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

**Suggested 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 ɹ€" 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 ɹ€" 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 (61%) A (39%)

**b3arb0yb1m** Highly Voted 3 years 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 12 times

**RodrigoT** 2 years, 9 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** 2 years, 8 months 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 7 times

**Darkfire** Most Recent 1 year, 3 months ago

Selected Answer: B

No is the answer.

Please update URL Ref: https://learn.microsoft.com/en-us/mem/intune/protect/windows-update-reports

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 Intune admin center.

Select Devices > Monitor. Then under Software updates select Per update ring deployment state and choose the deployment ring to review.
upvoted 1 times

**kerimnl** 1 year, 11 months ago

Selected Answer: B

B. No

The solution does not meet the goal. In order to review the servicing status of a specific computer, you should navigate to the "Updates" page in the Intune console, rather than the "Audit logs" page. On the "Updates" page, you can view the current servicing channel for each device, as well as any pending updates and the status of those updates. This information can help you to identify any issues with servicing and take appropriate action to resolve them. The "Audit logs" page, on the other hand, provides a record of activity and changes made within the Intune console, but does not provide information about the servicing status of specific devices.
upvoted 1 times

**Meebler** 2 years ago

Yes, navigating to the Device configuration page in Microsoft Intune and reviewing the device status for a specific computer will allow you to review the necessary policy report and determine the servicing status of the computer.

The Device configuration page in Microsoft Intune allows you to view and manage the configuration policies that have been applied to devices in your organization. You can use this page to view the current status of these policies, as well as any errors or issues that may have occurred during policy deployment.

To review the servicing status of a specific computer, you can navigate to the Device configuration page and select the specific device from the list of devices. This will display the current configuration policies that have been applied to the device, as well as any errors or issues that may have occurred during policy deployment. You can then use this information to determine the servicing status of the computer.
upvoted 1 times

**TonySuccess** 2 years, 3 months 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 4 times

**AVR31** 2 years, 8 months 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 4 times

**ashriem** 2 years, 8 months 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** 2 years, 9 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 3 times

**Vishbsoni** 2 years, 10 months ago

**Selected Answer: A**

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

upvoted 4 times

**FlitZ** 3 years, 1 month ago

B is correct

upvoted 3 times

**Goofer** 3 years, 2 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

**Suggested 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 ɹ€" 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 ɹ€" 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 3 years 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** 2 years, 9 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

**kerimnl** Most Recent 1 year, 11 months ago
Selected Answer: B
B. No

The solution does not meet the goal. In order to review the servicing status of a specific computer, you should navigate to the "Updates" page in the Intune console, rather than the "Audit logs" page. On the "Updates" page, you can view the current servicing channel for each device, as well as any pending updates and the status of those updates. This information can help you to identify any issues with servicing and take appropriate

action to resolve them. The "Audit logs" page, on the other hand, provides a record of activity and changes made within the Intune console, but does not provide information about the servicing status of specific devices.

upvoted 1 times

**TonySuccess** 2 years, 3 months ago

**Selected Answer: B**

It is B.

upvoted 1 times

**MR_Eliot** 2 years, 9 months 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** 2 years, 9 months ago

Agree B

upvoted 1 times

**nmurthy** 3 years ago

looks correct

upvoted 2 times

**FlitZ** 3 years, 1 month 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.

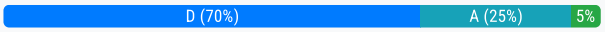
B. Wipe the computer.

C. Create a HTML file containing the computer info.

D. Create a CSV file containing the computer info.

**Suggested 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*




**Bones69** Highly Voted 2 years, 9 months ago
If the device is already used by the company I would have assumed the device was already registered, so just needed resetting.
upvoted 18 times

**now4you** 1 year, 8 months ago
A. Reset the computer.

Before redeploying the Windows 10 computer using Windows AutoPilot, the first action you should take is to reset the computer to its factory settings to remove any existing user data and configurations. This will ensure that the computer is ready to be redeployed to a new user.

Once the computer has been reset, you can proceed with configuring Windows AutoPilot and preparing the necessary files (such as a CSV file containing the computer information) for the redeployment process.
upvoted 1 times

**BAbdalla** Highly Voted 3 years, 2 months ago
It's Correct to me!
upvoted 5 times

**Examwinnernl** Most Recent 3 months, 2 weeks ago
Should be A. If the device is already enrolled and you RESET Windows, then it enters the Windows setup, connect to internet and you get the COmpnay welcome screen.
If you re-upload the hardware has, you will get the error stating that the device is already part of the tenant.
upvoted 1 times

**Examwinnernl** 10 months, 3 weeks ago
If you say A then you read the case wrong. It is D, because in this scenario the case say “You PLAN to use auto pilot..” so it was not before in Intune yet. But if it was already in intune, then it would he anwser A.
upvoted 1 times

**MasterMxx** 1 year, 5 months ago
**Selected Answer: B**
Before redeploying a Windows 10 computer using Windows AutoPilot, it is important to ensure that all existing user data and configurations are removed from the system. This process is commonly referred to as wiping the computer or performing a clean installation of the operating system.

By wiping the computer, you will be able to start with a clean slate and ensure that the new user will have a fresh, customized experience when they begin using the machine. This step also helps to maintain security and privacy by removing any residual data from the previous user.

Once the computer has been wiped, you can proceed with the remaining steps, such as resetting the computer and creating the necessary files (HTML or CSV) containing the computer information, to prepare it for redeployment using Windows AutoPilot.
upvoted 1 times

**Dlmiller90** 1 year, 9 months ago
The answer is A . It could never be D because you you need to collect the hardware ID or HWID , not computer info.
upvoted 1 times

**Dnyc** 1 year, 10 months ago
Terrible phrasing for this question. If I see it though, I'm answering A. Here's why:

- laptop was already in use in current environment so either it was OEM registered to tenant or manually registered if it existed during setup/deployment of autopilot infrastructure, and will hit autopilot on next OOBE, which would require a reset or sysprep /oobe
- you don't create a csv file directly. You run a script that creates the csv file containing the hardware hash. Answer D makes no mention of a script being run, or the hardware hash.
upvoted 1 times

**okkies** 2 years ago
we all know the real answer. the real answer is, you check if the serial number or service tag is included in endpoint and then you reset the device.

goto hate microsoft style of questioning on these exams
upvoted 3 times

**Meebler** 2 years ago
D. Create a CSV file containing the computer info.

To reuse a Windows 10 computer that was assigned to a user who is no longer with the company, the first action you should take is to create a CSV file containing the computer information. This file will be used to register the computer with Windows AutoPilot, and it should include the hardware hash and other relevant information for the computer.
upvoted 1 times

**mrjeet** 2 years ago
similar question on 12/10/22 exam
upvoted 2 times

**kerimnl** 2 years, 1 month ago
Selected Answer: D
The correct answer is D, because we dont know if the device was in Intune before. So look at the link of Microsoft Doc too, the first thing you must to do is HASH file upload as CSV to Intune.
upvoted 1 times

**TonySuccess** 2 years, 3 months 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 4 times

**AVR31** 2 years, 8 months 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 4 times

**Harold** 2 years, 8 months 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** 2 years, 8 months 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** 2 years, 8 months ago
Because the question says: You "plan" to make use of Windows AutoPilot to redeploy the computer. Meaning you never did it before.
upvoted 2 times

**MarvinG2** 2 years, 8 months ago
If it's already enrolled why do I need the CSV file for computer info again?
upvoted 1 times

**RodrigoT** 2 years, 8 months 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** 2 years, 9 months ago
**Selected Answer: D**
Its correct
upvoted 2 times

Question #4 *Topic 1*

DRAG DROP -

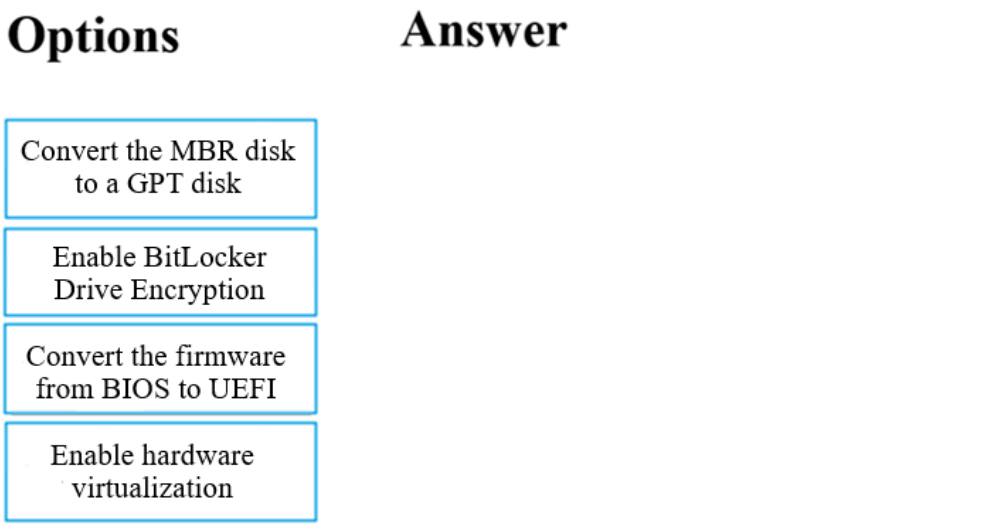
Your company has a number of Windows 7 computers that you want to upgrade to Windows 10.

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.

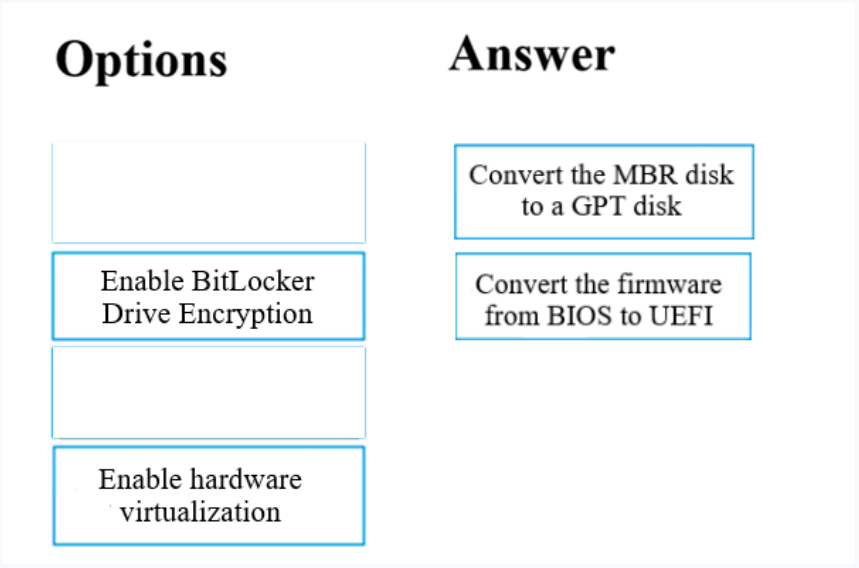
You have been tasked with making sure that Secure Boot can be used by the computers.

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:




**Suggested 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 3 years, 3 months ago

Seems good

upvoted 7 times

**RodrigoT** 2 years, 9 months ago

Same as Question #10 page 6

https://www.examtopics.com/exams/microsoft/md-101/view/6/

upvoted 1 times

**BAbdalla** Highly Voted 3 years, 2 months ago

It's Correct!

upvoted 5 times

**Tati_Oliveira** Most Recent 1 year, 3 months ago

It informs that the Firmware is UEFI then the correct answer is:

MBR > GPT

Enable Virtualization

https://learn.microsoft.com/en-us/training/modules/manage-defender-windows-client/3-explore-windows-defender-credential-guard

upvoted 1 times

**MR_Eliot** 2 years, 9 months ago

I agree with the solution.

upvoted 1 times

**AL99** 2 years, 9 months ago

Agree the answwer

upvoted 1 times

**Vishbsoni** 2 years, 10 months 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 3 times

**mikl** 3 years 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** 3 years 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.

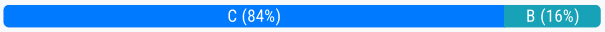
B. You should make use of a Windows AutoPilot deployment profile.

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

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

**Suggested 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*




**Haso** Highly Voted 3 years, 3 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 17 times

**mikl** 3 years 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 7 times

**Fuzzy43** Highly Voted 3 years 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 16 times

**RodrigoT** 2 years, 8 months ago
You are wrong, read my comments and the link provided. Answer is B.
upvoted 1 times

**Cristyy** Most Recent 1 year, 2 months ago

Selected Answer: B

Windows AutoPilot is a cloud-based service from Microsoft that streamlines the deployment and management of Windows 10 devices.

