docs.microsoft.com/en-us/mem/intune/configuration/device-restrictions-android-for-work

bensrayan 2 weeks ago
correct : "Configure a kiosk-style experience on your dedicated devices. Prior to configuring these settings, go to Client apps and deploy any apps you want to the devices. "
upvoted 1 times

HOTSPOT -

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

Name	Role
Admin1@contoso.com	Security administrator
Admin2@contoso.com	Cloud device administrator
User1@contoso.com	*None*

You have a computer named Computer1 that runs Windows 10. Computer1 is in a workgroup and has the local users shown in the following table.

Name	Member of
Administrator1	Network Configuration Operators
Administrator2	Power Users
UserA	Administrators

UserA joins Computer1 to Azure AD by using 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.

Hot Area:

Answer Area

Statements	Yes	No
User1@contoso.com is a member of the local Administrators group on Computer1.	○	○
Admin1@contoso.com can configure the firewall and Microsoft Defender on Computer1.	○	○
Admin2@contoso.com can install software on Computer1.	○	○

Correct Answer:

Answer Area

Statements	Yes	No
User1@contoso.com is a member of the local Administrators group on Computer1.	○	●
Admin1@contoso.com can configure the firewall and Microsoft Defender on Computer1.	●	○
Admin2@contoso.com can install software on Computer1.	○	●

Box 1: No -

Users may join devices to Azure AD: This setting enables you to select the users who can register their devices as Azure AD joined devices. The default is All.

Box 2: Yes -

Admin1@contoso.com is a Azure AD security administrator

Security Administrator -

Users with this role have permissions to manage security-related features in the Microsoft 365 Defender portal, Azure Active Directory Identity Protection, Azure

Active Directory Authentication, Azure Information Protection, and Office 365 Security & Compliance Center.

This includes:

* Microsoft Defender for Endpoint

Assign roles -

Manage machine groups -

Configure endpoint threat detection and automated remediation
View, investigate, and respond to alerts

View machines/device inventory -

Box 3: No -
Admin2@contoso.com is a Azure AD Cloud device administrator.

Cloud Device Administrator -
Users in this role can enable, disable, and delete devices in Azure AD and read Windows 10 BitLocker keys (if present) in the Azure portal. The role does not grant permissions to manage any other properties on the device.
Reference:
https://docs.microsoft.com/en-us/azure/active-directory/devices/device-management-azure-portal#configure-device-settings
https://docs.microsoft.com/en-us/azure/active-directory/roles/permissions-reference#security-administrator

ManFlo1603 3 days, 11 hours ago
can you say why it would be YNN?
upvoted 1 times

bensrayan 2 weeks ago
Correct answer is : YNN
upvoted 1 times

TonySuccess 1 week, 3 days ago
Why then?
upvoted 1 times

Topic 5 - Question Set 5

Question #1 *Topic 5*

You have Windows 10 devices that are managed by using Microsoft Intune. Intune and the Microsoft Store for Business are integrated.
You need to deploy the Remote Desktop modern app as an automatic install to the Windows 10 devices without user interaction.
Which three actions should you perform? Each correct answer presents part of the solution.
NOTE: Each correct selection is worth one point.

A. Create an Azure Active Directory group that contains all users.

B. From the Endpoint Manager admin center, create a Microsoft Store app for the Remote Desktop modern app.

C. From the Endpoint Manager admin center, assign the app to the Azure Active Directory group.

D. Create an Azure Active Directory group that contains the Windows 10 devices.

E. From the Microsoft Store for Business portal, assign a license for the app to all the users in the Azure Active Directory group.

F. For your organization, make the app available in the Microsoft Store for Business.

Correct Answer: *BCD*
Step 1: Create an Azure Active Directory group that contains the Windows 10 devices.
Step 2: From the Endpoint Manager admin center, create a Microsoft Store app for the Remote Desktop modern app.
Step 3: From the Endpoint Manager admin center, assign the app to the Azure Active Directory group.
Reference:
https://docs.microsoft.com/en-us/mem/intune/apps/store-apps-windows https://docs.microsoft.com/en-us/mem/intune/apps/apps-deploy
https://docs.microsoft.com/en-us/mem/intune/apps/windows-store-for-business https://docs.microsoft.com/en-us/mem/intune/apps/apps-add

zimdandy Highly Voted 1 year, 3 months ago
Correct
upvoted 9 times

Mujja 1 year, 3 months ago
I picked the same answers
upvoted 1 times

Dong1999 1 year, 2 months ago
Agree with this
upvoted 1 times

lijk_manson Highly Voted 11 months, 1 week ago
In order and why:

F: Make the app available in the Microsoft Store for Business
By default it is not there you need to add it for your org

D: Create an AAD groep with win10 devices (not assign it to all devices like android or win11 if the question is only for Win10)

C: Assign the app to the group, i think this tell you enough
upvoted 6 times

Malinaa 10 months, 1 week ago
In the quiestion was asked: "without user interaction."
So the answer BCD is correct.
upvoted 7 times

Solaris2002 Most Recent 7 months, 2 weeks ago
I'm not sure this is correct. I work in a production Intune environment and if it is a "modern" app available in the Business Store, there is no need to create the app in Endpoint Manager. You simply go to businessstore.microsoft.com, search for the app, add a license, then add it to your company store. Now go back to EndPoint Manager, and sync it. The app will appear in "Apps". You can then assign an Azure AD group for deployment
upvoted 2 times

RodrigoT 5 months, 1 week ago
But the answers provided are correct. I TESTED in my tenant. It works perfectly, although the steps are almost interlinked.
The path is:
Endpoint > Apps | All apps + Add > Microsoft store app > then the "strange" part: You have to open on another tab the https://www.microsoft.com/store/apps and search for the app. Copy the app URL then go back to Endpoint to paste it. Complete all the fields, assign to the Windows 10 devices, add a filter if you want (in my case I blocked personally-owned devices) etc. etc. It works.
upvoted 3 times

rennne 1 year, 1 month ago
Why should I make a group filed with all computers when there is an option to assign an app to All Devices?
upvoted 1 times

asdaa 11 months, 1 week ago
Because the requirement is not ALL DEVICES it is All Windows 10 Devices.
upvoted 5 times

Question #2 *Topic 5*

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

Name	Platform
Device1	Windows 8.1
Device2	Windows 10
Device3	Android
Device4	iOS

On which devices can you apply app configuration policies?

A. Device1, Device2, Device3, and Device4

B. Device2 only

C. Device3 and Device4 only

D. Device1 and Device2 only

E. Device2, Device3, and Device4 only

Correct Answer: *C*

You can create and use app configuration policies to provide configuration settings for both iOS/iPadOS or Android apps.

Reference:

https://docs.microsoft.com/en-us/mem/intune/apps/app-configuration-policies-overview

Kmaster1209 Highly Voted 1 year, 3 months ago

"You can create and use app configuration policies to provide configuration settings for both iOS/iPadOS or Android apps"

upvoted 10 times

KirilA Highly Voted 1 year, 4 months ago

Looks correct per reference link

upvoted 5 times

RodrigoT Most Recent 5 months, 1 week ago

Selected Answer: C

Tested in my tenant.

upvoted 2 times

RodrigoT 5 months ago

When you are creating an app "configuration" police (don't confuse it with "protection" police), if you chose Managed Devices, there are only 2 choices: Android od IOS.

upvoted 3 times

Perycles 1 year, 3 months ago

correct

upvoted 4 times

Question #3 *Topic 5*

You have a Microsoft Intune subscription.

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

Name	Operating system
Device1	Android 8.1.0
Device2	Android 9
Device3	iOS 11.4.1
Device4	iOS 12.3.1
Device5	iOS 12.3.2

An app named App1 is installed on each device.

What is the minimum number of app configuration policies required to manage App1?

A. 1

B. 2

C. 3

D. 4

E. 5

Correct Answer: *B*

One for Android, and one for iOS.

Reference:

https://docs.microsoft.com/en-us/mem/intune/apps/app-configuration-policies-overview

Dong1999 Highly Voted 1 year, 2 months ago

Correct
Device 1,2 = 1
Device 3,4,5 = 1
Total = 2

upvoted 10 times

RodrigoT 5 months, 1 week ago

Correct, one per platform.

upvoted 3 times

moobdoob Most Recent 8 months, 2 weeks ago

good ansa

upvoted 4 times

Mujja 1 year, 3 months ago

Correct

upvoted 2 times

Question #4 *Topic 5*

HOTSPOT -

Your network contains an Active Directory Domain Services (AD DS) domain named contoso.com. The domain contains Windows 10 devices that are managed by using Microsoft Endpoint Configuration Manager.

You plan to deploy Microsoft 365 Apps for enterprise to the devices by using Configuration Manager.

You create a Configuration.xml file as shown in the following exhibit.

```
<Configuration ID="67e*0d4f-814a-4466-9e3c-1388d66a527c">
  <Add OfficeClientEdition="64" Channel="Current" OfficeMgmtCOM="TRUE">>
    <Product ID="O365ProPlusRetail">
      <Language ID="MatchOS" />
      <ExcludeApp ID="Access" />
      <ExcludeApp ID="Groove" />
      <ExcludeApp ID="Lync" />
      <ExcludeApp ID="Publisher" />
    </Product>
  </Add>
  <Property Name="SharedComputerLicensing" Value="0"/>
  <Property Name="PinIconsToTaskbar" Value="TRUE"/>
  <Property Name="SCLCacheOverride" Value="0" />
  <Property Name="AUTOACTIVATE" Value="0" />
  <Property Name="FORCEAPPSHUTDOWN" Value="TRUE"/>
  <Property Name="DeviceBasedLicensing" Value="1" />
  <RemoveMSI />
  <AppSettings>
    <Setup Name="Company" Value="Contoso.com" />
  </AppSettings>
  <Display Level="None" AcceptEULA="TRUE" />
  <Logging Level="Standard" Path="\\Server1\Office" />
</Configuration>
```

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

Microsoft 365 Apps for enterprise will be installed from **[answer choice]**

- \\Server1\Office
- a Configuration Manager distribution point
- the Office 365 Content Delivery Network (CDN)

New Microsoft Office feature updates will be available to devices **[answer choice]**

- twice a year in January and July
- once a month, on the second Tuesday of the month
- as soon as the update is ready, but on no set schedule

Correct Answer:

Answer Area

Microsoft 365 Apps for enterprise will be installed from **[answer choice]**

- \\Server1\Office
- a Configuration Manager distribution point
- the Office 365 Content Delivery Network (CDN)

New Microsoft Office feature updates will be available to devices **[answer choice]**

- twice a year in January and July
- once a month, on the second Tuesday of the month
- as soon as the update is ready, but on no set schedule

Reference:

https://docs.microsoft.com/en-us/deployoffice/overview-update-channels

Alexbz Highly Voted 1 year, 4 months ago

O365 installed from: CDN (default is optional if the source path is not specified)
New updates will be available: as soon as the update is ready because Channel has been set to “Current”

upvoted 26 times

Jimbob77 1 year, 4 months ago

Thanks Alexbz. "Current Channel : Provide your users with new Office features as soon as they are ready, but on no set schedule."
https://docs.microsoft.com/en-us/deployoffice/overview-update-channels

upvoted 4 times

RodrigoT 5 months ago

To configure Office to receive updates from Configuration Manager use a text editor to modify the configuration file for the Office Deployment Tool. In the Add element, include the OfficeMgmtCOM attribute and set its value to True.
https://docs.microsoft.com/en-us/deployoffice/manage-microsoft-365-apps-updates-configuration-manager#method-3-use-the-office-deployment-tool-to-enable-updates-from-configuration-manager

upvoted 2 times

silver_bullet666 2 months, 2 weeks ago

But does 'updates' configured to come from Configuration Manager include initial installation will also come from Configuration manager? I don't think it does, I think the initial installation will come from CDN...

upvoted 1 times

silver_bullet666 2 months, 2 weeks ago

For Configuration Manager to be able to manage Microsoft 365 Apps updates, an Office COM object needs to be enabled on the computer where Office is installed.
Sounds to me like the initial installation is done via CDN still.
https://docs.microsoft.com/en-us/deployoffice/office-deployment-tool-configuration-options#officemgmtcom-attribute-part-of-add-element

upvoted 1 times

coppermine Highly Voted 9 months, 1 week ago

1. a Configuration Manager distribution point. OfficeMgmtCOM="TRUE" is in place
https://config.office.com and to see the difference btw CDN and Config Mgr

2. as soon as the update is ready, but on no set schedule. Channel="Current"
https://docs.microsoft.com/en-us/deployoffice/overview-update-channels#current-channel-overview

upvoted 7 times

PiPe 7 months, 3 weeks ago

Exactly...
Install From CDN:
<Add OfficeClientEdition="64" Channel="Current">
Install From Local Source:
<Add OfficeClientEdition="64" Channel="Current" SourcePath="\\server1\Office">
Install From MECM:
<Add OfficeClientEdition="64" Channel="Current" OfficeMgmtCOM="TRUE">

2nd answer is indeed 'as soon as the update is ready, but on no set schedule'

upvoted 3 times

Ka1Nn Most Recent 1 year, 1 month ago

By default O365 installed from: CDN (default is optional if the source path is not specified). BUT in this case we use Configuration Manager (SCCM) so you need to copy source on DP (distribution Point). like i said before
Installed from a CM DP : https://docs.microsoft.com/en-us/deployoffice/deploy-microsoft-365-apps-configuration-manager-2012r2
It's important that you don't include the SourcePath attribute in the Add section of your configuration.xml file. That's because Configuration Manager copies the installation files for an application into a folder under the Configuration Manager client cache folder

"Current Channel : Provide your users with new Office features as soon as they are ready, but on no set schedule."

You need to redeploy updates by updating DP on SCCM.

upvoted 5 times

Bradobrey 1 year, 1 month ago

From Link:https://docs.microsoft.com/en-us/deployoffice/deploy-microsoft-365-apps-configuration-manager-2012r2
First -To get started, download the Office Deployment Tool from the Microsoft Download Center to a shared folder on your organization's network. But then: After you create the Microsoft 365 Apps application and configure its deployment type, the next step is to copy all the files needed by the application to the appropriate distribution points in your Configuration Manager environment.

upvoted 2 times

Ka1Nn 1 year, 2 months ago

Installed from a CM DP : https://docs.microsoft.com/en-us/deployoffice/deploy-microsoft-365-apps-configuration-manager-2012r2
It's important that you don't include the SourcePath attribute in the Add section of your configuration.xml file. That's because Configuration Manager copies the installation files for an application into a folder under the Configuration Manager client cache folder

Current Chanel : https://docs.microsoft.com/en-us/deployoffice/overview-update-channels#current-channel-overview

Current Channel also receives other updates during the month, which include security and non-security updates. There is no set schedule for these updates, but in general there are two or three releases each month, including one on the second Tuesday of the month.

upvoted 2 times

Mujja 1 year, 3 months ago

OfficeMgmtCOM=True, means updates are managed by ConfigMgr. The Channel is Current, which means as soon as the updates are available\deployed they will be installed.

If ConfigMgr is used to service and install the app, then the source will be on a DP. The Path to the source doesn't need to be specified if the source in the the folder from where setup.exe is run.

upvoted 6 times

Jana08 1 year, 2 months ago

you are correct:

https://docs.microsoft.com/en-us/deployoffice/office-deployment-tool-configuration-options#:~:text=OfficeMgmtCOM%20attribute%20(part,for%20client%20devices.

upvoted 2 times

Malinaa 10 months, 1 week ago

For Configuration Manager to be able to manage Microsoft 365 Apps UPDATES , an Office COM object needs to be enabled on the computer where Office is installed. Not installation but UPDATES. In the question was asked about installation of the apps :) https://docs.microsoft.com/en-us/deployoffice/office-deployment-tool-configuration-options#:~:text=OfficeMgmtCOM%20attribute%20(part,for%20client%20devices.

upvoted 1 times

Perycles 1 year, 3 months ago

A : CDN because "UpdatePath" not define for a specific network Share

upvoted 1 times

Nome2025 1 year, 3 months ago

Why CDN and not \\server1\office as it shows in the script?

upvoted 1 times

Tanderson2491 1 month ago

Because in the script that is the logging location, not the location of the installation media.

upvoted 1 times

draadloos1973 1 year, 4 months ago

We recommend Current Channel, because it provides your users with the newest Office features as soon as they are ready. Current Channel usually receives new features at least once a month, but there is no set schedule for when those updates are released.

Current Channel also receives other updates during the month, which include security and non-security updates. There is no set schedule for these updates, but in general there are two or three releases each month, including one on the second Tuesday of the month.

upvoted 1 times

randy0077 1 year, 4 months ago

almost every suggested answer is incorrect..whats the point of having exam dump

upvoted 5 times

MyHawkeye 1 year, 4 months ago

It makes you think ... not very common these days, but nevertheless can be very helpful at certain times ... :-) (BTW: irony, no offense intended)

upvoted 3 times

Cowok 1 year, 4 months ago

1. A - because default is from CDN
2. C - because set as current. If set as monthly will be monthly or semi-annual will be 2 a year.

upvoted 3 times

HOTSPOT -

You have groups that use the Dynamic Device membership type as shown in the following table.

Name	Syntax
Group1	(device.deviceOwnership -eq "Company")
Group2	(device.deviceOwnership -eq "Personal")

You are deploying Microsoft 365 apps.

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

Name	Ownership	Platform
LT1	Company	Windows 10 Enterprise x64
LT2	Personal	Windows 10 Enterprise x64
LT3	Company	MacOS Big Sur

In the Microsoft Endpoint Manager admin center, you create a Microsoft 365 Apps app as shown in the exhibit. (Click the Exhibit tab.)

App Information Edit

Name	Microsoft 365 Apps for Windows 10
Description	Microsoft 365 Apps for Windows 10
Publisher	Microsoft
Category	Productivity
Show this as a featured app in the Company Portal	No
Information URL	https://products.office.com/en-us/explore-office-for-home
Privacy URL	https://privacy.microsoft.com/en-US/privacystatement
Developer	Microsoft
Owner	Microsoft
Notes	...
Logo	Office

Apps suite configuration Edit

Apps to be installed as part of the suite	Access Excel, OneNote, Outlook, PowerPoint, Publisher, Skype for Business, Teams, Word Teams, Word
Architecture	64-bit
Update channel	Current Channel
Remove other versions	Yes
Version to install	Latest
Use shared computer activation	No
Accept the Microsoft Software License Teams on behalf of users	No
Install background service for Microsoft Search in Bing	No
Apps to be installed as part of the suite	1 language(s) selected

Assignments Edit

Group mode	Group
Required	
Included	Group1

Available for enrolled devices

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
LT1 will have Microsoft 365 apps installed.	○	○
LT2 will have Microsoft 365 apps installed.	○	○
LT3 will have Microsoft 365 apps installed.	○	○

Correct Answer:

Answer Area

Statements	Yes	No
LT1 will have Microsoft 365 apps installed.	○	○
LT2 will have Microsoft 365 apps installed.	○	○
LT3 will have Microsoft 365 apps installed.	○	○

Box 1: Yes -

Policy applies to Group1.

Box 2: No -

Policy does not apply to Group2.

Box 3: No -

The policy will not apply for MacOs.

Reference:

https://docs.microsoft.com/en-us/mem/intune/apps/apps-add-office365 https://docs.microsoft.com/en-us/mem/intune/apps/apps-deploy https://docs.microsoft.com/en-us/mem/intune/apps/apps-add

RodrigoT 5 months, 1 week ago

Correct answers.
Y- Company and Windows
N- Personal and Windows
N- Company but MacOS

upvoted 3 times

HOTSPOT -

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

Name	Role
User1	Global admin
User2	Application admin
User3	None
User4	None

You provision the private store in Microsoft Store for Business and assign Microsoft Store for Business roles to the users as shown in the following table.

Name	Role
User2	Admin
User3	Purchaser
User4	Basic Purchaser

You configure the following Shopping behavior settings for the Microsoft Store for Business:

- Allow users to shop: Yes
- Make everyone a Basic Purchaser: Off
- Allow app requests: On

Shop offline apps: Off -

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 assign the Microsoft Store for Business Admin role to User4.	○	○
When User4 requests an app from the Microsoft Store for Business, User2 will be notified.	○	○
User3 can assign apps from the Microsoft Store for Business to User2.	○	○

Correct Answer:

Answer Area

Statements	Yes	No
User1 can assign the Microsoft Store for Business Admin role to User4.	○	○
When User4 requests an app from the Microsoft Store for Business, User2 will be notified.	○	○
User3 can assign apps from the Microsoft Store for Business to User2.	○	○

Reference:

https://docs.microsoft.com/en-us/microsoft-store/roles-and-permissions-microsoft-store-for-business https://docs.microsoft.com/en-us/microsoft-store/acquire-apps-microsoft-store-for-business

Question #7 *Topic 5*

You have a Microsoft 365 tenant that uses Microsoft Intune.
You use the Company Portal app to access and install published apps to enrolled devices.
From the Microsoft Endpoint Manager admin center, you add a Microsoft Store app.
Which two App information types are visible in the Company Portal?
NOTE: Each correct selection is worth one point.

A. Information URL

B. Owner

C. Privacy URL

D. Developer

Correct Answer: *CD*
In the Microsoft Store App information page available through Microsoft Endpoint Manager admin center, the app details include:
* Privacy URL: Optionally, enter the URL of a website that contains privacy information for this app. The URL is displayed to users in the company portal.
* Developer: Optionally, enter the name of the app developer.
Information URL or Owner are not included.
Reference:
https://docs.microsoft.com/en-us/mem/intune/apps/store-apps-windows

BieLey Highly Voted 11 months, 2 weeks ago
Given answer are wrong. The right answer are:
Information URL: The information URL will be visible to users in Company Portal.
Privacy URL: The privacy URL will be visible to users in Company Portal.

As for the wrong answers:
Developer: This information will be visible to people signed into the admin center.
Owner: This name will be visible to people signed in to the admin center.

Source: Intune, App blade
upvoted 20 times

R0b671 11 months ago
BieLey is correct. Information & Privacy URL will be displayed in company portal. Information can be found on endpoint manager when mousing over the ? next to Information URL/Privacy URL in adding application window.
upvoted 7 times

AVP_Riga Highly Voted 10 months, 2 weeks ago
Selected Answer: AC
The right answer are:
Information URL: The information URL will be visible to users in Company Portal.
Privacy URL: The privacy URL will be visible to users in Company Portal.
upvoted 6 times

ameli8222 Most Recent 8 months, 3 weeks ago
A and C 100%. Tested on my organization's Company portal
upvoted 6 times

RodrigoT 5 months, 1 week ago
Thank you for really testing.
upvoted 1 times

lucadp010 9 months, 2 weeks ago
Selected Answer: AC
Information URL
Privacy URL
upvoted 4 times

Question #8 *Topic 5*

You have a Microsoft 365 tenant that contains the objects shown in the following table.

Name	Type
Admin1	User
Group1	Microsoft 365 group
Group2	Distribution group
Group3	Mail-enabled security group
Group4	Security group

In the Microsoft Endpoint Manager admin center, you are creating a Microsoft 365 Apps app named App1.

To which objects can you assign App1?

A. Admin1, Group3, and Group4 only

B. Group1, Group2, Group3, and Group4 only

C. Admin1, Group1, Group2, Group3, and Group4

D. Group1, Group3, and Group4 only

E. Group3 and Group4 only

Correct Answer: *D*

Reference:

https://docs.microsoft.com/en-us/mem/intune/fundamentals/groups-add

learningmonkey Highly Voted 7 months, 2 weeks ago

Answer is correct. tested and got the same groups.

upvoted 6 times

FrancisLai Highly Voted 10 months, 1 week ago

The answer is correct. Took some time to do research and manage to find the Microsoft link that is more relevant and support to the answer. The given link doesn't really straight to the point.
https://docs.microsoft.com/en-us/mem/intune/fundamentals/groups-add

upvoted 5 times

RodrigoT 5 months, 1 week ago

The second link provided is excellent.

upvoted 1 times

moobdoob Most Recent 8 months, 2 weeks ago

good answer

upvoted 2 times

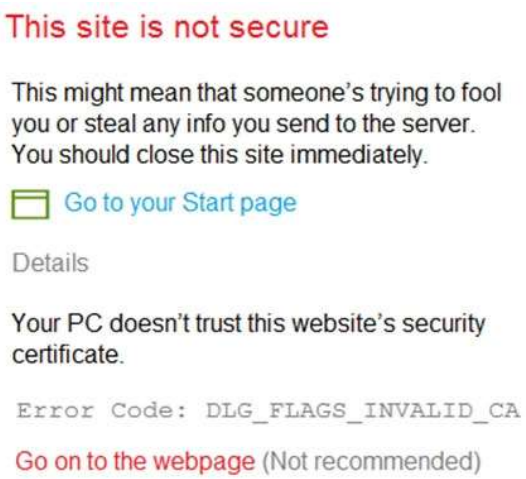
CARO54 9 months, 1 week ago

Just tested. Answer is correct

upvoted 3 times

Question #9 *Topic 5*

You use Windows Admin Center to remotely administer computers that run Windows 10.
When connecting to Windows Admin Center, you receive the message shown in the following exhibit.



You need to prevent the message from appearing when you connect to Windows Admin Center.
To which certificate store should you import the certificate?

A. Client Authentication Issuers

B. Trusted Root Certification Authorities

C. Personal

Correct Answer: *B*
The domain members should have trusted root certificate stored.
Reference:
https://social.technet.microsoft.com/Forums/en-US/6b3abb8e-007e-4047-bd30-2946b9c3aaba/windows-admin-center-three-questions-login-and-certs? forum=ws2016

examkiller321 Highly Voted 11 months, 3 weeks ago
Could it be B?
upvoted 9 times

tf444 11 months, 2 weeks ago
I agree, root certificate!
upvoted 10 times

RodrigoT 5 months, 1 week ago
The provided link doesn't help at all. I prefer this:
https://docs.microsoft.com/en-us/skype-sdk/sdn/articles/installing-the-trusted-root-certificate
upvoted 1 times

Tanderson2491 Most Recent 6 months, 1 week ago
Selected Answer: B
Root Certificate is the correct answer
upvoted 1 times

erwiense 8 months, 1 week ago
Selected Answer: B
B was the correct one
upvoted 3 times

IykeP 8 months, 2 weeks ago
Selected Answer: B
B is the Correct Answer.
upvoted 2 times

moobdoob 8 months, 2 weeks ago
Root certificate
upvoted 1 times

AVP_Riga 10 months, 2 weeks ago
B. At least I use Trusted roots for same cases.
upvoted 4 times

Question #10 *Topic 5*

DRAG DROP -

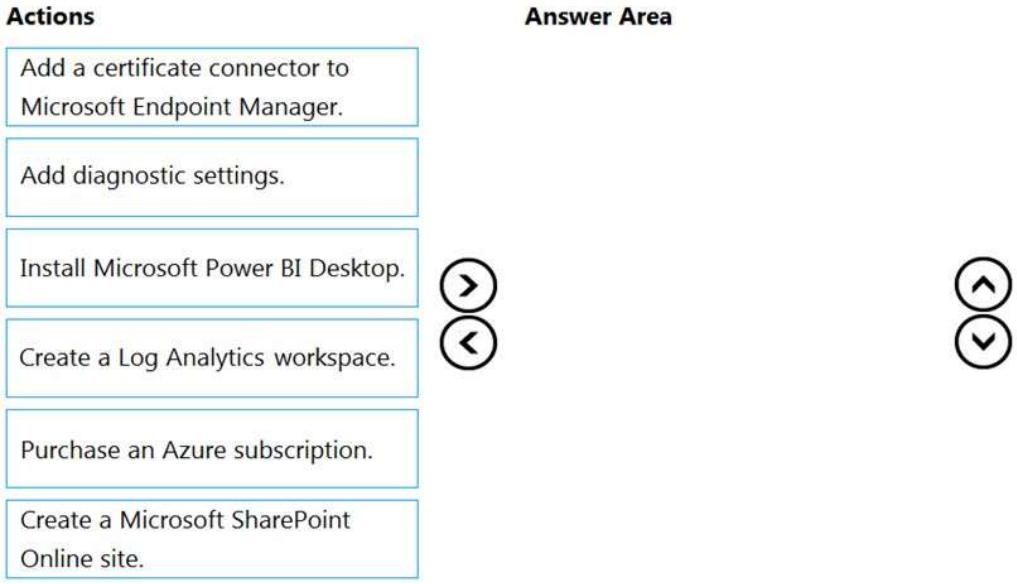
Your company has a Microsoft 365 E5 tenant.

All the devices of the company are enrolled in Microsoft Endpoint Manager.

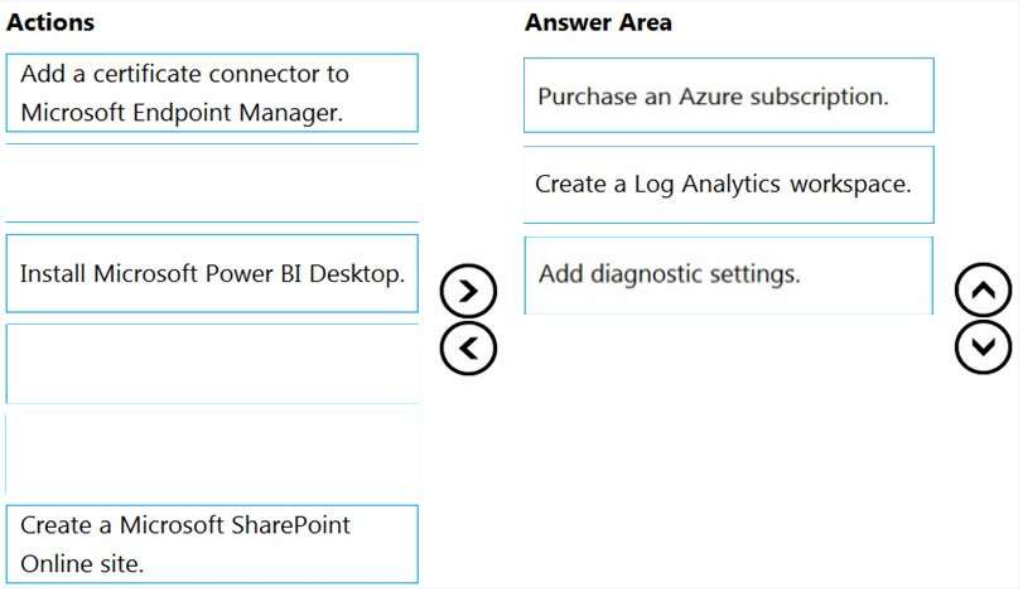
You need to create advanced reports by using custom queries and visualizations from raw Microsoft Endpoint Manager data.

Which three actions should you perform in sequence? To answer, move the appropriate actions from the list of actions to the answer area and arrange them in the correct order.

Select and Place:



Correct Answer:



Step 1: Purchase an Azure subscription.

Complex reporting functionality require an Azure subscription.

Step 2: Create a Log Analytics workspace.

Each Azure resource requires its own diagnostic setting. The diagnostic setting defines the following for a resource:

* One or more destinations to send the logs. Current destinations include Log Analytics workspace, Event Hubs, and Azure Storage.
* Categories of logs and metric data sent to the destinations defined in the setting. The available categories will vary for different resource types.
* Retention policy for data stored in Azure Storage.

Step 3: Add diagnostic settings.

You can create and view custom reports using the following steps:

1. Sign in to the Microsoft Endpoint Manager admin center.
2. Select Reports > Diagnostic settings add a diagnostic setting.
3. Etc.

Reference:

https://docs.microsoft.com/en-us/mem/intune/fundamentals/reports

ANDREVOX Highly Voted 11 months, 1 week ago

When going through the following pages, I understand that you....
1.) Require an Azure subscription.
2.) Create a Analytics workspace.
3.) Create a diagnostic setting.

1.)"Complex reporting functionality require an Azure subscription."
2.)"A Log Analytics workspace is a unique environment for Azure Monitor log data"
3.)"Create a diagnostic setting to send resource logs to a Log Analytics workspace."

https://docs.microsoft.com/en-us/azure/azure-monitor/logs/quick-create-workspace
https://docs.microsoft.com/en-us/azure/azure-monitor/essentials/resource-logs#send-to-log-analytics-workspace
https://docs.microsoft.com/en-us/azure/azure-monitor/essentials/diagnostic-settings?tabs=CMD

upvoted 9 times

RodrigoT 5 months ago

You're right, to use Log Analytics the first thing they ask is an Azure subscription. I tested in my tenant.

upvoted 1 times

AS007 Highly Voted 11 months, 1 week ago

I would swap step 2 and 3 - because you need to have a workspace before configuring the diagnostic settings

upvoted 7 times

RodrigoT 5 months, 1 week ago

You're right. I TESTED in my tenant. And the pictures on the link provided confirm that you need to select a previously created workspace to be able to create diagnostic settings.

upvoted 1 times

examkiller321 Most Recent 11 months, 1 week ago

The answer looks ok. Can anyone confirm?

upvoted 1 times

RodrigoT 5 months, 1 week ago

Correct answers in the wrong order. Swap 2 and 3. Tested.

upvoted 2 times

Question #11 *Topic 5*

HOTSPOT -

Your network contains an Active Directory domain. The domain contains computers that are managed by using Microsoft Endpoint Configuration Manager.

You plan to integrate Configuration Manager and Azure as part of a Desktop Analytics implementation.

You create a new organizational unit (OU) and place several test computers that run Windows 10 into the OU.

You need to collect diagnostic data from the test computers to Desktop Analytics.

- App usage and insights data
- Health monitoring data
- Deployment status data

The solution must minimize the data collected.

Which two Group Policy settings should you configure? To answer, select the appropriate settings in the answer area.

NOTE: Each correct selection is worth one point.

Hot Area:

Answer Area

Allow Telemetry	Not configured
This setting allows you to enable diagnostic data from this device to be processed by Update Compliance	Not configured
Configure the Commercial ID	Not configured
Configure diagnostic data upload endpoint for Desktop Analytics	Not configured
Configure telemetry opt-in change notifications	Not configured
Configure telemetry opt-in setting user interface	Not configured
Disable deleting diagnostic data	Not configured
Disable diagnostic data viewer	Not configured
Configure Authenticated Proxy usage for the Connected User Experience and Telemetry service	Not configured
Limit Enhanced diagnostic data to the minimum required by Windows Analytics	Not configured
Configure Connected User Experiences and Telemetry	Not configured
Do not show feedback notifications	Not configured
Configure collection of browsing data for Desktop Analytics	Not configured

Correct Answer:

Answer Area

Allow Telemetry	Not configured
This setting allows you to enable diagnostic data from this device to be processed by Update Compliance	Not configured
Configure the Commercial ID	Not configured
Configure diagnostic data upload endpoint for Desktop Analytics	Not configured
Configure telemetry opt-in change notifications	Not configured
Configure telemetry opt-in setting user interface	Not configured
Disable deleting diagnostic data	Not configured
Disable diagnostic data viewer	Not configured
Configure Authenticated Proxy usage for the Connected User Experience and Telemetry service	Not configured
Limit Enhanced diagnostic data to the minimum required by Windows Analytics	Not configured
Configure Connected User Experiences and Telemetry	Not configured
Do not show feedback notifications	Not configured
Configure collection of browsing data for Desktop Analytics	Not configured

Box 1: Allow Telemetry -

Use a Group Policy object to set your organization's telemetry level.

1. From the Group Policy Management Console, go to Computer Configuration > Administrative Templates > Windows Components > Data Collection and
Preview Builds.
2. Double-click Allow Telemetry.
3. In the Options box, select Full, and then click OK.

Box 2: Limit Enhanced diagnostic data..
Microsoft recommends that you enable the Optional (limited) diagnostic data level with Desktop Analytics to maximize the benefits you get from it.
The Optional (Limited) setting in Configuration Manager is the same setting as Limit Enhanced diagnostic data to the minimum required by Windows Analytics policy available on devices running Windows 10, version 1709 and later.
Reference:
https://docs.microsoft.com/en-us/enterprise-threat-detection/collector/collector-client-configuration-windows-10-telemetry-requirements
https://docs.microsoft.com/en-us/mem/configmgr/desktop-analytics/enable-data-sharing

camino Highly Voted 7 months, 2 weeks ago
answer looks correct.

From the following Link:
https://admx.help/?Category=Windows_10_2016&Policy=Microsoft.Policies.DataCollection::LimitEnhancedDiagnosticDataWindowsAnalytics

Limit Enhanced diagnostic data to the minimum required by Windows Analytics
This policy setting, in combination with the Allow Telemetry policy setting, enables organizations to send Microsoft a specific set of diagnostic data for IT insights via Windows Analytics services.

To enable this behavior, you must complete two steps:

1. Enable this policy setting
2. Set Allow Telemetry to level 2 (Enhanced)

upvoted 6 times

PiPe Most Recent 7 months, 2 weeks ago
Shouldn't this be 'configure commercial ID' and 'allow telemetry'?
upvoted 1 times

RodrigoT 5 months ago
Commercial ID is usually for update compliance in Log Analytics.
upvoted 1 times

AVP_Riga 10 months, 2 weeks ago
Any thoughts? Is it right?
upvoted 1 times

FrancisLai 10 months, 1 week ago
By looking at the answer link given, the provided answer should be correct.
upvoted 2 times

RodrigoT 5 months, 1 week ago
Answers are correct. The path is: GPO > Computer Configuration > Administrative Templates > Windows Components > Data Collection and Preview Builds. When you click the Limit Enhanced... you will see what camino commented above.
I just want to mention that on Windows 11 the "Allow Telemetry" police changed name to "Allow Diagnostic Data" and you have to set to "Send optional diagnostic data".
upvoted 1 times

Question #12 *Topic 5*

DRAG DROP -

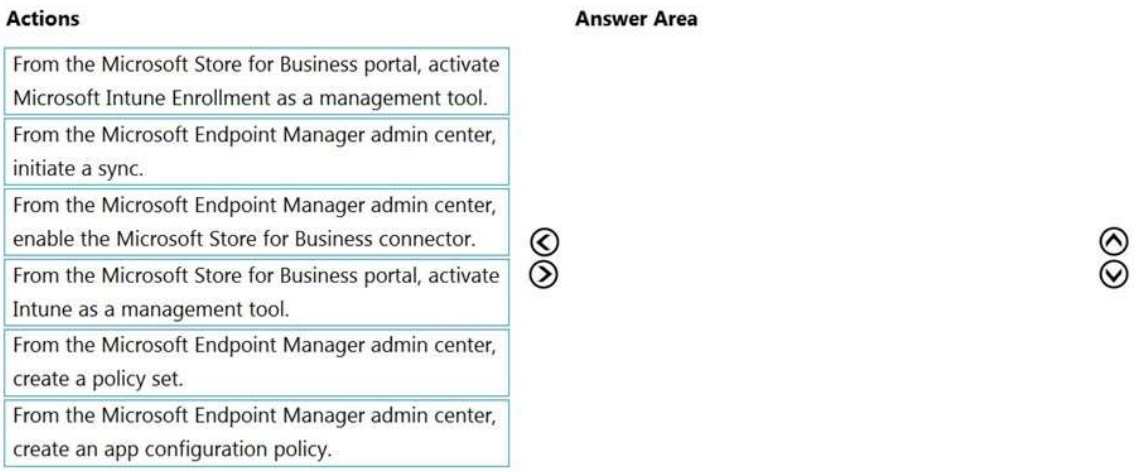
Your company uses Microsoft Intune. You have a Microsoft Store for Business account.

You need to ensure that you can deploy Microsoft Store for Business apps by using Intune.

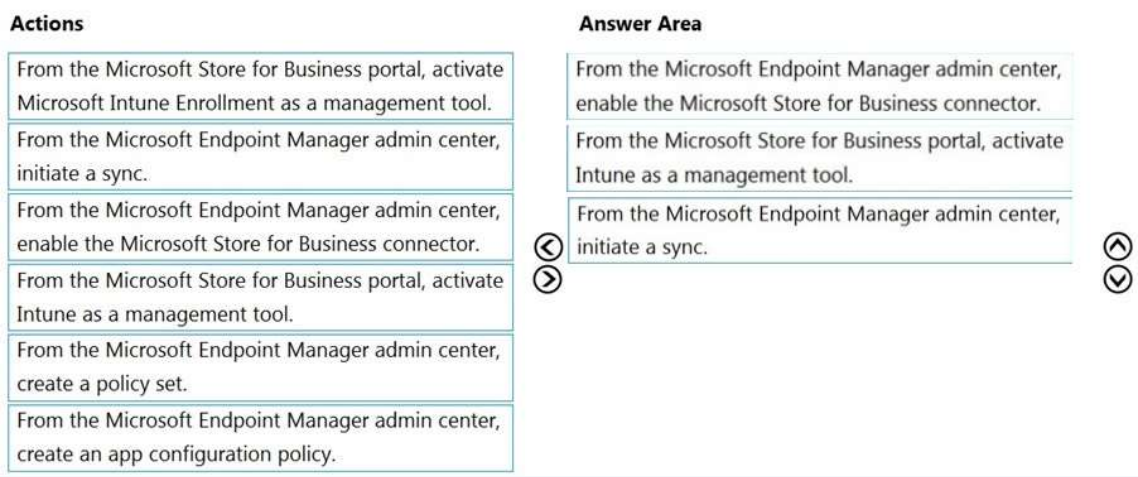
Which three actions should you perform in sequence? To answer, move the appropriate actions from the list of actions to the answer area and arrange them in the correct order.

NOTE: More than one order of answer choices is correct. You will receive credit for any of the correct orders you select.

Select and Place:



Correct Answer:



Step 1: From the Microsoft Endpoint Manager admin center, enable the Microsoft Store for Business connector.