SCP is used for discovering Exchange services, not for Azure AD or Intune enrollment.

upvoted 1 times

**Sakile** 1 year, 4 months ago

The Autodiscover Service Connection Point (SCP) is a feature in Microsoft Exchange Server that allows client applications, particularly Microsoft Outlook, to automatically discover and configure the connection settings for Exchange mailboxes. The Autodiscover process simplifies the configuration of email accounts by automatically providing the necessary information to clients, reducing the need for manual configuration

upvoted 1 times

**Kock** 1 year, 6 months ago

B -> https://techcommunity.microsoft.com/t5/windows-it-pro-blog/windows-autopilot-hybrid-azure-ad-join-and-automatic/ba-p/286126

upvoted 1 times

**Amphithere** 1 year, 7 months ago

ChatGPT says it's option B B, "You should make use of a Windows AutoPilot deployment profile."

upvoted 2 times

**ExamTopics1_EIS** 1 year, 9 months ago

Selected Answer: C

C is correct answer. This will add existing. It will not regester to Intune though, that is done with a GPO. Profile would work as well, but it would require wiping all computers and starting over with AutoPilot.

upvoted 2 times

**deniz150** 1 year, 10 months ago

Selected Answer: B

B is the correct answer.

upvoted 1 times

**ducklaorange** 1 year, 10 months ago

Selected Answer: C

I would say C based on this article:
https://petri.com/how-to-automatically-hybrid-azure-ad-join-and-intune-enroll-pcs/
Badly framed question and answer however

upvoted 2 times

**UncleTouchy** 1 year, 11 months ago

Was this question posted before the "intune company portal" came out?

upvoted 1 times

**Cycubxl** 1 year, 12 months ago

Selected Answer: B

I've asked an experiment guy who is working in the domain and his answer was B - Autopilot

upvoted 2 times

**Meebler** 2 years ago

The correct answer to the question is:

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

To make sure that all the current computers in your company's Active Directory domain are automatically registered to Azure AD and enrolled in Intune, you should make use of a Windows AutoPilot deployment profile. This will allow you to specify the settings and configurations that should be applied to the computers when they are enrolled in Intune, including automatically registering the computers with Azure AD and enrolling them in Intune. Using a Windows AutoPilot deployment profile will help reduce the administrative effort required to achieve your goal, as it allows you to automate the process of registering and enrolling the computers in Azure AD and Intune.

upvoted 3 times

**Reznet** 2 years, 2 months ago

Selected Answer: C

C is correct.
https://learn.microsoft.com/en-us/windows/client-management/enroll-a-windows-10-device-automatically-using-group-policy

upvoted 1 times

**Horhe** 2 years, 2 months ago

**Selected Answer: C**

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

This one explains it well...

upvoted 1 times

**raduM** 2 years, 2 months ago

autodiscover SCP is only for exchange as far as i know please correct me if i am wrong

upvoted 1 times

**cbjorn8931** 2 years, 2 months ago

What is the Autodiscover service and what does it do?

The Autodiscover service minimizes user configuration and deployment steps by providing clients access to Exchange features. For Exchange Web Services (EWS) clients, Autodiscover is typically used to find the EWS endpoint URL

upvoted 2 times

**cbjorn8931** 2 years, 2 months ago

Autodiscover (SCP) makes it easy to retrieve information that you need to connect to mailboxes on Exchange servers.

https://learn.microsoft.com/en-us/exchange/client-developer/exchange-web-services/how-to-find-autodiscover-endpoints-by-using-scp-lookup-in-exchange

upvoted 2 times

**cbjorn8931** 2 years, 2 months ago

So the answer is B

upvoted 1 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

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

*Community vote distribution*
B (100%)

**Davidchercm** Highly Voted 3 years, 5 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 12 times

**anzer123** 3 years, 3 months 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** 3 years, 3 months 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 4 times

**Solaris2002** 2 years, 9 months 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** 3 years, 5 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** 3 years, 1 month 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** 3 years, 2 months 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

**Darkfire** Most Recent 1 year, 3 months ago
Selected Answer: B
B = 10 = right

https://www.anoopcnair.com/computer-name-during-windows-autopilot-intune/
upvoted 1 times

**Sim2IT** 1 year, 4 months ago
I guess 5 was the item that was highlighted. If so, then yes the answer is B as 1 represents the number of digits that will be randomized.

upvoted 1 times

**Dnyc** 1 year, 10 months ago

I don't see anything underlined when viewing this in a web browser. If the 5 is underlined, then yes, it would be B, because %RAND:1% would give you a range from 0 - 9 (ten numbers total) so the number would change to 10.

upvoted 1 times

**Renza98** 1 year, 11 months ago

Answer should be 10 devices, but we use %RAND:4% at our company which results in duplicate device names. Microsoft states that it will create unique device names but in my experience this is not true.

upvoted 1 times

**Harold** 2 years, 8 months ago

Selected Answer: B

Rand:1 = 10 combinations, so B

upvoted 1 times

**MR_Eliot** 2 years, 8 months ago

Selected Answer: B

I mean, how is this even a question :)

upvoted 1 times

**AL99** 2 years, 9 months ago

Answer B

upvoted 1 times

**RodrigoT** 2 years, 10 months 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** 2 years, 10 months ago

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

Check the part: ComputerName.

upvoted 1 times

**forummj** 2 years, 11 months 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** 3 years ago

B. 10 is correct.

upvoted 1 times

**ElFrijole** 3 years 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** 3 years, 2 months 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** 3 years, 2 months ago

You will be able to successfully run the package on as many as 10 devices.

upvoted 2 times

**BAbdalla** 3 years, 3 months 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 "€ג).

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** 3 years, 2 months 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** 3 years, 3 months 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** 3 years, 3 months 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 4 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

**Suggested 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

*Community vote distribution*
CD (57%) BC (43%)

**mail2bala3011** 1 year, 2 months ago
Windows 8.1 also support wipe action from Intune, So answer should be BCD
upvoted 1 times

**Darkfire** 1 year, 3 months ago
Selected Answer: CD
CD is correct.

The iOS/iPadOS, Android, and Windows 10 platforms are the only platforms currently supported for wiping corporate data from Intune managed apps.
upvoted 1 times

**Sakile** 1 year, 4 months ago
Windows: Microsoft Intune supports remote wipe capabilities for Windows devices, including both Windows 10 and Windows 11. This allows administrators to initiate a remote wipe to remove corporate data and settings from Windows devices.

iOS: Intune supports remote wipe capabilities for Apple iOS devices, such as iPhones and iPads. This enables administrators to remotely wipe data from these devices.

Android: Microsoft Intune also supports remote wipe capabilities for Android devices, allowing administrators to remotely erase data and settings from managed Android devices.
upvoted 1 times

**Saint3118** 1 year, 5 months ago
Selected Answer: CD
"The iOS/iPadOS, Android, and Windows 10 platforms are the only platforms currently supported for wiping corporate data from Intune managed apps. Intune managed apps are applications that include the Intune APP SDK, and have at least one enabled and licensed user account in your organization. Deployment of Application Protection Policies is required to enable app selective wipe on Android and iOS."
upvoted 2 times

**Badr_123** 1 year, 6 months ago
B & C & D
https://learn.microsoft.com/en-us/mem/intune/remote-actions/devices-wipe
upvoted 2 times

**Shalen** 1 year, 10 months ago
Answer is C & D , Win 8.1 does not support wipe
upvoted 2 times

**crackneos** 1 year, 11 months ago

**Selected Answer: CD**

The iOS/iPadOS, Android, and Windows 10 platforms are the only platforms currently supported for clearing corporate data from Intune managed apps.
https://learn.microsoft.com/es-es/mem/intune/apps/apps-selective-wipe
upvoted 1 times

**kerimnl** 1 year, 11 months ago

**Selected Answer: BC**

B. Windows 8.1
C. Windows 10
D. iOS

The Wipe action is supported on devices running the following operating systems:

Windows 8.1
Windows 10
iOS
It is not supported on devices running Windows Vista.

The Wipe action is a feature of Microsoft Intune that allows you to remotely erase all data from a device, including personal data, settings, and apps. This can be useful in cases where a device is lost or stolen, or when a device is being retired from use and needs to be prepared for reuse. To perform a Wipe action on a device, you will need to use the Intune console and select the device that you want to erase. The Wipe action can be initiated remotely and will erase all data from the device, leaving it in a clean state ready for reuse.
upvoted 3 times

**Graz** 2 years ago

BCD

A similar question appears in Topic 2 Question 13 and Windows 8.1 is included in the answer of devices that have the "Wipe" feature
upvoted 1 times

**Graz** 2 years ago

https://learn.microsoft.com/en-us/mem/intune/remote-actions/devices-wipe

IOS is not included for User enrolled devices but if it can be wiped if company owned/enrolled. Only OS not included is vista
upvoted 1 times

**Meebler** 2 years ago

The Wipe action is supported on devices running the following operating systems:

Windows 10
iOS
Android
macOS
Therefore, you can perform a Wipe action on devices running any of these operating systems. The Wipe action is useful in situations where a device has been lost or stolen, or when you want to transfer a device to a new user and need to remove all personal data and configurations. To perform a Wipe action on a device, the device must be enrolled in Microsoft Intune and connected to the internet.
upvoted 1 times

**Meebler** 2 years ago

The Answer is C and D.
upvoted 2 times

**DaZa5** 2 years, 1 month ago

BCD - The qeustion asking about the wipe not the selective wipe. They are different functions.
https://learn.microsoft.com/en-us/mem/intune/apps/apps-selective-wipe
https://learn.microsoft.com/en-us/mem/intune/remote-actions/devices-wipe

The reason given is incorrect in that it is not consistent with the question.
upvoted 1 times

**cbjorn8931** 2 years, 1 month ago

https://learn.microsoft.com/en-us/mem/intune/remote-actions/devices-wipe

Answer: B,C,D

upvoted 1 times

**Angarali** 2 years, 8 months 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 years, 3 months ago

It clearly states that it is NOT available for iOS in the link.

upvoted 1 times

**DaZa5** 2 years, 1 month ago

Can you explain where please?

upvoted 1 times

**MR_Eliot** 2 years, 9 months 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** 2 years, 9 months ago

Shall be BCD, as the question just ask about "the following operating systems support the Wipe action".

upvoted 1 times

**PiPe** 2 years, 11 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** 2 years, 11 months 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

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

**Suggested 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 3 years, 5 months ago
The Fresh Start device action removes any apps that are installed on a PC running Windows 10, version 1709 or later.
upvoted 11 times

**anzer123** Highly Voted 3 years, 3 months ago
fresh starts works on W10 only. the answer is correct
upvoted 5 times

**Angarali** Most Recent 2 years, 8 months ago
Selected Answer: C
Only available on Win 10
upvoted 1 times

**MR_Eliot** 2 years, 9 months 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** 2 years, 11 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** 2 years, 11 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** 3 years 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** 3 years ago

C. Windows 10

upvoted 1 times

**waseemsmr** 3 years, 1 month 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

**Suggested 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%)

**Meebler** 2 years ago
A. The Device configuration settings.

To enable self-service password reset on the logon screen for Windows 10 workstations that are Azure AD joined and enrolled in Microsoft Intune, you should configure the Device configuration settings in the Microsoft Intune blade. The Device configuration settings allow you to specify configuration policies that will be applied to devices in your organization, including the ability to enable self-service password reset on the logon screen. To enable this feature, you will need to create a device configuration policy that includes the necessary settings and apply it to the relevant devices in your organization.
upvoted 1 times

**MR_Eliot** 2 years, 9 months ago
**Selected Answer: A**
I agree with the answer.
upvoted 1 times

**RodrigoT** 2 years, 8 months ago
And the same question will repeat on Page 7 Question #17.
upvoted 1 times

**mikl** 3 years ago
A is correct.
https://docs.microsoft.com/en-us/azure/active-directory/authentication/howto-sspr-windows
upvoted 2 times

**RodrigoT** 2 years, 10 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 4 times

**b3arb0yb1m** 3 years ago
A. The Device configuration settings.
upvoted 1 times

**Malinaa** 3 years, 2 months ago

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

**tf444** 3 years, 2 months ago
In AAD \password rest \SSPR.
upvoted 3 times

**badguytoo** 3 years, 4 months ago
none of these are correct, as self-password reset done in Azure Portal not in Intune.
upvoted 2 times

**[Removed]** 3 years, 3 months 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 9 times

**mikl** 3 years ago
Wrong : https://docs.microsoft.com/en-us/azure/active-directory/authentication/howto-sspr-windows
upvoted 1 times

**petersnet** 3 years ago
Remember: You have navigated to the Microsoft Intune blade, answer is correct
upvoted 3 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

**Suggested 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 3 years, 3 months 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 22 times

**RodrigoT** 2 years, 8 months ago
And this question will repeat on Page 7 Question #24. Same answer, install MMA.
upvoted 1 times

**ADHDave** Highly Voted 3 years, 3 months 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 2 years, 9 months ago
Selected Answer: D
I agree with the answer.
upvoted 1 times

**mikl** 3 years 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** 3 years 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

**Suggested 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 2 years, 11 months ago
This style of question is horrendous
upvoted 12 times

**ADHDave** Highly Voted 3 years, 3 months 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

**exeTeam01** Most Recent 1 year, 5 months ago
Selected Answer: B
Answer correct
upvoted 1 times

**mrjeet** 2 years ago
similar question on 12/10/22 exam
upvoted 2 times

**MR_Eliot** 2 years, 9 months ago
Selected Answer: B
B is indeed correct.
upvoted 1 times

**MR_Eliot** 2 years, 8 months ago
Default is 10 days, however, you can change the uninstall period up to 60 days with policies.
upvoted 2 times

**Ivandro** 2 years, 12 months ago
Correct
upvoted 1 times

**mikl** 3 years 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** 3 years 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** 3 years ago

B. 10 is correct.

upvoted 2 times

**BAbdalla** 3 years, 3 months 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.

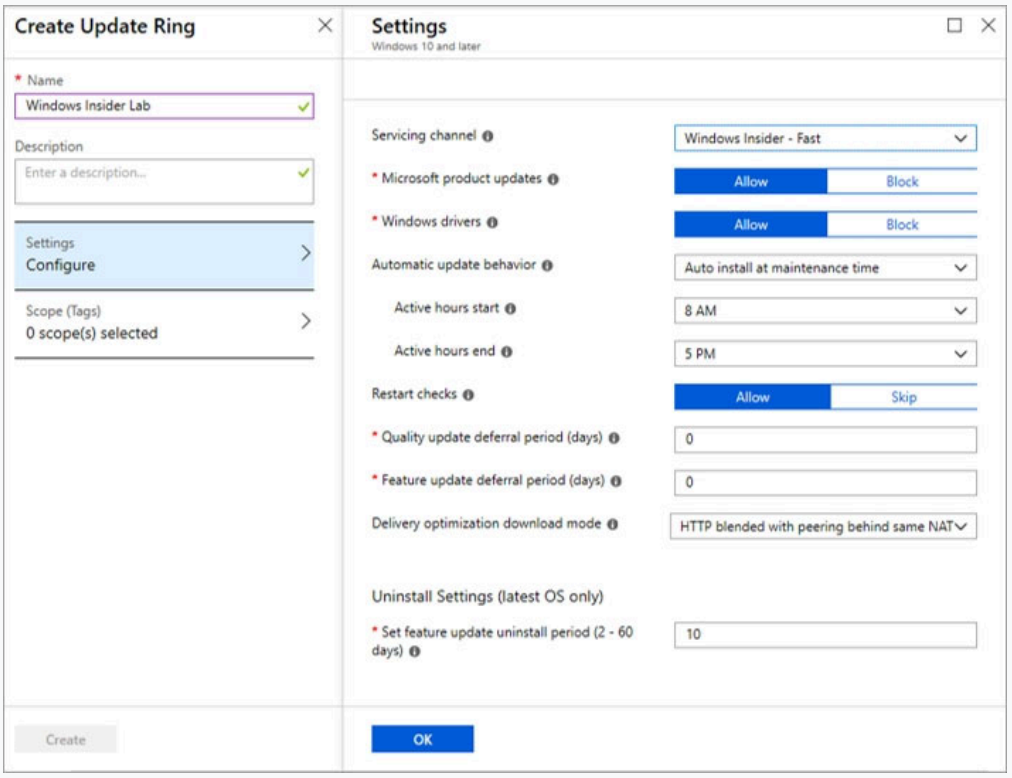
D. You should configure a Windows 10 update ring.

**Suggested 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

*Community vote distribution*

D (100%)

**OG_Diablo** 1 year, 5 months ago

**Selected Answer: D**

D is correct.

upvoted 1 times

**junior6995** 1 year, 8 months ago

To ensure that users are not allowed to enroll devices in the Windows Insider Program via Microsoft Intune, you need to create a device configuration profile with custom OMA-URI settings that disable the ability to join the Insider Program, not via Update Policies.

upvoted 2 times

**DDHP7** 2 years, 1 month ago

This is Microsoft's way, questions always confusing

upvoted 1 times

**Sironin** 2 years, 3 months ago

It's D. It's a confusing question since 365 really has very little to do with this.

It may be useful for aspiring admins out there to know that they can go to endpoint.microsoft.com then devices then update rings and create the update ring profile there.

upvoted 2 times

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

**Suggested 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

*Community vote distribution*
B (100%)

**Anker** Highly Voted 2 years, 11 months 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 5 times

**syougun200x** 2 years, 4 months ago
I see. In conditinal access
conditions -> filter for devices -> exclude filtered devices.
upvoted 2 times

**MR_Eliot** Most Recent 2 years, 9 months 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** 2 years, 9 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

**Harisasikumar92** 3 years, 2 months ago
B is correct. You need to include the device state to include the Azure AD Hybrid Joined option.
upvoted 4 times

**Harisasikumar92** 3 years, 2 months ago
Edit: Create a new conditional access policy and configure the device state to EXCLUDE Hybrid Azure AD Joined devices
upvoted 8 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?

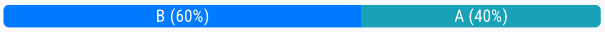
A. Yes

B. No

**Suggested 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

*Community vote distribution*




**AVP_Riga** Highly Voted 3 years, 2 months ago
Create a new conditional access policy and configure the device state to EXCLUDE Hybrid Azure AD Joined devices
upvoted 10 times

**kerimnl** Most Recent 1 year, 11 months ago
Selected Answer: B
Correct answer is: B
upvoted 1 times

**Meebler** 2 years ago
No, configuring the Client apps settings in a conditional access policy will not allow you to block access to Exchange Online while still allowing access for hybrid Azure AD-joined devices.

The Client apps settings in a conditional access policy determine which client apps are subject to the policy and how they are allowed to access the protected resources. They do not allow you to specify the types of devices that are allowed to access the protected resources.

To block access to Exchange Online while still allowing access for hybrid Azure AD-joined devices, you should configure the Device conditions settings in the conditional access policy. The Device conditions settings allow you to specify the types of devices that are allowed to access the protected resources, including hybrid Azure AD-joined devices.
upvoted 2 times

**snoopie104** 2 years ago
Selected Answer: B
I think the answer is B
upvoted 1 times

**raduM** 2 years, 2 months ago
change access controls grant set to hybrid joined
upvoted 1 times

**ashriem** 2 years, 8 months ago
Selected Answer: A

https://www.enowsoftware.com/solutions-engine/conditional-access-to-exchange-online-and-office-365

upvoted 1 times

**ashriem** 2 years, 8 months ago

Sorry, meant to select B

upvoted 1 times

**MR_Eliot** 2 years, 8 months 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** 2 years, 9 months 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** 2 years, 8 months ago

Changed my Answer to B

upvoted 3 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

**Suggested 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

*Community vote distribution*
B (100%)

**anzer123** Highly Voted 3 years, 3 months 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 10 times

**ADHDave** Highly Voted 3 years, 3 months 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 8 times

**florinbvmail** Most Recent 1 year, 4 months ago
the feature is deprecated
upvoted 1 times

**dlast** 1 year, 5 months ago
Tested is replaced with Filter for Devices under Conditions. Created a filter based on TrustType equals Hybrid Azure AD Joined
upvoted 2 times

**cbjorn8931** 2 years, 2 months ago
This preview feature has been deprecated. Customers should use the Filter for devices condition in the Conditional Access policy, to satisfy scenarios previously achieved using device state (preview) condition. However, the answer is A. It was previously used as way to block devices if they don't meet the right criteria.
upvoted 1 times

**MR_Eliot** 2 years, 9 months 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 3 times

**RodrigoT** 2 years, 8 months ago
Thank you for your link. Even though the answer provided (A) is correct for this outdated question.
upvoted 2 times

**mikeliny228** 2 years, 10 months ago
Selected Answer: B
Device state was preview feature and for now it is deprecated.
For me, answer is no.
upvoted 4 times

**ExamTaker1995** 2 years, 9 months ago
answer is yes. the question is just old. the new question will refer to filters instead.
upvoted 9 times

**JGN** 3 years, 1 month 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 8 times

**TonySuccess** 2 years, 3 months ago
Word. This is right.
upvoted 2 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

**Suggested 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

*Community vote distribution*
C (100%)

**badguytoo** Highly Voted 3 years, 4 months ago
That one is easy... Not sure whether it will show up in the really world.
upvoted 10 times

**mrjeet** Most Recent 2 years ago
similar question on 12/10/22 exam
upvoted 4 times

**MR_Eliot** 2 years, 9 months ago
Selected Answer: C
Is this even a question? Easiest answer of my life!
upvoted 1 times

**mikl** 3 years ago
C. Windows 10
upvoted 1 times

**b3arb0yb1m** 3 years ago
C. Windows 10.
upvoted 1 times

**sbmkhize** 3 years, 3 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.

**Suggested 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

*Community vote distribution*
B (60%) A (40%)

**Jeff8989** Highly Voted 3 years, 3 months ago
Correct answer is to create a dynamic membership groups so none of the anwsers are correct.
upvoted 20 times

**AVP_Riga** 3 years, 2 months ago
Yes, correct!
upvoted 1 times

**mikl** 3 years 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 3 times

**RodrigoT** 2 years, 8 months 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

**gigiscula** 2 years ago

All answer are incorrect. B is incorrect because it said "Your company has a large number of Android and iOS devices, which are enrolled in Intune." So the option "Users may register their devices with Azure AD" it's already enable by default and you cannot modify IT.

upvoted 1 times

**RodrigoT** 2 years, 8 months 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 3 times

**Examwinnernl** Most Recent 3 months, 2 weeks ago

Sometimes I have trouble in what Microsoft means. Example with "A: You should start by accessing Intune and configuring corporate device identifiers". Define please? I would think to set up enrolement profiles for these platforms "maybe".

upvoted 1 times

**Contactfornitish** 1 year, 2 months ago

Selected Answer: B

A. You should start by accessing Intune and configuring corporate device identifiers.
This option decides if the device is corporate owned or personally owned. If you know the OS and want to manage this manually then remotely a solution is possible but that's not want Microsoft would like you to do.

B. You should start by accessing Microsoft Azure Active Directory (Azure AD) and configuring Device settings.
Only option which can work, so that's the solution.

C. You should start by accessing Microsoft Azure Active Directory (Azure AD) and configuring Application settings.
Application setting has nothing to do with the question.

D. You should start by creating a distribution group.
If it was dynamic security group then would have worked since you can create dynamic group basis OS version and then can apply or deny policies. But it says distribution group, so its not the answer

upvoted 1 times

**e635466** 1 year, 8 months ago

Selected Answer: B

A. Used to identifying if a device is corporate or personal owned via IMEI or Serial
B. CORRECT ANSWER
C. Has nothing to do with the OS version of a device
D. Is for mail purposed and thus, has nothing to do with the OS version of a device

upvoted 2 times

**Amphithere** 1 year, 9 months ago

Selected Answer: A

The correct answer is A. You should start by accessing Intune and configuring corporate device identifiers.

To target Android and iOS devices based on the version of the operating system they are running, you will need to create device groups in Intune based on the device type and version.

To do this, you will need to start by configuring corporate device identifiers in Intune. This will allow you to create device groups based on the device type and version, as well as other criteria such as device ownership and enrollment status.

Once you have configured corporate device identifiers, you can create device groups and assign policies to them based on the device type and version.

Accessing Microsoft Azure Active Directory (Azure AD) and configuring Device settings or Application settings is not directly related to targeting devices based on the version of the operating system they are running. Creating a distribution group is also not a relevant action in this context.

upvoted 2 times

**Meebler** 2 years ago

The answer is A, and here is why:

To deploy new Intune policies that will apply to Android and iOS devices based on the version of the operating system that is being run, you

should start by accessing Intune and configuring corporate device identifiers. Corporate device identifiers are a feature of Microsoft Intune that allow you to identify devices in your organization based on various criteria, such as the device model, manufacturer, or operating system version. You can use corporate device identifiers to target specific devices when deploying Intune policies. To configure corporate device identifiers, you will need to create a new device identifier rule that specifies the criteria for identifying the devices, and use this rule to target the devices when deploying policies.