Enable Microsoft store for business (Intune>Apps>Microsoft store for business> Enable).

Step 2: From the Microsoft Store for Business portal, activate Intune as a management tool.

Before you enable synchronization in the Intune console, you must configure your store account to use Intune as a management tool.

1. Ensure that you sign into the Microsoft Store for Business using the same tenant account you use to sign into Intune.
2. In the Business Store, choose the Manage tab, select Settings, and choose the Distribute tab.
3. If you don't specifically have Microsoft Intune available as a mobile device management tool, choose Add management tool to add Microsoft Intune.

Step 3: From the Microsoft Endpoint Manager admin center, initiate a sync.

If you've already associated your Microsoft Store for Business account with your Intune admin credentials, you can manually sync your Microsoft Store for

Business apps with Intune using the following steps.

1. Select Tenant administration > Connectors and tokens > Microsoft Store for Business.
2. Click Sync to get the apps you've purchased from the Microsoft Store into Intune.

Reference:

https://docs.microsoft.com/en-us/mem/intune/apps/windows-store-for-business

CVT24 Highly Voted 1 year, 3 months ago

Correct

upvoted 6 times

RodrigoT 5 months, 1 week ago

Steps valid until the first quarter of 2023 when Microsoft Store for Business will be retiring.
https://businessstore.microsoft.com/en-us/store

upvoted 3 times

coppermine Highly Voted 9 months ago

1. Sign into the Microsoft Store for Business using the same tenant account you use to sign into Intune. In the Business Store, choose the Manage tab, select Settings, and choose the Distribute tab. If you don't specifically have Microsoft Intune available as a mobile device management tool, choose Add management tool to add Microsoft Intune. If you don't have Microsoft Intune activated as your mobile device management tool, click Activate next to Microsoft Intune. Note that you should activate Microsoft Intune rather than Microsoft Intune Enrollment.

2. Sign in to the Microsoft Endpoint Manager admin center. Select Tenant administration > Connectors and tokens > Microsoft Store for Business. Click Enable.

3. Sync the apps you've purchased from the store with Intune

https://docs.microsoft.com/en-us/mem/intune/apps/windows-store-for-business

upvoted 5 times

letters1234 Most Recent 7 months, 1 week ago

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: https://aka.ms/windows/msfb_evolution

upvoted 2 times

Question #13 *Topic 5*

Your company has a Microsoft 365 subscription.

All the users in the finance department own personal devices that run iOS or Android. All the devices are enrolled in Microsoft Intune.

The finance department adds new users each month.

The company develops a mobile application named App1 for the finance department users.

You need to ensure that only the finance department users can download App1.

What should you do first?

A. Add App1 to Intune.

B. Add App1 to a Microsoft Deployment Toolkit (MDT) deployment share.

C. Add App1 to Microsoft Store for Business.

D. Add App1 to the vendor stores for iOS and Android applications.

Correct Answer: *A*

Before you can configure, assign, protect, or monitor apps, you must add them to Microsoft Intune.

Reference:

https://docs.microsoft.com/en-us/intune/apps-add

vm007 Highly Voted 2 years, 6 months ago

Before you can configure, assign, protect, or monitor apps, you must add them to Microsoft Intune.
ref: https://docs.microsoft.com/en-us/mem/intune/apps/apps-add

upvoted 15 times

Mr01z0 Most Recent 1 year, 6 months ago

Normally you would "buy" the app from the Google play Store / Apple Store and then sync it to intune, from there you can then make apps available to devices and users. Since this is an in-house developed app you can add the application file for Android (apk) and the application file for iOS (ipa) to intune as a Line of Business app.

The literal text from Intune blade reads:
"Line-of-business app

To add a custom or in-house app, upload the app's installation file. Make sure the file extension matches the app's intended platform. Intune supports the following line-of-business app platforms and extensions:

* Android (APK)
* iOS (IPA)
* macOS (.IntuneMac)
* Windows (.msi, .appx, .appxbundle, .msix, and .msixbundle)"

upvoted 4 times

Rstilekar 1 year, 9 months ago

Ignore my previous comment. After reading this i am convinced answer Intune is right.... https://docs.microsoft.com/en-us/mem/intune/apps/apps-add

upvoted 4 times

DergX 1 year, 7 months ago

A is correct because it's mobile devices - iOS/Android so that would rule out the Windows Store.

upvoted 3 times

Rstilekar 1 year, 9 months ago

Shouldnt it be C, users should be able to download themselve... thats Store for Business.

upvoted 1 times

Mujja 1 year, 3 months ago

Microsoft Store for Business is a Windows only App \ Portal.

upvoted 2 times

Alex_Cooney 1 year, 9 months ago

Is the answer A instead of C because the company developed the app, & it isn't a commercial one?

Not questioning, just in the process of learning this stuff!

upvoted 3 times

Timmi 1 year, 9 months ago

No, it's the standard process (A) of making any App available for Intune managed devices, as I understand.

upvoted 3 times

Question #14 *Topic 5*

HOTSPOT -

You have a Microsoft Azure Active Directory (Azure AD) tenant named contoso.com. All Windows 10 devices have apps named App1, App2 and App3 installed and are enrolled in Microsoft Intune.

You configure the following settings in Windows Information Protection (WIP):

- Protected apps: App1
- Exempt apps: App2

Windows Information Protection mode: Silent

App1, App2, and App3 use the same file format.

You create a file named File1 in App1.

You need to identify which apps can open File1.

Which apps 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

You can open File1 from:

- App1 only
- App1, and App2 only
- App1 and App3 only
- App1, App2, and App3

An action will be logged when you attempt to open File1 from:

- App1 only
- App3 only
- App1, and App2 only
- App2 and App3 only
- App1, App2, and App3

Correct Answer:

Answer Area

You can open File1 from:

- App1 only
- App1, and App2 only
- App1 and App3 only
- **App1, App2, and App3**

An action will be logged when you attempt to open File1 from:

- App1 only
- **App3 only**
- App1, and App2 only
- App2 and App3 only
- App1, App2, and App3

Reference:

https://docs.microsoft.com/en-us/windows/security/information-protection/windows-information-protection/create-wip-policy-using-intune

https://docs.microsoft.com/en-us/windows/security/information-protection/windows-information-protection/create-wip-policy-using-intune#exempt-apps-from-wip- restrictions

Greysi 3 months, 3 weeks ago

Same question as in MS-100 Q31 Topic 1.
1. Correct, all Apps have still access, because "Silent"
2. App3 only

upvoted 3 times

DPivc 1 year, 3 months ago

Shouldn't the action be logged only from App3?

upvoted 2 times

Tomtom11 1 year, 3 months ago

WIP runs silently, logging inappropriate data sharing, without blocking anything that would have been prompted for employee interaction while in Allow Override mode. Unallowed actions, like apps inappropriately trying to access a network resource or WIP-protected data, are still stopped.

upvoted 1 times

Tomtom11 1 year, 3 months ago

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

upvoted 1 times

Question #15 *Topic 5*

Your company has a main office and six branch offices. The branch offices connect to the main office by using a WAN link. All offices have a local Internet connection and a Hyper-V host cluster.
The company has a Microsoft Endpoint Configuration Manager deployment. The main office is the primary site. Each branch office has a distribution point.
All computers that run Windows 10 are managed by using both Configuration Manager and Microsoft Intune.
You plan to deploy the latest build of Microsoft Office 365 ProPlus to all the computers.
You need to minimize the amount of network traffic on the company's Internet links for the planned deployment.
What should you include in the deployment plan?

A. From Intune, configure app assignments for the Office 365 ProPlus suite. In each office, copy the Office 365 distribution files to a Microsoft Deployment Toolkit (MDT) deployment share.

B. From Intune, configure app assignments for the Office 365 ProPlus suite. In each office, copy the Office 365 distribution files to a Configuration Manager distribution point.

C. From Endpoint Configuration Manager, create an application deployment. Copy the Office 365 distribution files to a Configuration Manager cloud distribution point.

D. From Endpoint Configuration Manager, create an application deployment. In each office, copy the Office 365 distribution files to a Configuration Manager distribution point.

Correct Answer: *D*
Deploy the Microsoft 365 Apps application in Configuration Manager.
After the files for the Microsoft 365 Apps application are copied to the appropriate distribution points, the next step is to deploy the application. When you deploy the application, you specify which computers or users get the application and when.
To deploy the application:
1. In the Configuration Manager console, choose Software Library > Application Management > Applications.
2. Select the Microsoft 365 Apps application, and then on the Home tab, in the Deployment group, choose Deploy.
3. Etc.
Note: If you use Microsoft Endpoint Configuration Manager to deploy software, such as Office, to users and computers in your organization, you can also use that existing Configuration Manager environment to deploy Microsoft 365 Apps. By using Configuration Manager, you can control which users and computers get
Microsoft 365 Apps, where they get the installation files from, and when the Microsoft 365 Apps installation occurs.
Reference:
https://docs.microsoft.com/en-us/deployoffice/deploy-office-365-proplus-with-system-center-configuration-manager-2012r2#distribute-the-office-365-proplus- application-to-distribution-points-in-configuration-manager

vm007 Highly Voted 2 years, 6 months ago
Answer is correct: Process
1. Create an application for Office 365 ProPlus in Configuration Manager
2. Create a deployment type for the Office 365 ProPlus application in Configuration Manager
3. Distribute the Office 365 ProPlus application to distribution points in Configuration Manager
4. Deploy the Office 365 ProPlus application in Configuration Manager
ref: https://docs.microsoft.com/en-us/deployoffice/deploy-office-365-proplus-with-system-center-configuration-manager-2012r2#distribute-the-office-365-proplus-%20application-to-distribution-points-in-configuration-manager
upvoted 17 times

RodrigoT 5 months ago
And note the detail: It doesn't say that all the computers run Windows 10, but: all computers "that" run Windows 10 are managed by using both Configuration Manager and Microsoft Intune. We don't know if they have other computers, like Windows 8.1 for example. And we have to deploy Office 365 ProPlus to "all" the computers. To include "all" we can't use Intune at this point.
upvoted 1 times

Perycles Highly Voted 1 year, 3 months ago
correct. "vintage" solution but correct to limite internet traffic.
upvoted 6 times

hawkens Most Recent 1 year, 8 months ago
Correct me if I'm wrong, but doesn't the question state you should minimize the network links? Does uploading the files to all distribution points minimize the internet link?
upvoted 2 times

Anthony_2770 1 year, 8 months ago
You would only do this once. The various computers would then only download from the local distribution point.
It seems to be a very old question
upvoted 4 times

Mr01z0 1 year, 6 months ago
The DP's reside in each of the 6 branch offices that are connected using a WAN link. You are using the WAN link to the branch office to provision the DP, not the local internet links.
upvoted 2 times

Mujja 1 year, 3 months ago

The WAN is the internet though

upvoted 1 times

forExamCert2023 6 months, 3 weeks ago

You should get it from somewhere. So it is passed to the distribution point once. They distribute among units under them. They can transfer installation during off hours or when network load is light. We have been doing this using SCCM for a long time.

upvoted 2 times

Question #16 *Topic 5*

HOTSPOT -

Your company has a computer named Computer1 that runs Windows 10 Pro.

The company develops a proprietary Universal Windows Platform (UWP) app named App1. App1 is signed with a certificate from a trusted certification authority

(CA).

You need to sideload App1 to Computer1.

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

To enable sideloading:

- Configure the Apps & features settings in the Settings app
- Configure the For developers settings in the Settings app
- Run the Enable-WindowsOptionalFeature cmdlet
- Run the Set-WindowsEdition cmdlet

To sideload App1:

- Double-click App1.appx in File Explorer
- Use the Add a package option in the Settings app
- Run the Install-Package cmdlet
- Run the Add-AppxPackage cmdlet

Correct Answer:

Answer Area

To enable sideloading:

- Configure the Apps & features settings in the Settings app
- **Configure the For developers settings in the Settings app**
- Run the Enable-WindowsOptionalFeature cmdlet
- Run the Set-WindowsEdition cmdlet

To sideload App1:

- Double-click App1.appx in File Explorer
- Use the Add a package option in the Settings app
- Run the Install-Package cmdlet
- **Run the Add-AppxPackage cmdlet**

Box 1: Configure the For developers settings in the Settings app

How to allow Windows 10 to sideload apps on your computer

1. Open Settings.
2. Click on Update & security.
3. Click on For developers.
4. Under "Use developer features," select the Sideload apps option.
5. Click Yes to confirm the risks involved running an app outside the Windows Store.
6. Restart your computer if applicable to complete the task.

Box 2: Run the Add-AppxPackage cmdlet

Install the App.

From the folder with the .msix package, run the Windows PowerShell Add-AppxPackage command to install the .msix package.

Reference:

https://docs.microsoft.com/en-us/windows/application-management/sideload-apps-in-windows-10

vm007 Highly Voted 2 years, 6 months ago

Answer is correct:
To turn on sideloading for managed devices

Deploy an enterprise policy.
To turn on sideloading for unmanaged devices

Open Settings.

Click Update & Security > For developers.

On Use developer features, select Sideload apps
To install the app

From the folder with the appx package, run the PowerShell Add-AppxPackage command to install the appx package.
REf:
https://docs.microsoft.com/en-us/windows/application-management/sideload-apps-in-windows-10

upvoted 11 times

moobdoob Most Recent 8 months, 2 weeks ago

Good answer!

upvoted 1 times

KirilA 1 year, 4 months ago

To install the app:
From the folder with the appx package, run the PowerShell Add-AppxPackage command to install the appx package.

Important!
To install an app on Windows 10, in addition to following these procedures, users can also double-click any APPX/MSIX package.

Which one is more correct :(

upvoted 1 times

Danohav 1 year, 4 months ago

I have been asking the same myslef :/

upvoted 1 times

RodrigoT 5 months, 1 week ago

The more correct is running the PowerShell cmdlet. Got this on a KAPLAN exam practice.

upvoted 2 times

Technik 1 year, 4 months ago

I think it is also possible to double-click the .appx

upvoted 4 times

Question #17 *Topic 5*

You manage a Microsoft 365 environment that has co-management enabled.
All computers run Windows 10 and are deployed by using the Microsoft Deployment Toolkit (MDT).
You need to recommend a solution to deploy Microsoft Office 365 ProPlus to new computers. The latest version must always be installed. The solution must minimize administrative effort.
What is the best tool to use for the deployment? More than one answer choice may achieve the goal. Select the BEST answer.

A. Microsoft Intune

B. Microsoft Deployment Toolkit

C. Office Deployment Tool (ODT)

D. a Group Policy object (GPO)

E. Microsoft System Center Configuration Manager

Correct Answer: *C*
The Office Deployment Tool (ODT) is a command-line tool that you can use to download and deploy Microsoft 365 Apps to your client computers. The ODT gives you more control over an Office installation: you can define which products and languages are installed, how those products should be updated, and whether or not to display the install experience to your users.
Reference:
https://docs.microsoft.com/en-us/deployoffice/overview-of-the-office-2016-deployment-tool

Philinger Highly Voted 2 years, 8 months ago
i think it' the best with Intune >the Latest version must be always installed
upvoted 20 times

JakeStafar 2 years, 3 months ago
Intune was never stated as being available.
upvoted 4 times

PrimeSki 2 years, 2 months ago
Intune is available via co-management
upvoted 12 times

RodrigoT 5 months, 1 week ago
The "best tool" is ODT. On the link bellow under the section: "Best practices from the field: Choose how to install Microsoft 365 Apps" there is a picture showing 3 "Install options": On-premises, Hybrid and Cloud. Under the picture it says: "Note that the Office Deployment Tool (ODT) is used to install Microsoft 365 Apps in all these options".

https://docs.microsoft.com/en-us/deployoffice/fieldnotes/install-options
upvoted 3 times

bobboobsmith Highly Voted 2 years, 8 months ago
The answer should be E. It states the org is already using co-management. That means they are using the Current Branch of Configuration Manager already. Per Microsoft, they recommend that O365 ProPlus be deployed via System Center Configuration Manager Current Branch: https://docs.microsoft.com/en-us/DeployOffice/plan-office-365-proplus
upvoted 16 times

justabasicuser 1 year, 2 months ago
It does seem to be Microsoft recommended "Best practice"

"Best practice: If you use Configuration Manager already, make sure you are on the current branch and use it to deploy Office from distributions points on your network. " from:
https://docs.microsoft.com/en-us/mem/intune/apps/apps-add-office365

Although Intune makes more sense to me.
upvoted 3 times

TonySuccess Most Recent 1 week, 3 days ago
Selected Answer: C
CCCCCCCCCCCCCCCCCC
upvoted 1 times

TonySuccess 1 week, 3 days ago
ODT Fo Sho
upvoted 1 times

IcemanJim 3 months ago
Philinger is correct.
I would say Intune as "The latest version must always be installed" once deployed Intune will keep it up to date. If using any other methods it won't keep the product up to date without extra admin.
upvoted 1 times

Angarali 5 months, 2 weeks ago
Selected Answer: A

Intune will always keep Office 365 apps up to date, as the 365 apps are installed directly from Intune itself therefore will always update.
upvoted 2 times

PiPe 7 months, 3 weeks ago
Saw this in a practice exam but worded differently:

Instead of "The solution must minimize administrative effort" it said "Your solution must also follow the principle of least amount of privilege. What is the best command-line tool to use for the deployment?"

The answer options were the same. The answer to this question was: Office Deployment Toolkit (ODT)

So I'm guessing this question is wrong, hence the confusion.
upvoted 10 times

forExamCert2023 6 months, 3 weeks ago
I picked ODT since, I, too, remember this question from somewhere else, specially Microsoft. The answer was ODT.
upvoted 4 times

Tsa777 1 year ago
is still question still valid?
upvoted 2 times

RodrigoT 5 months, 1 week ago
If you arrived at this point, memorize this one also.
upvoted 1 times

Perycles 1 year, 3 months ago
A :intune - you don't have to distibute content to dp..... less administrative effort.
upvoted 3 times

Mujja 1 year, 3 months ago
It's a choice between CM and Intune. If only they said, minimise internet traffic like in previous questions.

I would go with CM. MDT is used for OSD, the org prefers traditional methods.
upvoted 1 times

Henk36 1 year, 5 months ago
Intune --> Create device group --> Select o365 app --> deploy to group
ODT --> Download files -> create XML --> how to trigger install (manual install/MDT Task seq/powershell script/logon script etc)
SCCM --> create new package via ODT or via wizard --> select DPs to distribute -->deploy to collection
MDT --> requires ODT to have latest version, but is fastest with install as O365 is installed during TS, so at the end I would use this in production, but is not wat MS asks.

In that regards I would say Intune is from total clicks the least, but its a bit ambiguous question.
upvoted 11 times

Henk36 1 year, 5 months ago
I would go for Intune as well. You can create a deployment via Intune to deploy O365. Even with additional settings. Or just upload an xml to Intune. (this is required to create for ODT/SCCM etc as well) so it nog extra work. Intune will than automatically deploy the latest version to the group of devices you set.
upvoted 1 times

Mr01z0 1 year, 6 months ago
In the question it states the machines are in co-management, which indicates the presence of ConfigMgr and Intune otherwise machines cannot be co-managed. In configMgr there is a co-management workload you can move to Intune specifically for Office 365 management. Office deployment and management from intune is by far the most simple way to deploy the Office apps (MS 365 Apps for business) I would lean towards Intune for this one.

https://docs.microsoft.com/en-us/mem/configmgr/comanage/workloads#office-click-to-run-apps

https://docs.microsoft.com/en-us/mem/intune/apps/apps-add-office365#select-microsoft-365-apps
upvoted 4 times

configmike 1 year, 6 months ago
Jeez, I've done it Intune and it doesn't get any easier than that....
upvoted 3 times

Beitran 1 year, 7 months ago
Since they're still using MDT and it wants the latest version you can use ODT with /configure to install O365 directly from the Microsoft website.
upvoted 4 times

mfalkjunk 1 year, 8 months ago
Answer is E

https://docs.microsoft.com/en-us/deployoffice/fieldnotes/install-options
upvoted 3 times

geoffC 1 year, 5 months ago
In that link it states:
"Note that the Office Deployment Tool (ODT) is used to install Microsoft 365 Apps in all these options"
The question asks which is the best TOOL. So C I think.
upvoted 2 times

vinnyct 1 year, 9 months ago
It's A & E
The question says multiple answer cab achieve the goal

upvoted 2 times

VCE_player 1 year, 9 months ago

Yep, and then it says " Select the BEST answer." So it ends up with one of the two after all..
I have deployed it many times using SCCM (using ODT once and then configuring monthly updates, which is pretty "administrative" already), but never had experience with deploying and managing it with Intune. But I can imagine Microsoft's "BEST" way would be Intune (cloud minded and simpler approach).
Tricky question...

upvoted 1 times

goape 1 year, 10 months ago

Several others have posted the same link and stated that ODT is the way to go, when the link clearly says in step 1 that if you have SCCM, to deploy this way. Persoanlly I think the easiest way would be Intune as you don't need to download source files and create package as you would in ODT, MDT or SCCM. You merely create the deployment and make available in portal app.

upvoted 1 times

DJM 1 year, 10 months ago

Agreed, however... SCCM still requires you to use ODT. InTune (EPM) would certainly be the method with the least amount of 'Administrative' effort, I can't decide on whether that is the best answer given how the question is worded though..

upvoted 2 times

Question #18 *Topic 5*

You have a Microsoft 365 subscription.
You have 10 computers that run Windows 10 and are enrolled in mobile device management (MDM).
You need to deploy the Microsoft 365 Apps for enterprise suite to all the computers.
What should you do?

A. From the Endpoint Manager admin center, add an app.

B. From Microsoft Azure Active Directory (Azure AD), add an app registration.

C. From Microsoft Azure Active Directory (Azure AD), add an enterprise application.

D. From the Endpoint Manager admin center, create a Windows 10 device profile.

Correct Answer: *A*
Before you can assign, monitor, configure, or protect apps, you must add them to Intune.
Select Microsoft 365 Apps.
1. Sign in to the Microsoft Endpoint Manager admin center.
2. Select Apps > All apps > Add.
3. Select Windows 10 in the Microsoft 365 Apps section of the Select app type pane.
4. Click Select. The Add Microsoft 365 Apps steps are displayed.
Reference:
https://docs.microsoft.com/en-us/mem/intune/apps/apps-add-office365

jibutoms Highly Voted 1 year, 3 months ago
A should be the answer.
upvoted 12 times

jibutoms 1 year, 3 months ago
On a closer look, it says " enrolled in mobile device management (MDM)", it is not saying intune.
upvoted 1 times

Mujja 1 year, 3 months ago
Enrolled in MDM is Intune.
upvoted 7 times

tf444 11 months, 2 weeks ago
Lol!
jibutoms IS TIRED.
upvoted 9 times

Cowok Highly Voted 1 year, 4 months ago
I believe its A, you can make the app " required " which will be installed on all devices / group.
upvoted 7 times

RodrigoT 5 months, 1 week ago
You're right. And there is absolutely nothing on the link provided that talks about Azure AD enterprise app.
These wrong answers kill me.
upvoted 3 times

Garito Most Recent 7 months, 1 week ago
Selected Answer: A
Adding App via intune
upvoted 2 times

lucadp010 8 months, 2 weeks ago
Selected Answer: A
A for sure
upvoted 2 times

IykeP 8 months, 2 weeks ago
Selected Answer: A
A is the correct answer. You cannot deploy the app via AZURE Enterprise applications as this is not in AZURE AD Gallery.
upvoted 2 times

moobdoob 8 months, 2 weeks ago
Answer is A
upvoted 2 times

Test99 1 year, 4 months ago
A is correct as this is Intune and the same answer was given in question 11
upvoted 3 times

Question #19 *Topic 5*

You have a Microsoft 365 subscription.
You need to deploy Microsoft 365 Apps for enterprise applications to Windows 10 devices.
What should you do first?

A. From Microsoft Azure Active Directory (Azure AD), create an app registration.

B. From the Endpoint Manager admin center, create an app.

C. From the Endpoint Manager admin center, create an app configuration policy.

D. From the Endpoint Manager admin center, enable Microsoft Store for Business synchronization.

Correct Answer: *B*
Before you can assign, monitor, configure, or protect apps, you must add them to Intune. One of the available app types is Microsoft 365 apps for Windows 10 devices. By selecting this app type in Intune, you can assign and install Microsoft 365 apps to devices you manage that run Windows 10.

Note: Review + create -
1. Review the values and settings you entered for the app suite.
2. When you are done, click Create to add the app to Intune.
3. The Overview blade is displayed.
Reference:
https://docs.microsoft.com/en-us/mem/intune/apps/apps-add-office365

CVT24 Highly Voted 1 year, 3 months ago
B is the correct answer, however, isn't "Add App" the correct term?
upvoted 7 times

FrancisLai 10 months, 1 week ago
Correct, the term "Add App" should be the correct term in this question.
upvoted 2 times

RodrigoT 4 months, 4 weeks ago
Yeah, but they will always use different terms to confuse us. Sometimes we have to use logic and elimination.
upvoted 2 times

TonySuccess Most Recent 1 week, 3 days ago
Selected Answer: B
Should be B
upvoted 1 times

jorlloen 1 year ago
But, Windows 10 are enrolled in Intune? How you can add app and assign it?
upvoted 2 times

badguytoo 1 year, 1 month ago
ignore the phase....
upvoted 1 times

Question #20 *Topic 5*

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

Name	Platform	Member of
Device1	Windows 10	Group1, Group3
Device2	Android	Group2, Group3
Device3	Windows 10	Group3
Device4	Windows 10	Group2
Device5	Windows 10	Group1

You create an app protection policy named Policy1 that has the following settings:

- Platform: Windows 10
- Protected apps: App1
- Exempt apps: App2
- Network boundary: Cloud resources, IPv4 ranges

You assign Policy1 to Group1 and Group2. You exclude Group3 from Policy1.

Which devices will apply Policy1?

A. Device1, Device2, Device4, and Device5

B. Device1, Device4, and Device5 only

C. Device4 and Device5 only

D. Device1, Device3, Device4 and Device5

Correct Answer: *C*

Intune device configuration profiles let you include and exclude groups from profile assignment. Exclusion takes precedence over inclusion in same group types.

Policy1 excludes Group3 and Group3 includes Device1, Device2, and Device3.

Incorrect Answers:

A, B, D: Device1, Device2, and Device3 are members of Group3. Policy1 excludes Group3. Exclusion takes precedence over inclusion.

Reference:

https://docs.microsoft.com/en-us/mem/intune/configuration/device-profile-assign#exclude-groups-from-a-profile-assignment

https://docs.microsoft.com/en-us/intune/app-protection-policies

Tahlin Highly Voted 2 years, 7 months ago

Only applies to 4 and 5. 'Exclude' overrides 'Apply'. 1, 2 and 3 are excluded by membership. 4 and 5 are the only ones that get it applied.

upvoted 44 times

Redders Highly Voted 2 years, 6 months ago

Answer is C -

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
For example, if you assign a device group to the All corporate users user group, but exclude members in the Senior Management Staff user group, All corporate users except the Senior Management staff get the assignment, because both groups are user groups.

upvoted 18 times

IcemanJim Most Recent 3 months ago

So many comments for an easy question. Answer is C.

upvoted 1 times

Angarali 5 months, 2 weeks ago

Selected Answer: C

Exclude with override.

upvoted 1 times

moobdoob 8 months, 2 weeks ago

4 - 5 is correct ! :D

upvoted 3 times

jibutoms 1 year, 3 months ago

It has to be C
https://docs.microsoft.com/en-us/mem/intune/configuration/device-profile-assign#exclude-groups-from-a-profile-assignment

upvoted 2 times

Harrysa 1 year, 5 months ago

Device 2 is a android platform is Windows only so def can't be device 2 so has to be C

upvoted 4 times

bui89 1 year, 5 months ago

correct answer must be device 4 and 5

upvoted 4 times

techh3ad 1 year, 6 months ago

When creating an App Protection Policy, in step 5 "Assignments" there's a link to an article that explains excluded groups.

https://docs.microsoft.com/en-us/mem/intune/configuration/device-profile-assign#exclude-groups-from-a-profile-assignment

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

Including user groups and excluding user groups
Including device groups and excluding device group

For example, you assign a device profile to the All corporate users user group, but exclude members in the Senior Management Staff user group. Since both groups are user groups, All corporate users except the Senior Management staff get the profile.

upvoted 2 times

MitchF 2 months ago

You have cut & pasted your answer about "Senior Management" below (not from the other sources you have provided). Answer is still C.

https://docs.microsoft.com/en-us/mem/intune/apps/apps-inc-exl-assignments

upvoted 1 times

marz 1 year, 7 months ago

For information about creating app protection policies for Windows apps, see Create and deploy Windows Information Protection (WIP) policy with Intune

upvoted 1 times

Millsy 1 year, 8 months ago

here's another link Exclude overrides include
https://docs.sophos.com/central/Mobile/help/en-us/esg/Sophos-Mobile/tasks/AssignUserGroupsToIntuneAppProtectionPolicy.html

upvoted 1 times

Millsy 1 year, 8 months ago

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

For example, if you assign a device group to the All corporate users user group, but exclude members in the Senior Management Staff user group, All corporate users except the Senior Management staff get the assignment, because both groups are user groups.

so then anything in group 3 does not apply the policy.... and since 2 is not win 10 it has to be C

upvoted 2 times

MitchF 2 months ago

You have cut & pasted your answer from below (not from the other sources you have provided). Answer is C.

https://docs.microsoft.com/en-us/mem/intune/apps/apps-inc-exl-assignments

upvoted 1 times

hawkens 1 year, 8 months ago

Guys, common, its obvious 4 and 5, no takes precendence over yes!

upvoted 4 times

Baxter 1 year, 9 months ago

Directly from the MS endpoint manager admin center:
When creating a new policy, the very first selection to be made is platform
That means we're only dealing with Windows 10 in this scenario (can cross out any answers with non-windows 10 platforms now)
Proceeding through the policy steps in the admin center brings you to Assignments
You can Include groups AND you can Exclude groups
Exclusions take precedence OVER Inclusions (see link below)

https://docs.microsoft.com/en-us/mem/intune/configuration/device-profile-assign#exclude-groups-from-a-profile-assignment

For example, you assign a device profile to the All corporate users user group, but exclude members in the Senior Management Staff user group. Since both groups are user groups, All corporate users except the Senior Management staff get the profile.

upvoted 2 times

Rstilekar 1 year, 9 months ago

Correct answer is C (Exclusion takes preferance over inclusion in same group scenerio)

upvoted 2 times

Samoanhulk 1 year, 10 months ago

Answer is C. From 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:
Including user groups and excluding user groups when assigning apps
Including device groups and excluding device group when assigning apps

upvoted 3 times

goran 1 year, 11 months ago

I believe its B

upvoted 1 times

Question #21 *Topic 5*

HOTSPOT -

Your network contains an Active Directory domain that is synced to Microsoft Azure Active Directory (Azure AD).

You have a Microsoft Office 365 subscription. All computers are joined to the domain and have the latest Microsoft OneDrive sync client (OneDrive.exe) installed.

On all the computers, you configure the OneDrive settings as shown in the following exhibit.

Setting	State
Allow syncing OneDrive accounts for only specific organizations	Enabled
Configure team site libraries to sync automatically	Not configured
Set the maximum percentage of upload bandwidth that OneDrive.exe uses	Not configured
Prevent users from moving their Windows known folders to OneDrive	Not configured
Block syncing OneDrive accounts for specific organizations	Not configured
Migrate Pre-existing TeamSites with OneDrive Files On-Demand	Not configured
The maximum size of a user's OneDrive for Business before they will be prompted to ch...	Not configured
Enable OneDrive Files On-Demand	Not configured
Prevent users from redirecting their Windows known folders to their PC	Disabled
Silently move Windows known folders to OneDrive	Enabled
Prompt users to move Windows known folders to OneDrive	Not configured
Prevent OneDrive from generating network traffic until the user signs in to OneDrive	Not configured
Prevent users from using the remote file fetch feature to access files on the computer	Enabled
SharePoint on-premises server URL and tenant folder name	Not configured
SharePoint prioritization setting for hybrid customers that use SharePoint Online (SPO)...	Not configured
Silently configure OneDrive using the primary Windows account	Enabled

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

[answer choice] will sync automatically by using OneDrive

- No folders
- The Documents folder
- The Favorites folder

To reduce the disk space used by a profile, you must **[answer choice]**

- configure team site libraries to sync automatically
- enable OneDrive Files On-Demand
- set the maximum percentage of upload bandwidth used by OneDrive.exe

Correct Answer:

Answer Area

[answer choice] will sync automatically by using OneDrive

- No folders
- The Documents folder
- The Favorites folder

To reduce the disk space used by a profile, you must **[answer choice]**

- configure team site libraries to sync automatically
- enable OneDrive Files On-Demand
- set the maximum percentage of upload bandwidth used by OneDrive.exe

Box 1: The Documents folder -

Silently move known folders to OneDrive is enabled. Known folder include:

Desktop, Documents, Pictures, Screenshots, and Camera Roll

Box 2: enable OneDrive files On-Demand

OneDrive Files On-Demand enables users to view, search for, and interact with files stored in OneDrive from within File Explorer without downloading them and taking up space on the local hard drive.

Reference:

https://docs.microsoft.com/en-us/onedrive/redirect-known-folders https://docs.microsoft.com/en-us/onedrive/plan-onedrive-enterprise

RodrigoT 5 months, 1 week ago

This one was easy. Tip: always read what they are asking first. Then go back to the information.

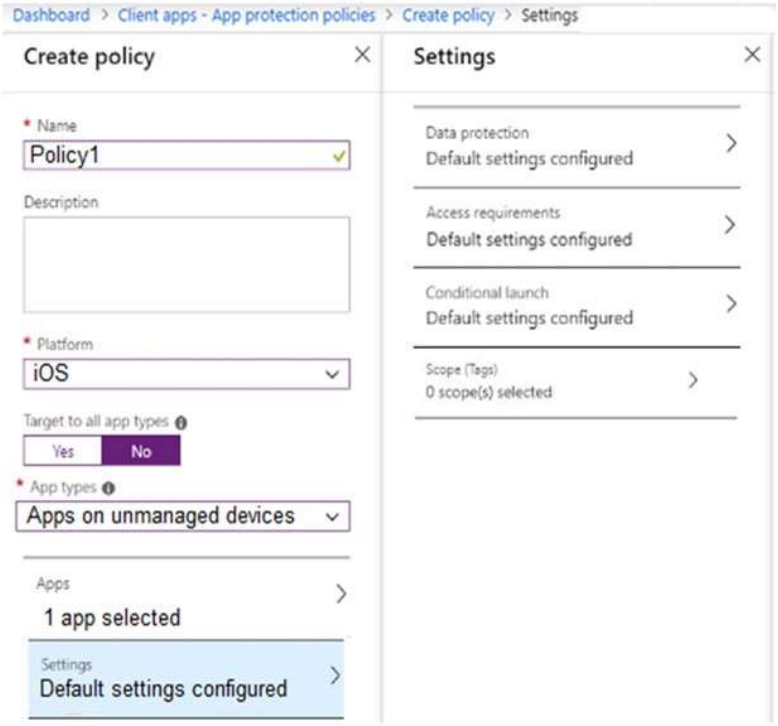
upvoted 1 times

HOTSPOT -

You have a Microsoft 365 subscription.

Users have iOS devices that are not enrolled in Microsoft 365 Device Management.

You create an app protection policy for the Microsoft Outlook app as shown in the exhibit. (Click the Exhibit tab.)



You need to configure the policy to meet the following requirements:

Prevent the users from using the Outlook app if the operating system version is less than 12.0.0.

▪

➪ Require the users to use an alphanumeric passcode to access the Outlook app.

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

NOTE:

Each correct selection is worth one point.

Hot Area:

Answer Area

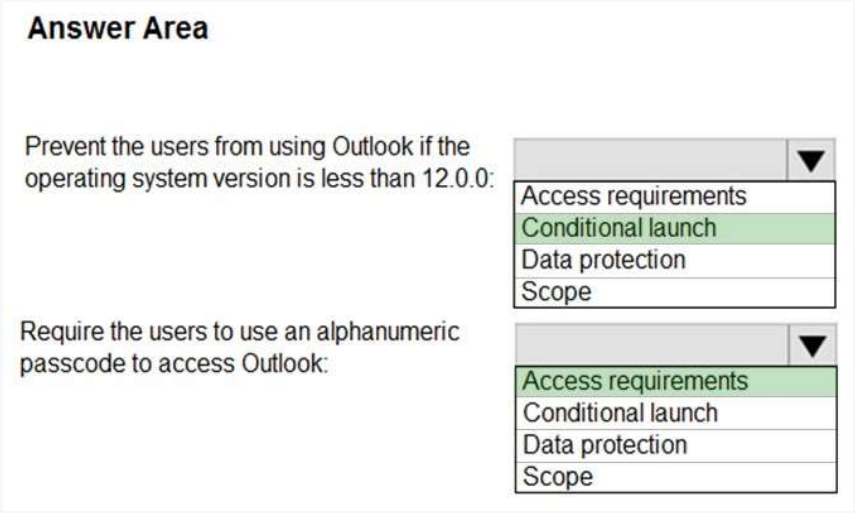
Prevent the users from using Outlook if the operating system version is less than 12.0.0:

- Access requirements
- Conditional launch
- Data protection
- Scope

Require the users to use an alphanumeric passcode to access Outlook:

- Access requirements
- Conditional launch
- Data protection
- Scope

Correct Answer:



Box 1: Conditional launch -

Configure conditional launch settings to set sign-in security requirements for your access protection policy.

By default, several settings are provided with pre-configured values and actions. You can delete some of these, like the Min OS version. You can also select additional settings from the Select one dropdown.

Note: There are three categories of policy settings: Data relocation, Access requirements, and Conditional launch.

Box 2. Access requirements -

Access requirements include:

PIN for access: Select Require to require a PIN to use this app. The user is prompted to set up this PIN the first time they run the app in a work or school context.

The PIN is applied when working either online or offline.

You can configure the PIN strength using the settings available under the PIN for access section.

Reference:

https://docs.microsoft.com/en-us/intune/app-protection-policy-settings-ios

Merma Highly Voted 1 year, 4 months ago

From the provided link:
Conditional launch
As apps often have distinct versioning schemes between them, create a policy with one minimum app version targeting one app (for example, Outlook version policy).
Access requirements
Set a requirement for either numeric or passcode type PINs before accessing an app that has app protection policies applied. Numeric requirements involve only numbers, while a passcode can be defined with at least 1 alphabetical letter or at least 1 special character.
https://docs.microsoft.com/en-us/intune/app-protection-policy-settings-ios

upvoted 9 times

Garito 7 months, 1 week ago

Pretty accurate except the reason it is Conditional Launch is because you can set 'device conditions' which allow you to block/allow OS versions; which is what the question asks.

upvoted 2 times

moobdoob Most Recent 8 months, 2 weeks ago

Good answer!

upvoted 1 times

Perycles 1 year, 3 months ago

correct

upvoted 4 times

Question #23 *Topic 5*

You have a Microsoft 365 E5 subscription.
You need to download a report that lists all the devices that are NOT enrolled in Microsoft Intune and are assigned an app protection policy.
What should you select in the Microsoft Endpoint Manager admin center?

A. Apps, and then App protection policies

B. Apps, and then Monitor

C. Devices, and then Monitor

D. Reports, and the Device compliance

Correct Answer: *A*
App report: You can search by platform and app, and then this report will provide two different app protection statuses that you can select before generating the report. The statuses can be Protected or Unprotected.
Reference:
https://docs.microsoft.com/en-us/mem/intune/apps/app-protection-policies-monitor

TonySuccess 3 days, 4 hours ago
Selected Answer: B
It should be B
upvoted 1 times

Timson 5 months, 1 week ago
Answer should be B. Apps, and then Monitor
upvoted 4 times

RodrigoT 5 months, 1 week ago
Selected Answer: B
It's simply impossible to be A. Their own link provided says "app-protection-policies-monitor" monitor, people! And App report is under Monitor | App protection status > Reports | App report
C'mon!
upvoted 4 times

RodrigoT 5 months ago
There is absolutely no report on Apps | App protection policies. Only policies!
upvoted 1 times

Question #24 *Topic 5*

You have a Microsoft 365 subscription that uses Microsoft Intune.
You need to ensure that you can deploy apps to Android Enterprise devices.
What should you do first?