Accessing Azure AD and configuring Device settings is not related to targeting devices based on the version of the operating system. Therefore, option B is not the correct answer.
upvoted 2 times

**Meebler** 1 year, 11 months ago
I apologize for the confusion, you are correct that the correct answer is B.
To target the policies to specific devices based on the version of Android or iOS that is being run, you should start by accessing Microsoft Azure Active Directory (Azure AD) and configuring Device settings.

In Azure AD, you can set device-based conditional access policies to protect access to cloud resources. By configuring device-based conditional access policies in Azure AD, you can ensure that devices that are compliant with specific policies such as specific version of android or iOS, are granted access to company resources.

I apologize for any confusion caused by my previous response, I apologize for the confusion, you are correct that the correct answer is B.
upvoted 2 times

**raduM** 2 years, 2 months ago
so how exactly does that help?
upvoted 1 times

**apurvasinghal** 2 years, 2 months ago
B, D..First step should be to create Distribution Group for targetting the right devices and they applying Device setting on the Group.
upvoted 1 times

**Toaster** 2 years, 10 months 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 4 times

**Mun11** 2 years, 11 months ago
distribution group is nothing but device collection for a specific model
upvoted 1 times

**badguytoo** 3 years, 4 months ago
none of these are correct. :(
upvoted 4 times

**RodrigoT** 2 years, 10 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** 3 years, 5 months ago
One can change device settings in Android and IOS via Intune.
upvoted 1 times

**nanerforever** 3 years, 5 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** 3 years, 5 months ago
A distribution group is for email
upvoted 8 times

**maciak** 3 years ago
distribution list is for email not group.
upvoted 2 times

**Bouncy** 2 years, 9 months 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

**Suggested 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/

*Community vote distribution*
D (100%)

**Malinaa** Highly Voted 3 years, 2 months ago
Correct: https://docs.microsoft.com/nl-nl/archive/blogs/skypehybridguy/intune-upgrade-windows-from-pro-to-enterprise-automatically
upvoted 11 times

**Meebler** Most Recent 2 years ago
C,

To upgrade Windows 10 Pro computers to Windows 10 Enterprise, you should configure a Windows AutoPilot deployment profile in Microsoft Intune.

Windows AutoPilot is a feature of Microsoft Intune that allows you to automate the deployment and provisioning of new Windows devices. You can use Windows AutoPilot to upgrade Windows 10 Pro computers to Windows 10 Enterprise by creating a deployment profile that specifies the desired operating system and other configuration settings.

A device configuration profile in Microsoft Intune allows you to specify configuration policies that will be applied to devices in your organization. You can use these policies to set various device-specific settings, such as device restrictions or software installation settings. However, a device configuration profile is not used to upgrade operating systems on devices.

Therefore, to meet the goal of upgrading Windows 10 Pro computers to Windows 10 Enterprise, you should configure a Windows AutoPilot deployment profile in Microsoft Intune, rather than a device configuration profile.
upvoted 2 times

**Shalen** 2 years, 1 month ago
Based on the latest Article and my testing new answer is A ( See Microsoft updated article )
https://learn.microsoft.com/en-us/windows/deployment/windows-10-subscription-activation#subscription-activation-for-enterprise
upvoted 1 times

**MR_Eliot** 2 years, 9 months ago
Selected Answer: D
The answer is correct.
upvoted 2 times

**lucadp010** 2 years, 11 months ago

**Selected Answer: D**

D is correct

upvoted 4 times

**RodrigoT** 2 years, 8 months ago

Of course, they are already enrolled in Microsoft Intune. Why enroll them again?

upvoted 1 times

**mikl** 3 years ago

D is correct.

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

upvoted 3 times

**b3arb0yb1m** 3 years 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.

**Suggested 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

*Community vote distribution*
D (100%)

**Cabanna94** Highly Voted 3 years, 5 months ago
I agree with the answer. Known locations can be configured under “conditions”.
upvoted 10 times

**GZD** Most Recent 1 year, 6 months ago
Selected Answer: D
I also agree with D. This is the right answer.
upvoted 1 times

**Angarali** 2 years, 8 months ago
Selected Answer: D
Correct
upvoted 1 times

**MR_Eliot** 2 years, 9 months ago
Selected Answer: D
The answer is indeed correct.
upvoted 1 times

**fmodel** 2 years, 10 months ago
Selected Answer: D
D is correct answer https://docs.microsoft.com/en-us/mem/intune/protect/conditional-access
upvoted 3 times

**DDHP7** 2 years, 10 months ago
Selected Answer: D
D is correct answer
upvoted 1 times

**mikl** 3 years ago
D. You should create a conditional access policy.

Conditions - Locations

upvoted 1 times

**b3arb0yb1m** 3 years ago

D. You should create a conditional access policy.

upvoted 1 times

**sbmkhize** 3 years, 3 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.

**Suggested 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

*Community vote distribution*
B (100%)

**NoursBear** 1 year ago
I think it's D, the blocking action is in conditional access policy not in the compliance policy. In the compliance policy I don't see if blah blah block
upvoted 1 times

**Tati_Oliveira** 1 year, 3 months ago
None of the answers are correct, the OS Version is configured under Device Restrictions.
upvoted 1 times

**Tati_Oliveira** 1 year, 3 months ago
Device Platform Restrictions
upvoted 1 times

**Darkfire** 1 year, 3 months ago
I also think correct answer should be B.
Nevertheless, A and D are needed to successfully configure B.

Main question is, which will be correct in the exam? Anybody knows?
upvoted 1 times

**USRobotics** 1 year, 4 months ago
I really don't understand why 3 options are marked as correct answer.
upvoted 2 times

**devin19** 1 year, 5 months ago
Selected Answer: B
Why all 3 selected when it doesn't say select all that apply
upvoted 4 times

**xJoelinez** 1 year, 9 months ago

Just to be clear, B alone will not be suffice. Yes you can block devices if they are not compliant, but this is only mobile devices running android and iOS. If you want to block devices that are running windows (Computers in the question) then you will need a conditional access policy too,
upvoted 1 times

**dawnbringer69** 1 year, 9 months ago
I Have tested and can confirm that this is Valid. The answer is neverltheless B.
upvoted 1 times

**okkies** 1 year, 11 months ago
Selected Answer: B
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.

just double checked it in a tenant
upvoted 1 times

**Hatsapatsa** 2 years ago
Answer seems to be correct according to this Microsoft Documentation.
https://docs.microsoft.com/en-us/intune/compliance-policy-create-android
upvoted 1 times

**Meebler** 2 years ago
the correct answer to the multiple choice question is B: You should create a device compliance policy. This is because device compliance policies allow you to set rules for ensuring that devices meet certain compliance standards, including the level of Windows Defender ATP risk, and specify actions to take if a device is non-compliant, such as locking the device.

Option A (creating a device configuration profile) is not directly related to locking devices with a high Windows Defender ATP risk score. Option C (creating a Windows AutoPilot deployment profile) is related to deploying and configuring devices, but it is not directly related to locking devices with a high Windows Defender ATP risk score. Option D (creating a conditional access policy) is related to controlling access to corporate resources based on various factors, but it is not directly related to locking devices with a high Windows Defender ATP risk score.
upvoted 1 times

**raduM** 2 years, 2 months ago
B is correct. Don't know why you put all the answers
upvoted 2 times

**MR_Eliot** 2 years, 9 months ago
Selected Answer: B
I agree.
upvoted 2 times

**PChi** 2 years, 9 months ago
Answer B. Compliance and Conditional Policies are dependent on each other ("To use device compliance policies to block devices from corporate resour
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%
CONTIDITONAL ACCESS:
https://docs.microsoft.com/en-us/mem/intune/protect/conditional-access-intune-common-ways-use
upvoted 2 times

**Anker** 2 years, 11 months 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** 3 years 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** 3 years ago

B. You should create a device compliance policy.

upvoted 1 times

**velosiraptor** 3 years, 1 month 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** 3 years, 2 months 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_** 3 years, 2 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** 2 years, 10 months 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

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

**Suggested 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 3 years, 7 months ago
We have suffered through countless convoluted questions. Let us rejoice for such an easy question. Rejoice, my brothers.
upvoted 60 times

**jh999** 3 years, 5 months ago
and sisters. :)
upvoted 20 times

**AVP_Riga** 3 years, 1 month ago
and other's (:
upvoted 7 times

**forExamCert2023** 2 years, 10 months 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 3 times

**mail2bala3011** Most Recent 1 year, 2 months ago
I understand that to have single app we are using Single app kiosk. However, there is no direction option called kiosk while creating profile. We will be able to select single app kiosk mode under device restriction. It's confusing, what is right answer for this question?
upvoted 1 times

**Moderator** 2 years, 11 months ago
Incredibly tough question but I heard through the grapevine that this probably should be answer A indeed! Very uncertain though ;-)
upvoted 3 times

**Perycles** 3 years, 6 months ago
A for sure
upvoted 2 times

**reyco** 3 years, 7 months ago
If only they could all be this simple ..
upvoted 3 times

**AzZnLuVaBol** 3 years, 10 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.

**Suggested 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

*Community vote distribution*


**Jana08** Highly Voted 3 years, 6 months ago
Correct - Microsoft Endpoint Manager Admin Center - Formerly known as intune.

Home > Endpoint Security > Device Compliance
upvoted 22 times

**AVP_Riga** 3 years, 2 months ago
Thanks
upvoted 3 times

**RodrigoT** 2 years, 10 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 2 times

**RodrigoT** 2 years, 10 months ago
Or also: Home > Devices > Monitor > Noncompliant devices
upvoted 3 times

**MR_Eliot** Most Recent 2 years, 8 months ago
Selected Answer: C
C, But keep in mind that the name is changed to MDM or Microsoft Endpoint Manager.
upvoted 1 times

**mikl** 3 years ago
C. The Intune admin center.

upvoted 1 times

**b3arb0yb1m** 3 years ago

C. The Intune admin center.

upvoted 1 times

**sbmkhize** 3 years, 3 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

**Suggested 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

*Community vote distribution*
B (100%)

**Jeff8989** Highly Voted 3 years, 3 months ago
UniversalAppUninstall
ConnectivityProfiles
upvoted 15 times

**PiPe** 2 years, 11 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** 2 years, 9 months 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 3 years, 4 months 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

**kerimnl** Most Recent 1 year, 11 months ago
Selected Answer: B
The correct option is B. ConnectivityProfiles and Policies.

To remove the Microsoft News and Xbox Microsoft Store apps and add a VPN connection to the company network, you should configure customization settings for ConnectivityProfiles and Policies.

ConnectivityProfiles settings allows you to specify the VPN connection settings, such as the VPN server address, authentication methods, and encryption settings.

Policies settings allows you to specify which apps are removed from the device. In this scenario, you would configure the policy to remove the Microsoft News and Xbox Microsoft Store apps.

Option A and D are not the correct options as they do not include the necessary settings to remove the apps and add VPN connection.
Option C is not the correct option as well as it doesn't include the settings to add VPN connection.
Please let me know if you have any other questions.
upvoted 1 times

**b3arb0yb1m** 3 years ago
B. ConnectivityProfiles and Policies
upvoted 6 times

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

**daonga** 3 years, 4 months ago
Anyone able to confirm if B? The link they provided does not work
upvoted 1 times

**RodrigoT** 2 years, 10 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?

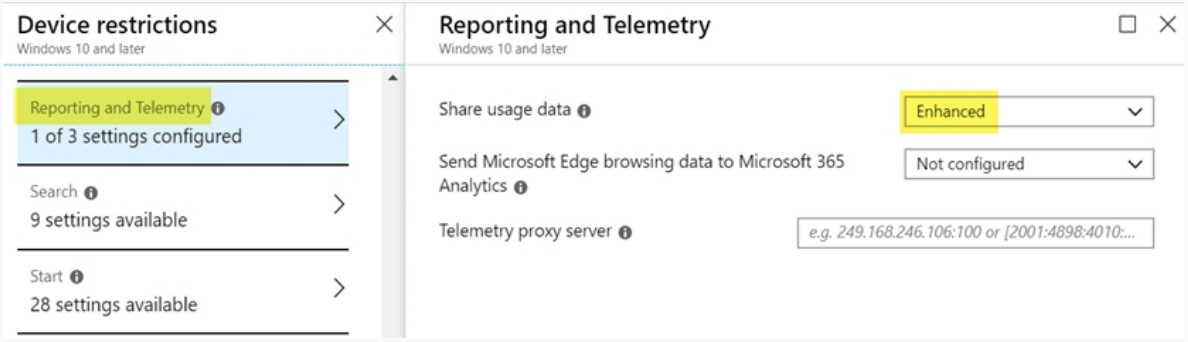
A. You should create a device configuration profile via Intune.