A. Add a certificate connector.

B. Link your managed Google Play account to Intune.

C. Configure the Partner device management settings.

D. Create a configuration profile.

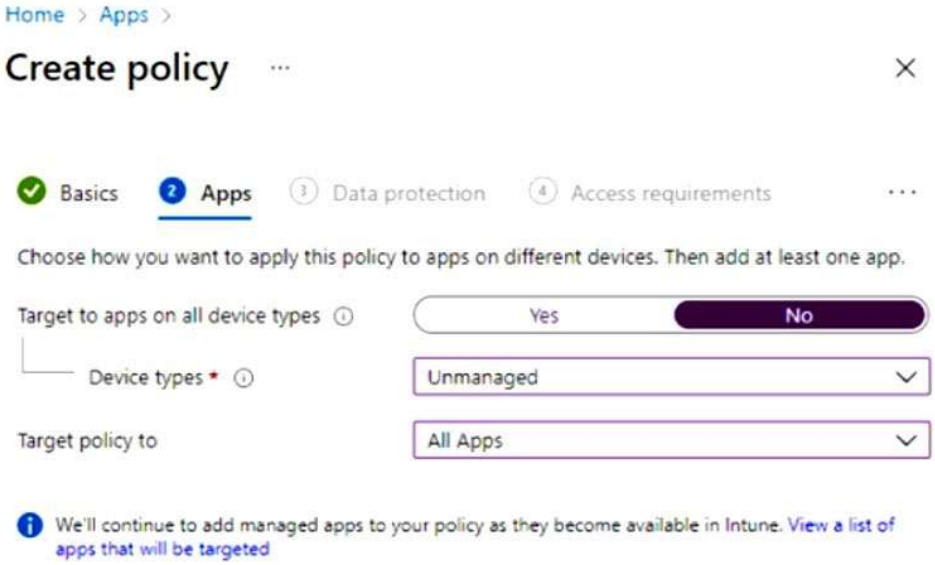
Correct Answer: *B*
Connect your Intune account to your Managed Google Play account.
Managed Google Play is Google's enterprise app store and sole source of applications for Android Enterprise in Intune. You can use Intune to orchestrate app deployment through Managed Google Play for any Android Enterprise scenario (including personally-owned work profile, dedicated, fully managed, and corporate- owned work profile enrollments).
Reference:
https://docs.microsoft.com/en-us/mem/intune/apps/apps-add-android-for-work https://docs.microsoft.com/en-us/mem/intune/enrollment/connect-intune-android-enterprise

Question #25 *Topic 5*

HOTSPOT -

You have a Microsoft 365 E5 subscription.

You create an app protection policy for Android devices named Policy1 as shown in the following exhibit.



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

NOTE: Each correct selection is worth one point.

Hot Area:

Answer Area

To apply Policy1 to an Android device, you must **[answer choice]**.

- install the Company Portal app on the device
- install the Microsoft Authenticator app on the device
- onboard the device to Microsoft Defender for Endpoint
- onboard the device to the Microsoft 365 compliance center

When Policy1 is assigned, the policy will apply to **[answer choice]**.

- users only
- devices only
- users and devices

Correct Answer:

Answer Area

To apply Policy1 to an Android device, you must **[answer choice]**.

- install the Company Portal app on the device
- install the Microsoft Authenticator app on the device
- onboard the device to Microsoft Defender for Endpoint
- onboard the device to the Microsoft 365 compliance center

When Policy1 is assigned, the policy will apply to **[answer choice]**.

- users only
- devices only
- users and devices

Box 1: Install the Intune Company Portal app on the device

On Android, Android devices will prompt to install the Intune Company Portal app regardless of which Device type is chosen.

Bix 2: Devices only -

For Android devices, unmanaged devices are devices where Intune MDM management has not been detected. This includes devices managed by third-party

MDM vendors.

Reference:

https://docs.microsoft.com/en-us/mem/intune/apps/app-protection-policies#app-protection-policies-for-iosipados-and-android-apps

Question #26 *Topic 5*

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

Name	Role
Admin1	Application admin
Admin2	Cloud application admin
Admin3	Office apps admin
Admin4	Security admin

In the Microsoft 365 Apps admin center, you create a Microsoft Office customization.
Which users can download the Office customization file from the admin center?

A. Admin1, Admin2, Admin3, and Admin4

B. Admin1, Admin2, and Admin3 only

C. Admin3 only

D. Admin3 and Admin4 only

E. Admin1 and Admin3 only

Correct Answer: *B*
* Admin1
An application admin has full access to enterprise applications, applications registrations, and application proxy settings.
* Admin2
Mark your app as publisher verified.
In Azure AD this user must be a member of one of the following roles: Application Admin, Cloud Application Admin, or Global Admin.
* Admin3
Office Apps admin - Assign the Office Apps admin role to users who need to do the following:
- Use the Office cloud policy service to create and manage cloud-based policies for Office
- Create and manage service requests
- Manage the What's New content that users see in their Office apps
- Monitor service health
Reference:
Office Apps admin - Assign the Office Apps admin role to users who need to do the following https://docs.microsoft.com/en-us/azure/active-directory/develop/mark-app-as-publisher-verified

Question #27 *Topic 5*

You have a Microsoft 365 subscription. The subscription contains 500 computers that run Windows 11 and are enrolled in Microsoft Endpoint Manager.
You need to manage the deployment of monthly security updates. The solution must meet the following requirements:
- Updates must be deployed to a group of test computers for quality assurance.
- Updates must be deployed automatically 15 days after the quality assurance testing.
What should you create in the Microsoft Endpoint Manager admin center?

A. a security baseline

B. a device configuration profile

C. an update ring

D. a feature update policy

Correct Answer: *C*

Question #28 *Topic 5*

You have a Microsoft 365 subscription that contains 100 devices enrolled in Microsoft Intune.
You need to review the startup processes and how often each device restarts.
What should you use?

A. Endpoint analytics

B. Intune Data Warehouse

C. Azure Monitor

D. Device Management

Correct Answer: *B*

Question #29 *Topic 5*

You have a Microsoft 365 subscription and several Conditional Access policies in Azure Active Directory (Azure AD) that contains the resources shown in the following table.
You need to identify which Conditional Access policies will apply to a user when the user signs in to the Microsoft Office 365 portal from a Windows 10 computer.
What should you use?

A. the What If tool

B. Event Viewer

C. the Microsoft 365 compliance center

D. Resultant Set of Policy (RSoP)

Correct Answer: *C*

thuba_TD 2 weeks ago

Selected Answer: A

https://learn.microsoft.com/en-us/azure/active-directory/conditional-access/what-if-tool

upvoted 1 times

RickyBee 2 weeks, 4 days ago

Selected Answer: B

What If tool can test certain conditions and what policies are applied.

upvoted 1 times

Question #30 *Topic 5*

You have a Microsoft Office 365 E1 subscription.
You plan to create Conditional Access policies.
You need to ensure that users have the required licenses. The solution must minimize costs.
Which type of license should you assign to each user?

A. Microsoft Intune

B. Azure Active Directory Premium Plan 1

C. Office 365 E3

D. Windows 365 Business

Correct Answer: *C*

TonySuccess 1 week, 3 days ago

Selected Answer: C

Answer is C, Ricky needs to cool it with the false information.

upvoted 1 times

RickyBee 2 weeks, 4 days ago

Selected Answer: B

Office 365 E3 does not come with Azure AD Premium

upvoted 1 times

rockhound 2 weeks, 3 days ago

Yes it does. Even F3 comes with Azure AD Premium. I think the cheapest is the O365 E3

upvoted 2 times

HOTSPOT -

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

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

You have the devices shown in the following table.

Name	Platform
Device1	Windows 11
Device2	Android

You have a Conditional Access policy named CAPolicy1 that has the following settings:

⇨ Assignments

- Users or workload identities: Group1
- Cloud apps or actions: All cloud apps

⇨ Conditions

- Device platforms: include: Windows, Android
- Grant access controls: Require multi-factor authentication

You have a Conditional Access named CAPolicy2 that has the following settings:

⇨ Assignments

- Users or workload identities: Group2
- Cloud apps or actions: All cloud apps

⇨ Conditions

- Device platforms: Android
- Access controls: 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 Device2.	◯	◯
User2 can access Microsoft Exchange Online from Device1.	◯	◯
User2 can access Microsoft Exchange Online from Device2.	◯	◯

Correct Answer:

Answer Area

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

Nerovats74 1 day, 5 hours ago

NYN, block for android

upvoted 1 times

Question #32 *Topic 5*

You have an on-premises server named Server1 that hosts a Microsoft Deployment Toolkit (MDT) deployment share named MDT1.
You need to ensure that MDT1 supports multicast deployments.
What should you install on Server1?

A. Windows Server Update Services (WSUS)

B. Multipath I/O (MPIO)

C. Windows Deployment Services (WDS)

D. Multipoint Connector

Correct Answer: *C*

thuba_TD 2 weeks ago

Selected Answer: C

https://learn.microsoft.com/en-us/previous-versions/windows/it-pro/windows-server-2012-R2-and-2012/hh831764(v=ws.11)

upvoted 1 times

HOTSPOT -

You have a Microsoft 365 tenant that uses Microsoft Intune and contains the devices shown in the following table.

Name	Platform
Device1	Windows 10
Device2	macOS

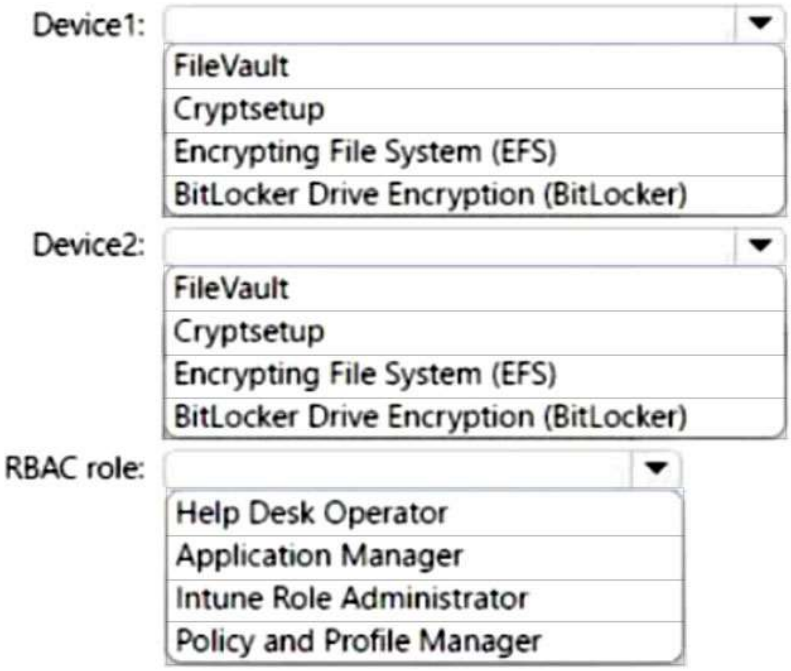
In Endpoint security, you need to configure a disk encryption policy for each device.

Which encryption type should you use for each device, and which role-based access control (RBAC) role in Intune should you use to manage the encryption keys? To answer, select the appropriate options in the answer area.

NOTE: Each correct selection is worth one point.

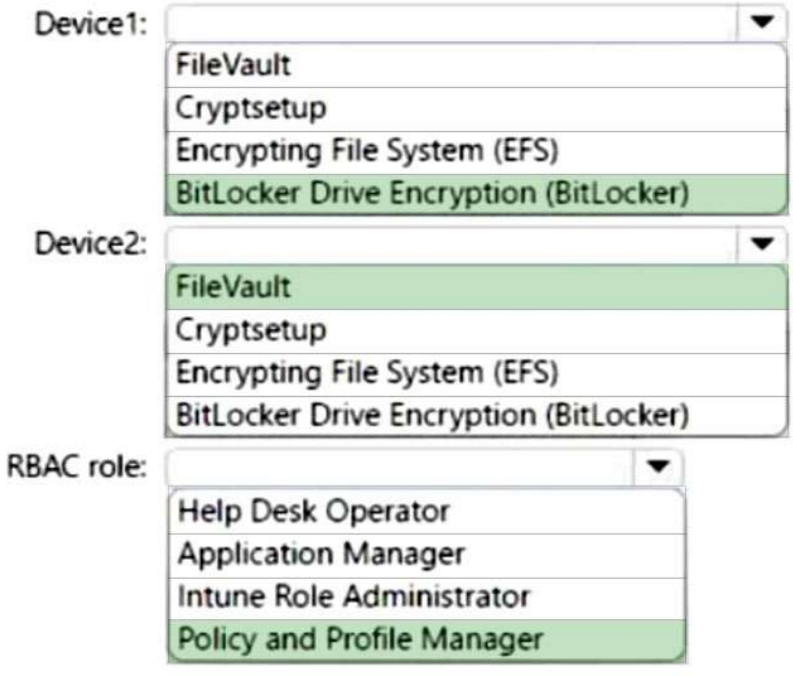
Hot Area:

Answer Area



Correct Answer:

Answer Area



TonySuccess 1 week, 3 days ago

Policy and Profile Manager: Manages compliance policy, configuration profiles, Apple enrollment, corporate device identifiers, and security baselines.

Help Desk Operator: Performs remote tasks on users and devices, and can assign applications or policies to users or devices.

https://learn.microsoft.com/en-us/mem/intune/fundamentals/role-based-access-control

I struggled to get a solid answer on the last question, we know you need Helpdesk Operator for the File Vault, but what about Bitlocker?

upvoted 1 times

bensrayan 2 weeks ago

- bitlocker
- Filevault
-Help Desk Operator
link : https://learn.microsoft.com/en-us/mem/intune/protect/encrypt-devices-filevault

upvoted 1 times

HOTSPOT -

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

You need to perform the following tasks for User1:

- Set the Usage location to Canada.
- Configure the Phone and Email authentication contact info for self-service password reset (SSPR).

Which two settings should you configure in the Azure Active Directory admin center? To answer, select the appropriate settings in the answer area.

NOTE: Each correct selection is worth one point.

Hot Area:

Answer Area

Correct Answer:

Answer Area

cmars 1 week, 2 days ago

Profile- https://connectioncloudsupport.zendesk.com/hc/en-us/articles/4405103699865-How-to-update-UsageLocation-user-setting-in-Azure-AD

Auth methods- https://learn.microsoft.com/en-us/azure/active-directory/authentication/concept-authentication-phone-options

upvoted 1 times

tecnicosoffshoretech 3 weeks, 2 days ago

it should be profile and authentication methods

upvoted 2 times

TonySuccess 1 week, 3 days ago

Where is your source?

upvoted 1 times

TonySuccess 3 days, 3 hours ago

It's actually under 'Overview' now for the Profile change to ensure the usage location is amended.

Auth Methods for the second part of the question.

Mods, we are payin' cash money baybay please sort this out.

upvoted 1 times

Question #35 *Topic 5*

You have a Microsoft 365 E5 subscription and 150 Windows 10 devices.
All the devices are enrolled in Microsoft Intune.
You need to use Intune to apply Windows updates to the devices.
What should you do first?

A. From the Microsoft Endpoint Manager admin center, configure scope tags.

B. Create a device restriction policy that has telemetry set to the minimum setting of Required.

C. From the Microsoft Endpoint Manager admin center, configure a security baseline.

D. Create a device restriction policy that has telemetry set to Security (Enterprise Only).

Correct Answer: *A*

Topic 6 - Testlet 1

Introductory Info

Case study -

This is a case study. Case studies are not timed separately. You can use as much exam time as you would like to complete each case. However, there may be additional case studies and sections on this exam. You must manage your time to ensure that you are able to complete all questions included on this exam in the time provided.

To answer the questions included in a case study, you will need to reference information that is provided in the case study. Case studies might contain exhibits and other resources that provide more information about the scenario that is described in the case study. Each question is independent of the other questions in this case study.

At the end of this case study, a review screen will appear. This screen allows you to review your answers and to make changes before you move to the next section of the exam. After you begin a new section, you cannot return to this section.

To start the case study -

To display the first question in this case study, click the Next button. Use the buttons in the left pane to explore the content of the case study before you answer the questions. Clicking these buttons displays information such as business requirements, existing environment, and problem statements. When you are ready to answer a question, click the Question button to return to the question.

General Overview -

Litware, Inc. is an international manufacturing company that has 3,000 employees. The company has sales, marketing, research, human resources (HR), development, and IT departments.

Litware has two main offices in New York and Los Angeles. Litware has five branch offices in Asia.

Existing Environment -

Current Business Model -

The Los Angeles office has 500 developers. The developers work flexible hours ranging from 11 AM to 10 PM.

Litware has a Microsoft Endpoint Configuration Manager deployment.

During discovery, the company discovers a process where users are emailing bank account information of its customers to internal and external recipients.

Current Environment -

The network contains an Active Directory domain that is synced to Microsoft Azure Active Directory (Azure AD). The functional level of the forest and the domain is

Windows Server 2012 R2. All domain controllers run Windows Server 2012 R2.

Litware has the computers shown in the following table.

Department	Windows version	Management platform	Domain-joined
Marketing	8.1	Endpoint Configuration Manager	Hybrid Azure-AD joined
Research	10	Endpoint Configuration Manager	Hybrid Azure-AD joined
HR	8.1	Endpoint Configuration Manager	Hybrid Azure-AD joined
Developers	10	Microsoft Intune	Azure AD-joined
Sales	10	Microsoft Intune	Azure AD-joined

The development department uses projects in Azure DevOps to build applications.

Most of the employees in the sales department are contractors. Each contractor is assigned a computer that runs Windows 10. At the end of each contract, the computer is assigned to a different contractor. Currently, the computers are re-provisioned manually by the IT department.

Problem Statements -

Litware identifies the following issues on the network:

Employees in the Los Angeles office report slow Internet performance when updates are downloading. The employees also report that the updates frequently consume considerable resources when they are installed. The Update settings are configured as shown in the Updates exhibit. (Click the Updates button.)

Management suspects that the source code for the proprietary applications in Azure DevOps in being shared externally.

Re-provisioning the sales department computers is too time consuming.

Requirements -

Business Goals -

Litware plans to transition to co-management for all the company-owned Windows 10 computers.

Whenever possible, Litware wants to minimize hardware and software costs.

Device Management Requirements -

Litware identifies the following device management requirements:

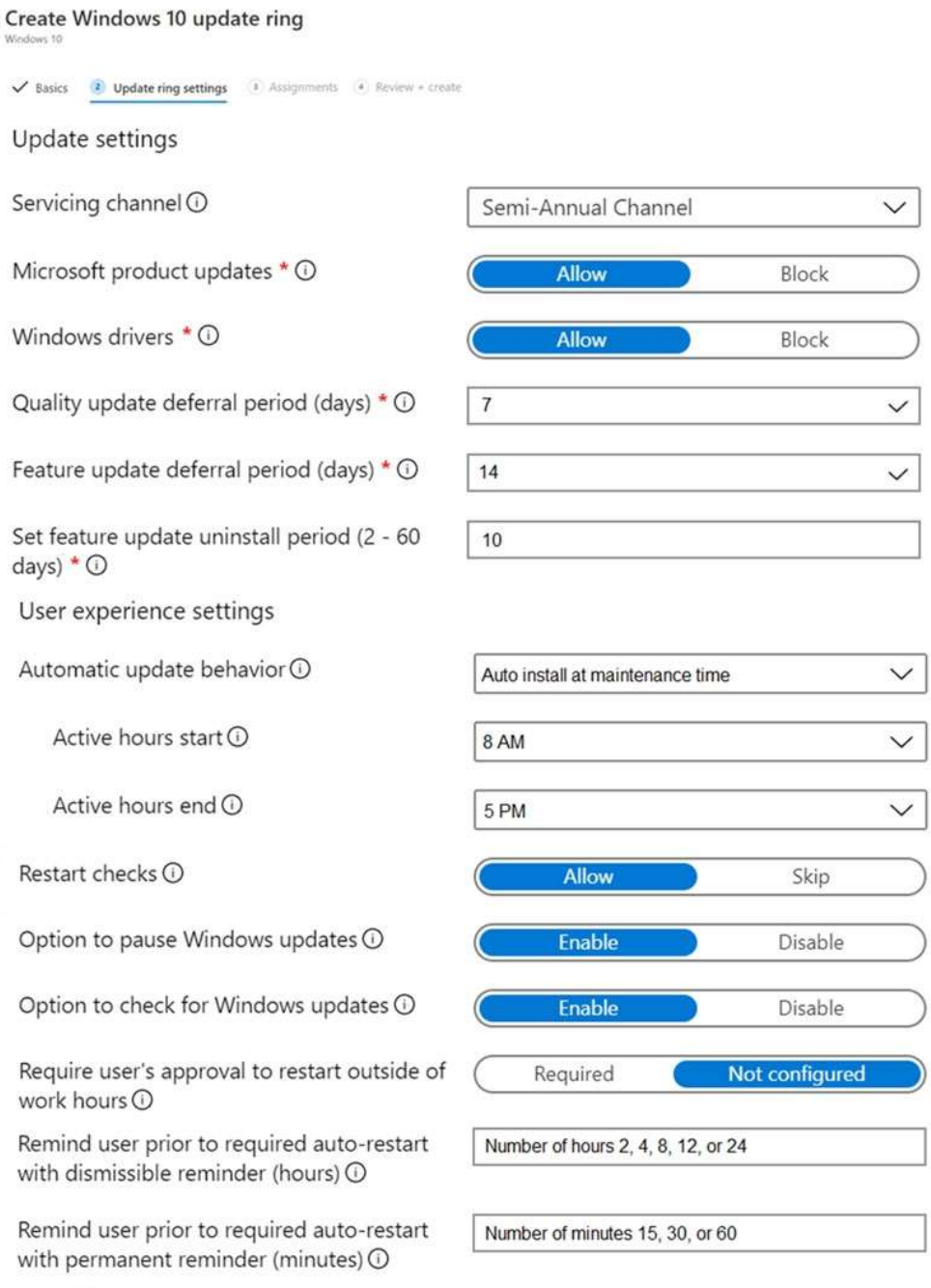
Prevent the sales department employees from forwarding email that contains bank account information.

Ensure that Microsoft Edge Favorites are accessible from all computers to which the developers sign in.
Prevent employees in the research department from copying patented information from trusted applications to untrusted applications.

Technical Requirements -
Litware identifies the following technical requirements for the planned deployment:
Re-provision the sales department computers by using Windows AutoPilot.
Ensure that the projects in Azure DevOps can be accessed from the corporate network only.
Ensure that users can sign in to the Azure AD-joined computers by using a PIN. The PIN must expire every 30 days.
Ensure that the company name and logo appears during the Out of Box Experience (OOBE) when using Windows AutoPilot.

Exhibits -

Updates -



Question
You need to capture the required information for the sales department computers to meet the technical requirements.
Which Windows PowerShell command should you run first?

A. Install-Module WindowsAutoPilotIntune

B. Install-Script Get-WindowsAutoPilotInfo

C. Import-AutoPilotCSV

D. Get-WindowsAutoPilotInfo

Correct Answer: *A*

Re-provision the sales department computers by using Windows AutoPilot.

Windows Autopilot Deployment for existing devices, install required modules:

- Install-PackageProvider -Name NuGet -MinimumVersion 2.8.5.201 -Force
- Install-Module AzureAD -Force
- Install-Module WindowsAutopilotIntune -Force
- Install-Module Microsoft.Graph.Intune -Force

Reference:

https://docs.microsoft.com/en-us/windows/deployment/windows-autopilot/existing-devices

AleDrinker 5 months ago

Selected Answer: A

RodrigoT thank you for providing the correct link

upvoted 2 times

Timson 5 months, 1 week ago

Answer should be: Install-Script Get-WindowsAutoPilotInfo

upvoted 2 times

RodrigoT 5 months, 1 week ago

Answer is correct. Moderator please update the link provided to:
https://docs.microsoft.com/en-us/mem/autopilot/existing-devices

upvoted 2 times

RodrigoT 5 months, 1 week ago

My tip for this part of the exam is: Read first what they are asking, then go back and search for the specific information instead of reading everything wasting precious time. Sometimes the whole information is very complicated but the question is very simple.

upvoted 1 times

RodrigoT 4 months, 4 weeks ago

More specific:
https://docs.microsoft.com/en-us/mem/autopilot/existing-devices#create-the-json-file

upvoted 1 times

Introductory Info

Case study -

This is a case study. Case studies are not timed separately. You can use as much exam time as you would like to complete each case. However, there may be additional case studies and sections on this exam. You must manage your time to ensure that you are able to complete all questions included on this exam in the time provided.

To answer the questions included in a case study, you will need to reference information that is provided in the case study. Case studies might contain exhibits and other resources that provide more information about the scenario that is described in the case study. Each question is independent of the other questions in this case study.

At the end of this case study, a review screen will appear. This screen allows you to review your answers and to make changes before you move to the next section of the exam. After you begin a new section, you cannot return to this section.

To start the case study -

To display the first question in this case study, click the Next button. Use the buttons in the left pane to explore the content of the case study before you answer the questions. Clicking these buttons displays information such as business requirements, existing environment, and problem statements. When you are ready to answer a question, click the Question button to return to the question.

General Overview -

Litware, Inc. is an international manufacturing company that has 3,000 employees. The company has sales, marketing, research, human resources (HR), development, and IT departments.

Litware has two main offices in New York and Los Angeles. Litware has five branch offices in Asia.

Existing Environment -

Current Business Model -

The Los Angeles office has 500 developers. The developers work flexible hours ranging from 11 AM to 10 PM.

Litware has a Microsoft Endpoint Configuration Manager deployment.

During discovery, the company discovers a process where users are emailing bank account information of its customers to internal and external recipients.

Current Environment -

The network contains an Active Directory domain that is synced to Microsoft Azure Active Directory (Azure AD). The functional level of the forest and the domain is

Windows Server 2012 R2. All domain controllers run Windows Server 2012 R2.

Litware has the computers shown in the following table.

Department	Windows version	Management platform	Domain-joined
Marketing	8.1	Endpoint Configuration Manager	Hybrid Azure-AD joined
Research	10	Endpoint Configuration Manager	Hybrid Azure-AD joined
HR	8.1	Endpoint Configuration Manager	Hybrid Azure-AD joined
Developers	10	Microsoft Intune	Azure AD-joined
Sales	10	Microsoft Intune	Azure AD-joined

The development department uses projects in Azure DevOps to build applications.

Most of the employees in the sales department are contractors. Each contractor is assigned a computer that runs Windows 10. At the end of each contract, the computer is assigned to a different contractor. Currently, the computers are re-provisioned manually by the IT department.

Problem Statements -

Litware identifies the following issues on the network:

Employees in the Los Angeles office report slow Internet performance when updates are downloading. The employees also report that the updates frequently consume considerable resources when they are installed. The Update settings are configured as shown in the Updates exhibit. (Click the Updates button.)

Management suspects that the source code for the proprietary applications in Azure DevOps in being shared externally.

Re-provisioning the sales department computers is too time consuming.

Requirements -

Business Goals -

Litware plans to transition to co-management for all the company-owned Windows 10 computers.

Whenever possible, Litware wants to minimize hardware and software costs.

Device Management Requirements -

Litware identifies the following device management requirements:

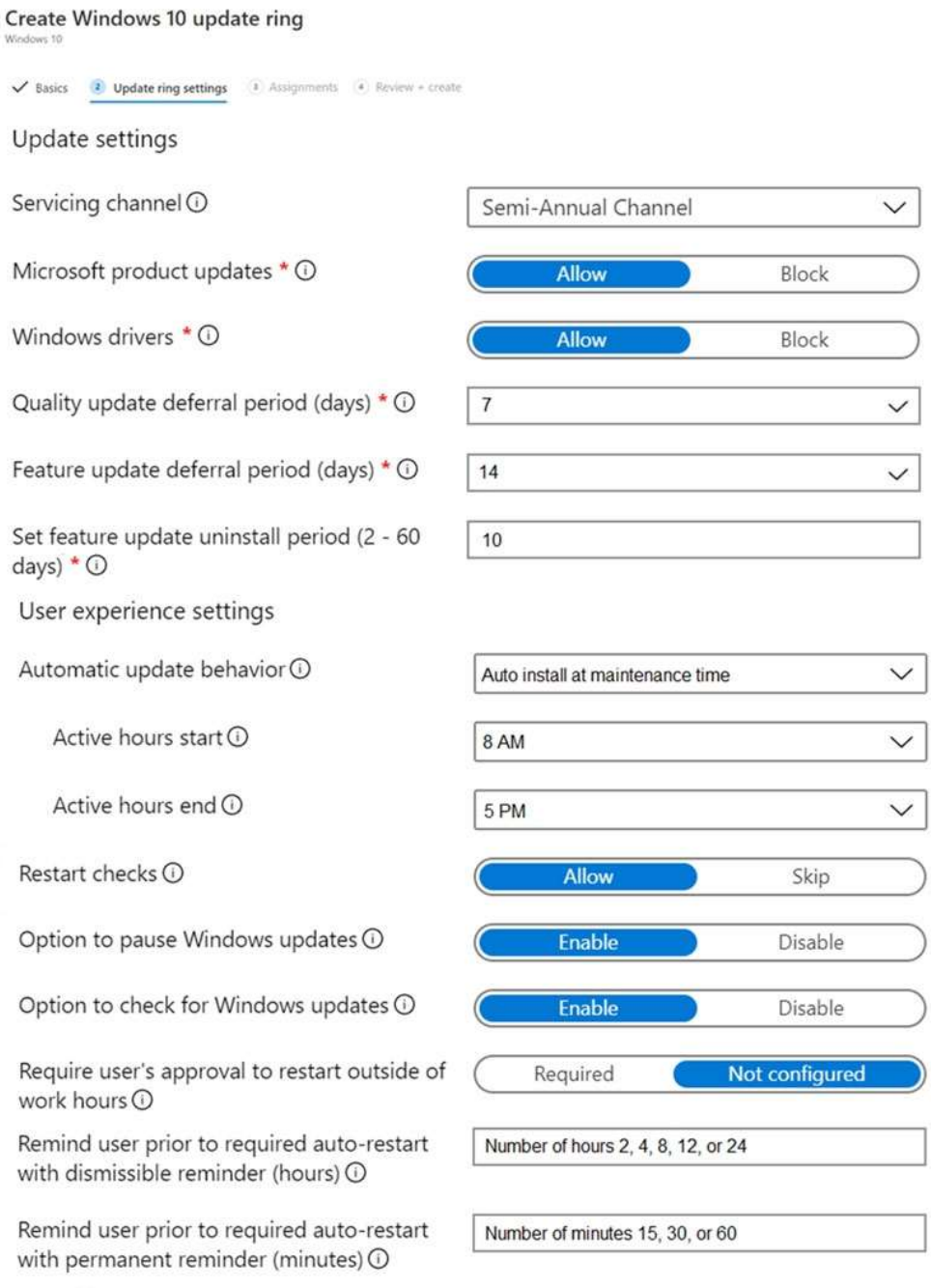
Prevent the sales department employees from forwarding email that contains bank account information.

Ensure that Microsoft Edge Favorites are accessible from all computers to which the developers sign in.
Prevent employees in the research department from copying patented information from trusted applications to untrusted applications.

Technical Requirements -
Litware identifies the following technical requirements for the planned deployment:
Re-provision the sales department computers by using Windows AutoPilot.
Ensure that the projects in Azure DevOps can be accessed from the corporate network only.
Ensure that users can sign in to the Azure AD-joined computers by using a PIN. The PIN must expire every 30 days.
Ensure that the company name and logo appears during the Out of Box Experience (OOBE) when using Windows AutoPilot.

Exhibits -

Updates -



Question
What should you configure to meet the technical requirements for the Azure AD-joined computers?

A. Windows Hello for Business from the Endpoint Manager admin center.

B. The Accounts options in an endpoint protection profile.

C. The Password Policy settings in a Group Policy object (GPO).

D. A password policy from the Microsoft 365 admin center.

Correct Answer: *A*

Ensure that users can sign in to the Azure AD-joined computers by using a PIN. The PIN must expire every 30 days.

Group Policy settings for Windows Hello for Business.

These policy settings are available in User configuration and Computer Configuration under Policies > Administrative Templates > Windows Components >

Windows Hello for Business.

Reference:

https://docs.microsoft.com/en-us/windows/security/identity-protection/hello-for-business/hello-manage-in-organization

RodrigoT 5 months, 1 week ago

My tip for this part of the exam is: Read first what they are asking, then go back and search for the specific information instead of reading everything wasting precious time. Sometimes the whole information is very complicated but the question is very simple.

upvoted 2 times

RodrigoT 5 months, 1 week ago

By the way, the answer provided is correct.

upvoted 2 times

Introductory Info

Case study -

This is a case study. Case studies are not timed separately. You can use as much exam time as you would like to complete each case. However, there may be additional case studies and sections on this exam. You must manage your time to ensure that you are able to complete all questions included on this exam in the time provided.

To answer the questions included in a case study, you will need to reference information that is provided in the case study. Case studies might contain exhibits and other resources that provide more information about the scenario that is described in the case study. Each question is independent of the other questions in this case study.

At the end of this case study, a review screen will appear. This screen allows you to review your answers and to make changes before you move to the next section of the exam. After you begin a new section, you cannot return to this section.

To start the case study -

To display the first question in this case study, click the Next button. Use the buttons in the left pane to explore the content of the case study before you answer the questions. Clicking these buttons displays information such as business requirements, existing environment, and problem statements. When you are ready to answer a question, click the Question button to return to the question.

General Overview -

Litware, Inc. is an international manufacturing company that has 3,000 employees. The company has sales, marketing, research, human resources (HR), development, and IT departments.

Litware has two main offices in New York and Los Angeles. Litware has five branch offices in Asia.

Existing Environment -

Current Business Model -

The Los Angeles office has 500 developers. The developers work flexible hours ranging from 11 AM to 10 PM.

Litware has a Microsoft Endpoint Configuration Manager deployment.

During discovery, the company discovers a process where users are emailing bank account information of its customers to internal and external recipients.

Current Environment -

The network contains an Active Directory domain that is synced to Microsoft Azure Active Directory (Azure AD). The functional level of the forest and the domain is

Windows Server 2012 R2. All domain controllers run Windows Server 2012 R2.

Litware has the computers shown in the following table.

Department	Windows version	Management platform	Domain-joined
Marketing	8.1	Endpoint Configuration Manager	Hybrid Azure-AD joined
Research	10	Endpoint Configuration Manager	Hybrid Azure-AD joined
HR	8.1	Endpoint Configuration Manager	Hybrid Azure-AD joined
Developers	10	Microsoft Intune	Azure AD-joined
Sales	10	Microsoft Intune	Azure AD-joined

The development department uses projects in Azure DevOps to build applications.

Most of the employees in the sales department are contractors. Each contractor is assigned a computer that runs Windows 10. At the end of each contract, the computer is assigned to a different contractor. Currently, the computers are re-provisioned manually by the IT department.

Problem Statements -

Litware identifies the following issues on the network:

Employees in the Los Angeles office report slow Internet performance when updates are downloading. The employees also report that the updates frequently consume considerable resources when they are installed. The Update settings are configured as shown in the Updates exhibit. (Click the Updates button.)

Management suspects that the source code for the proprietary applications in Azure DevOps in being shared externally.

Re-provisioning the sales department computers is too time consuming.

Requirements -

Business Goals -

Litware plans to transition to co-management for all the company-owned Windows 10 computers.

Whenever possible, Litware wants to minimize hardware and software costs.

Device Management Requirements -

Litware identifies the following device management requirements:

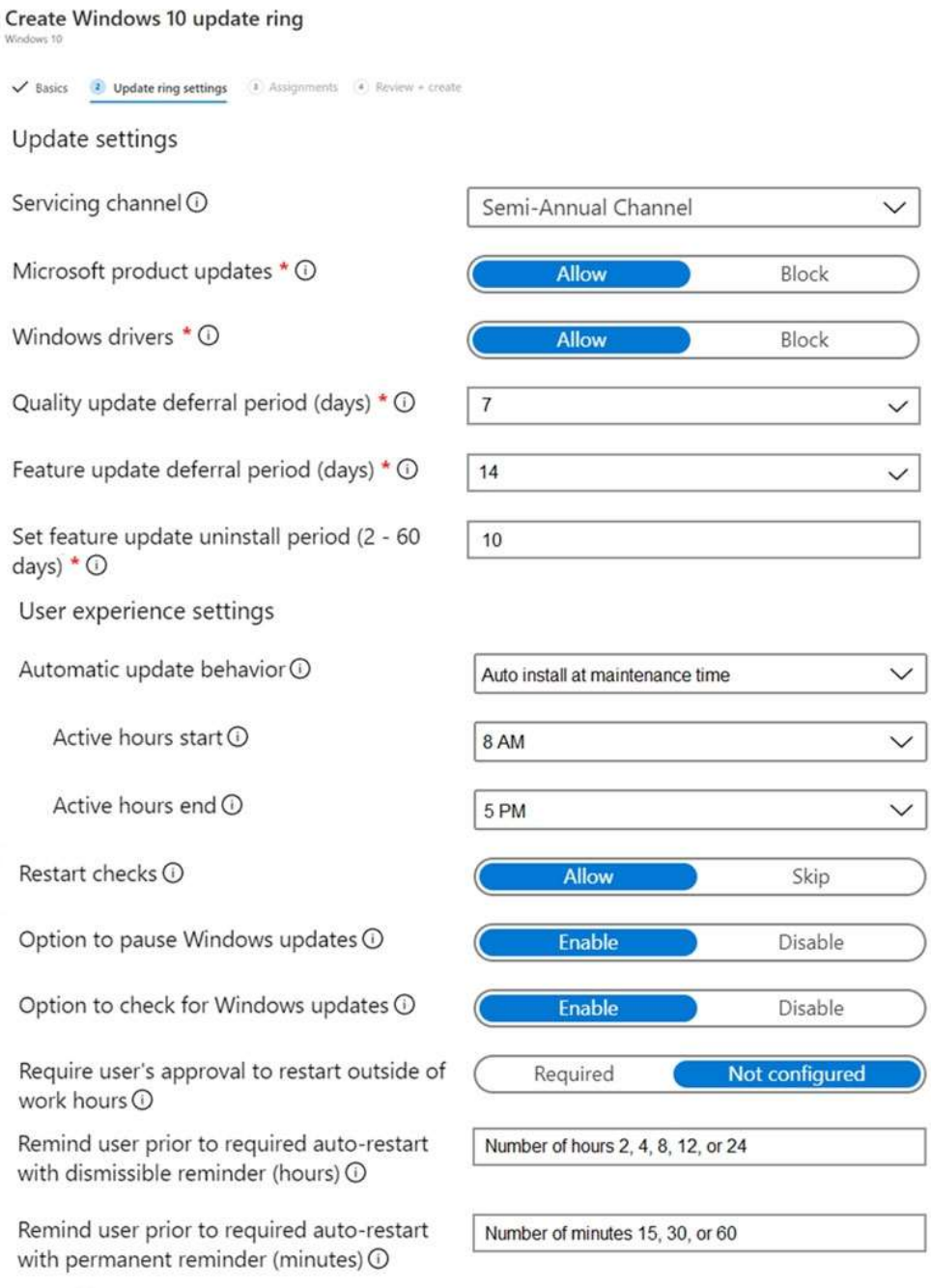
Prevent the sales department employees from forwarding email that contains bank account information.

Ensure that Microsoft Edge Favorites are accessible from all computers to which the developers sign in.
Prevent employees in the research department from copying patented information from trusted applications to untrusted applications.

Technical Requirements -
Litware identifies the following technical requirements for the planned deployment:
Re-provision the sales department computers by using Windows AutoPilot.
Ensure that the projects in Azure DevOps can be accessed from the corporate network only.
Ensure that users can sign in to the Azure AD-joined computers by using a PIN. The PIN must expire every 30 days.
Ensure that the company name and logo appears during the Out of Box Experience (OOBE) when using Windows AutoPilot.

Exhibits -

Updates -



Question
HOTSPOT -
You need to meet the OOBE requirements for Windows AutoPilot.
Which two settings should you configure from the Azure Active Directory blade? To answer, select the appropriate settings in the answer area.

NOTE: Each correct selection is worth one point.

Hot Area:

Correct Answer:

From the scenario:

Ensure that the company name and logo appears during the Out of Box Experience (OOBE) when using Windows AutoPilot.

Company Branding: When you use Windows AutoPilot to deploy new devices, you want the process to be friendly and familiar for the users going through the process. One of the ways that is done is by customizing the logon experience to include logos and company-specific text.

The basic steps:

1. Sign into the Azure Portal as a tenant admin.
2. Navigate to Azure Active Directory ג€"> Company branding.

3. Click Edit to configure the needed settings.

4. Fill in all the customizations (Including the company logo and company name)

Properties: you can set that value in the ג€Nameג€ field of the Azure AD tenant properties:

Reference:

https://blogs.technet.microsoft.com/mniehaus/2017/12/22/windows-autopilot-azure-ad-branding/

RodrigoT Highly Voted 5 months, 1 week ago

1. Company Branding: logo and background, just click on Default to edit this.
2. Properties: For Company name
CHECKED in my tenant.
Part of the picture is missing. Check the picture here:
https://vceguide.com/wp-content/uploads/2019/10/Microsoft-MD-101-date-01-06-2019-00001_Page_008_Image_0001.jpg

upvoted 6 times

AleDrinker 5 months ago

Thank you for providing the full picture!

upvoted 3 times

NZS Most Recent 5 months ago

Weird question. "Which two settings...". Only Company Branding applies

upvoted 1 times

thuba_TD 2 weeks ago

weird indeed

upvoted 1 times

Introductory Info

Case study -

This is a case study. Case studies are not timed separately. You can use as much exam time as you would like to complete each case. However, there may be additional case studies and sections on this exam. You must manage your time to ensure that you are able to complete all questions included on this exam in the time provided.

To answer the questions included in a case study, you will need to reference information that is provided in the case study. Case studies might contain exhibits and other resources that provide more information about the scenario that is described in the case study. Each question is independent of the other questions in this case study.

At the end of this case study, a review screen will appear. This screen allows you to review your answers and to make changes before you move to the next section of the exam. After you begin a new section, you cannot return to this section.

To start the case study -

To display the first question in this case study, click the Next button. Use the buttons in the left pane to explore the content of the case study before you answer the questions. Clicking these buttons displays information such as business requirements, existing environment, and problem statements. When you are ready to answer a question, click the Question button to return to the question.

General Overview -

Litware, Inc. is an international manufacturing company that has 3,000 employees. The company has sales, marketing, research, human resources (HR), development, and IT departments.

Litware has two main offices in New York and Los Angeles. Litware has five branch offices in Asia.

Existing Environment -

Current Business Model -

The Los Angeles office has 500 developers. The developers work flexible hours ranging from 11 AM to 10 PM.

Litware has a Microsoft Endpoint Configuration Manager deployment.

During discovery, the company discovers a process where users are emailing bank account information of its customers to internal and external recipients.

Current Environment -

The network contains an Active Directory domain that is synced to Microsoft Azure Active Directory (Azure AD). The functional level of the forest and the domain is

Windows Server 2012 R2. All domain controllers run Windows Server 2012 R2.

Litware has the computers shown in the following table.

Department	Windows version	Management platform	Domain-joined
Marketing	8.1	Endpoint Configuration Manager	Hybrid Azure-AD joined
Research	10	Endpoint Configuration Manager	Hybrid Azure-AD joined
HR	8.1	Endpoint Configuration Manager	Hybrid Azure-AD joined
Developers	10	Microsoft Intune	Azure AD-joined
Sales	10	Microsoft Intune	Azure AD-joined

The development department uses projects in Azure DevOps to build applications.

Most of the employees in the sales department are contractors. Each contractor is assigned a computer that runs Windows 10. At the end of each contract, the computer is assigned to a different contractor. Currently, the computers are re-provisioned manually by the IT department.

Problem Statements -

Litware identifies the following issues on the network:

Employees in the Los Angeles office report slow Internet performance when updates are downloading. The employees also report that the updates frequently consume considerable resources when they are installed. The Update settings are configured as shown in the Updates exhibit. (Click the Updates button.)

Management suspects that the source code for the proprietary applications in Azure DevOps in being shared externally.

Re-provisioning the sales department computers is too time consuming.

Requirements -

Business Goals -

Litware plans to transition to co-management for all the company-owned Windows 10 computers.

Whenever possible, Litware wants to minimize hardware and software costs.

Device Management Requirements -

Litware identifies the following device management requirements:

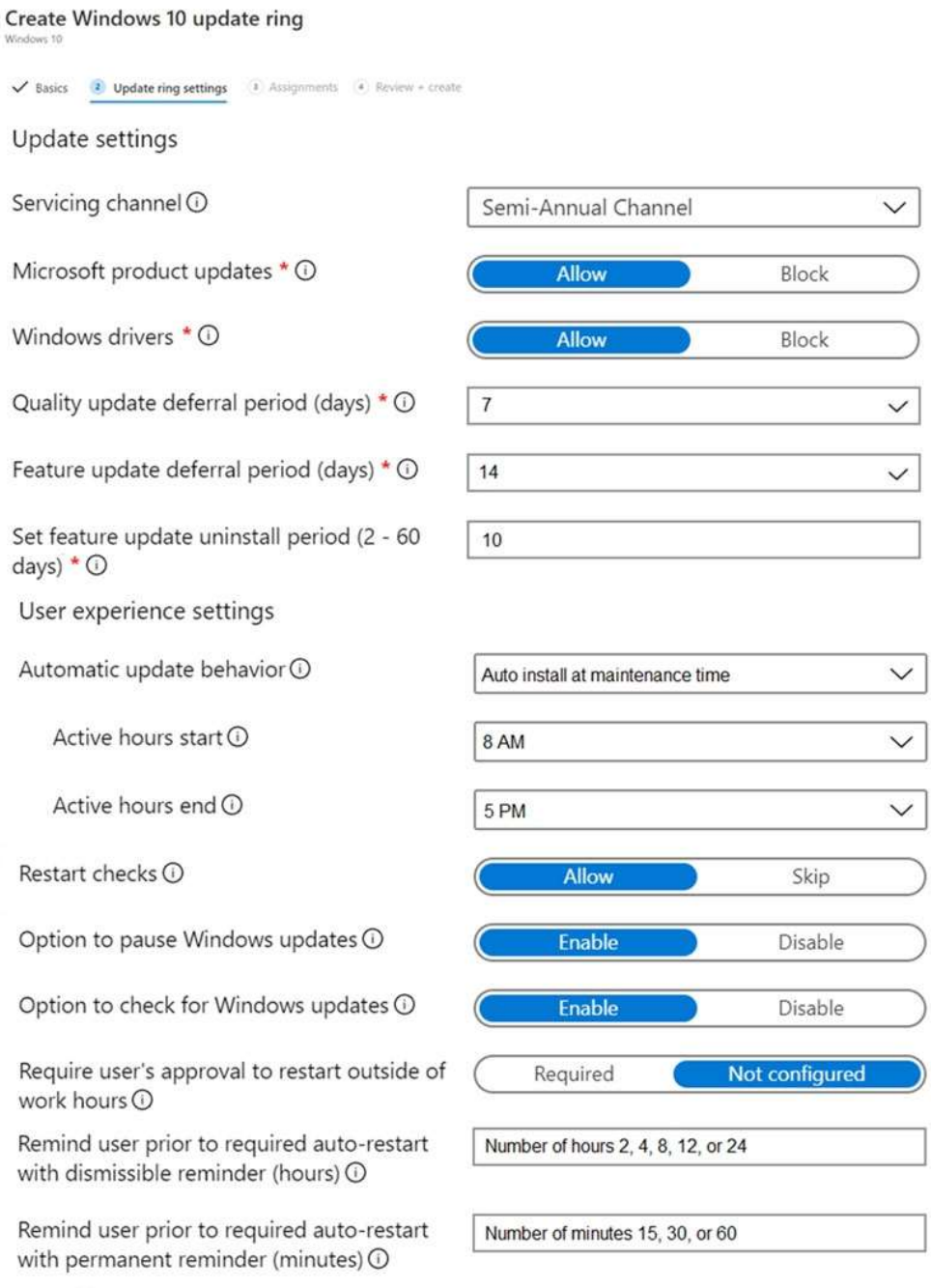
Prevent the sales department employees from forwarding email that contains bank account information.

Ensure that Microsoft Edge Favorites are accessible from all computers to which the developers sign in.
Prevent employees in the research department from copying patented information from trusted applications to untrusted applications.

Technical Requirements -
Litware identifies the following technical requirements for the planned deployment:
Re-provision the sales department computers by using Windows AutoPilot.
Ensure that the projects in Azure DevOps can be accessed from the corporate network only.
Ensure that users can sign in to the Azure AD-joined computers by using a PIN. The PIN must expire every 30 days.
Ensure that the company name and logo appears during the Out of Box Experience (OOBE) when using Windows AutoPilot.

Exhibits -

Updates -

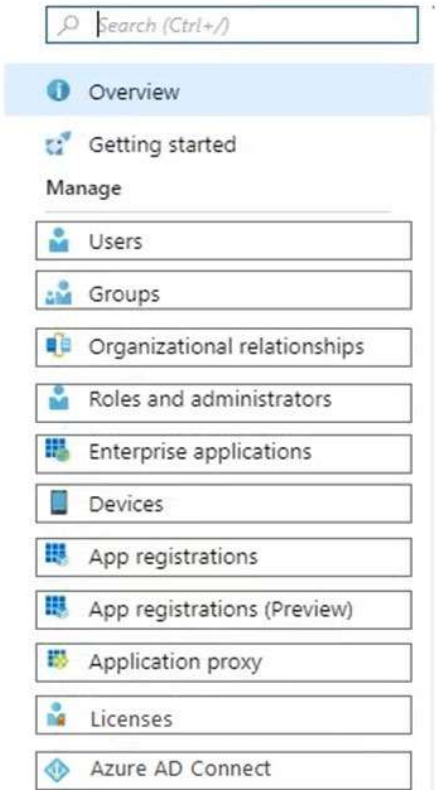


Question
HOTSPOT -
You need to meet the technical requirements for Windows AutoPilot.
Which two settings should you configure from the Azure Active Directory blade? To answer, select the appropriate settings in the answer area.

NOTE: Each correct selection is worth one point.

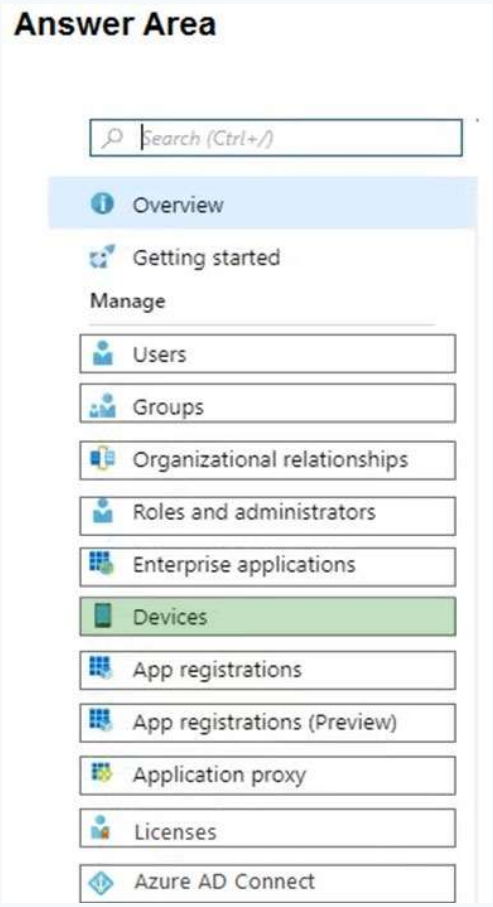
Hot Area:

Answer Area



Correct Answer:

Answer Area



1) Re-provision the sales department computers by using Windows AutoPilot.

Triggering a remote Windows Autopilot Reset

To trigger a remote Windows Autopilot Reset via Intune, follow these steps:

Navigate to Devices tab in the Intune console.

In the All devices view, select the targeted reset devices and then click More to view device actions.

Select Autopilot Reset to start the reset task.

2) Ensure that the company name and logo appears during the Out of Box Experience (OOBE) when using Windows AutoPilot.

Solve 1) by -

Solve 2) by Company branding -
Reference:
https://docs.microsoft.com/en-us/windows/deployment/windows-autopilot/windows-autopilot-reset https://docs.microsoft.com/en-za/azure/active-directory/fundamentals/customize-branding#add-company-branding-to-your-directory

RodrigoT 5 months, 1 week ago

-Users (for each user profile, set the location and apply a license)
-Devices | Device settings (select Users may join devices to Azure AD > All)
You can confirm this in the walkthrough video on this link:
https://docs.microsoft.com/en-us/mem/autopilot/configuration-requirements
The answer picture provided is wrong. Here is a correct one:
https://vceguide.com/wp-content/uploads/2020/05/Microsoft-MD-101-v2-date-05-08-2020_Page_010_Image_0001.jpg

upvoted 2 times

RodrigoT 5 months, 1 week ago

Company branding is also a necessary one time step but is not provided as part of the answer in this question. So, go for Users and Devices with peace of mind.

upvoted 1 times

Introductory Info

Case study -

This is a case study. Case studies are not timed separately. You can use as much exam time as you would like to complete each case. However, there may be additional case studies and sections on this exam. You must manage your time to ensure that you are able to complete all questions included on this exam in the time provided.

To answer the questions included in a case study, you will need to reference information that is provided in the case study. Case studies might contain exhibits and other resources that provide more information about the scenario that is described in the case study. Each question is independent of the other questions in this case study.

At the end of this case study, a review screen will appear. This screen allows you to review your answers and to make changes before you move to the next section of the exam. After you begin a new section, you cannot return to this section.

To start the case study -

To display the first question in this case study, click the Next button. Use the buttons in the left pane to explore the content of the case study before you answer the questions. Clicking these buttons displays information such as business requirements, existing environment, and problem statements. When you are ready to answer a question, click the Question button to return to the question.

General Overview -

Litware, Inc. is an international manufacturing company that has 3,000 employees. The company has sales, marketing, research, human resources (HR), development, and IT departments.

Litware has two main offices in New York and Los Angeles. Litware has five branch offices in Asia.

Existing Environment -

Current Business Model -

The Los Angeles office has 500 developers. The developers work flexible hours ranging from 11 AM to 10 PM.

Litware has a Microsoft Endpoint Configuration Manager deployment.

During discovery, the company discovers a process where users are emailing bank account information of its customers to internal and external recipients.

Current Environment -

The network contains an Active Directory domain that is synced to Microsoft Azure Active Directory (Azure AD). The functional level of the forest and the domain is

Windows Server 2012 R2. All domain controllers run Windows Server 2012 R2.

Litware has the computers shown in the following table.

Department	Windows version	Management platform	Domain-joined
Marketing	8.1	Endpoint Configuration Manager	Hybrid Azure-AD joined
Research	10	Endpoint Configuration Manager	Hybrid Azure-AD joined
HR	8.1	Endpoint Configuration Manager	Hybrid Azure-AD joined
Developers	10	Microsoft Intune	Azure AD-joined
Sales	10	Microsoft Intune	Azure AD-joined

The development department uses projects in Azure DevOps to build applications.

Most of the employees in the sales department are contractors. Each contractor is assigned a computer that runs Windows 10. At the end of each contract, the computer is assigned to a different contractor. Currently, the computers are re-provisioned manually by the IT department.

Problem Statements -

Litware identifies the following issues on the network:

Employees in the Los Angeles office report slow Internet performance when updates are downloading. The employees also report that the updates frequently consume considerable resources when they are installed. The Update settings are configured as shown in the Updates exhibit. (Click the Updates button.)

Management suspects that the source code for the proprietary applications in Azure DevOps in being shared externally.

Re-provisioning the sales department computers is too time consuming.

Requirements -

Business Goals -

Litware plans to transition to co-management for all the company-owned Windows 10 computers.

Whenever possible, Litware wants to minimize hardware and software costs.

Device Management Requirements -

Litware identifies the following device management requirements:

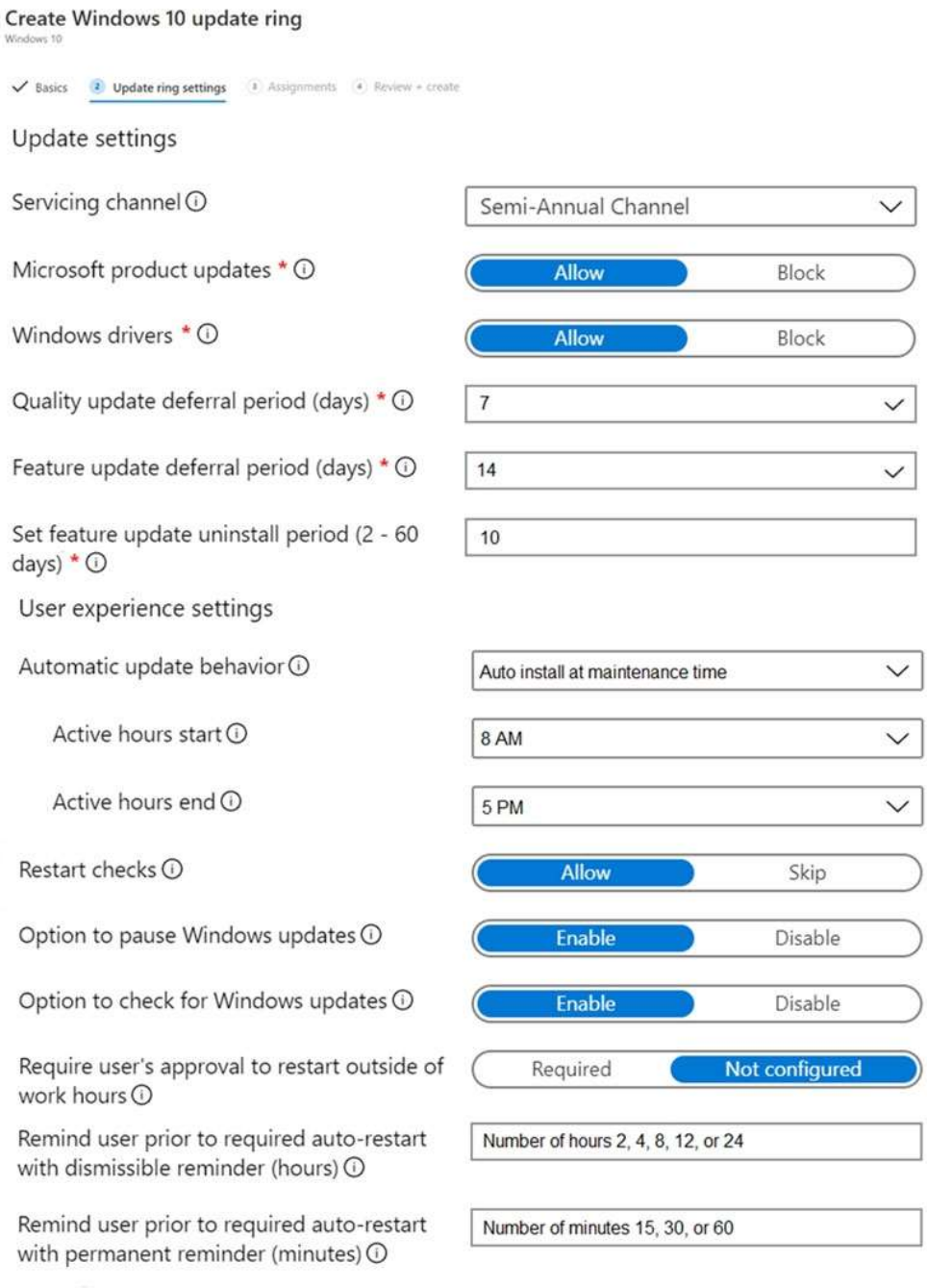
Prevent the sales department employees from forwarding email that contains bank account information.

Ensure that Microsoft Edge Favorites are accessible from all computers to which the developers sign in.
Prevent employees in the research department from copying patented information from trusted applications to untrusted applications.

Technical Requirements -
Litware identifies the following technical requirements for the planned deployment:
Re-provision the sales department computers by using Windows AutoPilot.
Ensure that the projects in Azure DevOps can be accessed from the corporate network only.
Ensure that users can sign in to the Azure AD-joined computers by using a PIN. The PIN must expire every 30 days.
Ensure that the company name and logo appears during the Out of Box Experience (OOBE) when using Windows AutoPilot.

Exhibits -

Updates -

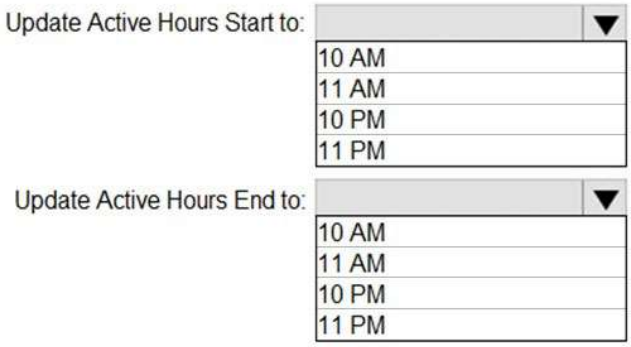


Question
HOTSPOT -
You need to resolve the performance issues in the Los Angeles office.
How should you configure the update settings? To answer, select the appropriate options in the answer area.

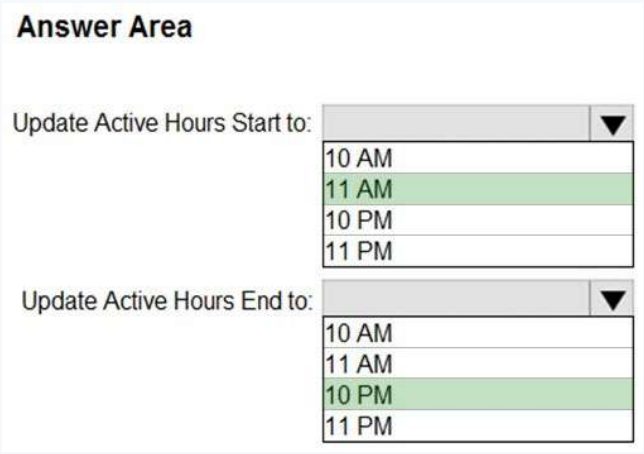
NOTE: Each correct selection is worth one point.

Hot Area:

Answer Area



Correct Answer:



The Los Angeles office has 500 developers. The developers work flexible hours ranging from 11 AM to 10 PM.

RodrigoT 5 months, 1 week ago

The answer was given in the Current Business Model section.

upvoted 1 times

Topic 7 - Testlet 10

Introductory Info

Case study -

This is a case study. Case studies are not timed separately. You can use as much exam time as you would like to complete each case. However, there may be additional case studies and sections on this exam. You must manage your time to ensure that you are able to complete all questions included on this exam in the time provided.

To answer the questions included in a case study, you will need to reference information that is provided in the case study. Case studies might contain exhibits and other resources that provide more information about the scenario that is described in the case study. Each question is independent of the other questions in this case study.

At the end of this case study, a review screen will appear. This screen allows you to review your answers and to make changes before you move to the next section of the exam. After you begin a new section, you cannot return to this section.

To start the case study -

To display the first question in this case study, click the Next button. Use the buttons in the left pane to explore the content of the case study before you answer the questions. Clicking these buttons displays information such as business requirements, existing environment, and problem statements. When you are ready to answer a question, click the Question button to return to the question.

General Overview -

Litware, Inc. is an international manufacturing company that has 3,000 employees. The company has sales, marketing, research, human resources (HR), development, and IT departments.

Litware has two main offices in New York and Los Angeles. Litware has five branch offices in Asia.

Existing Environment -

Current Business Model -

The Los Angeles office has 500 developers. The developers work flexible hours ranging from 11 AM to 10 PM.

Litware has a Microsoft Endpoint Configuration Manager deployment.

During discovery, the company discovers a process where users are emailing bank account information of its customers to internal and external recipients.

Current Environment -

The network contains an Active Directory domain that is synced to Microsoft Azure Active Directory (Azure AD). The functional level of the forest and the domain is

Windows Server 2012 R2. All domain controllers run Windows Server 2012 R2.

Litware has the computers shown in the following table.

Department	Windows version	Management platform	Domain-joined
Marketing	8.1	Endpoint Configuration Manager	Hybrid Azure-AD joined
Research	10	Endpoint Configuration Manager	Hybrid Azure-AD joined
HR	8.1	Endpoint Configuration Manager	Hybrid Azure-AD joined
Developers	10	Microsoft Intune	Azure AD-joined
Sales	10	Microsoft Intune	Azure AD-joined

The development department uses projects in Azure DevOps to build applications.

Most of the employees in the sales department are contractors. Each contractor is assigned a computer that runs Windows 10. At the end of each contract, the computer is assigned to a different contractor. Currently, the computers are re-provisioned manually by the IT department.

Problem Statements -

Litware identifies the following issues on the network:

Employees in sales department computers is too time the Los Angeles office report slow Internet performance when updates are downloading. The employees also report that the updates frequently consume considerable resources when they are installed. The Update settings are configured as shown in the Updates exhibit. (Click the Updates button.)

Management suspects that the source code for the proprietary applications in Azure DevOps in being shared externally.

Re-provisioning theconsuming.

Requirements -

Business Goals -

Litware plans to transition to co-management for all the company-owned Windows 10 computers. Whenever possible, Litware wants to minimize hardware and software costs.

Device Management Requirements -

Litware identifies the following device management requirements:

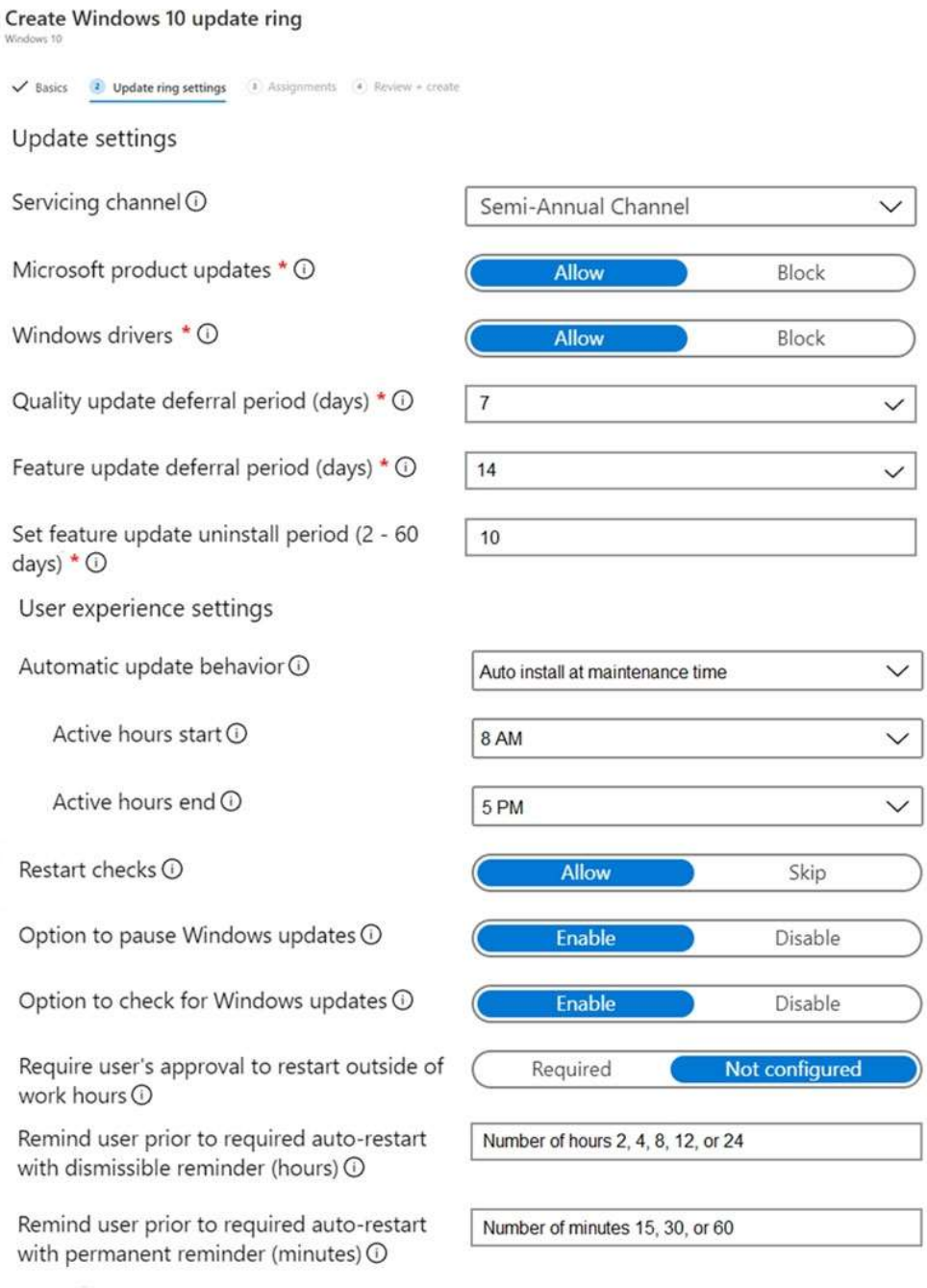
Prevent the sales department employees from forwarding email that contains bank account information.

Ensure that Microsoft Edge Favorites are accessible from all computers to which the developers sign in.
Prevent employees in the research department from copying patented information from trusted applications to untrusted applications.

Technical Requirements -
Litware identifies the following technical requirements for the planned deployment:
Re-provision the sales department computers by using Windows AutoPilot.
Ensure that the projects in Azure DevOps can be accessed from the corporate network only.
Ensure that users can sign in to the Azure AD-joined computers by using a PIN. The PIN must expire every 30 days.
Ensure that the company name and logo appears during the Out of Box Experience (OOBE) when using Windows AutoPilot.

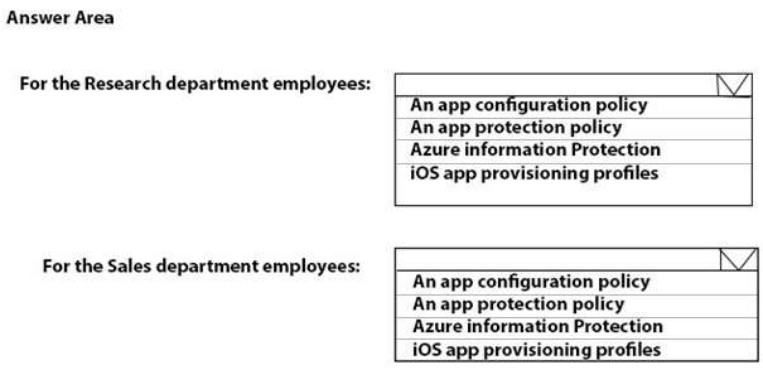
Exhibits -

Updates -

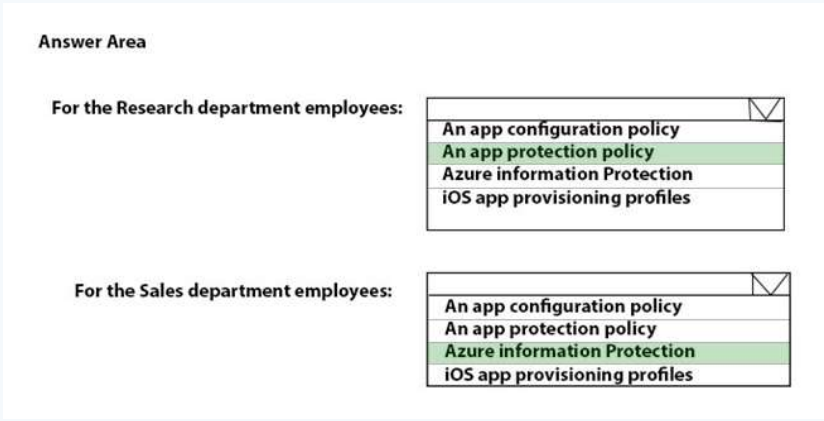


Question
HOTSPOT -
You need to recommend a solution to meet the device management requirements.
What should you include in the recommendation? To answer, select the appropriate options in the answer area.

NOTE: Each correct selection is worth one point.
Hot Area:



Correct Answer:



From the scenario:
Litware identifies the following device management requirements:
- Prevent the sales department employees from forwarding email that contains bank account information.
- Ensure that Microsoft Edge Favorites are accessible from all computers to which the developers sign in.
- Prevent employees in the research department from copying patented information from trusted applications to untrusted applications.

Box 1:
Employees in the research department must be prevented from copying patented information from trusted applications to untrusted applications. This requires an
App protection policy.
App protection policies make sure that the app-layer protections are in place. For example, you can:
- Require a PIN to open an app in a work context
- Control the sharing of data between apps

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

Box 2:
Employees in the sales department must be prevented from forwarding email that contains bank account information.
Azure Information Protection is a cloud-based solution that helps an organization to classify and optionally, protect its documents and emails by applying labels.
Labels can be applied automatically by administrators who define rules and conditions, manually by users, or a combination where users are given recommendations.
Reference:
https://docs.microsoft.com/en-us/intune/app-protection-policy https://docs.microsoft.com/en-us/azure/information-protection/what-is-information-protection

NZS 5 months ago
Correct
upvoted 1 times

RodrigoT 5 months, 1 week ago
Answers provided are correct. Read what they're asking first. Then go back to search the specific information.
upvoted 1 times

Topic 8 - Testlet 11

Introductory Info

Case study -

This is a case study. Case studies are not timed separately. You can use as much exam time as you would like to complete each case. However, there may be additional case studies and sections on this exam. You must manage your time to ensure that you are able to complete all questions included on this exam in the time provided.

To answer the questions included in a case study, you will need to reference information that is provided in the case study. Case studies might contain exhibits and other resources that provide more information about the scenario that is described in the case study. Each question is independent of the other questions in this case study.

At the end of this case study, a review screen will appear. This screen allows you to review your answers and to make changes before you move to the next section of the exam. After you begin a new section, you cannot return to this section.

To start the case study -

To display the first question in this case study, click the Next button. Use the buttons in the left pane to explore the content of the case study before you answer the questions. Clicking these buttons displays information such as business requirements, existing environment, and problem statements. When you are ready to answer a question, click the Question button to return to the question.

Overview -

Contoso, Ltd. is a consulting company that has a main office in Montreal and two branch offices in Seattle and New York.

Contoso has the users and computers shown in the following table.

Location	Users	Laptops	Desktop computers	Mobile devices
Montreal	2,500	2,800	300	3,100
Seattle	1,000	1,100	200	1,500
New York	300	320	30	400

The company has IT, human resources (HR), legal (LEG), marketing (MKG) and finance (FIN) departments.

Contoso uses Microsoft Store for Business and recently purchased a Microsoft 365 subscription.

The company is opening a new branch office in Phoenix. Most of the users in the Phoenix office will work from home.

Existing Environment -

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

All member servers run Windows Server 2016. All laptops and desktop computers run Windows 10 Enterprise.

The computers are managed by using Microsoft Endpoint Configuration Manager. The mobile devices are managed by using Microsoft Intune.

The naming convention for the computers is the department acronym, followed by a hyphen, and then four numbers, for example, FIN-6785. All the computers are joined to the on-premises Active Directory domain.

Each department has an organizational unit (OU) that contains a child OU named Computers. Each computer account is in the Computers OU of its respective department.

Intune Configuration -

The domain has the users shown in the following table.

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

User2 is a device enrollment manager (DEM) in Intune.

The devices enrolled in Intune are shown in the following table.

Name	Platform	Encryption	Member of
Device1	Android	Disabled	Group1
Device2	iOS	*Not applicable*	Group2, Group3
Device3	Android	Disabled	Group2, Group3
Device4	iOS	*Not applicable*	Group2

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

Name	Platform	Require encryption	Assigned
Policy1	Android	Not configured	Yes
Policy2	iOS	*Not applicable*	Yes
Policy3	Android	Require	Yes

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

Name	Include	Exclude
Policy1	Group3	*None*
Policy2	Group2	Group3
Policy3	Group1	*None*

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

Priority	Name	Device limit	Assigned to
1	Restriction1	15	GroupB
2	Restriction2	10	GroupA
Default	All users	5	All users

Requirements -

Planned Changes -
Contoso plans to implement the following changes:
Provide new computers to the Phoenix office users. The new computers have Windows 10 Pro preinstalled and were purchased already.
Start using a free Microsoft Store for Business app named App1.
Implement co-management for the computers.
▪

Technical Requirements -
Contoso must meet the following technical requirements:
Ensure that the users in a group named Group4 can only access Microsoft Exchange Online from devices that are enrolled in Intune.
Deploy Windows 10 Enterprise to the computers of the Phoenix office users by using Windows Autopilot.
Monitor the computers in the LEG department by using Windows Analytics.
Create a provisioning package for new computers in the HR department.
Block iOS devices from sending diagnostic and usage telemetry data.
Use the principle of least privilege whenever possible.
Enable the users in the MKG department to use App1.
Pilot co-management for the IT department.

Question
You need to meet the requirements for the MKG department users.
What should you do?

A. Assign the MKG department users the Purchaser role in Microsoft Store for Business

B. Download the APPX file for App1 from Microsoft Store for Business

C. Add App1 to the private store

D. Assign the MKG department users the Basic Purchaser role in Microsoft Store for Business

E. Acquire App1 from Microsoft Store for Business

Correct Answer: *E*
Enable the users in the MKG department to use App1.
The private store is a feature in Microsoft Store for Business and Education that organizations receive during the signup process. When admins add apps to the private store, all employees in the organization can view and download the apps. Your private store is available as a tab in Microsoft Store app, and is usually named for your company or organization. Only apps with online licenses can be added to the private store.
Reference:
https://docs.microsoft.com/en-us/microsoft-store/distribute-apps-from-your-private-store

RodrigoT 5 months, 1 week ago
Well, E. is certainly the initial step, but is not enough. You have to C.Add App1 to the private store, or the MKG department won't be able to use it. Bad question.
upvoted 1 times

TonySuccess 1 week, 3 days ago
Agreed.
upvoted 1 times

Topic 9 - Testlet 2

Introductory Info

Case study -

This is a case study. Case studies are not timed separately. You can use as much exam time as you would like to complete each case. However, there may be additional case studies and sections on this exam. You must manage your time to ensure that you are able to complete all questions included on this exam in the time provided.

To answer the questions included in a case study, you will need to reference information that is provided in the case study. Case studies might contain exhibits and other resources that provide more information about the scenario that is described in the case study. Each question is independent of the other questions in this case study.

At the end of this case study, a review screen will appear. This screen allows you to review your answers and to make changes before you move to the next section of the exam. After you begin a new section, you cannot return to this section.

To start the case study -

To display the first question in this case study, click the Next button. Use the buttons in the left pane to explore the content of the case study before you answer the questions. Clicking these buttons displays information such as business requirements, existing environment, and problem statements. When you are ready to answer a question, click the Question button to return to the question.

Overview -

Contoso, Ltd. is a consulting company that has a main office in Montreal and two branch offices in Seattle and New York.

Contoso has the users and computers shown in the following table.

Location	Users	Laptops	Desktop computers	Mobile devices
Montreal	2,500	2,800	300	3,100
Seattle	1,000	1,100	200	1,500
New York	300	320	30	400

The company has IT, human resources (HR), legal (LEG), marketing (MKG) and finance (FIN) departments.

Contoso uses Microsoft Store for Business and recently purchased a Microsoft 365 subscription.

The company is opening a new branch office in Phoenix. Most of the users in the Phoenix office will work from home.

Existing Environment -

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

All member servers run Windows Server 2016. All laptops and desktop computers run Windows 10 Enterprise.

The computers are managed by using Microsoft Endpoint Configuration Manager. The mobile devices are managed by using Microsoft Intune.

The naming convention for the computers is the department acronym, followed by a hyphen, and then four numbers, for example, FIN-6785. All the computers are joined to the on-premises Active Directory domain.

Each department has an organizational unit (OU) that contains a child OU named Computers. Each computer account is in the Computers OU of its respective department.

Intune Configuration -

The domain has the users shown in the following table.

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

User2 is a device enrollment manager (DEM) in Intune.

The devices enrolled in Intune are shown in the following table.

Name	Platform	Encryption	Member of
Device1	Android	Disabled	Group1
Device2	iOS	*Not applicable*	Group2, Group3
Device3	Android	Disabled	Group2, Group3
Device4	iOS	*Not applicable*	Group2

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

Name	Platform	Require encryption	Assigned
Policy1	Android	Not configured	Yes
Policy2	iOS	*Not applicable*	Yes
Policy3	Android	Require	Yes

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

Name	Include	Exclude
Policy1	Group3	*None*
Policy2	Group2	Group3
Policy3	Group1	*None*

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

Priority	Name	Device limit	Assigned to
1	Restriction1	15	GroupB
2	Restriction2	10	GroupA
Default	All users	5	All users

Requirements -

Planned Changes -

Contoso plans to implement the following changes:

Provide new computers to the Phoenix office users. The new computers have Windows 10 Pro preinstalled and were purchased already.

Start using a free Microsoft Store for Business app named App1.

Implement co-management for the computers.

▪

Technical Requirements -

Contoso must meet the following technical requirements:

Ensure that the users in a group named Group4 can only access Microsoft Exchange Online from devices that are enrolled in Intune.

Deploy Windows 10 Enterprise to the computers of the Phoenix office users by using Windows Autopilot.

Monitor the computers in the LEG department by using Windows Analytics.

Create a provisioning package for new computers in the HR department.

Block iOS devices from sending diagnostic and usage telemetry data.

Use the principle of least privilege whenever possible.

Enable the users in the MKG department to use App1.

Pilot co-management for the IT department.

Question

HOTSPOT -

You need to meet the technical requirements for the new HR department computers.

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

NOTE: Each correct selection is worth one point.

Hot Area:

Answer Area

Specify ComputerName as:

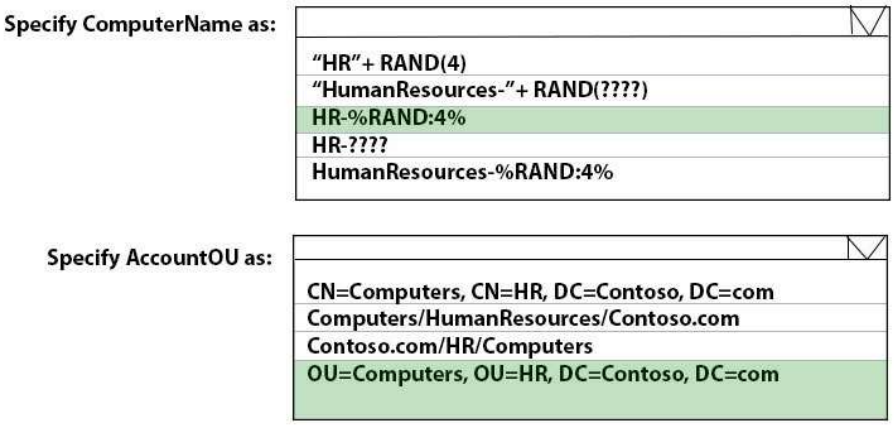
- "HR"+ RAND(4)
- "HumanResources-"+ RAND(????)
- HR-%RAND:4%
- HR-????
- HumanResources-%RAND:4%

Specify AccountOU as:

- CN=Computers, CN=HR, DC=Contoso, DC=com
- Computers/HumanResources/Contoso.com
- Contoso.com/HR/Computers
- OU=Computers, OU=HR, DC=Contoso, DC=com

Correct Answer:

Answer Area



Box 1: HR-%RAND:4%

Create a provisioning package for new computers in the HR department.

The naming convention for the computers is the department acronym, followed by a hyphen, and then four numbers, for example, FIN-6785.

Box 2: OU=Computers, OU=HR, DC=Contoso, DC=com

Each department has an organizational unit (OU) that contains a child OU named Computers. Each computer account is in the Computers OU of its respective department.

AccountOU:

Enter the full path for the organizational unit. For example: OU=testOU,DC=domain,DC=Domain,DC=com.