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.

**Suggested 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/

*Community vote distribution*
A (100%)

**daye** Highly Voted 2 years, 3 months 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 6 times

**junior6995** Most Recent 1 year, 8 months ago

Outdated question, Endpoint Analytics is now the current tool for Device Analytics.
upvoted 1 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

**Suggested 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

*Community vote distribution*
A (88%) 12%

**rdelgadof13** 1 year, 12 months ago
100% A
upvoted 1 times

**Meebler** 2 years ago
A,

To display a custom image on the sign-in screen of the workstations, you should configure the Locked screen experience device restriction setting.

The Locked screen experience device restriction setting allows you to customize the appearance of the lock screen on the workstations. You can use this setting to specify the background image that should be displayed on the lock screen, as well as other options such as the visibility of the lock screen clock and user name.

To configure the Locked screen experience device restriction setting, you will need to use the Microsoft Intune admin center to create a device configuration profile. In the profile, you can select the Locked screen experience setting and specify the desired configuration options.

Option B (Personalization) is not a valid device restriction setting. Option C (Display) is not directly related to customizing the lock screen. Option D (General) is not a valid device restriction setting.
upvoted 1 times

**TonySuccess** 2 years, 4 months ago
Configuration Profiles - Device Restrictions - Lock Screen Experience x
upvoted 2 times

**MR_Eliot** 2 years, 8 months ago
Selected Answer: A
100% A
upvoted 1 times

**ashriem** 2 years, 8 months 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** 2 years, 10 months ago

Selected Answer: A

A - Device restrictions > Locked Screen Experience

upvoted 3 times

**Dane12421** 2 years, 11 months ago

Selected Answer: A

A obviously for sign in screen

upvoted 3 times

**mikl** 3 years 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** 2 years, 10 months ago

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

upvoted 1 times

**b3arb0yb1m** 3 years ago

A. Locked screen experience

upvoted 2 times

**Ferrix** 3 years, 1 month ago

A is the Correct one. On personalization you can only set a Desktop background picture URL

upvoted 4 times

**Rick11221** 3 years, 1 month ago

Selected Answer: A

Gonna go with A on this one.

upvoted 3 times

**Duyons** 3 years, 1 month ago

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

upvoted 4 times

**Duyons** 3 years, 1 month 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** 2 years, 11 months 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 3 times

**encxorblood** 3 years, 1 month ago

Correct B - LockScreenImageUrl in Personalization

upvoted 2 times

**forummj** 2 years, 11 months 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** 3 years, 3 months 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

**Suggested 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

*Community vote distribution*
B (100%)

**blueninja** Highly Voted 3 years, 3 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 2 years, 4 months ago
Configuration Profiles - Device Restrictions - Personalisation x
upvoted 1 times

**MR_Eliot** 2 years, 8 months ago
Selected Answer: B
Correct.
upvoted 1 times

**b3arb0yb1m** 3 years ago
B. Personalization
upvoted 2 times

**ADHDave** 3 years, 3 months 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** 3 years, 3 months ago
It's about the Desktop background, not the locked screen. Given answer is correct.
upvoted 10 times

**Duyons** 3 years, 1 month ago
Correct
upvoted 2 times

**ADHDave** 3 years, 2 months 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.

**Suggested 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

*Community vote distribution*
A (100%)

**Jana08** Highly Voted 3 years, 6 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 14 times

**Jana08** 3 years, 6 months ago
^ From the provided article
upvoted 1 times

**TonySuccess** Most Recent 2 years, 4 months ago
Configuration Profiles - Delivery Optimization x
upvoted 1 times

**MR_Eliot** 2 years, 8 months ago
Selected Answer: A
Answer is correct.
upvoted 1 times

**mikl** 3 years ago
A. You should create a device configuration profile via Intune.

Totally agree!
upvoted 1 times

**b3arb0yb1m** 3 years 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.

**Suggested 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

*Community vote distribution*
C (100%)

**CaloyB_IT** Highly Voted 3 years, 1 month 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 10 times

**Darkfire** Most Recent 1 year, 3 months ago
Selected Answer: C
C = correct
upvoted 1 times

**lannythewizard** 1 year, 8 months ago
C is correct
upvoted 1 times

**DDHP7** 2 years, 10 months ago
C is correct
upvoted 3 times

**Moderator** 2 years, 12 months ago
Selected Answer: C
Yes, an app protection policy is the best option here.
upvoted 3 times

**mikl** 3 years ago
Selected Answer: C

C. You should create an app protection policy.

upvoted 2 times

**b3arb0yb1m** 3 years 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

**Suggested 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

*Community vote distribution*
B (100%)

**MR_Eliot** 2 years, 8 months ago
**Selected Answer: B**
B should be right
upvoted 1 times

**b3arb0yb1m** 3 years ago
B. No is correct.
upvoted 3 times

**ercluff** 3 years, 5 months 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** 3 years, 5 months ago
B. No on this question
upvoted 7 times

**ercluff** 3 years 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

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

**Suggested 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

*Community vote distribution*
B (100%)

**ercluff** Highly Voted 3 years, 5 months ago
B. NO - Mobile Application Management App Protection is what is needed.
upvoted 5 times

**ercluff** 3 years 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** 2 years, 10 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 2 years, 8 months ago
Selected Answer: B
B, smart screen is just protection and nothing more.
upvoted 1 times

**b3arb0yb1m** 3 years ago
B. No is correct.
upvoted 3 times

**CaloyB_IT** 3 years, 1 month ago

B - MAM is what is needed

https://docs.microsoft.com/en-us/mem/intune/apps/mam-faq

upvoted 2 times

**RodrigoT** 2 years, 10 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** 3 years, 1 month 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** 2 years, 10 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 3 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

**Suggested 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

*Community vote distribution*
B (100%)

**nyashac** Highly Voted 3 years, 6 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%20Defende
upvoted 22 times

**RodrigoT** 2 years, 10 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/thre
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'
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

**RodrigoT** 2 years, 8 months ago
Nowadays Windows Defender Application Guard is only for Edge and Office. It opens untrusted sites and files in an isolated Hyper-V-enabled conta
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 5 times

**justabasicuser** Highly Voted 3 years, 6 months ago

Its no as it should be Windows Defender Application Control.

upvoted 11 times

**Meebler** Most Recent 2 years ago

B,

Using Windows Defender Application Guard alone is not sufficient to ensure that the workstations are only able to run applications that you have explicitly permitted.

Windows Defender Application Guard is a security feature of Windows 10 that helps protect against malicious websites and apps by running them in a isolated, virtualized environment. While it can help prevent malicious software from being executed on the workstations, it is not designed to control which specific applications can be run on the workstations.

To meet the goal of ensuring that the workstations are only able to run applications that you have explicitly permitted, you will need to use additional controls such as AppLocker or an app deployment policy in Microsoft Intune. These tools allow you to specify a list of approved applications and block the execution of any other applications.

In summary, the solution of using Windows Defender Application Guard alone does not meet the goal of ensuring that the workstations are only able to run applications that you have explicitly permitted.

upvoted 3 times

**AK4U_111** 2 years, 2 months ago

Be carfeul as they sound almost identical.

windows defender application control vs windows defender application guard

upvoted 1 times

**MR_Eliot** 2 years, 8 months ago

Selected Answer: B

B is correct.

upvoted 2 times

**AL99** 2 years, 9 months ago

Agree B "No"|

upvoted 2 times

**Garito** 2 years, 10 months ago

Selected Answer: B

Application Control and not Application Guard

upvoted 4 times

**ameli8222** 2 years, 11 months ago

Selected Answer: B

Its B. App control would be the right answer

upvoted 3 times

**b3arb0yb1m** 3 years ago

B - Windows Defender Application Control.

upvoted 2 times

**GLL** 3 years, 1 month ago

It should be Application Control?

upvoted 3 times

**Duyons** 3 years, 1 month 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** 3 years, 1 month ago

Wrong. Should be Microsoft Defender Application Control.

upvoted 3 times

**Nen0** 3 years, 1 month ago

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

upvoted 4 times

**ANDREVOX** 3 years, 2 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** 3 years, 3 months ago

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

upvoted 3 times

**angelize** 3 years, 6 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.

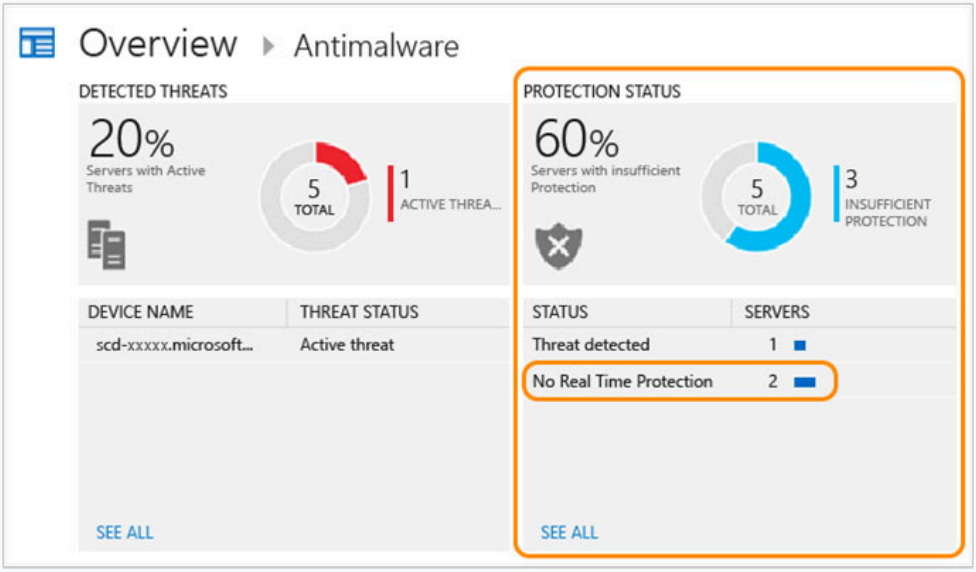
B. You need to install the Azure Diagnostic extension.

C. Windows Defender Credential Guard is incorrectly configured.

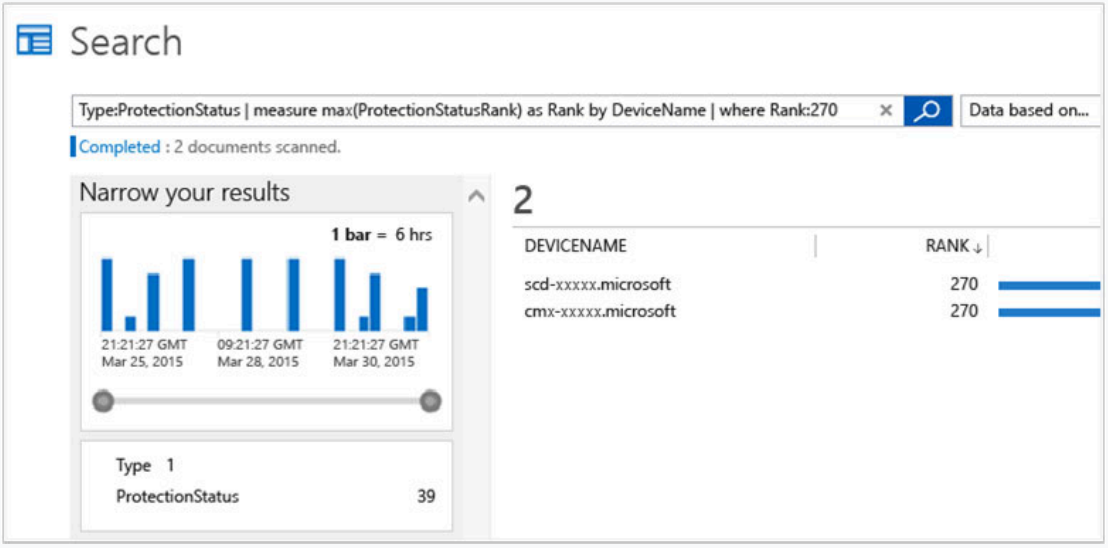
D. Windows Defender System Guard is incorrectly configured.

**Suggested 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

*Community vote distribution*
A (100%)

**jenraed** 2 years, 1 month ago

**Selected Answer: A**

Answer is correct.

upvoted 1 times

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.