Name of organizational unit for the computer account

Reference:

https://docs.microsoft.com/en-us/windows/configuration/wcd/wcd-accounts

NZS 5 months ago

Correct

upvoted 1 times

RodrigoT 5 months, 1 week ago

The answers provided are correct. I got this question on a KAPLAN practice test.

upvoted 1 times

Introductory Info

Case study -

This is a case study. Case studies are not timed separately. You can use as much exam time as you would like to complete each case. However, there may be additional case studies and sections on this exam. You must manage your time to ensure that you are able to complete all questions included on this exam in the time provided.

To answer the questions included in a case study, you will need to reference information that is provided in the case study. Case studies might contain exhibits and other resources that provide more information about the scenario that is described in the case study. Each question is independent of the other questions in this case study.

At the end of this case study, a review screen will appear. This screen allows you to review your answers and to make changes before you move to the next section of the exam. After you begin a new section, you cannot return to this section.

To start the case study -

To display the first question in this case study, click the Next button. Use the buttons in the left pane to explore the content of the case study before you answer the questions. Clicking these buttons displays information such as business requirements, existing environment, and problem statements. When you are ready to answer a question, click the Question button to return to the question.

Overview -

Contoso, Ltd. is a consulting company that has a main office in Montreal and two branch offices in Seattle and New York.

Contoso has the users and computers shown in the following table.

Location	Users	Laptops	Desktop computers	Mobile devices
Montreal	2,500	2,800	300	3,100
Seattle	1,000	1,100	200	1,500
New York	300	320	30	400

The company has IT, human resources (HR), legal (LEG), marketing (MKG) and finance (FIN) departments.

Contoso uses Microsoft Store for Business and recently purchased a Microsoft 365 subscription.

The company is opening a new branch office in Phoenix. Most of the users in the Phoenix office will work from home.

Existing Environment -

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

All member servers run Windows Server 2016. All laptops and desktop computers run Windows 10 Enterprise.

The computers are managed by using Microsoft Endpoint Configuration Manager. The mobile devices are managed by using Microsoft Intune.

The naming convention for the computers is the department acronym, followed by a hyphen, and then four numbers, for example, FIN-6785. All the computers are joined to the on-premises Active Directory domain.

Each department has an organizational unit (OU) that contains a child OU named Computers. Each computer account is in the Computers OU of its respective department.

Intune Configuration -

The domain has the users shown in the following table.

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

User2 is a device enrollment manager (DEM) in Intune.

The devices enrolled in Intune are shown in the following table.

Name	Platform	Encryption	Member of
Device1	Android	Disabled	Group1
Device2	iOS	*Not applicable*	Group2, Group3
Device3	Android	Disabled	Group2, Group3
Device4	iOS	*Not applicable*	Group2

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

Name	Platform	Require encryption	Assigned
Policy1	Android	Not configured	Yes
Policy2	iOS	*Not applicable*	Yes
Policy3	Android	Require	Yes

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

Name	Include	Exclude
Policy1	Group3	*None*
Policy2	Group2	Group3
Policy3	Group1	*None*

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

Priority	Name	Device limit	Assigned to
1	Restriction1	15	GroupB
2	Restriction2	10	GroupA
Default	All users	5	All users

Requirements -

Planned Changes -
Contoso plans to implement the following changes:
Provide new computers to the Phoenix office users. The new computers have Windows 10 Pro preinstalled and were purchased already.
Start using a free Microsoft Store for Business app named App1.
Implement co-management for the computers.
▪

Technical Requirements -
Contoso must meet the following technical requirements:
Ensure that the users in a group named Group4 can only access Microsoft Exchange Online from devices that are enrolled in Intune.
Deploy Windows 10 Enterprise to the computers of the Phoenix office users by using Windows Autopilot.
Monitor the computers in the LEG department by using Windows Analytics.
Create a provisioning package for new computers in the HR department.
Block iOS devices from sending diagnostic and usage telemetry data.
Use the principle of least privilege whenever possible.
Enable the users in the MKG department to use App1.
Pilot co-management for the IT department.

Question
You need to prepare for the deployment of the Phoenix office computers.
What should you do first?

A. Extract the hardware ID information of each computer to a CSV file and upload the file from the Microsoft Endpoint Management admin center.

B. Extract the serial number information of each computer to a XML file and upload the file from the Microsoft Endpoint Management admin center.

C. Extract the serial number information of each computer to a CSV file and upload the file from the Microsoft Endpoint Management admin center.

D. Generalize the computers and configure the Device settings from the Azure Active Directory admin center.

Correct Answer: *A*
To manage devices through Microsoft Store for Business and Education, you'll need a .csv file that contains specific information about the devices. You should be able to get this from your Microsoft account contact, or the store where you purchased the devices. Upload the .csv file to Microsoft Store to add the devices.
Note:
Provide new computers to the Phoenix office users. The new computers have Windows 10 Pro preinstalled and were purchased already.
Deploy Windows 10 Enterprise to the computers of the Phoenix office users by using Windows Autopilot.
Reference:
https://docs.microsoft.com/en-us/microsoft-store/add-profile-to-devices

TonySuccess 1 week, 3 days ago
Selected Answer: C
CCCCCCCCCC
upvoted 1 times

AVR31 5 months ago
Selected Answer: C
Bad question.
Neither is complete and correct. You need the serial number and the hardware hash.
But, as RodrigoT said, C comes close.
upvoted 1 times

NZS 5 months ago

Correct

upvoted 1 times

RodrigoT 5 months, 1 week ago

Selected Answer: C

The answer provided (A) is wrong. This has nothing to do with hardware ID (don't confuse it with hardware hash).
You have to Extract the serial number. It's there on their own link:
https://docs.microsoft.com/en-us/microsoft-store/add-profile-to-devices#add-devices-and-apply-autopilot-deployment-profile

upvoted 1 times

Introductory Info

Case study -

This is a case study. Case studies are not timed separately. You can use as much exam time as you would like to complete each case. However, there may be additional case studies and sections on this exam. You must manage your time to ensure that you are able to complete all questions included on this exam in the time provided.

To answer the questions included in a case study, you will need to reference information that is provided in the case study. Case studies might contain exhibits and other resources that provide more information about the scenario that is described in the case study. Each question is independent of the other questions in this case study.

At the end of this case study, a review screen will appear. This screen allows you to review your answers and to make changes before you move to the next section of the exam. After you begin a new section, you cannot return to this section.

To start the case study -

To display the first question in this case study, click the Next button. Use the buttons in the left pane to explore the content of the case study before you answer the questions. Clicking these buttons displays information such as business requirements, existing environment, and problem statements. When you are ready to answer a question, click the Question button to return to the question.

Overview -

Contoso, Ltd. is a consulting company that has a main office in Montreal and two branch offices in Seattle and New York.

Contoso has the users and computers shown in the following table.

Location	Users	Laptops	Desktop computers	Mobile devices
Montreal	2,500	2,800	300	3,100
Seattle	1,000	1,100	200	1,500
New York	300	320	30	400

The company has IT, human resources (HR), legal (LEG), marketing (MKG) and finance (FIN) departments.

Contoso uses Microsoft Store for Business and recently purchased a Microsoft 365 subscription.

The company is opening a new branch office in Phoenix. Most of the users in the Phoenix office will work from home.

Existing Environment -

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

All member servers run Windows Server 2016. All laptops and desktop computers run Windows 10 Enterprise.

The computers are managed by using Microsoft Endpoint Configuration Manager. The mobile devices are managed by using Microsoft Intune.

The naming convention for the computers is the department acronym, followed by a hyphen, and then four numbers, for example, FIN-6785. All the computers are joined to the on-premises Active Directory domain.

Each department has an organizational unit (OU) that contains a child OU named Computers. Each computer account is in the Computers OU of its respective department.

Intune Configuration -

The domain has the users shown in the following table.

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

User2 is a device enrollment manager (DEM) in Intune.

The devices enrolled in Intune are shown in the following table.

Name	Platform	Encryption	Member of
Device1	Android	Disabled	Group1
Device2	iOS	*Not applicable*	Group2, Group3
Device3	Android	Disabled	Group2, Group3
Device4	iOS	*Not applicable*	Group2

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

Name	Platform	Require encryption	Assigned
Policy1	Android	Not configured	Yes
Policy2	iOS	*Not applicable*	Yes
Policy3	Android	Require	Yes

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

Name	Include	Exclude
Policy1	Group3	*None*
Policy2	Group2	Group3
Policy3	Group1	*None*

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

Priority	Name	Device limit	Assigned to
1	Restriction1	15	GroupB
2	Restriction2	10	GroupA
Default	All users	5	All users

Requirements -

Planned Changes -
Contoso plans to implement the following changes:
Provide new computers to the Phoenix office users. The new computers have Windows 10 Pro preinstalled and were purchased already.
Start using a free Microsoft Store for Business app named App1.
Implement co-management for the computers.
▪

Technical Requirements -
Contoso must meet the following technical requirements:
Ensure that the users in a group named Group4 can only access Microsoft Exchange Online from devices that are enrolled in Intune.
Deploy Windows 10 Enterprise to the computers of the Phoenix office users by using Windows Autopilot.
Monitor the computers in the LEG department by using Windows Analytics.
Create a provisioning package for new computers in the HR department.
Block iOS devices from sending diagnostic and usage telemetry data.
Use the principle of least privilege whenever possible.
Enable the users in the MKG department to use App1.
Pilot co-management for the IT department.

Question
You need to prepare for the deployment of the Phoenix office computers.
What should you do first?

A. Generalize the computers and configure the Mobility (MDM and MAM) settings from the Azure Active Directory admin center.

B. Extract the hardware ID information of each computer to a CSV file and upload the file from the Microsoft Intune blade in the Azure portal.

C. Extract the hardware ID information of each computer to an XML file and upload the file from the Devices settings in Microsoft Store for Business.

D. Extract the serial number information of each computer to a CSV file and upload the file from the Microsoft Intune blade in the Azure portal.

Correct Answer: *A*
Windows Autopilot Deployment for existing devices.
Configure the Enrollment Status Page.
If you want, you can set up an enrollment status page for Autopilot using Intune.
To enable and configure the enrollment and status page:
1. Open Intune in the Azure portal.
2. Access Intune > Device enrollment > Windows enrollment and Set up an enrollment status page.
3. Access Azure Active Directory > Mobility (MDM and MAM) > Microsoft Intune and Configure automatic MDM enrollment and configure the MDM user scope for some or all users.
Note:
Provide new computers to the Phoenix office users. The new computers have Windows 10 Pro preinstalled and were purchased already.
Deploy Windows 10 Enterprise to the computers of the Phoenix office users by using Windows Autopilot.
Reference:
https://docs.microsoft.com/en-us/microsoft-store/add-profile-to-devices https://docs.microsoft.com/en-us/windows/deployment/windows-autopilot/existing-devices

TonySuccess 3 days, 3 hours ago
TRASH, please remove.
upvoted 1 times

thuba_TD 1 week, 6 days ago
Hoekom
upvoted 1 times

RodrigoT 5 months, 1 week ago

This question is so outdated. It's impossible to do any of these under Azure portal. You have to use Endpoint for everything. B and C are totally wrong. I would vote for D if it was under Endpoint.
A. could be the first step, also under Endpoint, but, generalize new computers just bough? Why? We are using Autopilot, not deploying images.

https://docs.microsoft.com/en-us/mem/autopilot/existing-devices#procedures

upvoted 1 times

Introductory Info

Case study -

This is a case study. Case studies are not timed separately. You can use as much exam time as you would like to complete each case. However, there may be additional case studies and sections on this exam. You must manage your time to ensure that you are able to complete all questions included on this exam in the time provided.

To answer the questions included in a case study, you will need to reference information that is provided in the case study. Case studies might contain exhibits and other resources that provide more information about the scenario that is described in the case study. Each question is independent of the other questions in this case study.

At the end of this case study, a review screen will appear. This screen allows you to review your answers and to make changes before you move to the next section of the exam. After you begin a new section, you cannot return to this section.

To start the case study -

To display the first question in this case study, click the Next button. Use the buttons in the left pane to explore the content of the case study before you answer the questions. Clicking these buttons displays information such as business requirements, existing environment, and problem statements. When you are ready to answer a question, click the Question button to return to the question.

Overview -

Contoso, Ltd. is a consulting company that has a main office in Montreal and two branch offices in Seattle and New York.

Contoso has the users and computers shown in the following table.

Location	Users	Laptops	Desktop computers	Mobile devices
Montreal	2,500	2,800	300	3,100
Seattle	1,000	1,100	200	1,500
New York	300	320	30	400

The company has IT, human resources (HR), legal (LEG), marketing (MKG) and finance (FIN) departments.

Contoso uses Microsoft Store for Business and recently purchased a Microsoft 365 subscription.

The company is opening a new branch office in Phoenix. Most of the users in the Phoenix office will work from home.

Existing Environment -

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

All member servers run Windows Server 2016. All laptops and desktop computers run Windows 10 Enterprise.

The computers are managed by using Microsoft Endpoint Configuration Manager. The mobile devices are managed by using Microsoft Intune.

The naming convention for the computers is the department acronym, followed by a hyphen, and then four numbers, for example, FIN-6785. All the computers are joined to the on-premises Active Directory domain.

Each department has an organizational unit (OU) that contains a child OU named Computers. Each computer account is in the Computers OU of its respective department.

Intune Configuration -

The domain has the users shown in the following table.

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

User2 is a device enrollment manager (DEM) in Intune.

The devices enrolled in Intune are shown in the following table.

Name	Platform	Encryption	Member of
Device1	Android	Disabled	Group1
Device2	iOS	*Not applicable*	Group2, Group3
Device3	Android	Disabled	Group2, Group3
Device4	iOS	*Not applicable*	Group2

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

Name	Platform	Require encryption	Assigned
Policy1	Android	Not configured	Yes
Policy2	iOS	*Not applicable*	Yes
Policy3	Android	Require	Yes

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

Name	Include	Exclude
Policy1	Group3	*None*
Policy2	Group2	Group3
Policy3	Group1	*None*

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

Priority	Name	Device limit	Assigned to
1	Restriction1	15	GroupB
2	Restriction2	10	GroupA
Default	All users	5	All users

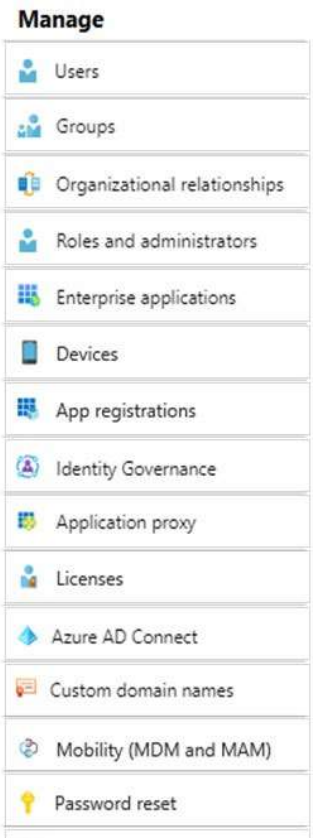
Requirements -

Planned Changes -
Contoso plans to implement the following changes:
Provide new computers to the Phoenix office users. The new computers have Windows 10 Pro preinstalled and were purchased already.
Start using a free Microsoft Store for Business app named App1.
Implement co-management for the computers.
▪

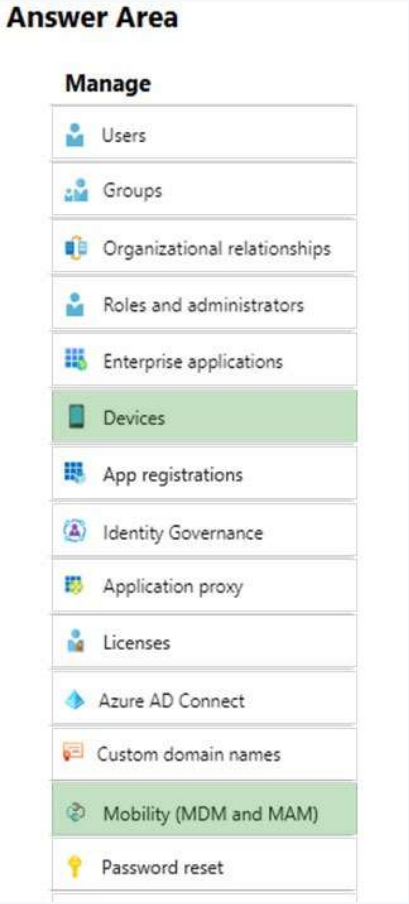
Technical Requirements -
Contoso must meet the following technical requirements:
Ensure that the users in a group named Group4 can only access Microsoft Exchange Online from devices that are enrolled in Intune.
Deploy Windows 10 Enterprise to the computers of the Phoenix office users by using Windows Autopilot.
Monitor the computers in the LEG department by using Windows Analytics.
Create a provisioning package for new computers in the HR department.
Block iOS devices from sending diagnostic and usage telemetry data.
Use the principle of least privilege whenever possible.
Enable the users in the MKG department to use App1.
Pilot co-management for the IT department.

Question
HOTSPOT -
You need to meet the technical requirements for Windows Autopilot.
Which two settings should you configure from the Azure Active Directory blade? To answer, select the appropriate settings in the answer area.
NOTE: Each correct selection is worth one point.
Hot Area:

Answer Area



Correct Answer:



Box 1: Devices -

Note: Deploy Windows 10 Enterprise to the computers of the Phoenix office users by using Windows Autopilot.

Configure device settings -

If you want to manage device identities by using the Azure portal, the devices need to be either registered or joined to Azure AD. As an administrator, you can control the process of registering and joining devices by configuring device settings.

Box 2: Mobility (MDM and MAM)

Windows Autopilot Deployment for existing devices.

Configure the Enrollment Status Page.

If you want, you can set up an enrollment status page for Autopilot using Intune.

To enable and configure the enrollment and status page:

1) Open Intune in the Azure portal.

2) Access Intune > Device enrollment > Windows enrollment and Set up an enrollment status page.

3) Access Azure Active Directory > Mobility (MDM and MAM) > Microsoft Intune and Configure automatic MDM enrollment and configure the MDM user scope for some or all users.

Reference:

https://docs.microsoft.com/en-us/azure/active-directory/devices/device-management-azure-portal#configure-device-settings

https://docs.microsoft.com/en-us/mem/autopilot/existing-devices

TonySuccess 3 days, 3 hours ago

Users and Devices was my choice.

upvoted 1 times

RodrigoT 5 months, 1 week ago

Since Configure the Enrollment Status Page (MDM and MAM) is optional, yes, check here: https://docs.microsoft.com/en-us/mem/autopilot/existing-devices#configure-the-enrollment-status-page-optional
I would go for Users and Devices. These are mandatory steps explained in this walkthrough video on this link: https://docs.microsoft.com/en-us/mem/autopilot/configuration-requirements

upvoted 2 times

Topic 10 - Testlet 3

Introductory Info

Case study -

This is a case study. Case studies are not timed separately. You can use as much exam time as you would like to complete each case. However, there may be additional case studies and sections on this exam. You must manage your time to ensure that you are able to complete all questions included on this exam in the time provided.

To answer the questions included in a case study, you will need to reference information that is provided in the case study. Case studies might contain exhibits and other resources that provide more information about the scenario that is described in the case study. Each question is independent of the other questions in this case study.

At the end of this case study, a review screen will appear. This screen allows you to review your answers and to make changes before you move to the next section of the exam. After you begin a new section, you cannot return to this section.

To start the case study -

To display the first question in this case study, click the Next button. Use the buttons in the left pane to explore the content of the case study before you answer the questions. Clicking these buttons displays information such as business requirements, existing environment, and problem statements. If the case study has an

All Information tab, note that the information displayed is identical to the information displayed on the subsequent tabs. When you are ready to answer a question, click the Question button to return to the question.

Overview -

Contoso, Ltd. is a consulting company that has a main office in Montreal and branch offices in Seattle and New York.

Contoso has a Microsoft 365 E5 subscription.

Environment -

Network Environment -

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

Name	Operating system	Role
DC1	Windows Server 2019	Domain controller
Server1	Windows Server 2016	Member server
Server2	Windows Server 2019	Member server

Contoso has a hybrid Azure Active Directory (Azure AD) tenant named contoso.com.

Contoso has a Microsoft Store for Business instance.

Users and Groups -

The contoso.com tenant contains the users shown in the following table.

Name	Azure AD role	Microsoft Store for Business role	Member of
User1	Cloud device administrator	Basic Purchaser	GroupA
User2	Azure AD joined device local administrator	Device Guard signer	GroupB
User3	Global reader	Purchaser	GroupA, GroupB
User4	Global administrator	None	Group1

All users are assigned a Microsoft Office 365 license and an Enterprise Mobility + Security E3 license.

Enterprise State Roaming is enabled for Group1 and GroupA.

Group1 and Group2 have a Membership type of Assigned.

Devices -

Contoso has the Windows 10 devices shown in the following table.

Name	Type	Member of	Scope (Tags)
Device1	Corporate-owned	Group1	Default
Device2	Corporate-owned	Group1, Group2	Tag2
Device3	Personally-owned	Group1	Tag1
Device4	Personally-owned	Group2	Tag2
Device5	Corporate-owned	Group3	Default

The Windows 10 devices are joined to Azure AD and enrolled in Microsoft Intune.

The Windows 10 devices are configured as shown in the following table.

Name	BitLocker Drive Encryption (BitLocker)	Secure Boot	VPN connection
Device1	Yes	No	VPN1
Device2	Yes	Yes	VPN1, VPN3
Device3	No	No	VPN3
Device4	No	Yes	**None**
Device5	Yes	No	**None**

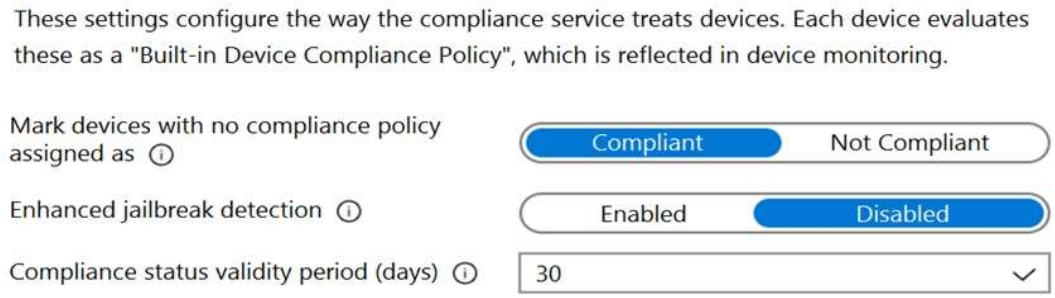
All the Azure AD joined devices have an executable file named C:\AppA.exe and a folder named D:\Folder1.

Microsoft Endpoint Manager Configuration

Microsoft Endpoint Manager has the compliance policies shown in the following table.

Name	Configuration	Assignment
Policy1	Require BitLocker only	Group1
Policy2	Require Secure Boot only	Group1
Policy3	Require BitLocker and Secure Boot	Group2

The Compliance policy settings are shown in the following exhibit.



The Automatic Enrollment settings have the following configurations:

MDM user scope: GroupA

MAM user scope: GroupB

You have an Endpoint protection configuration profile that has the following Controlled folder access settings:

Name: Protection1

Folder protection: Enable

List of apps that have access to protected folders: C:*\AppA.exe

List of additional folders that need to be protected: D:\Folder1

Assignments:

- Included groups: Group2, GroupB

Windows Autopilot Configuration -

Contoso has a Windows Autopilot deployment profile configured as shown in the following exhibit.

Create profile
Windows PC

✓ Basics ✓ Out-of-box experience (OOBE) ✓ Assignments 4 **Review + create**

Summary

Basics

Name	Profile1
Description	--
Convert all targeted devices to Autopilot	Yes
Device type	Windows PC

Out-of-box experience (OOBE)

Deployment mode	User-Driven
Join to Azure AD as	Azure AD joined
Skip AD connectivity check (preview)	No
Language (Region)	Operating system default
Automatically configure keyboard	Yes
Microsoft Software License Terms	Hide
Privacy settings	Hide
Hide change account options	Hide
User account type	Standard
Allow White Glove OOBE	No
Apply device name template	No

Assignments

Included groups	Group1
Excluded groups	Group2

Currently, there are no devices deployed by using Window Autopilot.
The Intune connector for Active Directory is installed on Server1.

Requirements -

Planned Changes -
Contoso plans to implement the following changes:
Purchase a new Windows 10 device named Device6 and enroll the device in Intune.
New computers will be deployed by using Windows Autopilot and will be hybrid Azure AD joined.
Deploy a network boundary configuration profile that will have the following settings:
- Name: Boundary1
- Network boundary: 192.168.1.0/24
- Scope tags: Tag1
- Assignments:
- - Included groups: Group1, Group2
Deploy two VPN configuration profiles named Connection1 and Connection2 that will have the following settings:
- Name: Connection1
- Connection name: VPN1
- Connection type: L2TP
- Assignments:
- - Included groups: Group1, Group2, GroupA
- - Excluded groups: --
- Name: Connection2
- Connection name: VPN2
- Connection type: IKEv2
- Assignments:
- - Included groups: GroupA
- - Excluded groups: GroupB
Purchase an app named App1 that is available in Microsoft Store for Business and to assign the app to all the users.

Technical Requirements -
Contoso must meet the following technical requirements:
Users in GroupA must be able to deploy new computers.
Administrative effort must be minimized.

Question

HOTSPOT -

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 adds a shortcut to the desktop of Device1, when User1 signs in to Device3, the same shortcut will appear on the desktop.	○	○
If User1 sets the desktop background to blue on Device2, when User1 signs in to Device4, the desktop background will be blue.	○	○
If User2 increases the size of the font in the command prompt of Device2, when User2 signs in to Device3, the command prompt will show the increased font size.	○	○

Correct Answer:

Answer Area

Statements	Yes	No
If User1 adds a shortcut to the desktop of Device1, when User1 signs in to Device3, the same shortcut will appear on the desktop.	●	○
If User1 sets the desktop background to blue on Device2, when User1 signs in to Device4, the desktop background will be blue.	○	●
If User2 increases the size of the font in the command prompt of Device2, when User2 signs in to Device3, the command prompt will show the increased font size.	○	●

NZS 5 months ago

Should be No, No, No as ESR doesn't apply on Personal owned devices

upvoted 1 times

RodrigoT 5 months, 1 week ago

No- User1 is in GroupA, but Device3 is Personally-owned
No- User1 is in GroupA, but Device4 is Personally-owned
No- User2 is in GroupB and Device3 is Personally-owned
You can only add groups of users on Enterprise State Roaming, not groups of devices.
If a device is Personally-owned you shouldn't be able to sign-in with an Azure AD account.

upvoted 1 times

RodrigoT 5 months ago

On the other hand the question says that: the Windows 10 devices are joined to Azure AD. So, if they are JOINED, even if some are personally-owned, the ESR should work. In this case the answer could be:
Yes- because a desktop shortcut to an existent app on the computers would sync. But not a shortcut to a file.
Yes- Because settings on the desktop are synced.
No- Because User2 is in GroupB.
Anyway, I don't believe this kind of question would appear on the exam from May 3rd, 2022 because user profiles is excluded. Check here:
https://docs.microsoft.com/en-us/learn/certifications/exams/md-101
by clicking on Download exam skills outline

upvoted 1 times

Introductory Info

Case study -

This is a case study. Case studies are not timed separately. You can use as much exam time as you would like to complete each case. However, there may be additional case studies and sections on this exam. You must manage your time to ensure that you are able to complete all questions included on this exam in the time provided.

To answer the questions included in a case study, you will need to reference information that is provided in the case study. Case studies might contain exhibits and other resources that provide more information about the scenario that is described in the case study. Each question is independent of the other questions in this case study.

At the end of this case study, a review screen will appear. This screen allows you to review your answers and to make changes before you move to the next section of the exam. After you begin a new section, you cannot return to this section.

To start the case study -

To display the first question in this case study, click the Next button. Use the buttons in the left pane to explore the content of the case study before you answer the questions. Clicking these buttons displays information such as business requirements, existing environment, and problem statements. If the case study has an

All Information tab, note that the information displayed is identical to the information displayed on the subsequent tabs. When you are ready to answer a question, click the Question button to return to the question.

Overview -

Contoso, Ltd. is a consulting company that has a main office in Montreal and branch offices in Seattle and New York.

Contoso has a Microsoft 365 E5 subscription.

Environment -

Network Environment -

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

Name	Operating system	Role
DC1	Windows Server 2019	Domain controller
Server1	Windows Server 2016	Member server
Server2	Windows Server 2019	Member server

Contoso has a hybrid Azure Active Directory (Azure AD) tenant named contoso.com.

Contoso has a Microsoft Store for Business instance.

Users and Groups -

The contoso.com tenant contains the users shown in the following table.

Name	Azure AD role	Microsoft Store for Business role	Member of
User1	Cloud device administrator	Basic Purchaser	GroupA
User2	Azure AD joined device local administrator	Device Guard signer	GroupB
User3	Global reader	Purchaser	GroupA, GroupB
User4	Global administrator	None	Group1

All users are assigned a Microsoft Office 365 license and an Enterprise Mobility + Security E3 license.

Enterprise State Roaming is enabled for Group1 and GroupA.

Group1 and Group2 have a Membership type of Assigned.

Devices -

Contoso has the Windows 10 devices shown in the following table.

Name	Type	Member of	Scope (Tags)
Device1	Corporate-owned	Group1	Default
Device2	Corporate-owned	Group1, Group2	Tag2
Device3	Personally-owned	Group1	Tag1
Device4	Personally-owned	Group2	Tag2
Device5	Corporate-owned	Group3	Default

The Windows 10 devices are joined to Azure AD and enrolled in Microsoft Intune.

The Windows 10 devices are configured as shown in the following table.

Name	BitLocker Drive Encryption (BitLocker)	Secure Boot	VPN connection
Device1	Yes	No	VPN1
Device2	Yes	Yes	VPN1, VPN3
Device3	No	No	VPN3
Device4	No	Yes	**None**
Device5	Yes	No	**None**

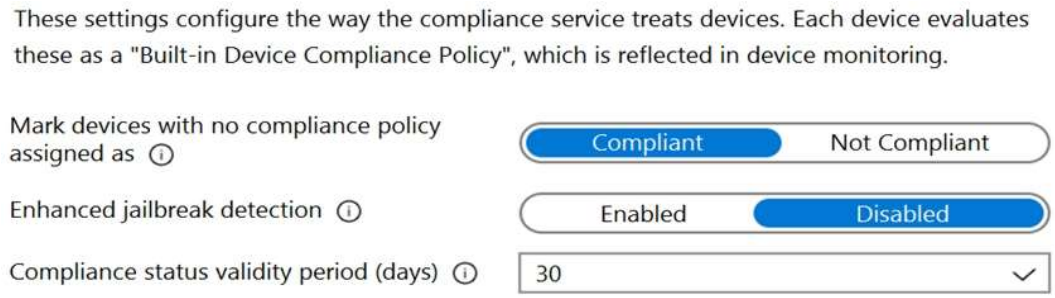
All the Azure AD joined devices have an executable file named C:\AppA.exe and a folder named D:\Folder1.

Microsoft Endpoint Manager Configuration

Microsoft Endpoint Manager has the compliance policies shown in the following table.

Name	Configuration	Assignment
Policy1	Require BitLocker only	Group1
Policy2	Require Secure Boot only	Group1
Policy3	Require BitLocker and Secure Boot	Group2

The Compliance policy settings are shown in the following exhibit.



The Automatic Enrollment settings have the following configurations:

MDM user scope: GroupA

MAM user scope: GroupB

You have an Endpoint protection configuration profile that has the following Controlled folder access settings:

Name: Protection1

Folder protection: Enable

List of apps that have access to protected folders: C:*\AppA.exe

List of additional folders that need to be protected: D:\Folder1

Assignments:

- Included groups: Group2, GroupB

Windows Autopilot Configuration -

Contoso has a Windows Autopilot deployment profile configured as shown in the following exhibit.

Create profile
Windows PC

✓ Basics ✓ Out-of-box experience (OOBE) ✓ Assignments 4 **Review + create**

Summary

Basics

Name	Profile1
Description	--
Convert all targeted devices to Autopilot	Yes
Device type	Windows PC

Out-of-box experience (OOBE)

Deployment mode	User-Driven
Join to Azure AD as	Azure AD joined
Skip AD connectivity check (preview)	No
Language (Region)	Operating system default
Automatically configure keyboard	Yes
Microsoft Software License Terms	Hide
Privacy settings	Hide
Hide change account options	Hide
User account type	Standard
Allow White Glove OOBE	No
Apply device name template	No

Assignments

Included groups	Group1
Excluded groups	Group2

Currently, there are no devices deployed by using Window Autopilot.
The Intune connector for Active Directory is installed on Server1.

Requirements -

Planned Changes -
Contoso plans to implement the following changes:
Purchase a new Windows 10 device named Device6 and enroll the device in Intune.
New computers will be deployed by using Windows Autopilot and will be hybrid Azure AD joined.
Deploy a network boundary configuration profile that will have the following settings:
- Name: Boundary1
- Network boundary: 192.168.1.0/24
- Scope tags: Tag1
- Assignments:
- - Included groups: Group1, Group2
Deploy two VPN configuration profiles named Connection1 and Connection2 that will have the following settings:
- Name: Connection1
- Connection name: VPN1
- Connection type: L2TP
- Assignments:
- - Included groups: Group1, Group2, GroupA
- - Excluded groups: --
- Name: Connection2
- Connection name: VPN2
- Connection type: IKEv2
- Assignments:
- - Included groups: GroupA
- - Excluded groups: GroupB
Purchase an app named App1 that is available in Microsoft Store for Business and to assign the app to all the users.

Technical Requirements -
Contoso must meet the following technical requirements:
Users in GroupA must be able to deploy new computers.
Administrative effort must be minimized.

Question

You need to ensure that computer objects can be created as part of the Windows Autopilot deployment. The solution must meet the technical requirements.
To what should you grant the right to create the computer objects?

A. Server2

B. Server1

Topic 11 - Testlet 4

D. DC1

Correct Answer: *B*
Scenario:
The Intune connector for Active Directory is installed on Server1.
Contoso must meet the following technical requirements:
Users in GroupA must be able to deploy new computers.
Administrative effort must be minimized.
Note: To be clear, the entire domain join process will work without any direct connection to the on-premise network and domain controllers. The computer object is created on-premises through the Intune Connector for Active Directory triggered by the Windows Autopilot and Intune.
Reference:
https://blog.matrixpost.net/set-up-windows-autopilot-production-environment-part-2/

rockhound 1 week, 4 days ago
But why not server 2? This is also a member server. MS says its better to install the Intune Connector on multiple servers.
upvoted 1 times

NZS 5 months ago
Correct. Server1 has the Intune connector installed
upvoted 1 times

RodrigoT 5 months, 1 week ago
Selected Answer: B
Correct answer, but the link provided is painful. Better have the official documentation:
https://docs.microsoft.com/en-us/mem/autopilot/windows-autopilot-hybrid#increase-the-computer-account-limit-in-the-organizational-unit
"The computer that hosts the Intune Connector must have the rights to create the computer objects within the domain."
upvoted 1 times

Introductory Info

Case study -

This is a case study. Case studies are not timed separately. You can use as much exam time as you would like to complete each case. However, there may be additional case studies and sections on this exam. You must manage your time to ensure that you are able to complete all questions included on this exam in the time provided.

To answer the questions included in a case study, you will need to reference information that is provided in the case study. Case studies might contain exhibits and other resources that provide more information about the scenario that is described in the case study. Each question is independent of the other questions in this case study.

At the end of this case study, a review screen will appear. This screen allows you to review your answers and to make changes before you move to the next section of the exam. After you begin a new section, you cannot return to this section.

To start the case study -

To display the first question in this case study, click the Next button. Use the buttons in the left pane to explore the content of the case study before you answer the questions. Clicking these buttons displays information such as business requirements, existing environment, and problem statements. When you are ready to answer a question, click the Question button to return to the question.

General Overview -

Litware, Inc. is an international manufacturing company that has 3,000 employees. The company has sales, marketing, research, human resources (HR), development, and IT departments.

Litware has two main offices in New York and Los Angeles. Litware has five branch offices in Asia.

Existing Environment -

Current Business Model -

The Los Angeles office has 500 developers. The developers work flexible hours ranging from 11 AM to 10 PM.

Litware has a Microsoft Endpoint Configuration Manager deployment.

During discovery, the company discovers a process where users are emailing bank account information of its customers to internal and external recipients.

Current Environment -

The network contains an Active Directory domain that is synced to Microsoft Azure Active Directory (Azure AD). The functional level of the forest and the domain is

Windows Server 2012 R2. All domain controllers run Windows Server 2012 R2.

Litware has the computers shown in the following table.

Department	Windows version	Management platform	Domain-joined
Marketing	8.1	Endpoint Configuration Manager	Hybrid Azure-AD joined
Research	10	Endpoint Configuration Manager	Hybrid Azure-AD joined
HR	8.1	Endpoint Configuration Manager	Hybrid Azure-AD joined
Developers	10	Microsoft Intune	Azure AD-joined
Sales	10	Microsoft Intune	Azure AD-joined

The development department uses projects in Azure DevOps to build applications.

Most of the employees in the sales department are contractors. Each contractor is assigned a computer that runs Windows 10. At the end of each contract, the computer is assigned to a different contractor. Currently, the computers are re-provisioned manually by the IT department.

Problem Statements -

Litware identifies the following issues on the network:

Employees in the Los Angeles office report slow Internet performance when updates are downloading. The employees also report that the updates frequently consume considerable resources when they are installed. The Update settings are configured as shown in the Updates exhibit. (Click the Updates button.)

Management suspects that the source code for the proprietary applications in Azure DevOps in being shared externally.

Re-provisioning the sales department computers is too time consuming.

Requirements -

Business Goals -

Litware plans to transition to co-management for all the company-owned Windows 10 computers. Whenever possible, Litware wants to minimize hardware and software costs.

Device Management Requirements -

Litware identifies the following device management requirements:

Prevent the sales department employees from forwarding email that contains bank account information.

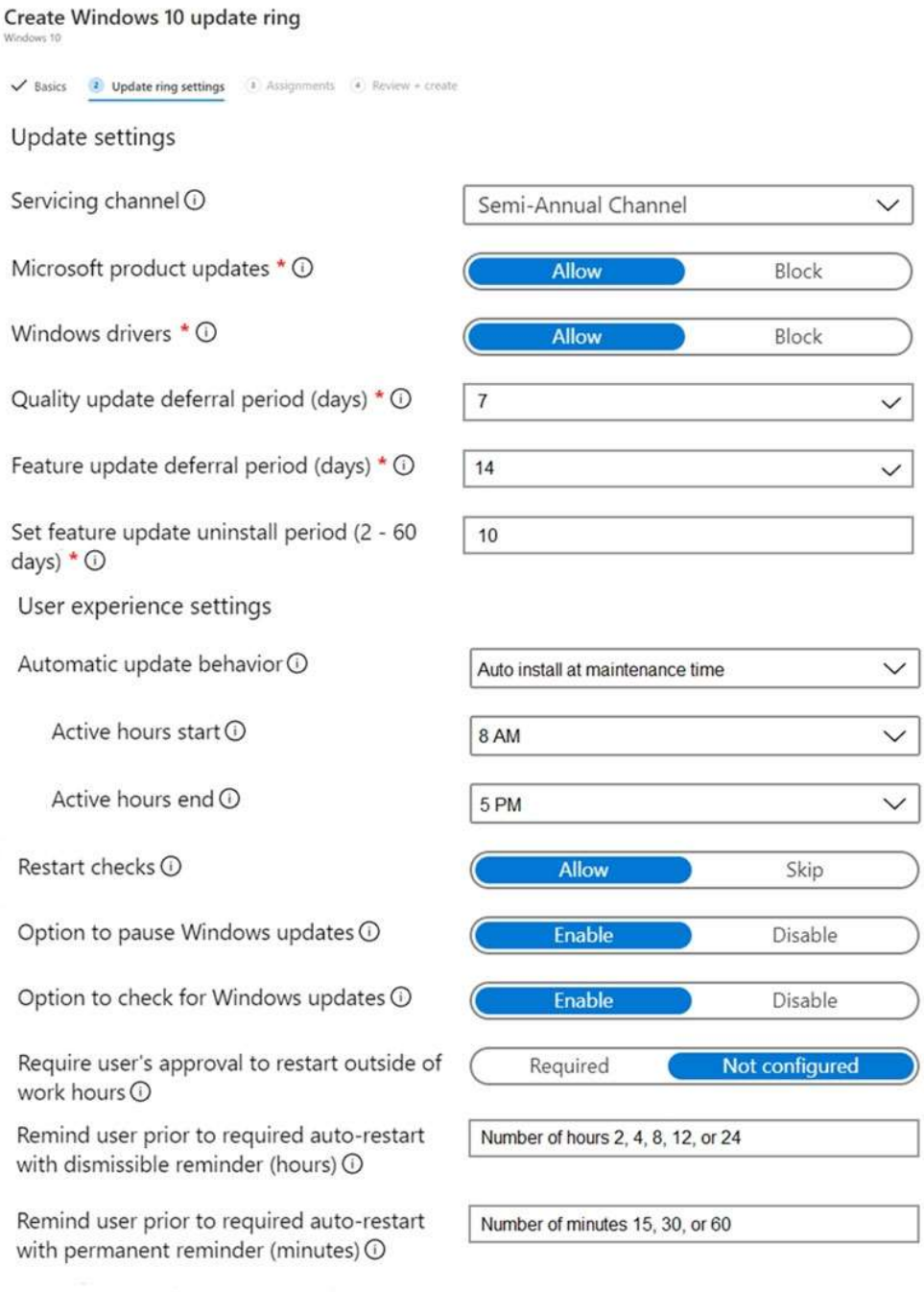
▪

Ensure that Microsoft Edge Favorites are accessible from all computers to which the developers sign in.
Prevent employees in the research department from copying patented information from trusted applications to untrusted applications.