**Suggested 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

*Community vote distribution*


**Ka1Nn** Highly Voted 3 years, 5 months ago
The answer is not present :
The Microsoft Monitoring Agent is uninstalled.
upvoted 22 times

**mikl** 3 years 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 3 times

**RodrigoT** 2 years, 10 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 4 times

**RodrigoT** 2 years, 8 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 2 times

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

**HellRaver80** 3 years, 1 month ago
in my eyes that is active on the server not on clients
upvoted 1 times

**RodrigoT** 2 years, 10 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

**Darkfire** Most Recent 1 year, 3 months ago
Selected Answer: B
B = correct

Key words: not reporting + Windows Diagnotics Extension (needs to be installed to monitor + report)
upvoted 1 times

**Meebler** 2 years ago
B,

There are several potential reasons why a device may not be reporting when using the Antimalware Assessment solution in Microsoft Azure Log Analytics. One potential reason is that the Azure Diagnostic extension is not installed on the device.

The Azure Diagnostic extension is a tool that is used to collect diagnostic data from Azure virtual machines and other resources. It is required for the Antimalware Assessment solution to work properly and report on the status of devices. If the extension is not installed on a device, it may not be able to report to Azure Log Analytics.

Other potential reasons for a device not reporting could include incorrect configuration of Windows Defender System Guard, Windows Defender Application Guard, or the Microsoft Malicious Software Removal tool. However, these are less likely causes compared to the Azure Diagnostic extension not being installed.
upvoted 2 times

**RodrigoT** 2 years, 10 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 6 times

**RodrigoT** 2 years, 10 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** 2 years, 10 months 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** 2 years, 10 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** 2 years, 10 months ago

Where do the questions come from exactly?
None of the options make much sense

upvoted 2 times

**Bettito** 2 years, 11 months ago

ninguna ya que no esta presente MMA

upvoted 1 times

**AK311** 3 years, 1 month ago

I dont think any of the options present here are correct?

upvoted 4 times

**amarro** 3 years, 2 months ago

Is the answer correct because I have a doubt with the option B

upvoted 1 times

**Ka1Nn** 3 years, 5 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

**Suggested 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

*Community vote distribution*


**Jana08** Highly Voted 3 years, 6 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 10 times

**Angarali** 2 years, 8 months ago
https://docs.microsoft.com/en-us/windows/security/identity-protection/credential-guard/credential-guard-manage
upvoted 1 times

**RodrigoT** 2 years, 10 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 12 times

**KiwE** 2 years, 2 months ago
For anyone confused about the noise in these comments - always go with RodrigoT's answers honestly.
upvoted 4 times

**osxzvkwpfcfxobqjby** 1 year, 6 months ago
Check again: "Starting with Windows 10, version 1607 and Windows Server 2016, enabling Windows features to use virtualization-based security isn't necessary and this step can be skipped."
upvoted 1 times

**lucadp010** Highly Voted 2 years, 11 months ago
Selected Answer: C
C. a virtual machine
Hyper-V is not required. You can use also VMware for virtualization.
upvoted 6 times

**RodrigoT** 2 years, 10 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 12 times

**osxzvkwpfcfxobqjby** 1 year, 6 months ago
Check again: "Starting with Windows 10, version 1607 and Windows Server 2016, enabling Windows features to use virtualization-based security isn't necessary and this step can be skipped."
upvoted 1 times

**reastman66** Most Recent 1 year, 5 months ago
Selected Answer: A
For Credential Guard to work, the device must support virtualization-based security and have secure boot functions. Virtualization-based security only works if the device has a 64-bit CPU, CPU virtualization extensions and extended page table, and a Windows hypervisor. The device must also include Trusted Platform Module (TPM) 2.0 and Unified Extensible Firmware Interface lock.

Credential Guard can function on virtual machines in the same way it does on physical machines. To work on a VM, however, it must be a Generation 2 VM with a TPM enabled. In addition, the Microsoft Hyper-V host must run at least Windows Server 2016 and Windows 10 version 1607 and have an input-output memory management unit.
upvoted 1 times

**Kock** 1 year, 6 months ago
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)

https://learn.microsoft.com/en-us/windows/security/identity-protection/credential-guard/credential-guard-requirements
upvoted 1 times

**jt2214** 1 year, 10 months ago
Selected Answer: A
I trust RodrigoT's answers. A
upvoted 1 times

**osxzvkwpfcfxobqjby** 1 year, 6 months ago
Check again: "Starting with Windows 10, version 1607 and Windows Server 2016, enabling Windows features to use virtualization-based security isn't necessary and this step can be skipped."
upvoted 1 times

**Meebler** 2 years ago

A,

No adjustment required, To enable Windows Defender Credential Guard on Windows 10 computers, the computers must have Hyper-V installed.

Windows Defender Credential Guard is a security feature of Windows 10 that helps protect against pass-the-hash attacks and other credential theft techniques. It uses hardware virtualization to create isolated environments for storing sensitive information, such as credentials. To use this feature, the computers must have Hyper-V installed, as Hyper-V is required for hardware virtualization.

Therefore, the correct option to select is A: No adjustment required. Option B (installing Windows Defender Smartscreen) is not related to Windows Defender Credential Guard. Option C (installing a virtual machine) is not necessary, as Hyper-V is already required for Windows Defender Credential Guard. Option D (installing a container cluster) is not related to Windows Defender Credential Guard.

upvoted 3 times

**cbjorn8931** 2 years, 2 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.

upvoted 1 times

**cbjorn8931** 2 years, 2 months ago

Virtualization-based security uses Hyper-V

upvoted 1 times

**cbjorn8931** 2 years, 2 months ago

Open the Programs and Features control panel.

Select Turn Windows feature on or off.

Go to Hyper-V > Hyper-V Platform, and then select the Hyper-V Hypervisor check box.

Select the Isolated User Mode check box at the top level of the feature selection.

Select OK.

upvoted 1 times

**TonySuccess** 2 years, 3 months ago

Selected Answer: A

A Fo Sho

upvoted 1 times

**asturmark** 2 years, 3 months 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** 2 years, 8 months 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** 2 years, 8 months ago

Selected Answer: A

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

upvoted 1 times

**Angarali** 2 years, 8 months 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** 2 years, 9 months ago

**Selected Answer: A**

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

upvoted 2 times

**PChi** 2 years, 9 months 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** 3 years ago

A. No adjustment is required.

upvoted 2 times

**vinodhg** 3 years 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** 2 years, 10 months ago

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

upvoted 1 times

**ritte1337** 3 years, 3 months 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** 3 years 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** 2 years, 10 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** 3 years, 5 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** 2 years, 10 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 3 times

**Angarali** 2 years, 8 months 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?

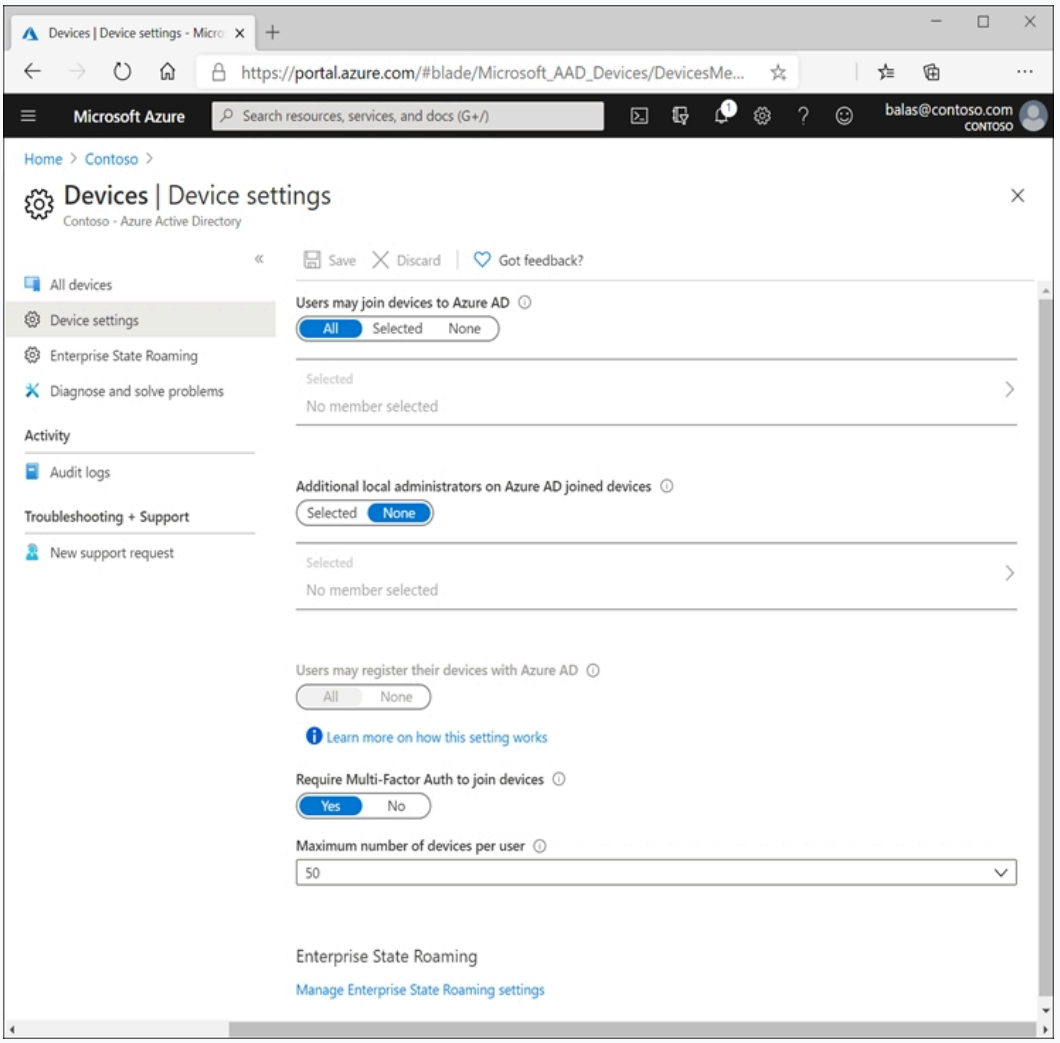
A. You should configure the Enrollment restriction settings via the Device enrollment blade in the Intune admin center.

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.

**Suggested 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

*Community vote distribution*
A (57%) C (43%)

**BRoald** Highly Voted 2 years, 3 months 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 9 times

**daye** 2 years, 3 months ago

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

upvoted 9 times

**cbjorn8931** 2 years, 2 months ago

C, This is correct...

Azure AD join needs users input your credentials of Azure AD Account. If you want to limit Azure AD join devices, you can limit users who can join their devices to AzureAD:

Go to Azure Portal > Azure Acitve Directory > Devices > Add memebers who can join devices to Azure AD.

https://serverfault.com/questions/893881/how-to-restrict-device-join-in-azure-ad

upvoted 6 times

**TonySuccess** 2 years, 3 months ago

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

upvoted 2 times

**BRoald** 2 years, 2 months ago

C is not correct since there is no "block Home PC" option available in Azure.

Thats only in the Intune/Endpoint Manager admin center i described in my first comment.

I stand with answer A

upvoted 4 times

**daye** 2 years, 2 months ago

Re Read the question, there is no Intune enrollment requirement. It's all about AD Join (Identity), where it's managed in Azure AD and you are able to block if the users are able to register any computer with their corporative accounts or not.

upvoted 1 times

**BRoald** 2 years ago

Youre right aswell, but the question states

"You want to make sure that users are unable to join their home PC's to Azure AD."

But if you disable the choosen option, nobody can join AzureAD anymore, even with a company computer, so thats why i choosed A

upvoted 2 times

**AngelusNL** Highly Voted 2 years, 2 months ago

Selected Answer: C

It's not about Intune, it's only about Joining Azure AD, C is correct

upvoted 8 times

**NoursBear** Most Recent 12 months ago

https://techcommunity.microsoft.com/t5/microsoft-intune/preventing-azure-ad-registration-microsoft-support-can-not-help/m-p/3864797

upvoted 1 times

**Kock** 1 year, 6 months ago

Azure Active Directory (Azure AD) provides a central place to manage device identities and monitor related event information.

https://learn.microsoft.com/en-us/azure/active-directory/devices/device-management-azure-portal

upvoted 1 times

**[Removed]** 1 year, 8 months ago

Selected Answer: C

Its C, no meniton of Intune.

upvoted 1 times

**golijat** 1 year, 8 months ago

Selected Answer: C

There is no mention of Intune

upvoted 1 times

**Meebler** 2 years ago

C,

Option A: configuring the Enrollment restriction settings via the Device enrollment blade in the Intune admin center, is not the correct answer.