Technical Requirements -
Litware identifies the following technical requirements for the planned deployment:
Re-provision the sales department computers by using Windows AutoPilot.
Ensure that the projects in Azure DevOps can be accessed from the corporate network only.
Ensure that users can sign in to the Azure AD-joined computers by using a PIN. The PIN must expire every 30 days.
Ensure that the company name and logo appears during the Out of Box Experience (OOBE) when using Windows AutoPilot.

Exhibits -

Updates -



Question
What should you use to meet the technical requirements for Azure DevOps?

A. An app protection policy

B. Windows Information Protection (WIP)

C. Conditional access

D. A device configuration profile

Correct Answer: *C*

Ensure that the projects in Azure DevOps can be accessed from the corporate network only.

Reference:

https://docs.microsoft.com/en-us/azure/devops/organizations/accounts/manage-conditional-access?view=azure-devops

Alvaroll Highly Voted 8 months, 1 week ago

Conditional Access
- Cloud apps or actions: Azure DevOps App
- Conditions --> Locations: Exclude office IPs
- Action: Block
If someone is trying to access this particular App outside the Office, the access is blocked.

upvoted 7 times

RodrigoT Most Recent 5 months, 1 week ago

Selected Answer: C

Answer provided is correct.

upvoted 1 times

Solaris2002 7 months, 2 weeks ago

This is wrong, conditional access only dictates access to an app, but does not protect the sharing of App DATA such as coping code - that is Windows Information Protection. See below link.

https://docs.microsoft.com/en-us/windows/security/information-protection/windows-information-protection/protect-enterprise-data-using-wip

key quotes are
"For example, if WIP management is set to Block, your employees can copy and paste from one protected app to another protected app, but not to personal apps."

"WIP lets you block, allow overrides, or audit employees' data sharing actions. Hiding overrides stops the action immediately. Allowing overrides lets the employee know there's a risk, but lets him or her continue to share the data while recording and auditing the action. "

Therefore, since the question is asking to prevent the sharing of proprietary code. We're not restricting who has ACCESS to that data, but restricting how someone with access can SHARE that data.

Final answer. B - Windows Information Protection (WIP)

upvoted 1 times

99redeyeflight 7 months ago

"Technical Requirements - Ensure that the projects in Azure DevOps can be accessed from the corporate network only."

Conditional access

upvoted 4 times

nipsey 6 months, 3 weeks ago

Conditional access is fine.
WIP is applied after the user already made the connection for blocking information sharing.
The question is to not even make the connection - so Conditional access

upvoted 3 times

fatape 10 months, 2 weeks ago

Wip and conditional access both sound like possibilities

upvoted 3 times

Garito 7 months, 1 week ago

Considering the overall situation WIP would be better suited but agreed - both can be possibilities.

upvoted 1 times

Introductory Info

Case study -

This is a case study. Case studies are not timed separately. You can use as much exam time as you would like to complete each case. However, there may be additional case studies and sections on this exam. You must manage your time to ensure that you are able to complete all questions included on this exam in the time provided.

To answer the questions included in a case study, you will need to reference information that is provided in the case study. Case studies might contain exhibits and other resources that provide more information about the scenario that is described in the case study. Each question is independent of the other questions in this case study.

At the end of this case study, a review screen will appear. This screen allows you to review your answers and to make changes before you move to the next section of the exam. After you begin a new section, you cannot return to this section.

To start the case study -

To display the first question in this case study, click the Next button. Use the buttons in the left pane to explore the content of the case study before you answer the questions. Clicking these buttons displays information such as business requirements, existing environment, and problem statements. When you are ready to answer a question, click the Question button to return to the question.

General Overview -

Litware, Inc. is an international manufacturing company that has 3,000 employees. The company has sales, marketing, research, human resources (HR), development, and IT departments.

Litware has two main offices in New York and Los Angeles. Litware has five branch offices in Asia.

Existing Environment -

Current Business Model -

The Los Angeles office has 500 developers. The developers work flexible hours ranging from 11 AM to 10 PM.

Litware has a Microsoft Endpoint Configuration Manager deployment.

During discovery, the company discovers a process where users are emailing bank account information of its customers to internal and external recipients.

Current Environment -

The network contains an Active Directory domain that is synced to Microsoft Azure Active Directory (Azure AD). The functional level of the forest and the domain is

Windows Server 2012 R2. All domain controllers run Windows Server 2012 R2.

Litware has the computers shown in the following table.

Department	Windows version	Management platform	Domain-joined
Marketing	8.1	Endpoint Configuration Manager	Hybrid Azure-AD joined
Research	10	Endpoint Configuration Manager	Hybrid Azure-AD joined
HR	8.1	Endpoint Configuration Manager	Hybrid Azure-AD joined
Developers	10	Microsoft Intune	Azure AD-joined
Sales	10	Microsoft Intune	Azure AD-joined

The development department uses projects in Azure DevOps to build applications.

Most of the employees in the sales department are contractors. Each contractor is assigned a computer that runs Windows 10. At the end of each contract, the computer is assigned to a different contractor. Currently, the computers are re-provisioned manually by the IT department.

Problem Statements -

Litware identifies the following issues on the network:

Employees in the Los Angeles office report slow Internet performance when updates are downloading. The employees also report that the updates frequently consume considerable resources when they are installed. The Update settings are configured as shown in the Updates exhibit. (Click the Updates button.)

Management suspects that the source code for the proprietary applications in Azure DevOps in being shared externally.

Re-provisioning the sales department computers is too time consuming.

Requirements -

Business Goals -

Litware plans to transition to co-management for all the company-owned Windows 10 computers. Whenever possible, Litware wants to minimize hardware and software costs.

Device Management Requirements -

Litware identifies the following device management requirements:

Prevent the sales department employees from forwarding email that contains bank account information.

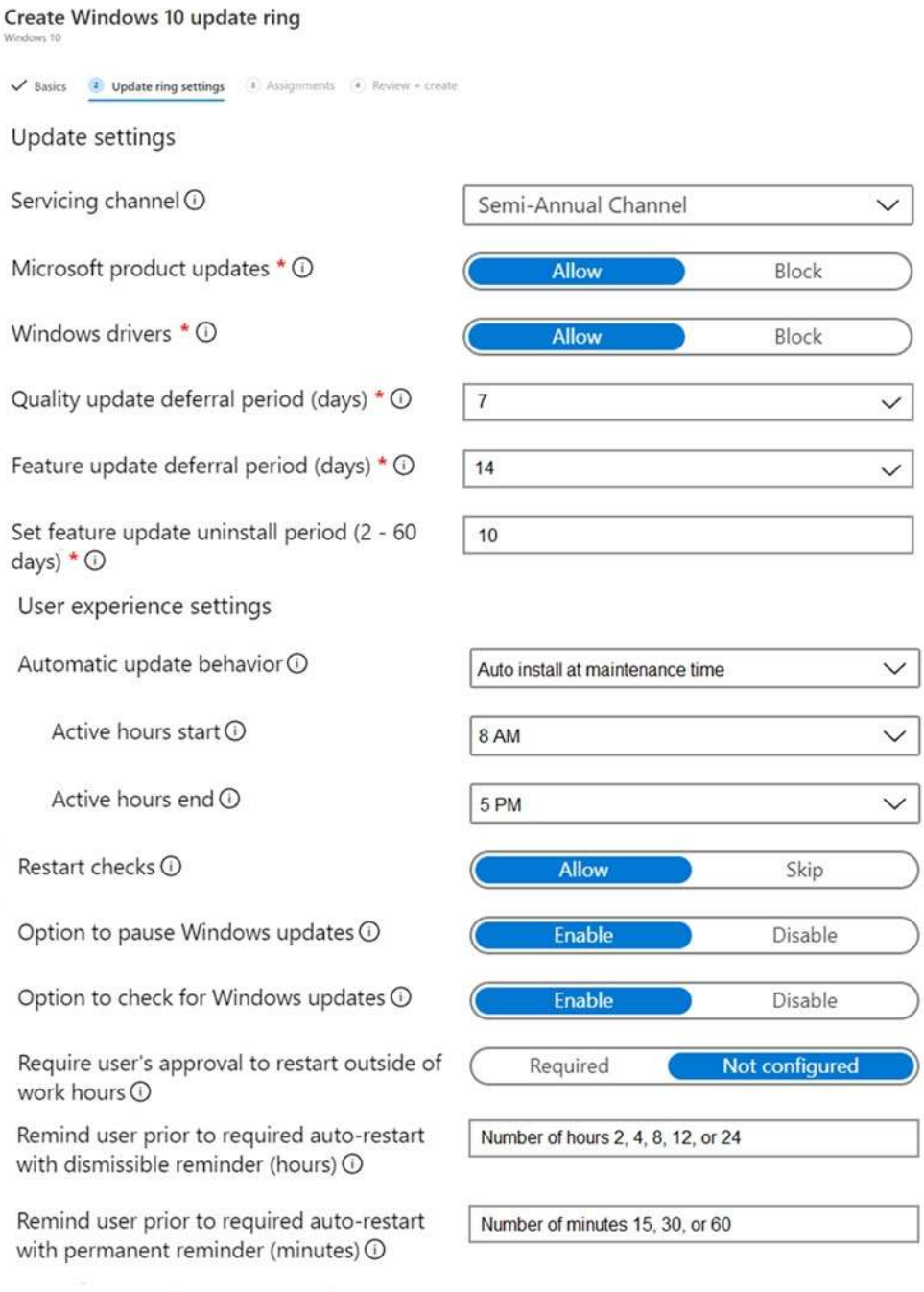
▪

Ensure that Microsoft Edge Favorites are accessible from all computers to which the developers sign in.
Prevent employees in the research department from copying patented information from trusted applications to untrusted applications.

Technical Requirements -
Litware identifies the following technical requirements for the planned deployment:
Re-provision the sales department computers by using Windows AutoPilot.
Ensure that the projects in Azure DevOps can be accessed from the corporate network only.
Ensure that users can sign in to the Azure AD-joined computers by using a PIN. The PIN must expire every 30 days.
Ensure that the company name and logo appears during the Out of Box Experience (OOBE) when using Windows AutoPilot.

Exhibits -

Updates -



Question
What should you upgrade before you can configure the environment to support co-management?

A. the domain functional level

B. Microsoft Endpoint Configuration Manager

C. the domain controllers

D. Windows Server Update Services (WSUS)

Correct Answer: *B*

Enable co-management in Configuration Manager.

Note: Litware plans to transition to co-management for all the company-owned Windows 10 computers. Whenever possible, Litware wants to minimize hardware and software costs.

Reference:

https://docs.microsoft.com/en-us/sccm/comanage/tutorial-co-manage-clients

AVP_Riga Highly Voted 10 months, 2 weeks ago

Tricky question, we don't which version already installed....

upvoted 6 times

coppermine Most Recent 9 months, 1 week ago

Selected Answer: B

For Windows 10 hybrid Azure AD join, the minimum domain controller version is Windows Server 2008 R2, so there's no need to upgrade domain controllers or domain functional levels.
https://docs.microsoft.com/en-us/azure/active-directory/devices/hybrid-azuread-join-plan

Windows Server Update Services (WSUS) is not mentioned in the requirement as Schra mentioned. The possible answer is Microsoft Endpoint Configuration Manager.

upvoted 4 times

RodrigoT 5 months, 1 week ago

Thank you for the link. This is the way 👍
https://docs.microsoft.com/en-us/azure/active-directory/devices/hybrid-azuread-join-plan#prerequisites

upvoted 1 times

Schra 9 months, 2 weeks ago

https://docs.microsoft.com/en-us/mem/configmgr/comanage/overview#windows
Co-management has these prerequisites in the following areas:
Licensing
Configuration Manager
Azure Active Directory (Azure AD)
Microsoft Intune
Windows
Permissions and roles

- Co-management requires Configuration Manager version 1710 or later
- Windows 10, version 1709 or later
- no specific domain controller or level requirement specified

so the answer must be correct

upvoted 2 times

Introductory Info

Case study -

This is a case study. Case studies are not timed separately. You can use as much exam time as you would like to complete each case. However, there may be additional case studies and sections on this exam. You must manage your time to ensure that you are able to complete all questions included on this exam in the time provided.

To answer the questions included in a case study, you will need to reference information that is provided in the case study. Case studies might contain exhibits and other resources that provide more information about the scenario that is described in the case study. Each question is independent of the other questions in this case study.

At the end of this case study, a review screen will appear. This screen allows you to review your answers and to make changes before you move to the next section of the exam. After you begin a new section, you cannot return to this section.

To start the case study -

To display the first question in this case study, click the Next button. Use the buttons in the left pane to explore the content of the case study before you answer the questions. Clicking these buttons displays information such as business requirements, existing environment, and problem statements. When you are ready to answer a question, click the Question button to return to the question.

General Overview -

Litware, Inc. is an international manufacturing company that has 3,000 employees. The company has sales, marketing, research, human resources (HR), development, and IT departments.

Litware has two main offices in New York and Los Angeles. Litware has five branch offices in Asia.

Existing Environment -

Current Business Model -

The Los Angeles office has 500 developers. The developers work flexible hours ranging from 11 AM to 10 PM.

Litware has a Microsoft Endpoint Configuration Manager deployment.

During discovery, the company discovers a process where users are emailing bank account information of its customers to internal and external recipients.

Current Environment -

The network contains an Active Directory domain that is synced to Microsoft Azure Active Directory (Azure AD). The functional level of the forest and the domain is

Windows Server 2012 R2. All domain controllers run Windows Server 2012 R2.

Litware has the computers shown in the following table.

Department	Windows version	Management platform	Domain-joined
Marketing	8.1	Endpoint Configuration Manager	Hybrid Azure-AD joined
Research	10	Endpoint Configuration Manager	Hybrid Azure-AD joined
HR	8.1	Endpoint Configuration Manager	Hybrid Azure-AD joined
Developers	10	Microsoft Intune	Azure AD-joined
Sales	10	Microsoft Intune	Azure AD-joined

The development department uses projects in Azure DevOps to build applications.

Most of the employees in the sales department are contractors. Each contractor is assigned a computer that runs Windows 10. At the end of each contract, the computer is assigned to a different contractor. Currently, the computers are re-provisioned manually by the IT department.

Problem Statements -

Litware identifies the following issues on the network:

Employees in the Los Angeles office report slow Internet performance when updates are downloading. The employees also report that the updates frequently consume considerable resources when they are installed. The Update settings are configured as shown in the Updates exhibit. (Click the Updates button.)

Management suspects that the source code for the proprietary applications in Azure DevOps in being shared externally.

Re-provisioning the sales department computers is too time consuming.

Requirements -

Business Goals -

Litware plans to transition to co-management for all the company-owned Windows 10 computers. Whenever possible, Litware wants to minimize hardware and software costs.

Device Management Requirements -

Litware identifies the following device management requirements:

Prevent the sales department employees from forwarding email that contains bank account information.

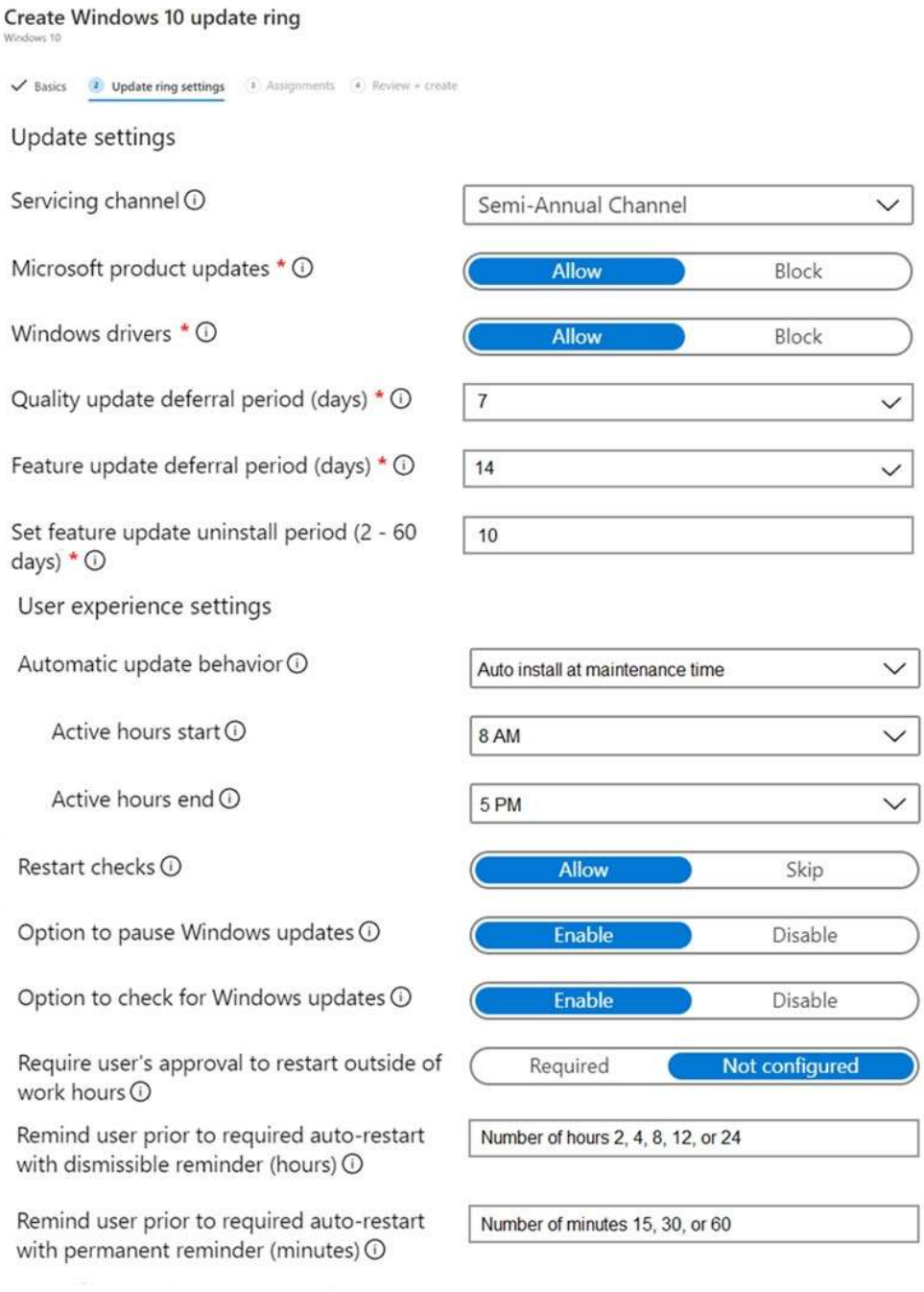
▪

Ensure that Microsoft Edge Favorites are accessible from all computers to which the developers sign in.
Prevent employees in the research department from copying patented information from trusted applications to untrusted applications.

Technical Requirements -
Litware identifies the following technical requirements for the planned deployment:
Re-provision the sales department computers by using Windows AutoPilot.
Ensure that the projects in Azure DevOps can be accessed from the corporate network only.
Ensure that users can sign in to the Azure AD-joined computers by using a PIN. The PIN must expire every 30 days.
Ensure that the company name and logo appears during the Out of Box Experience (OOBE) when using Windows AutoPilot.

Exhibits -

Updates -



Question
You need to meet the device management requirements for the developers.
What should you implement?

A. Enterprise State Roaming

B. folder redirection

C. home folders

D. known folder redirection in Microsoft OneDrive

Correct Answer: *A*

Litware identifies the following device management requirements:

Ensure that Microsoft Edge Favorites are accessible from all computers to which the developers sign in.

Enterprise State Roaming allows for the synchronization of Microsoft Edge browser setting, including favorites and reading list, across devices.

Reference:

https://docs.microsoft.com/en-us/azure/active-directory/devices/enterprise-state-roaming-windows-settings-reference

wyindualizer Highly Voted 8 months, 2 weeks ago

https://docs.microsoft.com/en-us/azure/active-directory/devices/enterprise-state-roaming-faqs
Microsoft Edge browser settings, such as favorites and reading list.

upvoted 5 times

thuba_TD Most Recent 1 week, 6 days ago

more questions like these please

upvoted 1 times

Angarali 5 months, 2 weeks ago

Selected Answer: A

Answer is correct

upvoted 1 times

AVP_Riga 10 months, 2 weeks ago

Is it right? Anyone?

upvoted 1 times

FrancisLai 10 months, 1 week ago

Answer is correct. Link to support https://docs.microsoft.com/en-us/deployedge/microsoft-edge-enterprise-state-roaming other than the provided.

upvoted 3 times

Topic 12 - Testlet 5

Introductory Info

Case study -

This is a case study. Case studies are not timed separately. You can use as much exam time as you would like to complete each case. However, there may be additional case studies and sections on this exam. You must manage your time to ensure that you are able to complete all questions included on this exam in the time provided.

To answer the questions included in a case study, you will need to reference information that is provided in the case study. Case studies might contain exhibits and other resources that provide more information about the scenario that is described in the case study. Each question is independent of the other questions in this case study.

At the end of this case study, a review screen will appear. This screen allows you to review your answers and to make changes before you move to the next section of the exam. After you begin a new section, you cannot return to this section.

To start the case study -

To display the first question in this case study, click the Next button. Use the buttons in the left pane to explore the content of the case study before you answer the questions. Clicking these buttons displays information such as business requirements, existing environment, and problem statements. When you are ready to answer a question, click the Question button to return to the question.

Overview -

Contoso, Ltd. is a consulting company that has a main office in Montreal and two branch offices in Seattle and New York.

Contoso has the users and computers shown in the following table.

Location	Users	Laptops	Desktop computers	Mobile devices
Montreal	2,500	2,800	300	3,100
Seattle	1,000	1,100	200	1,500
New York	300	320	30	400

The company has IT, human resources (HR), legal (LEG), marketing (MKG) and finance (FIN) departments.

Contoso uses Microsoft Store for Business and recently purchased a Microsoft 365 subscription.

The company is opening a new branch office in Phoenix. Most of the users in the Phoenix office will work from home.

Existing Environment -

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

All member servers run Windows Server 2016. All laptops and desktop computers run Windows 10 Enterprise.

The computers are managed by using Microsoft Endpoint Configuration Manager. The mobile devices are managed by using Microsoft Intune.

The naming convention for the computers is the department acronym, followed by a hyphen, and then four numbers, for example, FIN-6785. All the computers are joined to the on-premises Active Directory domain.

Each department has an organizational unit (OU) that contains a child OU named Computers. Each computer account is in the Computers OU of its respective department.

Intune Configuration -

The domain has the users shown in the following table.

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

User2 is a device enrollment manager (DEM) in Intune.

The devices enrolled in Intune are shown in the following table.

Name	Platform	Encryption	Member of
Device1	Android	Disabled	Group1
Device2	iOS	*Not applicable*	Group2, Group3
Device3	Android	Disabled	Group2, Group3
Device4	iOS	*Not applicable*	Group2

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

Name	Platform	Require encryption	Assigned
Policy1	Android	Not configured	Yes
Policy2	iOS	*Not applicable*	Yes
Policy3	Android	Require	Yes

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

Name	Include	Exclude
Policy1	Group3	*None*
Policy2	Group2	Group3
Policy3	Group1	*None*

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

Priority	Name	Device limit	Assigned to
1	Restriction1	15	GroupB
2	Restriction2	10	GroupA
Default	All users	5	All users

Requirements -

Planned Changes -
Contoso plans to implement the following changes:
Provide new computers to the Phoenix office users. The new computers have Windows 10 Pro preinstalled and were purchased already.
Start using a free Microsoft Store for Business app named App1.
Implement co-management for the computers.
▪

Technical Requirements -
Contoso must meet the following technical requirements:
Ensure that the users in a group named Group4 can only access Microsoft Exchange Online from devices that are enrolled in Intune.
Deploy Windows 10 Enterprise to the computers of the Phoenix office users by using Windows Autopilot.
Monitor the computers in the LEG department by using Windows Analytics.
Create a provisioning package for new computers in the HR department.
Block iOS devices from sending diagnostic and usage telemetry data.
Use the principle of least privilege whenever possible.
Enable the users in the MKG department to use App1.
Pilot co-management for the IT department.

Question
You need to meet the technical requirements for the iOS devices.
Which object should you create in Intune?

A. A compliance policy
B. An app protection policy
C. A deployment profile
D. A device configuration profile

Correct Answer: *D*
Scenario: Technical requirements include: Block iOS devices from sending diagnostic and usage telemetry data.
Intune includes device restriction policies that help administrators control Android, iOS, macOS, and Windows devices. These restrictions let you control a wide range of settings and features to protect your organization's resources. For example, administrators can:
Allow or block the device camera
Control access to Google Play, app stores, viewing documents, and gaming
Block built-in apps, or create a list of apps that allowed or prohibited
Allow or prevent backing up files to cloud and storage accounts
Set a minimum password length, and block simple passwords
Reference:
https://docs.microsoft.com/en-us/intune/device-restrictions-configure

RodrigoT 5 months, 1 week ago
Selected Answer: D
Answer provided is correct. TESTED in my tenant. Here is the official link:
https://docs.microsoft.com/en-us/mem/intune/configuration/device-restrictions-ios#settings-apply-to-all-enrollment-types-4
upvoted 2 times

Introductory Info

Case study -

This is a case study. Case studies are not timed separately. You can use as much exam time as you would like to complete each case. However, there may be additional case studies and sections on this exam. You must manage your time to ensure that you are able to complete all questions included on this exam in the time provided.

To answer the questions included in a case study, you will need to reference information that is provided in the case study. Case studies might contain exhibits and other resources that provide more information about the scenario that is described in the case study. Each question is independent of the other questions in this case study.

At the end of this case study, a review screen will appear. This screen allows you to review your answers and to make changes before you move to the next section of the exam. After you begin a new section, you cannot return to this section.

To start the case study -

To display the first question in this case study, click the Next button. Use the buttons in the left pane to explore the content of the case study before you answer the questions. Clicking these buttons displays information such as business requirements, existing environment, and problem statements. When you are ready to answer a question, click the Question button to return to the question.

Overview -

Contoso, Ltd. is a consulting company that has a main office in Montreal and two branch offices in Seattle and New York.

Contoso has the users and computers shown in the following table.

Location	Users	Laptops	Desktop computers	Mobile devices
Montreal	2,500	2,800	300	3,100
Seattle	1,000	1,100	200	1,500
New York	300	320	30	400

The company has IT, human resources (HR), legal (LEG), marketing (MKG) and finance (FIN) departments.

Contoso uses Microsoft Store for Business and recently purchased a Microsoft 365 subscription.

The company is opening a new branch office in Phoenix. Most of the users in the Phoenix office will work from home.

Existing Environment -

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

All member servers run Windows Server 2016. All laptops and desktop computers run Windows 10 Enterprise.

The computers are managed by using Microsoft Endpoint Configuration Manager. The mobile devices are managed by using Microsoft Intune.

The naming convention for the computers is the department acronym, followed by a hyphen, and then four numbers, for example, FIN-6785. All the computers are joined to the on-premises Active Directory domain.

Each department has an organizational unit (OU) that contains a child OU named Computers. Each computer account is in the Computers OU of its respective department.

Intune Configuration -

The domain has the users shown in the following table.

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

User2 is a device enrollment manager (DEM) in Intune.

The devices enrolled in Intune are shown in the following table.

Name	Platform	Encryption	Member of
Device1	Android	Disabled	Group1
Device2	iOS	*Not applicable*	Group2, Group3
Device3	Android	Disabled	Group2, Group3
Device4	iOS	*Not applicable*	Group2

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

Name	Platform	Require encryption	Assigned
Policy1	Android	Not configured	Yes
Policy2	iOS	*Not applicable*	Yes
Policy3	Android	Require	Yes

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

Name	Include	Exclude
Policy1	Group3	*None*
Policy2	Group2	Group3
Policy3	Group1	*None*

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

Priority	Name	Device limit	Assigned to
1	Restriction1	15	GroupB
2	Restriction2	10	GroupA
Default	All users	5	All users

Requirements -

Planned Changes -

Contoso plans to implement the following changes:

Provide new computers to the Phoenix office users. The new computers have Windows 10 Pro preinstalled and were purchased already.

Start using a free Microsoft Store for Business app named App1.

Implement co-management for the computers.

▪

Technical Requirements -

Contoso must meet the following technical requirements:

Ensure that the users in a group named Group4 can only access Microsoft Exchange Online from devices that are enrolled in Intune.

Deploy Windows 10 Enterprise to the computers of the Phoenix office users by using Windows Autopilot.

Monitor the computers in the LEG department by using Windows Analytics.

Create a provisioning package for new computers in the HR department.

Block iOS devices from sending diagnostic and usage telemetry data.

Use the principle of least privilege whenever possible.

Enable the users in the MKG department to use App1.

Pilot co-management for the IT department.

Question

HOTSPOT -

To which devices do Policy1 and Policy2 apply? To answer, select the appropriate options in the answer area.

NOTE: Each correct selection is worth one point.

Hot Area:

Answer Area

Policy1:

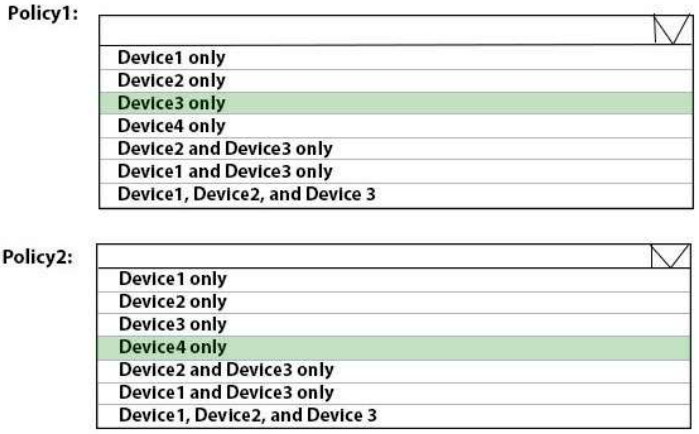
- Device1 only
- Device2 only
- Device3 only
- Device4 only
- Device2 and Device3 only
- Device1 and Device3 only
- Device1, Device2, and Device 3

Policy2:

- Device1 only
- Device2 only
- Device3 only
- Device4 only
- Device2 and Device3 only
- Device1 and Device3 only
- Device1, Device2, and Device 3

Correct Answer:

Answer Area



Box 1: Device 3 only -

Policy1 applies to Device3 (Android)

Box 2: Device 4 only -

Policy2 applies to Device4 (iOS)

Reference:

https://docs.microsoft.com/en-us/intune/device-profile-assign

NZS 5 months ago

Wrong answer. Policy1 for Device3 only, but Policy2 for Device4, as Device2 is in an excluded group.

upvoted 1 times

thuba_TD 1 week, 6 days ago

That's what the answer says mate

upvoted 1 times

bensrayan 1 week, 6 days ago

i think the moderators correct the answer afterwards , before it was wrong

upvoted 2 times

RodrigoT 5 months, 1 week ago

Second answer is wrong. It's impossible for Device2 because is also Group3 that is excluded by Policy2.
Correct answers are:
-Device3, Android, Group3
-Device4, IOS, Group2

upvoted 1 times

Introductory Info

Case study -

This is a case study. Case studies are not timed separately. You can use as much exam time as you would like to complete each case. However, there may be additional case studies and sections on this exam. You must manage your time to ensure that you are able to complete all questions included on this exam in the time provided.

To answer the questions included in a case study, you will need to reference information that is provided in the case study. Case studies might contain exhibits and other resources that provide more information about the scenario that is described in the case study. Each question is independent of the other questions in this case study.

At the end of this case study, a review screen will appear. This screen allows you to review your answers and to make changes before you move to the next section of the exam. After you begin a new section, you cannot return to this section.

To start the case study -

To display the first question in this case study, click the Next button. Use the buttons in the left pane to explore the content of the case study before you answer the questions. Clicking these buttons displays information such as business requirements, existing environment, and problem statements. When you are ready to answer a question, click the Question button to return to the question.

Overview -

Contoso, Ltd. is a consulting company that has a main office in Montreal and two branch offices in Seattle and New York.

Contoso has the users and computers shown in the following table.

Location	Users	Laptops	Desktop computers	Mobile devices
Montreal	2,500	2,800	300	3,100
Seattle	1,000	1,100	200	1,500
New York	300	320	30	400

The company has IT, human resources (HR), legal (LEG), marketing (MKG) and finance (FIN) departments.

Contoso uses Microsoft Store for Business and recently purchased a Microsoft 365 subscription.

The company is opening a new branch office in Phoenix. Most of the users in the Phoenix office will work from home.

Existing Environment -

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

All member servers run Windows Server 2016. All laptops and desktop computers run Windows 10 Enterprise.

The computers are managed by using Microsoft Endpoint Configuration Manager. The mobile devices are managed by using Microsoft Intune.

The naming convention for the computers is the department acronym, followed by a hyphen, and then four numbers, for example, FIN-6785. All the computers are joined to the on-premises Active Directory domain.

Each department has an organizational unit (OU) that contains a child OU named Computers. Each computer account is in the Computers OU of its respective department.

Intune Configuration -

The domain has the users shown in the following table.

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

User2 is a device enrollment manager (DEM) in Intune.

The devices enrolled in Intune are shown in the following table.

Name	Platform	Encryption	Member of
Device1	Android	Disabled	Group1
Device2	iOS	*Not applicable*	Group2, Group3
Device3	Android	Disabled	Group2, Group3
Device4	iOS	*Not applicable*	Group2

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

Name	Platform	Require encryption	Assigned
Policy1	Android	Not configured	Yes
Policy2	iOS	*Not applicable*	Yes
Policy3	Android	Require	Yes

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

Name	Include	Exclude
Policy1	Group3	*None*
Policy2	Group2	Group3
Policy3	Group1	*None*

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

Priority	Name	Device limit	Assigned to
1	Restriction1	15	GroupB
2	Restriction2	10	GroupA
Default	All users	5	All users

Requirements -

Planned Changes -

Contoso plans to implement the following changes:

Provide new computers to the Phoenix office users. The new computers have Windows 10 Pro preinstalled and were purchased already.

Start using a free Microsoft Store for Business app named App1.

Implement co-management for the computers.

▪

Technical Requirements -

Contoso must meet the following technical requirements:

Ensure that the users in a group named Group4 can only access Microsoft Exchange Online from devices that are enrolled in Intune.

Deploy Windows 10 Enterprise to the computers of the Phoenix office users by using Windows Autopilot.

Monitor the computers in the LEG department by using Windows Analytics.

Create a provisioning package for new computers in the HR department.

Block iOS devices from sending diagnostic and usage telemetry data.

Use the principle of least privilege whenever possible.

Enable the users in the MKG department to use App1.

Pilot co-management for the IT department.

Question

HOTSPOT -

What is the maximum number of devices that User1 and User2 can enroll in Intune? To answer, select the appropriate options in the answer area.

NOTE: Each correct selection is worth one point.

Hot Area:

Answer Area

User1 can enroll a maximum of:

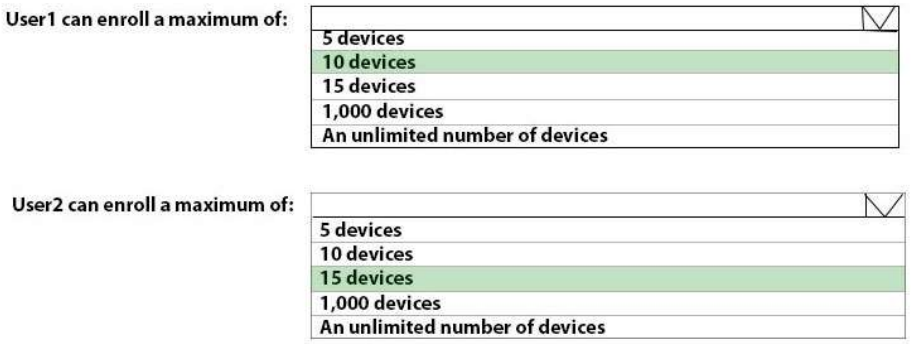
- 5 devices
- 10 devices
- 15 devices
- 1,000 devices
- An unlimited number of devices

User2 can enroll a maximum of:

- 5 devices
- 10 devices
- 15 devices
- 1,000 devices
- An unlimited number of devices

Correct Answer:

Answer Area



Box 1: 10 devices -

User1 is a member of GroupA. GroupA device limit is 10.

Box 2: 15 devices -

User2 is a member of GroupB. GroupB device limit is 15.

NZS 5 months ago

Correct, 10 and 15

upvoted 1 times

RodrigoT 5 months ago

Why? Links please.

upvoted 1 times

RodrigoT 5 months ago

Got it now. Check the last table. The restrictions override the Default.

upvoted 1 times

RodrigoT 5 months, 1 week ago

Totally wrong answers.
User1 - Default 15 devices
User2 is a device enrollment manager (DEM)- 1000 devices
Default:
https://docs.microsoft.com/en-us/mem/intune/enrollment/enrollment-restrictions-set#create-a-device-limit-restriction
DEM:
https://docs.microsoft.com/en-us/mem/intune/enrollment/device-enrollment-manager-enroll

upvoted 2 times

RodrigoT 5 months ago

I was wrong. The answers provided are correct. The restrictions override the Default. You need to check the last table on the question. I need more coffee 😓🫖🍒🍒🍎

upvoted 2 times

bensrayan 1 week, 6 days ago

for the DEM , should be 1000 !!
in your link it said: " DEM enrolls Windows 10/11 devices in shared device mode, so device limit restrictions won't work on them. Instead, you can configure a hard limit for these devices in the Azure AD admin center. For more information, see Manage device identities by using the Azure portal"

upvoted 1 times

TonySuccess 3 days, 2 hours ago

bensrayan is correct, furthermore he has passed the exam soooo I'ma go with cha boi

upvoted 1 times

thuba_TD 1 week, 6 days ago

Clearly

upvoted 1 times

Introductory Info

Case study -

This is a case study. Case studies are not timed separately. You can use as much exam time as you would like to complete each case. However, there may be additional case studies and sections on this exam. You must manage your time to ensure that you are able to complete all questions included on this exam in the time provided.

To answer the questions included in a case study, you will need to reference information that is provided in the case study. Case studies might contain exhibits and other resources that provide more information about the scenario that is described in the case study. Each question is independent of the other questions in this case study.

At the end of this case study, a review screen will appear. This screen allows you to review your answers and to make changes before you move to the next section of the exam. After you begin a new section, you cannot return to this section.

To start the case study -

To display the first question in this case study, click the Next button. Use the buttons in the left pane to explore the content of the case study before you answer the questions. Clicking these buttons displays information such as business requirements, existing environment, and problem statements. When you are ready to answer a question, click the Question button to return to the question.

Overview -

Contoso, Ltd. is a consulting company that has a main office in Montreal and two branch offices in Seattle and New York.

Contoso has the users and computers shown in the following table.

Location	Users	Laptops	Desktop computers	Mobile devices
Montreal	2,500	2,800	300	3,100
Seattle	1,000	1,100	200	1,500
New York	300	320	30	400

The company has IT, human resources (HR), legal (LEG), marketing (MKG) and finance (FIN) departments.

Contoso uses Microsoft Store for Business and recently purchased a Microsoft 365 subscription.

The company is opening a new branch office in Phoenix. Most of the users in the Phoenix office will work from home.

Existing Environment -

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

All member servers run Windows Server 2016. All laptops and desktop computers run Windows 10 Enterprise.

The computers are managed by using Microsoft Endpoint Configuration Manager. The mobile devices are managed by using Microsoft Intune.

The naming convention for the computers is the department acronym, followed by a hyphen, and then four numbers, for example, FIN-6785. All the computers are joined to the on-premises Active Directory domain.

Each department has an organizational unit (OU) that contains a child OU named Computers. Each computer account is in the Computers OU of its respective department.

Intune Configuration -

The domain has the users shown in the following table.

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

User2 is a device enrollment manager (DEM) in Intune.

The devices enrolled in Intune are shown in the following table.

Name	Platform	Encryption	Member of
Device1	Android	Disabled	Group1
Device2	iOS	*Not applicable*	Group2, Group3
Device3	Android	Disabled	Group2, Group3
Device4	iOS	*Not applicable*	Group2

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

Name	Platform	Require encryption	Assigned
Policy1	Android	Not configured	Yes
Policy2	iOS	*Not applicable*	Yes
Policy3	Android	Require	Yes

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

Name	Include	Exclude
Policy1	Group3	*None*
Policy2	Group2	Group3
Policy3	Group1	*None*

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

Priority	Name	Device limit	Assigned to
1	Restriction1	15	GroupB
2	Restriction2	10	GroupA
Default	All users	5	All users

Requirements -

Planned Changes -
Contoso plans to implement the following changes:
Provide new computers to the Phoenix office users. The new computers have Windows 10 Pro preinstalled and were purchased already.
Start using a free Microsoft Store for Business app named App1.
Implement co-management for the computers.
▪

Technical Requirements -
Contoso must meet the following technical requirements:
Ensure that the users in a group named Group4 can only access Microsoft Exchange Online from devices that are enrolled in Intune.
Deploy Windows 10 Enterprise to the computers of the Phoenix office users by using Windows Autopilot.
Monitor the computers in the LEG department by using Windows Analytics.
Create a provisioning package for new computers in the HR department.
Block iOS devices from sending diagnostic and usage telemetry data.
Use the principle of least privilege whenever possible.
Enable the users in the MKG department to use App1.
Pilot co-management for the IT department.

Question
You need to meet the technical requirements for the IT department.
What should you do first?

A. From the Azure Active Directory blade in the Azure portal, enable Seamless single sign-on.

B. From the Configuration Manager console, add an Intune subscription.

C. From the Azure Active Directory blade in the Azure portal, configure the Mobility (MDM and MAM) settings.

D. From the Microsoft Intune blade in the Azure portal, configure the Windows enrollment settings.

Correct Answer: *C*
Pilot co-management for the IT department.
Configure auto-enrollment of devices to Intune.
1. Sign in to the Azure portal and select Azure Active Directory > Mobility (MDM and MAM) > Microsoft Intune.
2. Configure MDM user scope.
3. Etc.
Reference:
https://docs.microsoft.com/en-us/sccm/comanage/tutorial-co-manage-clients

RodrigoT 5 months, 1 week ago
Old question, but C is the best answer. MDM and MAM are not under Azure portal anymore. You have to go to Endpoint > Devices > Enroll devices | Windows enrollment > Automatic Enrollment.
upvoted 4 times

bensrayan 1 week, 6 days ago
it says : Azure active directory and not Azure !! and you have Mobility (MDM and MAM) link in AAD
upvoted 2 times

Introductory Info

Case study -

This is a case study. Case studies are not timed separately. You can use as much exam time as you would like to complete each case. However, there may be additional case studies and sections on this exam. You must manage your time to ensure that you are able to complete all questions included on this exam in the time provided.

To answer the questions included in a case study, you will need to reference information that is provided in the case study. Case studies might contain exhibits and other resources that provide more information about the scenario that is described in the case study. Each question is independent of the other questions in this case study.

At the end of this case study, a review screen will appear. This screen allows you to review your answers and to make changes before you move to the next section of the exam. After you begin a new section, you cannot return to this section.

To start the case study -

To display the first question in this case study, click the Next button. Use the buttons in the left pane to explore the content of the case study before you answer the questions. Clicking these buttons displays information such as business requirements, existing environment, and problem statements. When you are ready to answer a question, click the Question button to return to the question.

Overview -

Contoso, Ltd. is a consulting company that has a main office in Montreal and two branch offices in Seattle and New York.

Contoso has the users and computers shown in the following table.

Location	Users	Laptops	Desktop computers	Mobile devices
Montreal	2,500	2,800	300	3,100
Seattle	1,000	1,100	200	1,500
New York	300	320	30	400

The company has IT, human resources (HR), legal (LEG), marketing (MKG) and finance (FIN) departments.

Contoso uses Microsoft Store for Business and recently purchased a Microsoft 365 subscription.

The company is opening a new branch office in Phoenix. Most of the users in the Phoenix office will work from home.

Existing Environment -

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

All member servers run Windows Server 2016. All laptops and desktop computers run Windows 10 Enterprise.

The computers are managed by using Microsoft Endpoint Configuration Manager. The mobile devices are managed by using Microsoft Intune.

The naming convention for the computers is the department acronym, followed by a hyphen, and then four numbers, for example, FIN-6785. All the computers are joined to the on-premises Active Directory domain.

Each department has an organizational unit (OU) that contains a child OU named Computers. Each computer account is in the Computers OU of its respective department.

Intune Configuration -

The domain has the users shown in the following table.

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

User2 is a device enrollment manager (DEM) in Intune.

The devices enrolled in Intune are shown in the following table.

Name	Platform	Encryption	Member of
Device1	Android	Disabled	Group1
Device2	iOS	*Not applicable*	Group2, Group3
Device3	Android	Disabled	Group2, Group3
Device4	iOS	*Not applicable*	Group2

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

Name	Platform	Require encryption	Assigned
Policy1	Android	Not configured	Yes
Policy2	iOS	*Not applicable*	Yes
Policy3	Android	Require	Yes

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

Name	Include	Exclude
Policy1	Group3	*None*
Policy2	Group2	Group3
Policy3	Group1	*None*

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

Priority	Name	Device limit	Assigned to
1	Restriction1	15	GroupB
2	Restriction2	10	GroupA
Default	All users	5	All users

Requirements -

Planned Changes -
Contoso plans to implement the following changes:
Provide new computers to the Phoenix office users. The new computers have Windows 10 Pro preinstalled and were purchased already.
Start using a free Microsoft Store for Business app named App1.
Implement co-management for the computers.
▪

Technical Requirements -
Contoso must meet the following technical requirements:
Ensure that the users in a group named Group4 can only access Microsoft Exchange Online from devices that are enrolled in Intune.
Deploy Windows 10 Enterprise to the computers of the Phoenix office users by using Windows Autopilot.
Monitor the computers in the LEG department by using Windows Analytics.
Create a provisioning package for new computers in the HR department.
Block iOS devices from sending diagnostic and usage telemetry data.
Use the principle of least privilege whenever possible.
Enable the users in the MKG department to use App1.
Pilot co-management for the IT department.

Question
HOTSPOT -
You are evaluating which devices are 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:

Answer Area

Statements	Yes	No
Device1 is compliant	○	○
Device3 is compliant	○	○
Device4 is compliant	○	○

Correct Answer:

Answer Area

Statements	Yes	No
Device1 is compliant	○	●
Device3 is compliant	●	○
Device4 is compliant	●	○

Box 1: No -
Policy3, which requires encryption, applies to Device1.

Box 2: Yes -

Policy1, which has no encryption requirement, applies to Device3.

Box 3: Yes -

Policy2, which has no encryption requirement, applies to Device4.

NZS 5 months ago

Correct.
Device1 - Android, no encryption, Group1. Policy3 requires encryption, hence non-compliant
Device3 - Android, no encryption, G2 and G3. Policy1 applies, hence compliant
Device4 - iOS, no encryption, Group2. Policy2 applies, hence compliant

upvoted 1 times

RodrigoT 5 months, 1 week ago

Answers provided are correct.

upvoted 1 times

RodrigoT 5 months ago

N - Device1 - Group1 - Policy3 - Encryption disabled
Y - Device3 - Group3 - Policy1 (Policy2 excluded by IOS and Group3)
Y - Device4 - Group2

upvoted 1 times

Introductory Info

Case study -

This is a case study. Case studies are not timed separately. You can use as much exam time as you would like to complete each case. However, there may be additional case studies and sections on this exam. You must manage your time to ensure that you are able to complete all questions included on this exam in the time provided.

To answer the questions included in a case study, you will need to reference information that is provided in the case study. Case studies might contain exhibits and other resources that provide more information about the scenario that is described in the case study. Each question is independent of the other questions in this case study.

At the end of this case study, a review screen will appear. This screen allows you to review your answers and to make changes before you move to the next section of the exam. After you begin a new section, you cannot return to this section.

To start the case study -

To display the first question in this case study, click the Next button. Use the buttons in the left pane to explore the content of the case study before you answer the questions. Clicking these buttons displays information such as business requirements, existing environment, and problem statements. When you are ready to answer a question, click the Question button to return to the question.

Overview -

Contoso, Ltd. is a consulting company that has a main office in Montreal and two branch offices in Seattle and New York.

Contoso has the users and computers shown in the following table.

Location	Users	Laptops	Desktop computers	Mobile devices
Montreal	2,500	2,800	300	3,100
Seattle	1,000	1,100	200	1,500
New York	300	320	30	400

The company has IT, human resources (HR), legal (LEG), marketing (MKG) and finance (FIN) departments.

Contoso uses Microsoft Store for Business and recently purchased a Microsoft 365 subscription.

The company is opening a new branch office in Phoenix. Most of the users in the Phoenix office will work from home.

Existing Environment -

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

All member servers run Windows Server 2016. All laptops and desktop computers run Windows 10 Enterprise.

The computers are managed by using Microsoft Endpoint Configuration Manager. The mobile devices are managed by using Microsoft Intune.

The naming convention for the computers is the department acronym, followed by a hyphen, and then four numbers, for example, FIN-6785. All the computers are joined to the on-premises Active Directory domain.

Each department has an organizational unit (OU) that contains a child OU named Computers. Each computer account is in the Computers OU of its respective department.

Intune Configuration -

The domain has the users shown in the following table.

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

User2 is a device enrollment manager (DEM) in Intune.

The devices enrolled in Intune are shown in the following table.

Name	Platform	Encryption	Member of
Device1	Android	Disabled	Group1
Device2	iOS	*Not applicable*	Group2, Group3
Device3	Android	Disabled	Group2, Group3
Device4	iOS	*Not applicable*	Group2

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

Name	Platform	Require encryption	Assigned
Policy1	Android	Not configured	Yes
Policy2	iOS	*Not applicable*	Yes
Policy3	Android	Require	Yes

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

Name	Include	Exclude
Policy1	Group3	*None*
Policy2	Group2	Group3
Policy3	Group1	*None*

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

Priority	Name	Device limit	Assigned to
1	Restriction1	15	GroupB
2	Restriction2	10	GroupA
Default	All users	5	All users

Requirements -

Planned Changes -

Contoso plans to implement the following changes:

Provide new computers to the Phoenix office users. The new computers have Windows 10 Pro preinstalled and were purchased already.

Start using a free Microsoft Store for Business app named App1.

Implement co-management for the computers.

▪

Technical Requirements -

Contoso must meet the following technical requirements:

Ensure that the users in a group named Group4 can only access Microsoft Exchange Online from devices that are enrolled in Intune.

Deploy Windows 10 Enterprise to the computers of the Phoenix office users by using Windows Autopilot.

Monitor the computers in the LEG department by using Windows Analytics.

Create a provisioning package for new computers in the HR department.

Block iOS devices from sending diagnostic and usage telemetry data.

Use the principle of least privilege whenever possible.

Enable the users in the MKG department to use App1.

Pilot co-management for the IT department.

Question

HOTSPOT -

You create a new conditional access policy that has an assignment for Office 365 Exchange Online.

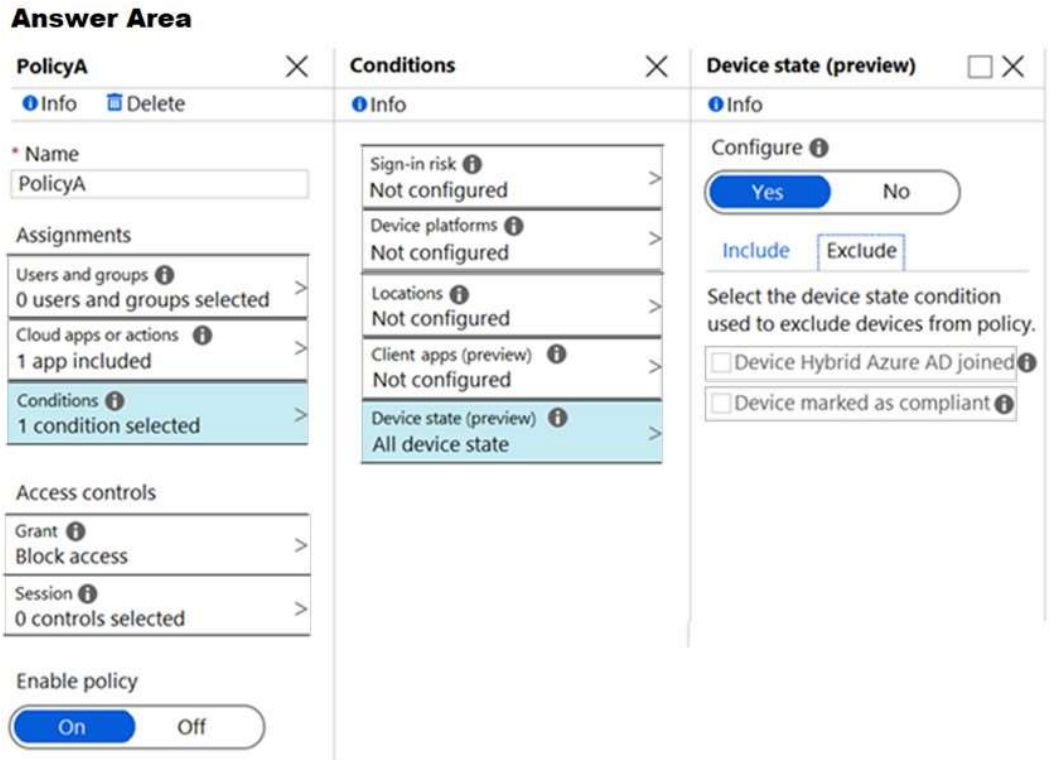
You need to configure the policy to meet the technical requirements for Group4.

Which two settings should you configure in the policy? To answer, select the appropriate settings in the answer area.

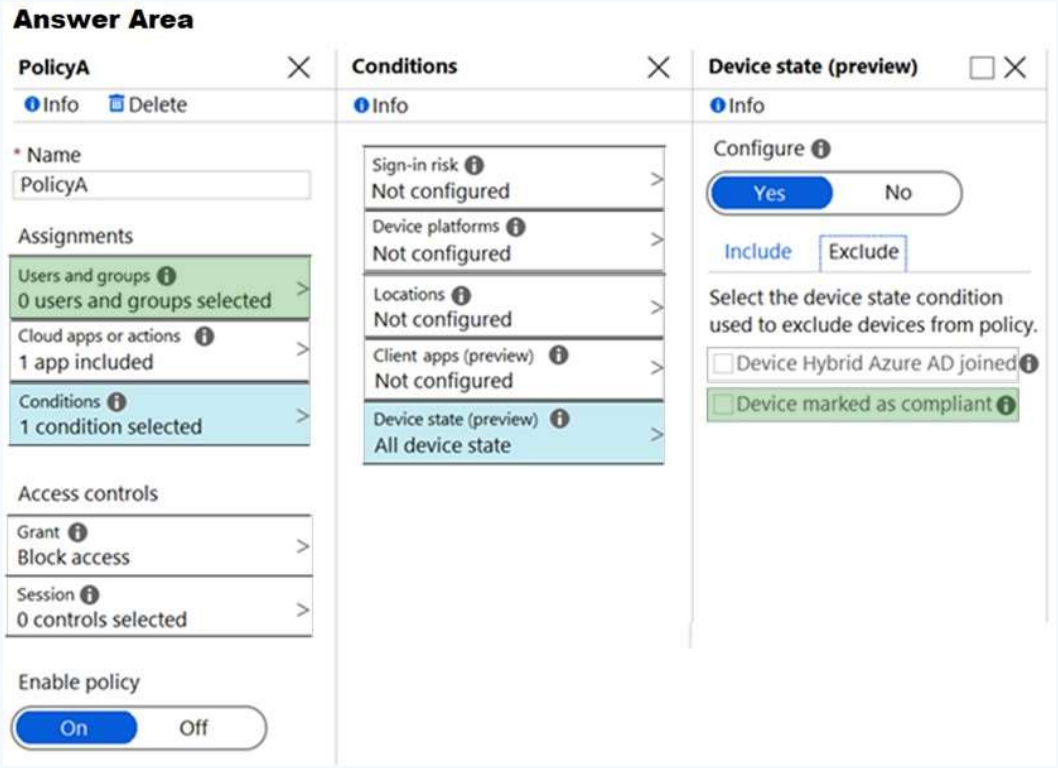
NOTE: Each correct selection is worth one point.

Hot Area:

Answer Area



Correct Answer:



The policy needs to be applied to Group4 so we need to configure Users and Groups.

The Access controls are set to Block access

We therefore need to exclude compliant devices.

From the scenario:

⇨ Ensure that the users in a group named Group4 can only access Microsoft Exchange Online from devices that are enrolled in Intune.

Note: When a device enrolls in Intune, the device information is updated in Azure AD to include the device compliance status. This compliance status is used by conditional access policies to block or allow access to e-mail and other organization resources.

Reference:

https://docs.microsoft.com/en-us/azure/active-directory/conditional-access/overview https://docs.microsoft.com/en-us/azure/active-directory/conditional-access/conditions https://docs.microsoft.com/en-us/intune/device-compliance-get-started

junior6995 2 weeks, 6 days ago

I'm not sure how old this screenshot is but as of now, to offer a complete solution we need to go to:

1 - under Cloud Apps or Actions -> Exchange Online
2 - under Grant -> Require device to be marked as compliant.

upvoted 2 times

NZS 5 months ago

Wait, who is in Group4?

upvoted 1 times

RodrigoT 5 months ago

In this case it doesn't matter. Under "Technical Requirements":
Ensure that the users in a group named Group4 can only access Microsoft Exchange Online from devices that are enrolled in Intune.

upvoted 1 times

RodrigoT 5 months, 1 week ago

Correct answers, but Device State (preview) now is called Filter for devices.

upvoted 2 times

TonySuccess 3 days, 2 hours ago

Correct x

upvoted 1 times

Topic 13 - Testlet 6

Introductory Info

Case study -

This is a case study. Case studies are not timed separately. You can use as much exam time as you would like to complete each case. However, there may be additional case studies and sections on this exam. You must manage your time to ensure that you are able to complete all questions included on this exam in the time provided.

To answer the questions included in a case study, you will need to reference information that is provided in the case study. Case studies might contain exhibits and other resources that provide more information about the scenario that is described in the case study. Each question is independent of the other questions in this case study.

At the end of this case study, a review screen will appear. This screen allows you to review your answers and to make changes before you move to the next section of the exam. After you begin a new section, you cannot return to this section.

To start the case study -

To display the first question in this case study, click the Next button. Use the buttons in the left pane to explore the content of the case study before you answer the questions. Clicking these buttons displays information such as business requirements, existing environment, and problem statements. If the case study has an

All Information tab, note that the information displayed is identical to the information displayed on the subsequent tabs. When you are ready to answer a question, click the Question button to return to the question.

Overview -

Contoso, Ltd. is a consulting company that has a main office in Montreal and branch offices in Seattle and New York.

Contoso has a Microsoft 365 E5 subscription.

Environment -

Network Environment -

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

Name	Operating system	Role
DC1	Windows Server 2019	Domain controller
Server1	Windows Server 2016	Member server
Server2	Windows Server 2019	Member server

Contoso has a hybrid Azure Active Directory (Azure AD) tenant named contoso.com.

Contoso has a Microsoft Store for Business instance.

Users and Groups -

The contoso.com tenant contains the users shown in the following table.

Name	Azure AD role	Microsoft Store for Business role	Member of
User1	Cloud device administrator	Basic Purchaser	GroupA
User2	Azure AD joined device local administrator	Device Guard signer	GroupB
User3	Global reader	Purchaser	GroupA, GroupB
User4	Global administrator	None	Group1

All users are assigned a Microsoft Office 365 license and an Enterprise Mobility + Security E3 license.

Enterprise State Roaming is enabled for Group1 and GroupA.

Group1 and Group2 have a Membership type of Assigned.

Devices -

Contoso has the Windows 10 devices shown in the following table.

Name	Type	Member of	Scope (Tags)
Device1	Corporate-owned	Group1	Default
Device2	Corporate-owned	Group1, Group2	Tag2
Device3	Personally-owned	Group1	Tag1
Device4	Personally-owned	Group2	Tag2
Device5	Corporate-owned	Group3	Default

The Windows 10 devices are joined to Azure AD and enrolled in Microsoft Intune.

The Windows 10 devices are configured as shown in the following table.

Name	BitLocker Drive Encryption (BitLocker)	Secure Boot	VPN connection
Device1	Yes	No	VPN1
Device2	Yes	Yes	VPN1, VPN3
Device3	No	No	VPN3
Device4	No	Yes	**None**
Device5	Yes	No	**None**

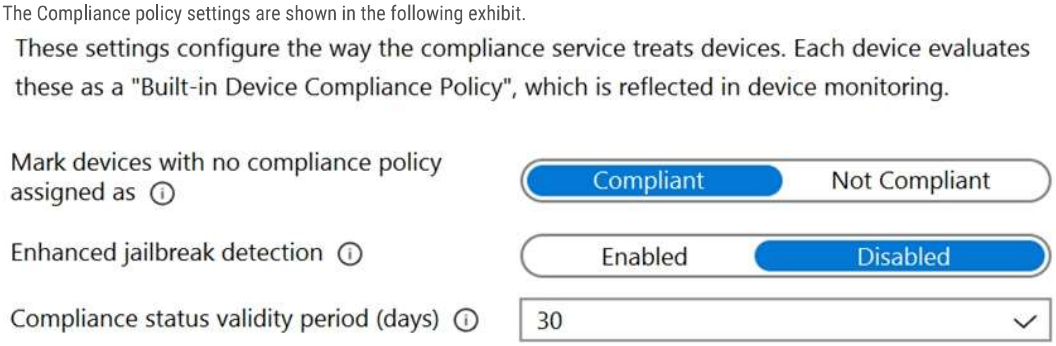
All the Azure AD joined devices have an executable file named C:\AppA.exe and a folder named D:\Folder1.

Microsoft Endpoint Manager Configuration

Microsoft Endpoint Manager has the compliance policies shown in the following table.

Name	Configuration	Assignment
Policy1	Require BitLocker only	Group1
Policy2	Require Secure Boot only	Group1
Policy3	Require BitLocker and Secure Boot	Group2

The Compliance policy settings are shown in the following exhibit.



The Automatic Enrollment settings have the following configurations:

MDM user scope: GroupA

MAM user scope: GroupB

You have an Endpoint protection configuration profile that has the following Controlled folder access settings:

Name: Protection1

Folder protection: Enable

List of apps that have access to protected folders: C:*\AppA.exe

List of additional folders that need to be protected: D:\Folder1

Assignments:

- Included groups: Group2, GroupB

Windows Autopilot Configuration -

Contoso has a Windows Autopilot deployment profile configured as shown in the following exhibit.

Create profile
Windows PC

✓ Basics ✓ Out-of-box experience (OOBE) ✓ Assignments 4 **Review + create**

Summary

Basics

Name	Profile1
Description	--
Convert all targeted devices to Autopilot	Yes
Device type	Windows PC

Out-of-box experience (OOBE)

Deployment mode	User-Driven
Join to Azure AD as	Azure AD joined
Skip AD connectivity check (preview)	No
Language (Region)	Operating system default
Automatically configure keyboard	Yes
Microsoft Software License Terms	Hide
Privacy settings	Hide
Hide change account options	Hide
User account type	Standard
Allow White Glove OOBE	No
Apply device name template	No

Assignments

Included groups	Group1
Excluded groups	Group2

Currently, there are no devices deployed by using Window Autopilot.
The Intune connector for Active Directory is installed on Server1.

Requirements -

Planned Changes -
Contoso plans to implement the following changes:
Purchase a new Windows 10 device named Device6 and enroll the device in Intune.
New computers will be deployed by using Windows Autopilot and will be hybrid Azure AD joined.
Deploy a network boundary configuration profile that will have the following settings:
- Name: Boundary1
- Network boundary: 192.168.1.0/24
- Scope tags: Tag1
- Assignments:
- - Included groups: Group1, Group2
Deploy two VPN configuration profiles named Connection1 and Connection2 that will have the following settings:
- Name: Connection1
- Connection name: VPN1
- Connection type: L2TP
- Assignments:
- - Included groups: Group1, Group2, GroupA
- - Excluded groups: --
- Name: Connection2
- Connection name: VPN2
- Connection type: IKEv2
- Assignments:
- - Included groups: GroupA
- - Excluded groups: GroupB
Purchase an app named App1 that is available in Microsoft Store for Business and to assign the app to all the users.

Technical Requirements -
Contoso must meet the following technical requirements:
Users in GroupA must be able to deploy new computers.
Administrative effort must be minimized.

Question

HOTSPOT -

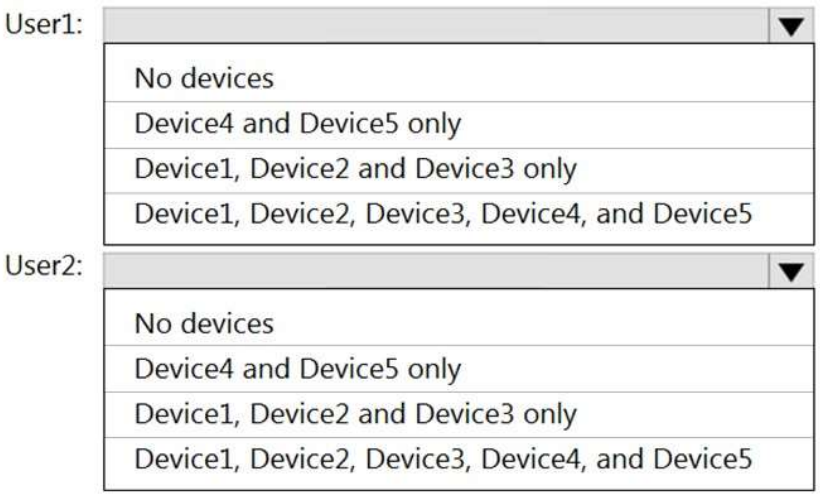
User1 and User2 plan to use Sync your settings.

On which devices can the users use Sync your settings? To answer, select the appropriate options in the answer area.

NOTE: Each correct selection is worth one point.

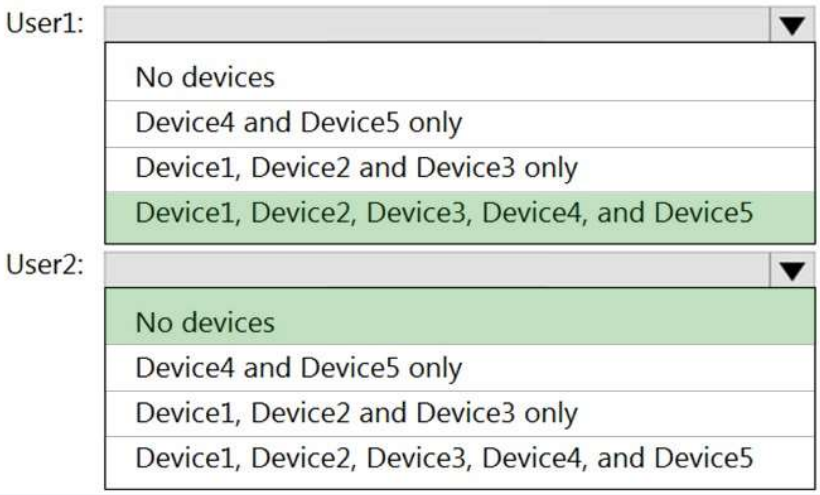
Hot Area:

Answer Area



Correct Answer:

Answer Area



Reference:

https://www.jeffgilb.com/managing-local-administrators-with-azure-ad-and-intune/

TonySuccess 1 week, 3 days ago

Another out of date one?

upvoted 1 times

NZS 5 months ago

Wrong.
User1 - Group A, ESR enabled. Group 1 devices - 1 and 2
User 2 - Group B, ESR not enabled.

upvoted 1 times

RodrigoT 5 months ago

Other opinions can be found here:
https://www.examtopics.com/discussions/microsoft/view/63126-exam-md-101-topic-12-question-1-discussion/

upvoted 1 times

RodrigoT 5 months, 1 week ago

I could only agree with this answer thinking that User1 is in GroupA, then using Enterprise State Roaming and not the Sync your settings feature.
User2 is an Azure AD joined device local administrator not included in the ESR. So he "could" use Sync your settings. But the documentation says: When Sync settings is turned on, Windows syncs the settings you choose across all your Windows 10 devices that you've signed in to with your Microsoft account. To stop syncing your settings and remove them from the cloud, turn off synced settings on all the devices connected to your Microsoft account. I don't see Microsoft Accounts in this case. Very odd question.
https://support.microsoft.com/en-us/windows/about-windows-backup-and-sync-settings-deebcba2-5bc0-4e63-279a-329926955708#WindowsVersion=Windows_10

upvoted 1 times

RodrigoT 5 months, 1 week ago

Also, the "Sync your settings" option is greyed out for all domain users, even if the domain user has connected a Microsoft account for other apps (e-mail, calendar, store, etc.).

upvoted 1 times

Introductory Info

Case study -

This is a case study. Case studies are not timed separately. You can use as much exam time as you would like to complete each case. However, there may be additional case studies and sections on this exam. You must manage your time to ensure that you are able to complete all questions included on this exam in the time provided.

To answer the questions included in a case study, you will need to reference information that is provided in the case study. Case studies might contain exhibits and other resources that provide more information about the scenario that is described in the case study. Each question is independent of the other questions in this case study.

At the end of this case study, a review screen will appear. This screen allows you to review your answers and to make changes before you move to the next section of the exam. After you begin a new section, you cannot return to this section.

To start the case study -

To display the first question in this case study, click the Next button. Use the buttons in the left pane to explore the content of the case study before you answer the questions. Clicking these buttons displays information such as business requirements, existing environment, and problem statements. If the case study has an

All Information tab, note that the information displayed is identical to the information displayed on the subsequent tabs. When you are ready to answer a question, click the Question button to return to the question.

Overview -

Contoso, Ltd. is a consulting company that has a main office in Montreal and branch offices in Seattle and New York.

Contoso has a Microsoft 365 E5 subscription.

Environment -

Network Environment -

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

Name	Operating system	Role
DC1	Windows Server 2019	Domain controller
Server1	Windows Server 2016	Member server
Server2	Windows Server 2019	Member server

Contoso has a hybrid Azure Active Directory (Azure AD) tenant named contoso.com.

Contoso has a Microsoft Store for Business instance.

Users and Groups -

The contoso.com tenant contains the users shown in the following table.

Name	Azure AD role	Microsoft Store for Business role	Member of
User1	Cloud device administrator	Basic Purchaser	GroupA
User2	Azure AD joined device local administrator	Device Guard signer	GroupB
User3	Global reader	Purchaser	GroupA, GroupB
User4	Global administrator	None	Group1

All users are assigned a Microsoft Office 365 license and an Enterprise Mobility + Security E3 license.

Enterprise State Roaming is enabled for Group1 and GroupA.

Group1 and Group2 have a Membership type of Assigned.

Devices -

Contoso has the Windows 10 devices shown in the following table.

Name	Type	Member of	Scope (Tags)
Device1	Corporate-owned	Group1	Default
Device2	Corporate-owned	Group1, Group2	Tag2
Device3	Personally-owned	Group1	Tag1
Device4	Personally-owned	Group2	Tag2
Device5	Corporate-owned	Group3	Default

The Windows 10 devices are joined to Azure AD and enrolled in Microsoft Intune.

The Windows 10 devices are configured as shown in the following table.

Name	BitLocker Drive Encryption (BitLocker)	Secure Boot	VPN connection
Device1	Yes	No	VPN1
Device2	Yes	Yes	VPN1, VPN3
Device3	No	No	VPN3
Device4	No	Yes	**None**
Device5	Yes	No	**None**

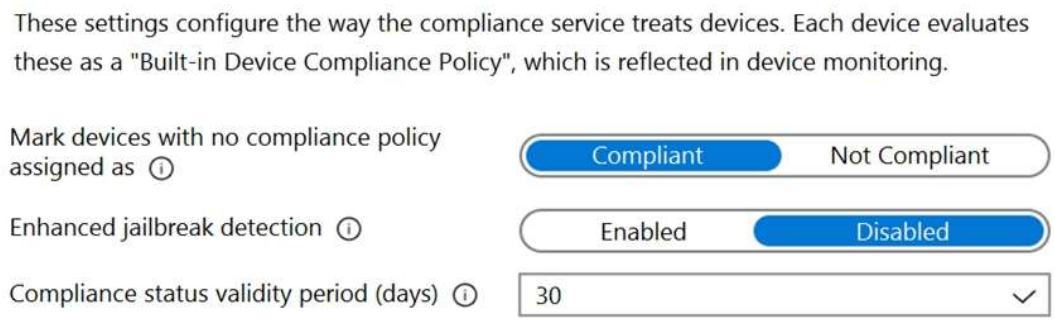
All the Azure AD joined devices have an executable file named C:\AppA.exe and a folder named D:\Folder1.

Microsoft Endpoint Manager Configuration

Microsoft Endpoint Manager has the compliance policies shown in the following table.

Name	Configuration	Assignment
Policy1	Require BitLocker only	Group1
Policy2	Require Secure Boot only	Group1
Policy3	Require BitLocker and Secure Boot	Group2

The Compliance policy settings are shown in the following exhibit.



The Automatic Enrollment settings have the following configurations:

MDM user scope: GroupA

MAM user scope: GroupB

You have an Endpoint protection configuration profile that has the following Controlled folder access settings:

Name: Protection1

Folder protection: Enable

List of apps that have access to protected folders: C:*\AppA.exe

List of additional folders that need to be protected: D:\Folder1

Assignments:

- Included groups: Group2, GroupB

Windows Autopilot Configuration -

Contoso has a Windows Autopilot deployment profile configured as shown in the following exhibit.

Create profile
Windows PC

✓ Basics ✓ Out-of-box experience (OOBE) ✓ Assignments 4 **Review + create**

Summary

Basics

Name	Profile1
Description	--
Convert all targeted devices to Autopilot	Yes
Device type	Windows PC

Out-of-box experience (OOBE)

Deployment mode	User-Driven
Join to Azure AD as	Azure AD joined
Skip AD connectivity check (preview)	No
Language (Region)	Operating system default
Automatically configure keyboard	Yes
Microsoft Software License Terms	Hide
Privacy settings	Hide
Hide change account options	Hide
User account type	Standard
Allow White Glove OOBE	No
Apply device name template	No

Assignments

Included groups	Group1
Excluded groups	Group2

Currently, there are no devices deployed by using Window Autopilot.
The Intune connector for Active Directory is installed on Server1.

Requirements -

Planned Changes -
Contoso plans to implement the following changes:
Purchase a new Windows 10 device named Device6 and enroll the device in Intune.
New computers will be deployed by using Windows Autopilot and will be hybrid Azure AD joined.
Deploy a network boundary configuration profile that will have the following settings:
- Name: Boundary1
- Network boundary: 192.168.1.0/24
- Scope tags: Tag1
- Assignments:
- - Included groups: Group1, Group2
Deploy two VPN configuration profiles named Connection1 and Connection2 that will have the following settings:
- Name: Connection1
- Connection name: VPN1
- Connection type: L2TP
- Assignments:
- - Included groups: Group1, Group2, GroupA
- - Excluded groups: --
- Name: Connection2
- Connection name: VPN2
- Connection type: IKEv2
- Assignments:
- - Included groups: GroupA
- - Excluded groups: GroupB
Purchase an app named App1 that is available in Microsoft Store for Business and to assign the app to all the users.

Technical Requirements -
Contoso must meet the following technical requirements:
Users in GroupA must be able to deploy new computers.
Administrative effort must be minimized.

Question
Which user can enroll Device6 in Intune?

A. User4 and User2 only

B. User4 and User1 only

C. User4, User1, and User2 only

D. User1, User2, User3, and User4

Correct Answer: *D*

All the users can enroll devices to Intune.

RodrigoT 5 months, 1 week ago

The point is User2 and User3 are very limited users no Azure AD.

upvoted 1 times

RodrigoT 5 months ago

User1 is in GroupA (MDM user scope: GroupA), and User4 is a Global Administrator.

upvoted 2 times

Introductory Info

Case study -

This is a case study. Case studies are not timed separately. You can use as much exam time as you would like to complete each case. However, there may be additional case studies and sections on this exam. You must manage your time to ensure that you are able to complete all questions included on this exam in the time provided.

To answer the questions included in a case study, you will need to reference information that is provided in the case study. Case studies might contain exhibits and other resources that provide more information about the scenario that is described in the case study. Each question is independent of the other questions in this case study.

At the end of this case study, a review screen will appear. This screen allows you to review your answers and to make changes before you move to the next section of the exam. After you begin a new section, you cannot return to this section.

To start the case study -

To display the first question in this case study, click the Next button. Use the buttons in the left pane to explore the content of the case study before you answer the questions. Clicking these buttons displays information such as business requirements, existing environment, and problem statements. If the case study has an

All Information tab, note that the information displayed is identical to the information displayed on the subsequent tabs. When you are ready to answer a question, click the Question button to return to the question.

Overview -

Contoso, Ltd. is a consulting company that has a main office in Montreal and branch offices in Seattle and New York.

Contoso has a Microsoft 365 E5 subscription.

Environment -

Network Environment -

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

Name	Operating system	Role
DC1	Windows Server 2019	Domain controller
Server1	Windows Server 2016	Member server
Server2	Windows Server 2019	Member server

Contoso has a hybrid Azure Active Directory (Azure AD) tenant named contoso.com.

Contoso has a Microsoft Store for Business instance.

Users and Groups -

The contoso.com tenant contains the users shown in the following table.

Name	Azure AD role	Microsoft Store for Business role	Member of
User1	Cloud device administrator	Basic Purchaser	GroupA
User2	Azure AD joined device local administrator	Device Guard signer	GroupB
User3	Global reader	Purchaser	GroupA, GroupB
User4	Global administrator	None	Group1

All users are assigned a Microsoft Office 365 license and an Enterprise Mobility + Security E3 license.

Enterprise State Roaming is enabled for Group1 and GroupA.

Group1 and Group2 have a Membership type of Assigned.

Devices -

Contoso has the Windows 10 devices shown in the following table.

Name	Type	Member of	Scope (Tags)
Device1	Corporate-owned	Group1	Default
Device2	Corporate-owned	Group1, Group2	Tag2
Device3	Personally-owned	Group1	Tag1
Device4	Personally-owned	Group2	Tag2
Device5	Corporate-owned	Group3	Default

The Windows 10 devices are joined to Azure AD and enrolled in Microsoft Intune.

The Windows 10 devices are configured as shown in the following table.

Name	BitLocker Drive Encryption (BitLocker)	Secure Boot	VPN connection
Device1	Yes	No	VPN1
Device2	Yes	Yes	VPN1, VPN3
Device3	No	No	VPN3
Device4	No	Yes	**None**
Device5	Yes	No	**None**

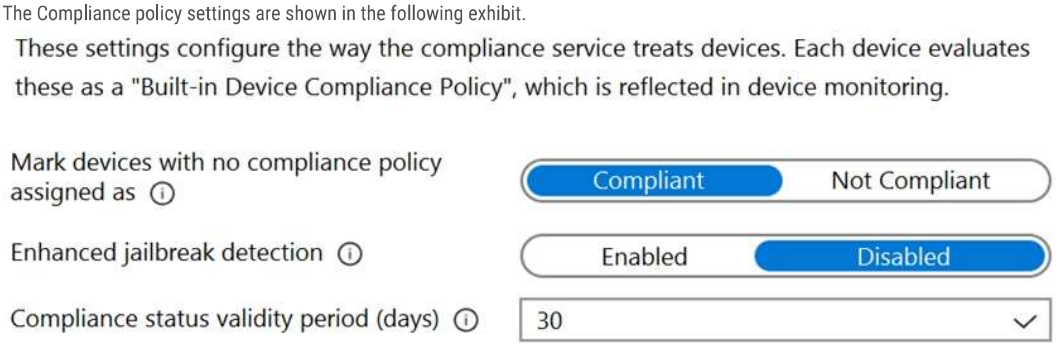
All the Azure AD joined devices have an executable file named C:\AppA.exe and a folder named D:\Folder1.

Microsoft Endpoint Manager Configuration

Microsoft Endpoint Manager has the compliance policies shown in the following table.

Name	Configuration	Assignment
Policy1	Require BitLocker only	Group1
Policy2	Require Secure Boot only	Group1
Policy3	Require BitLocker and Secure Boot	Group2

The Compliance policy settings are shown in the following exhibit.



The Automatic Enrollment settings have the following configurations:

MDM user scope: GroupA

MAM user scope: GroupB

You have an Endpoint protection configuration profile that has the following Controlled folder access settings:

Name: Protection1

Folder protection: Enable

List of apps that have access to protected folders: C:*\AppA.exe

List of additional folders that need to be protected: D:\Folder1

Assignments:

- Included groups: Group2, GroupB

Windows Autopilot Configuration -

Contoso has a Windows Autopilot deployment profile configured as shown in the following exhibit.

Create profile
Windows PC

✓ Basics ✓ Out-of-box experience (OOBE) ✓ Assignments (4) **Review + create**

Summary

Basics

Name	Profile1
Description	--
Convert all targeted devices to Autopilot	Yes
Device type	Windows PC

Out-of-box experience (OOBE)

Deployment mode	User-Driven
Join to Azure AD as	Azure AD joined
Skip AD connectivity check (preview)	No
Language (Region)	Operating system default
Automatically configure keyboard	Yes
Microsoft Software License Terms	Hide
Privacy settings	Hide
Hide change account options	Hide
User account type	Standard
Allow White Glove OOBE	No
Apply device name template	No

Assignments

Included groups	Group1
Excluded groups	Group2

Currently, there are no devices deployed by using Window Autopilot.
The Intune connector for Active Directory is installed on Server1.

Requirements -

Planned Changes -
Contoso plans to implement the following changes:
Purchase a new Windows 10 device named Device6 and enroll the device in Intune.
New computers will be deployed by using Windows Autopilot and will be hybrid Azure AD joined.
Deploy a network boundary configuration profile that will have the following settings:
- Name: Boundary1
- Network boundary: 192.168.1.0/24
- Scope tags: Tag1
- Assignments:
- - Included groups: Group1, Group2
Deploy two VPN configuration profiles named Connection1 and Connection2 that will have the following settings:
- Name: Connection1
- Connection name: VPN1
- Connection type: L2TP
- Assignments:
- - Included groups: Group1, Group2, GroupA
- - Excluded groups: --
- Name: Connection2
- Connection name: VPN2
- Connection type: IKEv2
- Assignments:
- - Included groups: GroupA
- - Excluded groups: GroupB
Purchase an app named App1 that is available in Microsoft Store for Business and to assign the app to all the users.

Technical Requirements -
Contoso must meet the following technical requirements:
Users in GroupA must be able to deploy new computers.
Administrative effort must be minimized.