The Intune admin center is a tool used to manage devices and their associated policies, such as device compliance and app deployment. While the Intune admin center does have a Device enrollment blade, this blade is used to manage the enrollment of devices into Intune, not Azure AD.

To make sure that users are unable to join their home PCs to Azure AD, you should configure the enrollment restriction setting in the Azure Active Directory admin center. This is the central location for managing Azure AD and its related services, including the enrollment of devices into Azure AD. The Device enrollment blade in the Intune admin center is not relevant to this task.

upvoted 1 times

**Zarkata** 2 years, 3 months ago

**Selected Answer: A**

BRoald is correct indeed.

upvoted 2 times

**RickyBee** 2 years, 3 months ago

**Selected Answer: A**

Broald is correct

upvoted 2 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

**Suggested 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

*Community vote distribution*
A (100%)

**Darkfire** 1 year, 3 months ago
**Selected Answer: A**
A = correct
upvoted 1 times

**Deric** 2 years, 3 months ago
**Selected Answer: A**
Agreed, the answer is A.
upvoted 1 times

**MR_Eliot** 2 years, 8 months ago
**Selected Answer: A**
I'm going with A. No Adjustment is required.
upvoted 1 times

**AL99** 2 years, 9 months ago
B, C, D are incorrect. So remaining is A
upvoted 1 times

**mikl** 3 years ago
**Selected Answer: A**
A. No adjustment required.
upvoted 2 times

**b3arb0yb1m** 3 years ago
A. No adjustment is required.
upvoted 1 times

**CaloyB_IT** 3 years, 1 month ago
**Selected Answer: A**
correct answer
https://www.windowscentral.com/how-enable-windows-10-sideload-apps-outside-store
upvoted 3 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

**Suggested 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

*Community vote distribution*

D (100%)

**Darkfire** 1 year, 3 months ago

**Selected Answer: D**

D = correct

Keywords are " sideload a LOB" to the install command "Add-AppxPackage".

upvoted 1 times

**MR_Eliot** 2 years, 8 months ago

**Selected Answer: D**

D is correct.

upvoted 3 times

**mikl** 3 years 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** 3 years ago

D. Add-AppxPackage

upvoted 1 times

**ercluff** 3 years 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** 3 years, 2 months 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** 3 years 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** 3 years, 2 months 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

**Suggested 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

*Community vote distribution*
B (100%)

**ercluff** Highly Voted 3 years, 5 months 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

**xJoelinez** Most Recent 1 year, 9 months ago
Also, store for business is soon to be retired :D
upvoted 1 times

**MR_Eliot** 2 years, 8 months ago
Selected Answer: B
B is correct. Microsoft Store for Business is for Windows devices & it's being deprecated soon.
upvoted 2 times

**b3arb0yb1m** 3 years ago
B. No is correct. Add the app to Intune first.
upvoted 2 times

**Alfred666** 3 years, 5 months ago
why is there no article backing up answer?
upvoted 2 times

**Davidchercm** 3 years, 5 months ago
similar to topic 4 , add to app to intunes
upvoted 1 times

Question #39 *Topic 1*

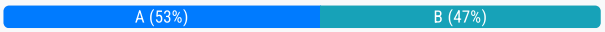
Note: The question is included in a number of questions that depicts the identical set-up. However, every question has a distinctive result. Establish if the solution satisfies the requirements.
Your company's environment includes a Microsoft 365 subscription.
Users in the company's sales division have 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

**Suggested 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

*Community vote distribution*




**Ka1Nn** Highly Voted 3 years, 4 months ago
Yes, but you need FIRST to create the App in intune before assign to a group
upvoted 14 times

**maggie_petrova** Highly Voted 2 years, 9 months ago
Selected Answer: A
The question states that the application is already created "After a mobile application...".
So the answer is YES.
upvoted 5 times

**cbjorn8931** 2 years, 2 months ago
The app that was created there you are right, however the was must be added to Intune, in order for certain users or groups can have access to download the app. so the answer is B
upvoted 2 times

**SlickPatty** Most Recent 1 year, 6 months ago
Selected Answer: B
I think this is a stupid and confusing question. If the app is not added to intune, you cannot add a group to it. Of course you add the app to intune first and then apply a group, but i can see how A is also correct because once the app is created in intune you must apply a group.
upvoted 1 times

**SR1991** 1 year, 6 months ago
How can you create apps in Intune, you can add them ..... so it is B, because you must add the app in Intune
upvoted 1 times

**jt2214** 1 year, 10 months ago
Selected Answer: B
I vote B
upvoted 1 times

**okkies** 1 year, 11 months ago
Selected Answer: B
B us correct, and these questions are the reason for using this website.
because adding the application is just as obvious as keep breathing after you crashed your car in a car acccident.
upvoted 1 times

**mikekrt** 2 years, 1 month ago
Selected Answer: A

"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 app has already been made. The answer is A

upvoted 3 times

**raduM** 2 years, 1 month ago

well to which group? because if you add the application to a group of finance users it is not correct

upvoted 1 times

**MR_Eliot** 2 years, 8 months 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** 2 years, 8 months ago

Changed my mind to B. See Topic 1, Question #40.

upvoted 2 times

**Moderator** 3 years 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 5 times

**b3arb0yb1m** 3 years ago

B. No is correct. Add the app to Intune first.

upvoted 2 times

**john909** 3 years, 2 months 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** 3 years, 2 months ago

Yes! Create /add the app in Intune, select the platform, include /exclude the group.

upvoted 2 times

**ExamStudy101** 3 years, 5 months ago

Wouldn't this be correct? You can assign apps to ios and android devices through a group

upvoted 2 times

**daonga** 3 years, 4 months ago

You need to first create the app in Intune. Only then you can assign it.

upvoted 3 times

**auton** 3 years, 2 months 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** 3 years, 1 month 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*

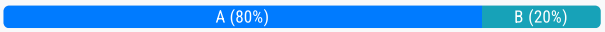
Note: The question is included in a number of questions that depicts the identical set-up. However, every question has a distinctive result. Establish if the solution satisfies the requirements.
Your company's environment includes a Microsoft 365 subscription.
Users in the company's sales division have 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

**Suggested 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

*Community vote distribution*




**BRoald** 2 years ago

**Selected Answer: A**

I think A is correct, because the question states "after the mobile application is created", but it doenst say anywhere in the question that the application is uploaded to intune, so yes, the first thing you do is upload the app to intune

upvoted 2 times

**Graz** 2 years ago

I think if they're only looking for step one of the process, this is the correct answer.

Order of operation would be First adding to Intune, then store for business, followed by assigning it to a group.

I hate that it bluntly asks "Does this meet the goal" because it doesn't and all of these 'Yes' or 'No' questions involve a series of steps and always spark the most debate.

upvoted 2 times

**mikekrt** 2 years, 1 month ago

**Selected Answer: B**

Guys it states: "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 app has already been made. The first next step is to add it to a group.

upvoted 1 times

**bitjos** 2 years ago

after VW has made your new car in the factory can you drive it right away or you need some more steps like that they ship it to you? same logic, the app is created for them but not delivered

upvoted 3 times

**TonySuccess** 2 years, 3 months ago

**Selected Answer: A**

AAAAAAAAAAAA

upvoted 2 times

**Solaris2002** 2 years, 10 months 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** 3 years ago

Solution: You start by adding the application to Intune.

A is ok.

upvoted 1 times

**b3arb0yb1m** 3 years ago

A. Yes is correct. Add the app to Intune first.

upvoted 1 times

**Nicholas** 3 years ago

A is correct answer

upvoted 1 times

**AVP_Riga** 3 years, 3 months 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

**Suggested 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

*Community vote distribution*
B (100%)

**AVP_Riga** Highly Voted 3 years, 3 months ago
Seems good 😊
upvoted 7 times

**Darkfire** Most Recent 1 year, 3 months ago
Selected Answer: B
B is correct
upvoted 1 times

**reastman66** 1 year, 5 months ago
Selected Answer: B
Correct answer
upvoted 1 times

**junior6995** 1 year, 8 months ago
Block: Blocks enterprise data from leaving protected apps.
Allow overrides: User is prompted when attempting to relocate data from a protected to a non-protected app. If they choose to override this prompt, the action will be logged.
Silent: User is free to relocate data off of protected apps. These actions are logged.
Off: User is free to relocate data off of protected apps. No actions are logged.
upvoted 1 times

**TonySuccess** 2 years, 3 months ago
Selected Answer: B
BBBBBBBBB
upvoted 1 times

**AL99** 2 years, 9 months ago
Answer B: Silent
upvoted 1 times

**mikl** 3 years ago
B. Silent is correct.

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

**Moderator** 3 years 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 3 times

**b3arb0yb1m** 3 years 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

**Suggested 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

*Community vote distribution*
A (100%)

**AVP_Riga** Highly Voted 3 years, 3 months ago
Seems correct 😊. A.
upvoted 6 times

**Darkfire** Most Recent 1 year, 3 months ago
Selected Answer: A
A = correct

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

**osxzvkwpfcfxobqjby** 1 year, 6 months ago
Should be A+B. First move the files from the local drive to OneDrive then claim diskspace with Files On-Demand....
upvoted 1 times

**JN_311** 2 years, 1 month ago
Selected Answer: A
Easy one. A
upvoted 1 times

**AhmadMa** 2 years, 2 months ago
the question is to minimize the disk space consumed by a user profile , the correct answer is B since files on demand work on all files
upvoted 3 times

**TonySuccess** 2 years, 3 months ago
Selected Answer: A
A A A A A A
upvoted 1 times

**MR_Eliot** 2 years, 8 months ago
Selected Answer: A
A is correct.
upvoted 1 times

**distortion** 2 years, 11 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 3 times

**mikl** 3 years 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 2 times

**b3arb0yb1m** 3 years ago

A. OneDrive Files On-Demand

upvoted 1 times

**CaloyB_IT** 3 years, 1 month 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

**Suggested 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

*Community vote distribution*
AD (100%)

**Jana08** Highly Voted 3 years, 5 months ago
Answer is correct
upvoted 9 times

**TonySuccess** Most Recent 2 years, 3 months ago
Selected Answer: AD
AD, thnks
upvoted 1 times

**MR_Eliot** 2 years, 8 months ago
Selected Answer: AD
answer is correct.
upvoted 1 times

**mikl** 3 years ago
Seems right.
upvoted 2 times

**Moderator** 3 years ago
Yes, correct answer given.
upvoted 2 times

**b3arb0yb1m** 3 years 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

**Suggested 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

*Community vote distribution*
C (100%)

**Davidchercm** Highly Voted 3 years, 5 months ago
https://docs.microsoft.com/en-us/deployoffice/plan-office-365-proplus
upvoted 6 times

**TonySuccess** Most Recent 2 years, 3 months ago
Selected Answer: C
I see that it is C
upvoted 1 times

**MR_Eliot** 2 years, 8 months 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** 3 years ago
Agree - ODT.
upvoted 1 times

**b3arb0yb1m** 3 years ago
C. You should make use of the Office Deployment Tool (ODT).
upvoted 2 times

**Rick11221** 3 years, 2 months ago
Office Deployment Tool (ODT)
upvoted 2 times

Question #1 *Topic 2*

Note: This question is part of a series of questions that present the same scenario. Each question in the series contains a unique solution that might meet the stated goals. Some question sets might have more than one correct solution, while others might not have a correct solution.
After you answer a question in this section, you will NOT be able to return to it. As a result, these questions will not appear in the review screen.
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

**Suggested 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.

*Community vote distribution*


**Wilf32** Highly Voted 3 years, 8 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 3 years, 10 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

**Darkfire** Most Recent 1 year, 3 months ago
Selected Answer: B
No = correct

https://learn.microsoft.com/en-us/autopilot/self-deploying
This feature is used to NOT let the user choose settings.
So in this case it does not set the goal.
upvoted 1 times

**MR_Eliot** 2 years, 8 months ago
Selected Answer: B
B is correct. You should first reset the device from the endpoint manager.
upvoted 1 times

**Moderator** 3 years 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** 3 years ago
Answer is correct, no option for user select (language) using self-deploying
upvoted 1 times

**Goofer** 3 years, 1 month 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** 4 years, 1 month 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** 4 years, 2 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** 4 years, 3 months 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** 4 years, 8 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** 4 years, 8 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** 4 years, 8 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** 4 years, 3 months 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

**Suggested 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

*Community vote distribution*


**MikeMatt2020** Highly Voted 3 years, 7 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 11 times

**Wilf32** 3 years, 7 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 3 years, 5 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 10 times

**RodrigoT** 2 years, 9 months 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

**syougun200x** 2 years, 4 months ago

Among all the comments here, your observation goes the deepest and seems right. Thank you.

upvoted 1 times

**Dnyc** Most Recent 1 year, 10 months ago

Answer is B, this would not let you install updates during a maintenance window.