Question

HOTSPOT -

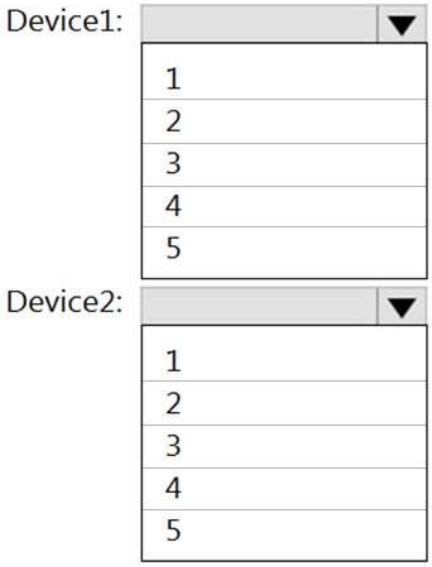
You implement the planned changes for Connection1 and Connection2.

How many VPN connections will there be for User1 when the user signs in to Device1 and Device2? To answer, select the appropriate options in the answer area.

NOTE: Each correct selection is worth one point.

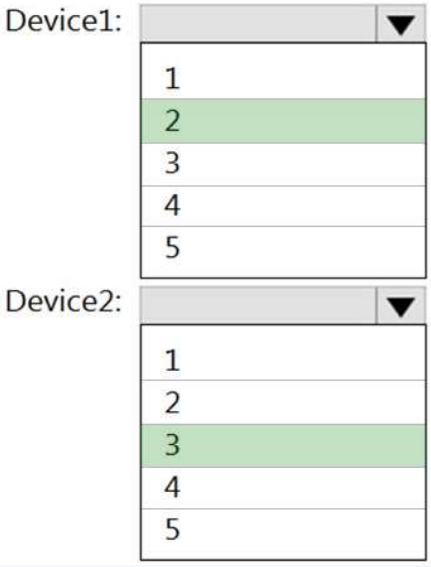
Hot Area:

Answer Area



Correct Answer:

Answer Area



Box 1: 2 -

Device1 has VPN1 and VPN2.

Box 2: 3 -

Device2 has VPN1, VPN2 (group assignment), and VPN3

RodrigoT 5 months, 1 week ago

Answers provided are wrong.
User1 is in GroupA. So:
2- Device1: VPN1 (pre configured) and VPN2 (added by Group A)
3- Device2: VPN1 and VPN3 (pre configured), VPN2 (added by Group A)

upvoted 3 times

Introductory Info

Case study -

This is a case study. Case studies are not timed separately. You can use as much exam time as you would like to complete each case. However, there may be additional case studies and sections on this exam. You must manage your time to ensure that you are able to complete all questions included on this exam in the time provided.

To answer the questions included in a case study, you will need to reference information that is provided in the case study. Case studies might contain exhibits and other resources that provide more information about the scenario that is described in the case study. Each question is independent of the other questions in this case study.

At the end of this case study, a review screen will appear. This screen allows you to review your answers and to make changes before you move to the next section of the exam. After you begin a new section, you cannot return to this section.

To start the case study -

To display the first question in this case study, click the Next button. Use the buttons in the left pane to explore the content of the case study before you answer the questions. Clicking these buttons displays information such as business requirements, existing environment, and problem statements. If the case study has an

All Information tab, note that the information displayed is identical to the information displayed on the subsequent tabs. When you are ready to answer a question, click the Question button to return to the question.

Overview -

Contoso, Ltd. is a consulting company that has a main office in Montreal and branch offices in Seattle and New York.

Contoso has a Microsoft 365 E5 subscription.

Environment -

Network Environment -

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

Name	Operating system	Role
DC1	Windows Server 2019	Domain controller
Server1	Windows Server 2016	Member server
Server2	Windows Server 2019	Member server

Contoso has a hybrid Azure Active Directory (Azure AD) tenant named contoso.com.

Contoso has a Microsoft Store for Business instance.

Users and Groups -

The contoso.com tenant contains the users shown in the following table.

Name	Azure AD role	Microsoft Store for Business role	Member of
User1	Cloud device administrator	Basic Purchaser	GroupA
User2	Azure AD joined device local administrator	Device Guard signer	GroupB
User3	Global reader	Purchaser	GroupA, GroupB
User4	Global administrator	None	Group1

All users are assigned a Microsoft Office 365 license and an Enterprise Mobility + Security E3 license.

Enterprise State Roaming is enabled for Group1 and GroupA.

Group1 and Group2 have a Membership type of Assigned.

Devices -

Contoso has the Windows 10 devices shown in the following table.

Name	Type	Member of	Scope (Tags)
Device1	Corporate-owned	Group1	Default
Device2	Corporate-owned	Group1, Group2	Tag2
Device3	Personally-owned	Group1	Tag1
Device4	Personally-owned	Group2	Tag2
Device5	Corporate-owned	Group3	Default

The Windows 10 devices are joined to Azure AD and enrolled in Microsoft Intune.

The Windows 10 devices are configured as shown in the following table.

Name	BitLocker Drive Encryption (BitLocker)	Secure Boot	VPN connection
Device1	Yes	No	VPN1
Device2	Yes	Yes	VPN1, VPN3
Device3	No	No	VPN3
Device4	No	Yes	**None**
Device5	Yes	No	**None**

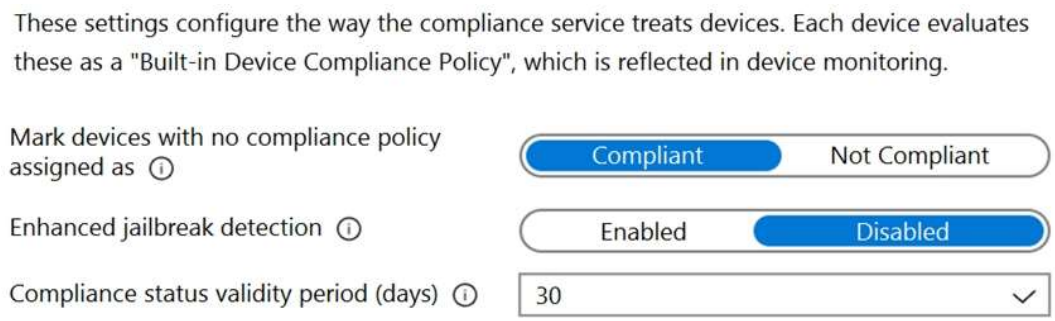
All the Azure AD joined devices have an executable file named C:\AppA.exe and a folder named D:\Folder1.

Microsoft Endpoint Manager Configuration

Microsoft Endpoint Manager has the compliance policies shown in the following table.

Name	Configuration	Assignment
Policy1	Require BitLocker only	Group1
Policy2	Require Secure Boot only	Group1
Policy3	Require BitLocker and Secure Boot	Group2

The Compliance policy settings are shown in the following exhibit.



The Automatic Enrollment settings have the following configurations:

MDM user scope: GroupA

MAM user scope: GroupB

You have an Endpoint protection configuration profile that has the following Controlled folder access settings:

Name: Protection1

Folder protection: Enable

List of apps that have access to protected folders: C:*\AppA.exe

List of additional folders that need to be protected: D:\Folder1

Assignments:

- Included groups: Group2, GroupB

Windows Autopilot Configuration -

Contoso has a Windows Autopilot deployment profile configured as shown in the following exhibit.

Create profile
Windows PC

✓ Basics ✓ Out-of-box experience (OOBE) ✓ Assignments (4) **Review + create**

Summary

Basics

Name	Profile1
Description	--
Convert all targeted devices to Autopilot	Yes
Device type	Windows PC

Out-of-box experience (OOBE)

Deployment mode	User-Driven
Join to Azure AD as	Azure AD joined
Skip AD connectivity check (preview)	No
Language (Region)	Operating system default
Automatically configure keyboard	Yes
Microsoft Software License Terms	Hide
Privacy settings	Hide
Hide change account options	Hide
User account type	Standard
Allow White Glove OOBE	No
Apply device name template	No

Assignments

Included groups	Group1
Excluded groups	Group2

Currently, there are no devices deployed by using Window Autopilot.
The Intune connector for Active Directory is installed on Server1.

Requirements -

Planned Changes -
Contoso plans to implement the following changes:
Purchase a new Windows 10 device named Device6 and enroll the device in Intune.
New computers will be deployed by using Windows Autopilot and will be hybrid Azure AD joined.
Deploy a network boundary configuration profile that will have the following settings:
- Name: Boundary1
- Network boundary: 192.168.1.0/24
- Scope tags: Tag1
- Assignments:
- - Included groups: Group1, Group2
Deploy two VPN configuration profiles named Connection1 and Connection2 that will have the following settings:
- Name: Connection1
- Connection name: VPN1
- Connection type: L2TP
- Assignments:
- - Included groups: Group1, Group2, GroupA
- - Excluded groups: --
- Name: Connection2
- Connection name: VPN2
- Connection type: IKEv2
- Assignments:
- - Included groups: GroupA
- - Excluded groups: GroupB
Purchase an app named App1 that is available in Microsoft Store for Business and to assign the app to all the users.

Technical Requirements -
Contoso must meet the following technical requirements:
Users in GroupA must be able to deploy new computers.
Administrative effort must be minimized.

Question

HOTSPOT -

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 compliant.	○	○
Device4 is marked as compliant.	○	○
Device5 is marked as compliant.	○	○

Correct Answer:

Answer Area

Statements	Yes	No
Device1 is marked as compliant.	○	○
Device4 is marked as compliant.	○	○
Device5 is marked as compliant.	○	○

thuba_TD 1 week, 6 days ago

the first answer is wrong
its NNY

upvoted 1 times

RodrigoT 5 months, 1 week ago

The first answer is wrong.
N-Device1 Group1: Policy1 and Policy2 - No secure Boot
N-Device4 Group2: Policy3 - No BitLocker
Y-Device5 Group3: No policy applied
Mark devices with no compliance policy assigned as Compliant is set

upvoted 2 times

Introductory Info

Case study -

This is a case study. Case studies are not timed separately. You can use as much exam time as you would like to complete each case. However, there may be additional case studies and sections on this exam. You must manage your time to ensure that you are able to complete all questions included on this exam in the time provided.

To answer the questions included in a case study, you will need to reference information that is provided in the case study. Case studies might contain exhibits and other resources that provide more information about the scenario that is described in the case study. Each question is independent of the other questions in this case study.

At the end of this case study, a review screen will appear. This screen allows you to review your answers and to make changes before you move to the next section of the exam. After you begin a new section, you cannot return to this section.

To start the case study -

To display the first question in this case study, click the Next button. Use the buttons in the left pane to explore the content of the case study before you answer the questions. Clicking these buttons displays information such as business requirements, existing environment, and problem statements. If the case study has an

All Information tab, note that the information displayed is identical to the information displayed on the subsequent tabs. When you are ready to answer a question, click the Question button to return to the question.

Overview -

Contoso, Ltd. is a consulting company that has a main office in Montreal and branch offices in Seattle and New York.

Contoso has a Microsoft 365 E5 subscription.

Environment -

Network Environment -

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

Name	Operating system	Role
DC1	Windows Server 2019	Domain controller
Server1	Windows Server 2016	Member server
Server2	Windows Server 2019	Member server

Contoso has a hybrid Azure Active Directory (Azure AD) tenant named contoso.com.

Contoso has a Microsoft Store for Business instance.

Users and Groups -

The contoso.com tenant contains the users shown in the following table.

Name	Azure AD role	Microsoft Store for Business role	Member of
User1	Cloud device administrator	Basic Purchaser	GroupA
User2	Azure AD joined device local administrator	Device Guard signer	GroupB
User3	Global reader	Purchaser	GroupA, GroupB
User4	Global administrator	None	Group1

All users are assigned a Microsoft Office 365 license and an Enterprise Mobility + Security E3 license.

Enterprise State Roaming is enabled for Group1 and GroupA.

Group1 and Group2 have a Membership type of Assigned.

Devices -

Contoso has the Windows 10 devices shown in the following table.

Name	Type	Member of	Scope (Tags)
Device1	Corporate-owned	Group1	Default
Device2	Corporate-owned	Group1, Group2	Tag2
Device3	Personally-owned	Group1	Tag1
Device4	Personally-owned	Group2	Tag2
Device5	Corporate-owned	Group3	Default

The Windows 10 devices are joined to Azure AD and enrolled in Microsoft Intune.

The Windows 10 devices are configured as shown in the following table.

Name	BitLocker Drive Encryption (BitLocker)	Secure Boot	VPN connection
Device1	Yes	No	VPN1
Device2	Yes	Yes	VPN1, VPN3
Device3	No	No	VPN3
Device4	No	Yes	**None**
Device5	Yes	No	**None**

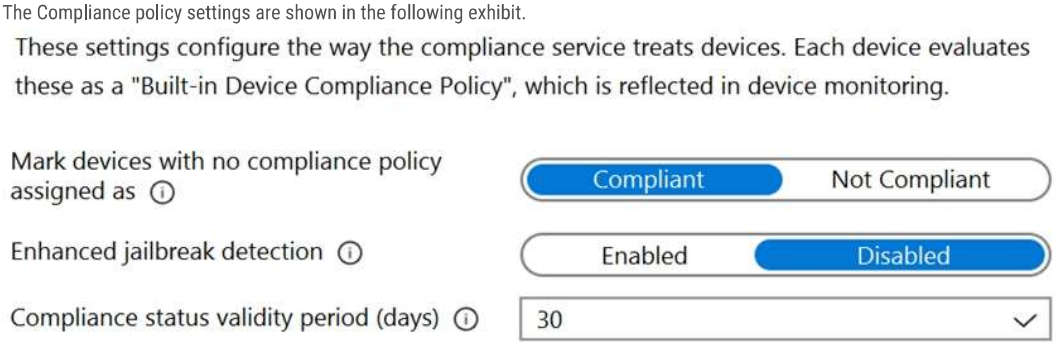
All the Azure AD joined devices have an executable file named C:\AppA.exe and a folder named D:\Folder1.

Microsoft Endpoint Manager Configuration

Microsoft Endpoint Manager has the compliance policies shown in the following table.

Name	Configuration	Assignment
Policy1	Require BitLocker only	Group1
Policy2	Require Secure Boot only	Group1
Policy3	Require BitLocker and Secure Boot	Group2

The Compliance policy settings are shown in the following exhibit.



The Automatic Enrollment settings have the following configurations:

MDM user scope: GroupA

MAM user scope: GroupB

You have an Endpoint protection configuration profile that has the following Controlled folder access settings:

Name: Protection1

Folder protection: Enable

List of apps that have access to protected folders: C:*\AppA.exe

List of additional folders that need to be protected: D:\Folder1

Assignments:

- Included groups: Group2, GroupB

Windows Autopilot Configuration -

Contoso has a Windows Autopilot deployment profile configured as shown in the following exhibit.

Create profile
Windows PC

✓ Basics ✓ Out-of-box experience (OOBE) ✓ Assignments 4 **Review + create**

Summary

Basics

Name	Profile1
Description	--
Convert all targeted devices to Autopilot	Yes
Device type	Windows PC

Out-of-box experience (OOBE)

Deployment mode	User-Driven
Join to Azure AD as	Azure AD joined
Skip AD connectivity check (preview)	No
Language (Region)	Operating system default
Automatically configure keyboard	Yes
Microsoft Software License Terms	Hide
Privacy settings	Hide
Hide change account options	Hide
User account type	Standard
Allow White Glove OOBE	No
Apply device name template	No

Assignments

Included groups	Group1
Excluded groups	Group2

Currently, there are no devices deployed by using Window Autopilot.
The Intune connector for Active Directory is installed on Server1.

Requirements -

Planned Changes -
Contoso plans to implement the following changes:
Purchase a new Windows 10 device named Device6 and enroll the device in Intune.
New computers will be deployed by using Windows Autopilot and will be hybrid Azure AD joined.
Deploy a network boundary configuration profile that will have the following settings:
- Name: Boundary1
- Network boundary: 192.168.1.0/24
- Scope tags: Tag1
- Assignments:
- - Included groups: Group1, Group2
Deploy two VPN configuration profiles named Connection1 and Connection2 that will have the following settings:
- Name: Connection1
- Connection name: VPN1
- Connection type: L2TP
- Assignments:
- - Included groups: Group1, Group2, GroupA
- - Excluded groups: --
- Name: Connection2
- Connection name: VPN2
- Connection type: IKEv2
- Assignments:
- - Included groups: GroupA
- - Excluded groups: GroupB
Purchase an app named App1 that is available in Microsoft Store for Business and to assign the app to all the users.

Technical Requirements -
Contoso must meet the following technical requirements:
Users in GroupA must be able to deploy new computers.
Administrative effort must be minimized.

Question

HOTSPOT -

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 create a file named D:\Folder1\file1.txt on Device4 by using Notepad.	○	○
User2 can remove D:\Folder1 from the list of protected folders on Device2.	○	○
User3 can create a file named C:\Users\User3\Desktop\file1.txt on Device2 by running a custom Windows PowerShell script.	○	○

Correct Answer:

Answer Area

Statements	Yes	No
User1 can create a file named D:\Folder1\file1.txt on Device4 by using Notepad.	○	●
User2 can remove D:\Folder1 from the list of protected folders on Device2.	●	○
User3 can create a file named C:\Users\User3\Desktop\file1.txt on Device2 by running a custom Windows PowerShell script.	○	●

Topic 14 - Testlet 7

My opinion:
N- User1 - GroupA and not using AppA.exe
Y- User2 - GroupB and Azure AD joined device local administrator. Users with this role become local machine administrators on all Windows 10 devices that are joined to Azure Active Directory. Link: https://docs.microsoft.com/en-us/azure/active-directory/roles/permissions-reference#azure-ad-joined-device-local-administrator
Y- User3 - The Desktop folder is not protected.

upvoted 2 times

Introductory Info

Case study -

This is a case study. Case studies are not timed separately. You can use as much exam time as you would like to complete each case. However, there may be additional case studies and sections on this exam. You must manage your time to ensure that you are able to complete all questions included on this exam in the time provided.

To answer the questions included in a case study, you will need to reference information that is provided in the case study. Case studies might contain exhibits and other resources that provide more information about the scenario that is described in the case study. Each question is independent of the other questions in this case study.

At the end of this case study, a review screen will appear. This screen allows you to review your answers and to make changes before you move to the next section of the exam. After you begin a new section, you cannot return to this section.

To start the case study -

To display the first question in this case study, click the Next button. Use the buttons in the left pane to explore the content of the case study before you answer the questions. Clicking these buttons displays information such as business requirements, existing environment, and problem statements. When you are ready to answer a question, click the Question button to return to the question.

Overview -

Contoso, Ltd. is a consulting company that has a main office in Montreal and two branch offices in Seattle and New York.

Contoso has the users and computers shown in the following table.

Location	Users	Laptops	Desktop computers	Mobile devices
Montreal	2,500	2,800	300	3,100
Seattle	1,000	1,100	200	1,500
New York	300	320	30	400

The company has IT, human resources (HR), legal (LEG), marketing (MKG) and finance (FIN) departments.

Contoso uses Microsoft Store for Business and recently purchased a Microsoft 365 subscription.

The company is opening a new branch office in Phoenix. Most of the users in the Phoenix office will work from home.

Existing Environment -

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

All member servers run Windows Server 2016. All laptops and desktop computers run Windows 10 Enterprise.

The computers are managed by using Microsoft Endpoint Configuration Manager. The mobile devices are managed by using Microsoft Intune.

The naming convention for the computers is the department acronym, followed by a hyphen, and then four numbers, for example, FIN-6785. All the computers are joined to the on-premises Active Directory domain.

Each department has an organizational unit (OU) that contains a child OU named Computers. Each computer account is in the Computers OU of its respective department.

Intune Configuration -

The domain has the users shown in the following table.

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

User2 is a device enrollment manager (DEM) in Intune.

The devices enrolled in Intune are shown in the following table.

Name	Platform	Encryption	Member of
Device1	Android	Disabled	Group1
Device2	iOS	*Not applicable*	Group2, Group3
Device3	Android	Disabled	Group2, Group3
Device4	iOS	*Not applicable*	Group2

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

Name	Platform	Require encryption	Assigned
Policy1	Android	Not configured	Yes
Policy2	iOS	*Not applicable*	Yes
Policy3	Android	Require	Yes

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

Name	Include	Exclude
Policy1	Group3	None
Policy2	Group2	Group3
Policy3	Group1	None

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

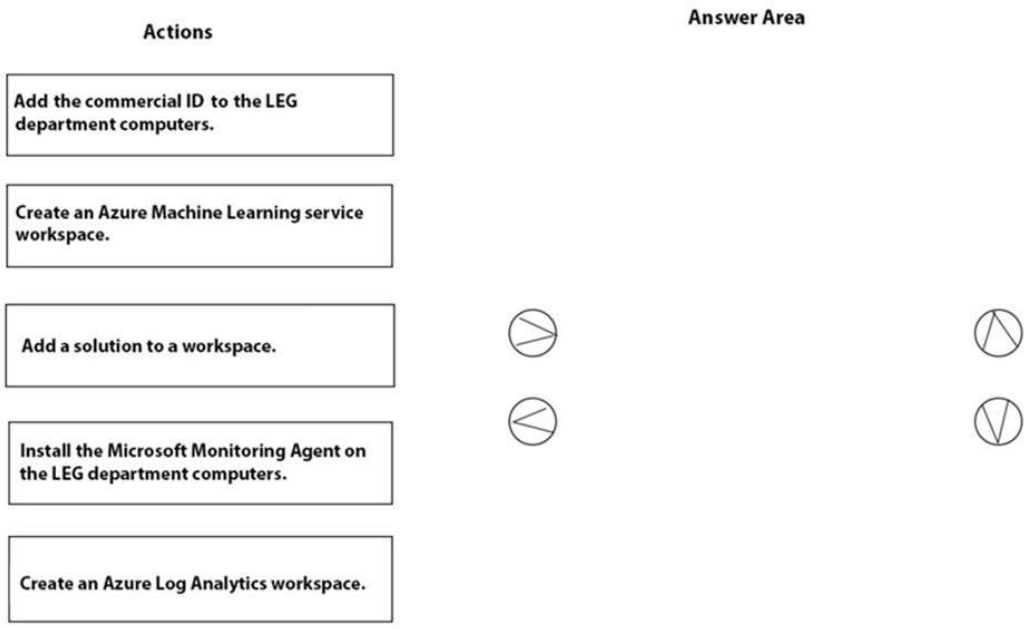
Priority	Name	Device limit	Assigned to
1	Restriction1	15	GroupB
2	Restriction2	10	GroupA
Default	All users	5	All users

Requirements -

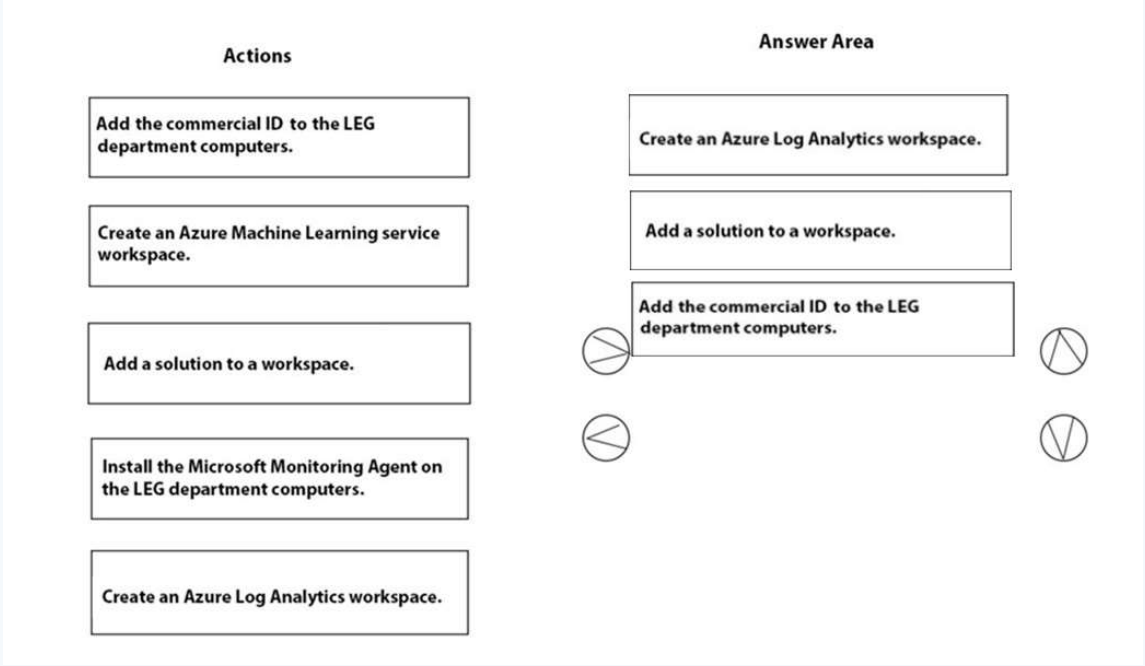
Planned Changes -
Contoso plans to implement the following changes:
Provide new computers to the Phoenix office users. The new computers have Windows 10 Pro preinstalled and were purchased already.
Start using a free Microsoft Store for Business app named App1.
Implement co-management for the computers.
▪

Technical Requirements -
Contoso must meet the following technical requirements:
Ensure that the users in a group named Group4 can only access Microsoft Exchange Online from devices that are enrolled in Intune.
Deploy Windows 10 Enterprise to the computers of the Phoenix office users by using Windows Autopilot.
Monitor the computers in the LEG department by using Windows Analytics.
Create a provisioning package for new computers in the HR department.
Block iOS devices from sending diagnostic and usage telemetry data.
Use the principle of least privilege whenever possible.
Enable the users in the MKG department to use App1.
Pilot co-management for the IT department.

Question
DRAG DROP -
You need to meet the technical requirements for the LEG department computers.
Which three actions should you perform in sequence? To answer, move the appropriate actions from the list of actions to the answer area and arrange them in the correct order.
Select and Place:



Correct Answer:



Step 3: Add the commercial ID to the LEG department computers

The build in diagnostics/telemetry data needs to be configured to with the correct commercial ID.

Reference:

https://docs.microsoft.com/en-us/mem/configmgr/desktop-analytics/set-up https://systemcenterdudes.com/sccm-windows-analytics-log-analytics/

NIOBruno 5 months ago

Wrong answer.
According to the link below.

1. Create Log Analytics workspace
2. Add a solution to the workspace
3. Add the Commercial ID

https://www.systemcenterdudes.com/sccm-windows-analytics-log-analytics/

upvoted 3 times

Topic 15 - Testlet 8

Introductory Info

Case study -

This is a case study. Case studies are not timed separately. You can use as much exam time as you would like to complete each case. However, there may be additional case studies and sections on this exam. You must manage your time to ensure that you are able to complete all questions included on this exam in the time provided.

To answer the questions included in a case study, you will need to reference information that is provided in the case study. Case studies might contain exhibits and other resources that provide more information about the scenario that is described in the case study. Each question is independent of the other questions in this case study.

At the end of this case study, a review screen will appear. This screen allows you to review your answers and to make changes before you move to the next section of the exam. After you begin a new section, you cannot return to this section.

To start the case study -

To display the first question in this case study, click the Next button. Use the buttons in the left pane to explore the content of the case study before you answer the questions. Clicking these buttons displays information such as business requirements, existing environment, and problem statements. If the case study has an

All Information tab, note that the information displayed is identical to the information displayed on the subsequent tabs. When you are ready to answer a question, click the Question button to return to the question.

Overview -

Contoso, Ltd. is a consulting company that has a main office in Montreal and branch offices in Seattle and New York.

Contoso has a Microsoft 365 E5 subscription.

Environment -

Network Environment -

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

Name	Operating system	Role
DC1	Windows Server 2019	Domain controller
Server1	Windows Server 2016	Member server
Server2	Windows Server 2019	Member server

Contoso has a hybrid Azure Active Directory (Azure AD) tenant named contoso.com.

Contoso has a Microsoft Store for Business instance.

Users and Groups -

The contoso.com tenant contains the users shown in the following table.

Name	Azure AD role	Microsoft Store for Business role	Member of
User1	Cloud device administrator	Basic Purchaser	GroupA
User2	Azure AD joined device local administrator	Device Guard signer	GroupB
User3	Global reader	Purchaser	GroupA, GroupB
User4	Global administrator	None	Group1

All users are assigned a Microsoft Office 365 license and an Enterprise Mobility + Security E3 license.

Enterprise State Roaming is enabled for Group1 and GroupA.

Group1 and Group2 have a Membership type of Assigned.

Devices -

Contoso has the Windows 10 devices shown in the following table.

Name	Type	Member of	Scope (Tags)
Device1	Corporate-owned	Group1	Default
Device2	Corporate-owned	Group1, Group2	Tag2
Device3	Personally-owned	Group1	Tag1
Device4	Personally-owned	Group2	Tag2
Device5	Corporate-owned	Group3	Default

The Windows 10 devices are joined to Azure AD and enrolled in Microsoft Intune.

The Windows 10 devices are configured as shown in the following table.

Name	BitLocker Drive Encryption (BitLocker)	Secure Boot	VPN connection
Device1	Yes	No	VPN1
Device2	Yes	Yes	VPN1, VPN3
Device3	No	No	VPN3
Device4	No	Yes	**None**
Device5	Yes	No	**None**

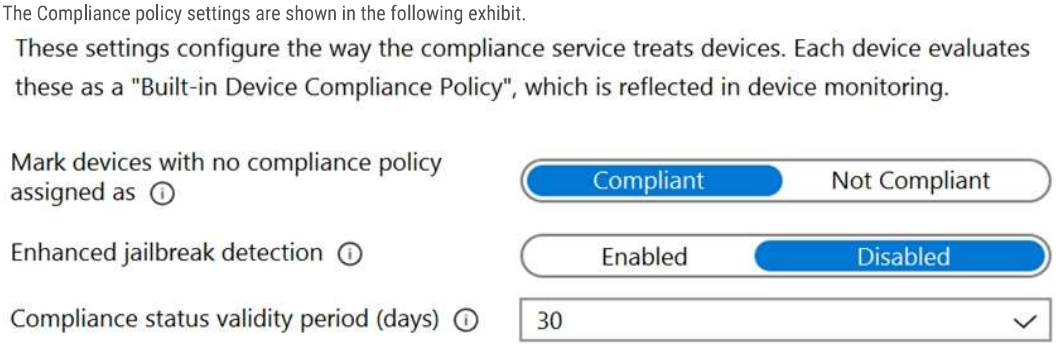
All the Azure AD joined devices have an executable file named C:\AppA.exe and a folder named D:\Folder1.

Microsoft Endpoint Manager Configuration

Microsoft Endpoint Manager has the compliance policies shown in the following table.

Name	Configuration	Assignment
Policy1	Require BitLocker only	Group1
Policy2	Require Secure Boot only	Group1
Policy3	Require BitLocker and Secure Boot	Group2

The Compliance policy settings are shown in the following exhibit.



The Automatic Enrollment settings have the following configurations:

MDM user scope: GroupA

MAM user scope: GroupB

You have an Endpoint protection configuration profile that has the following Controlled folder access settings:

Name: Protection1

Folder protection: Enable

List of apps that have access to protected folders: C:*\AppA.exe

List of additional folders that need to be protected: D:\Folder1

Assignments:

- Included groups: Group2, GroupB

Windows Autopilot Configuration -

Contoso has a Windows Autopilot deployment profile configured as shown in the following exhibit.

Create profile
Windows PC

✓ Basics ✓ Out-of-box experience (OOBE) ✓ Assignments 4 **Review + create**

Summary

Basics

Name	Profile1
Description	--
Convert all targeted devices to Autopilot	Yes
Device type	Windows PC

Out-of-box experience (OOBE)

Deployment mode	User-Driven
Join to Azure AD as	Azure AD joined
Skip AD connectivity check (preview)	No
Language (Region)	Operating system default
Automatically configure keyboard	Yes
Microsoft Software License Terms	Hide
Privacy settings	Hide
Hide change account options	Hide
User account type	Standard
Allow White Glove OOBE	No
Apply device name template	No

Assignments

Included groups	Group1
Excluded groups	Group2

Currently, there are no devices deployed by using Window Autopilot.
The Intune connector for Active Directory is installed on Server1.

Requirements -

Planned Changes -
Contoso plans to implement the following changes:
Purchase a new Windows 10 device named Device6 and enroll the device in Intune.
New computers will be deployed by using Windows Autopilot and will be hybrid Azure AD joined.
Deploy a network boundary configuration profile that will have the following settings:
- Name: Boundary1
- Network boundary: 192.168.1.0/24
- Scope tags: Tag1
- Assignments:
- - Included groups: Group1, Group2
Deploy two VPN configuration profiles named Connection1 and Connection2 that will have the following settings:
- Name: Connection1
- Connection name: VPN1
- Connection type: L2TP
- Assignments:
- - Included groups: Group1, Group2, GroupA
- - Excluded groups: --
- Name: Connection2
- Connection name: VPN2
- Connection type: IKEv2
- Assignments:
- - Included groups: GroupA
- - Excluded groups: GroupB
Purchase an app named App1 that is available in Microsoft Store for Business and to assign the app to all the users.

Technical Requirements -
Contoso must meet the following technical requirements:
Users in GroupA must be able to deploy new computers.
Administrative effort must be minimized.

Question
You implement Boundary1 based on the planned changes.

Topic 16 - Testlet 9

A. Device2 only

B. Device3 only

C. Device1, Device2, and Device5 only

D. Device1, Device2, Device3, and Device4 only

Correct Answer: *D*
Device5 does not belong to Group1 or to Group2.
Note: Deploy a network boundary configuration profile that will have the following settings:

Name: Boundary1 -
Network boundary: 192.168.1.0/24

Scope tags: Tag1 -
Assignments:

Included groups: Group1, Group2 -
Reference:
https://docs.microsoft.com/en-us/mem/intune/configuration/network-boundary-windows

NZS 5 months ago
Correct. Tags are irrelevant in this case
upvoted 2 times

Introductory Info

Case study -

This is a case study. Case studies are not timed separately. You can use as much exam time as you would like to complete each case. However, there may be additional case studies and sections on this exam. You must manage your time to ensure that you are able to complete all questions included on this exam in the time provided.

To answer the questions included in a case study, you will need to reference information that is provided in the case study. Case studies might contain exhibits and other resources that provide more information about the scenario that is described in the case study. Each question is independent of the other questions in this case study.

At the end of this case study, a review screen will appear. This screen allows you to review your answers and to make changes before you move to the next section of the exam. After you begin a new section, you cannot return to this section.

To start the case study -

To display the first question in this case study, click the Next button. Use the buttons in the left pane to explore the content of the case study before you answer the questions. Clicking these buttons displays information such as business requirements, existing environment, and problem statements. If the case study has an

All Information tab, note that the information displayed is identical to the information displayed on the subsequent tabs. When you are ready to answer a question, click the Question button to return to the question.

Overview -

Contoso, Ltd. is a consulting company that has a main office in Montreal and branch offices in Seattle and New York.

Contoso has a Microsoft 365 E5 subscription.

Environment -

Network Environment -

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

Name	Operating system	Role
DC1	Windows Server 2019	Domain controller
Server1	Windows Server 2016	Member server
Server2	Windows Server 2019	Member server

Contoso has a hybrid Azure Active Directory (Azure AD) tenant named contoso.com.

Contoso has a Microsoft Store for Business instance.

Users and Groups -

The contoso.com tenant contains the users shown in the following table.

Name	Azure AD role	Microsoft Store for Business role	Member of
User1	Cloud device administrator	Basic Purchaser	GroupA
User2	Azure AD joined device local administrator	Device Guard signer	GroupB
User3	Global reader	Purchaser	GroupA, GroupB
User4	Global administrator	None	Group1

All users are assigned a Microsoft Office 365 license and an Enterprise Mobility + Security E3 license.

Enterprise State Roaming is enabled for Group1 and GroupA.

Group1 and Group2 have a Membership type of Assigned.

Devices -

Contoso has the Windows 10 devices shown in the following table.

Name	Type	Member of	Scope (Tags)
Device1	Corporate-owned	Group1	Default
Device2	Corporate-owned	Group1, Group2	Tag2
Device3	Personally-owned	Group1	Tag1
Device4	Personally-owned	Group2	Tag2
Device5	Corporate-owned	Group3	Default

The Windows 10 devices are joined to Azure AD and enrolled in Microsoft Intune.

The Windows 10 devices are configured as shown in the following table.

Name	BitLocker Drive Encryption (BitLocker)	Secure Boot	VPN connection
Device1	Yes	No	VPN1
Device2	Yes	Yes	VPN1, VPN3
Device3	No	No	VPN3
Device4	No	Yes	**None**
Device5	Yes	No	**None**

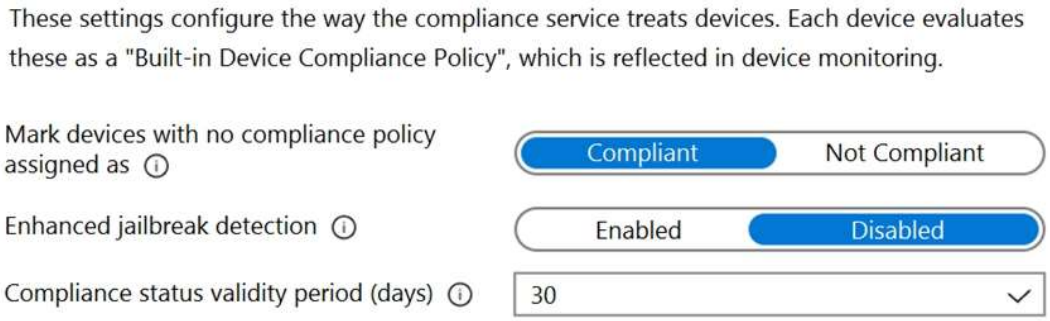
All the Azure AD joined devices have an executable file named C:\AppA.exe and a folder named D:\Folder1.

Microsoft Endpoint Manager Configuration

Microsoft Endpoint Manager has the compliance policies shown in the following table.

Name	Configuration	Assignment
Policy1	Require BitLocker only	Group1
Policy2	Require Secure Boot only	Group1
Policy3	Require BitLocker and Secure Boot	Group2

The Compliance policy settings are shown in the following exhibit.



The Automatic Enrollment settings have the following configurations:

MDM user scope: GroupA

MAM user scope: GroupB

You have an Endpoint protection configuration profile that has the following Controlled folder access settings:

Name: Protection1

Folder protection: Enable

List of apps that have access to protected folders: C:*\AppA.exe

List of additional folders that need to be protected: D:\Folder1

Assignments:

- Included groups: Group2, GroupB

Windows Autopilot Configuration -

Contoso has a Windows Autopilot deployment profile configured as shown in the following exhibit.

Create profile
Windows PC

✓ Basics ✓ Out-of-box experience (OOBE) ✓ Assignments (4) **Review + create**

Summary

Basics

Name	Profile1
Description	--
Convert all targeted devices to Autopilot	Yes
Device type	Windows PC

Out-of-box experience (OOBE)

Deployment mode	User-Driven
Join to Azure AD as	Azure AD joined
Skip AD connectivity check (preview)	No
Language (Region)	Operating system default
Automatically configure keyboard	Yes
Microsoft Software License Terms	Hide
Privacy settings	Hide
Hide change account options	Hide
User account type	Standard
Allow White Glove OOBE	No
Apply device name template	No

Assignments

Included groups	Group1
Excluded groups	Group2

Currently, there are no devices deployed by using Window Autopilot.
The Intune connector for Active Directory is installed on Server1.

Requirements -

Planned Changes -
Contoso plans to implement the following changes:
Purchase a new Windows 10 device named Device6 and enroll the device in Intune.
New computers will be deployed by using Windows Autopilot and will be hybrid Azure AD joined.
Deploy a network boundary configuration profile that will have the following settings:
- Name: Boundary1
- Network boundary: 192.168.1.0/24
- Scope tags: Tag1
- Assignments:
- - Included groups: Group1, Group2
Deploy two VPN configuration profiles named Connection1 and Connection2 that will have the following settings:
- Name: Connection1
- Connection name: VPN1
- Connection type: L2TP
- Assignments:
- - Included groups: Group1, Group2, GroupA
- - Excluded groups: --
- Name: Connection2
- Connection name: VPN2
- Connection type: IKEv2
- Assignments:
- - Included groups: GroupA
- - Excluded groups: GroupB
Purchase an app named App1 that is available in Microsoft Store for Business and to assign the app to all the users.

Technical Requirements -
Contoso must meet the following technical requirements:
Users in GroupA must be able to deploy new computers.
Administrative effort must be minimized.

Question
Which users can purchase and assign App1?

A. User3 only

B. User1 and User3 only

C. User1, User2, User3, and User4

D. User1, User3, and User4 only

E. User3 and User4 only

Correct Answer: *D*

Reference:

https://docs.microsoft.com/en-us/microsoft-store/acquire-apps-microsoft-store-for-business

NIOBruno 5 months ago

Wrong.
Answer is User 1, User 3, and User 4.

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.
https://docs.microsoft.com/en-us/microsoft-store/roles-and-permissions-microsoft-store-for-business

upvoted 1 times

RodrigoT 5 months ago

I agree.
https://docs.microsoft.com/en-us/microsoft-store/assign-apps-to-employees

upvoted 1 times

NZS 5 months ago

Correct

upvoted 1 times

Suxi22 5 months, 1 week ago

Good Luck to everyone, tomorrow I have the exam, have a bear on me after I pass it.

upvoted 3 times

thuba_TD 1 week, 6 days ago

Preferably an ice cold Corona

upvoted 2 times