However, the reasoning provided is also not correct I think, because of the way the question is phrased.

The wording of this question is very specific: during a MAINTENANCE WINDOW. This means setting an automatic maintenance activation boundary: 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

Once you have set the maintenance boundary, you could then set the random delay if you wanted to, but the actual maintenance window itself is setup via the boundary.

No mention is made of collections or Config Manager so it doesn't seem to be referring to Config Manager maintenance windows.

upvoted 1 times

**Meebler** 2 years ago

B,

The Automatic Maintenance Random Delay setting allows you to specify a random delay time for Automatic Maintenance to run on a computer. Automatic Maintenance is a feature in Windows 10 that performs routine maintenance tasks, such as installing updates and running system diagnostics, while the computer is not in use.

While configuring the Automatic Maintenance Random Delay setting may help to ensure that maintenance tasks are performed at a convenient time for the user, it will not ensure that feature and quality updates are installed automatically on the computer.

To ensure that feature and quality updates install automatically on a Windows 10 computer during a maintenance window, you will need to configure the Windows Update settings in Group Policy or use the Windows Update for Business feature.

upvoted 1 times

**ShanePh** 2 years, 6 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** 2 years, 9 months 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** 2 years, 11 months 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** 2 years, 11 months 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%
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** 3 years, 1 month 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** 3 years, 3 months 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** 3 years, 7 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** 3 years, 7 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** 3 years, 7 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** 3 years, 8 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** 3 years, 8 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** 2 years, 8 months 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

**Suggested 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

*Community vote distribution*


**MikeMatt2020** Highly Voted 3 years, 7 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 28 times

**Pleebb** 3 years, 6 months ago
I agree
https://docs.microsoft.com/en-us/windows/deployment/update/waas-restart
upvoted 1 times

**ClaudioItCosta** 3 years, 6 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** 2 years, 10 months 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 2 times

**ExamStudy101** 3 years, 5 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 6 times

**RodrigoT** 2 years, 9 months 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** 2 years, 8 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

**rendog** 2 years, 2 months ago
I think you may have overthought this one... couldn't you just change this policy again to fit it within the new maintenance window ?
upvoted 2 times

**badguytoo** Highly Voted 3 years, 5 months 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 6 times

**Brandon_Marlin** Most Recent 1 year, 10 months ago
Selected Answer: A
ChatGPT said the answer is yes, so I'm going with that.
upvoted 4 times

**Meebler** 2 years ago
A,

Yes, configuring the Windows Update settings in Group Policy as described in the solution would meet the goal of ensuring that feature and quality updates install automatically on a Windows 10 computer during a maintenance window.

By enabling the "Configure Automatic Updates" policy and selecting the "Auto download and schedule the install" option, you will instruct the computer to automatically download and install updates at the specified time. This will ensure that feature and quality updates are installed automatically on the computer during the maintenance window, as required.

It is important to note that you will need to ensure that the computer is turned on and connected to the internet during the maintenance window in order for the updates to be installed successfully.
upvoted 1 times

**coelho4cc** 2 years, 6 months 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** 2 years, 8 months 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** 2 years, 8 months ago
I agree with you.
upvoted 1 times

**Cisco** 2 years, 8 months 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** 2 years, 9 months 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** 2 years, 11 months ago

**Selected Answer: A**

I agree with everything MikeMatt2020 said

upvoted 2 times

**defrey** 3 years ago

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

upvoted 1 times

**forummj** 3 years, 5 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** 2 years, 9 months 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** 3 years, 7 months ago

No : nothing about "maintenance" inside this GPO.

upvoted 1 times

**ExamStudy101** 3 years, 5 months ago

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

upvoted 2 times

**Wilf32** 3 years, 8 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

**MikeMatt2020** 3 years, 7 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 4 times

**ExamStudy101** 3 years, 5 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 4 times

Question #4 *Topic 2*

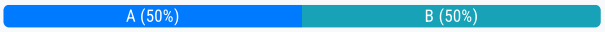
Note: This question is part of a series of questions that present the same scenario. Each question in the series contains a unique solution that might meet the stated goals. Some question sets might have more than one correct solution, while others might not have a correct solution.
After you answer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

**Suggested 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

*Community vote distribution*




**Mujja** Highly Voted 3 years, 6 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

**Brandon_Marlin** Most Recent 1 year, 10 months ago
Selected Answer: B
Chat GPT said the answer was no
No, the solution you provided would not meet the goal of ensuring that feature and quality updates install automatically on a Windows 10 computer during a maintenance window.

The "Automatic Maintenance Activation Boundary" setting in the Maintenance Scheduler settings of Group Policy does not control the installation of feature and quality updates on Windows 10 computers. Instead, it controls the activation of automatic maintenance tasks, such as disk optimization and system diagnostics, during a defined time period. This setting allows you to configure a start time and end time for the automatic maintenance window.

To ensure that feature and quality updates install automatically on a Windows 10 computer during a maintenance window, you would need to enable the "Configure Automatic Updates" setting in Group Policy, as described in my previous answer. This would allow you to specify when and how updates are downloaded and installed on the computer, including during a maintenance window.
upvoted 2 times

**Meebler** 2 years ago
B,

configuring the Automatic Maintenance Activation Boundary setting in Group Policy will not ensure that feature and quality updates install automatically on a Windows 10 computer during a maintenance window.

The Automatic Maintenance Activation Boundary setting specifies the time after which Automatic Maintenance will run if the computer has been idle and on battery power. Automatic Maintenance is a feature in Windows 10 that performs routine maintenance tasks, such as installing updates and running system diagnostics, while the computer is not in use.

While configuring the Automatic Maintenance Activation Boundary setting may help to ensure that maintenance tasks are performed at a convenient time for the user, it will not ensure that feature and quality updates are installed automatically on the computer.

To ensure that feature and quality updates install automatically on a Windows 10 computer during a maintenance window, you will need to configure the Windows Update settings in Group Policy or use the Windows Update for Business feature.

upvoted 2 times

**Deric** 2 years, 3 months 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 years, 5 months 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** 2 years, 8 months 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 2 times

**RodrigoT** 2 years, 8 months ago

And if you enable this policy it will override the maintenance window setting.

upvoted 3 times

**nipsey** 2 years, 9 months 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** 2 years, 9 months 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** 2 years, 10 months 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** 2 years, 8 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** 2 years, 11 months 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

**lykeP** 2 years, 11 months ago

**Selected Answer: A**

The maintenance activation boundary is the daily scheduled time at which Automatic Maintenance starts.
upvoted 3 times

**tf444** 3 years, 2 months 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** 3 years, 5 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** 3 years, 5 months ago

Actually I'd change my answer to A
upvoted 4 times

**Tomtom11** 3 years, 7 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** 3 years, 8 months ago

This will overide the maintenance window setting.

https://www.windows-security.org/070988756d95e4fc3ebfe6be6cc1094b/automatic-maintenance-activation-boundary
upvoted 3 times

**Wilf32** 3 years, 8 months ago

I agree with answer is NO
upvoted 1 times

Question #5 *Topic 2*

DRAG DROP -

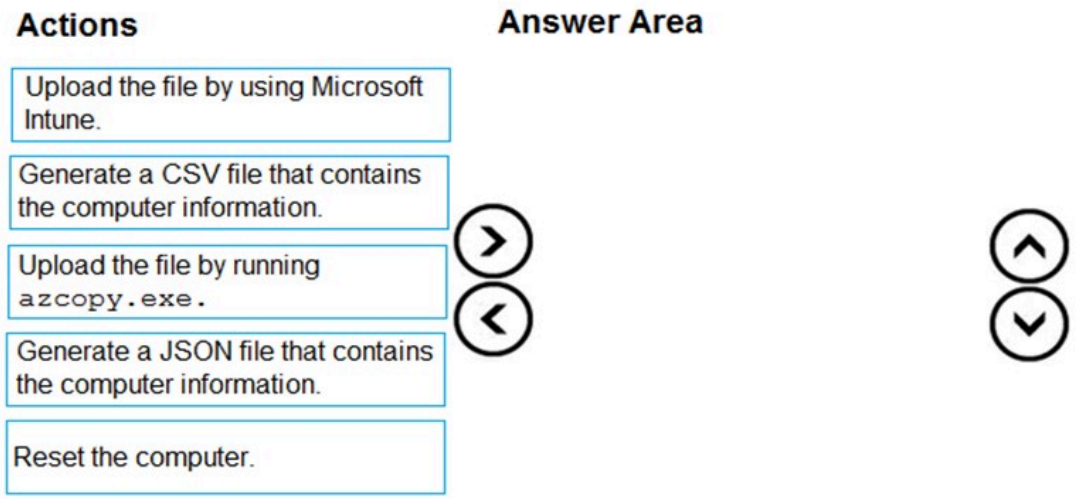
Your company has a computer named Computer1 that runs Windows 10.

Computer1 was used by a user who left the company.

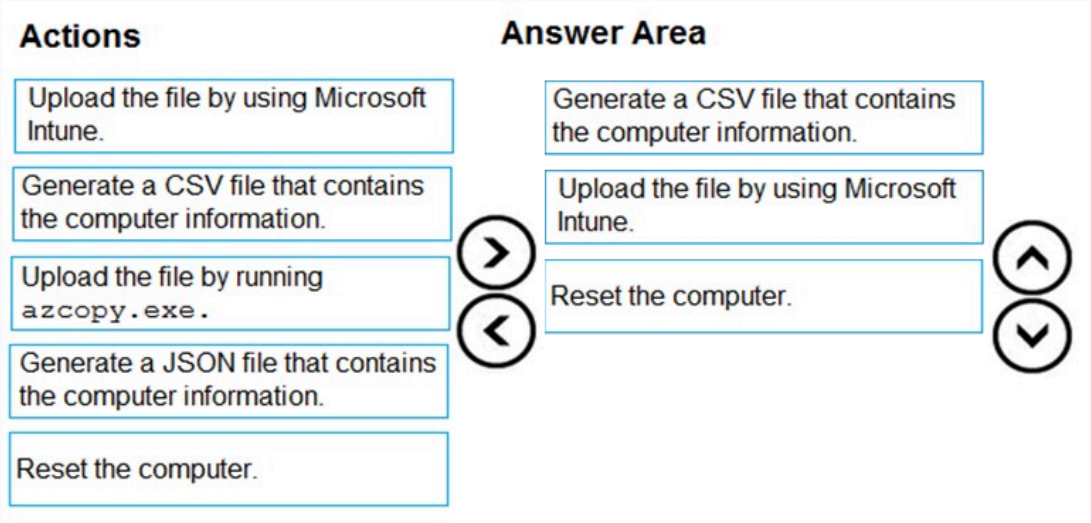
You plan to repurpose Computer1 and assign the computer to a new user. You need to redeploy Computer1 by using Windows AutoPilot.

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:




**Suggested 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 3 years, 8 months ago
I agree with the Answer.

Generate CSV
Upload to intune
Reset PC
upvoted 23 times

**jt2214** Most Recent 1 year, 11 months ago
This is how I do it at my company when I re-provision a device.
upvoted 2 times

**Princee450** 2 years, 1 month ago
Why don't we reset the computer first?
upvoted 1 times

**Graz** 2 years ago
it won't receive the policies when it network access is restored. until the device information is uploaded first. You can reset it first but it would just be redundant because you'd have to do it again.
upvoted 1 times

**Lodan** 2 years, 8 months 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 2 times

**RodrigoT** 2 years, 8 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 3 times

**mikl** 3 years ago
Correct.

Generate CSV
Upload
Reset
upvoted 1 times

**Perycles** 3 years, 7 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** 3 years, 7 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

**Suggested 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** Highly Voted 2 years, 8 months ago

Answer is correct.

upvoted 7 times

**Amir1909** Most Recent 11 months, 3 weeks ago

Correct

upvoted 1 times

**jt2214** 1 year, 11 months ago

Looks correct to me.

upvoted 1 times

**Meebler** 1 year, 11 months ago

B) Endpoint Manager admin Center

To manage the new computers using Windows Autopilot, you should use the Endpoint Manager admin center. This is the management tool that allows you to enroll devices in Intune, create Autopilot deployment profiles, and configure the settings for the new computers.

AAD admin center is used to manage Azure AD, it is not used to manage the devices directly, it's used to manage the users, groups, and other objects in the directory.

VAMT (Volume Activation Management Tool) is used for managing product keys and activation for Windows and Office products, and it's not related to Autopilot or Intune.

upvoted 2 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.

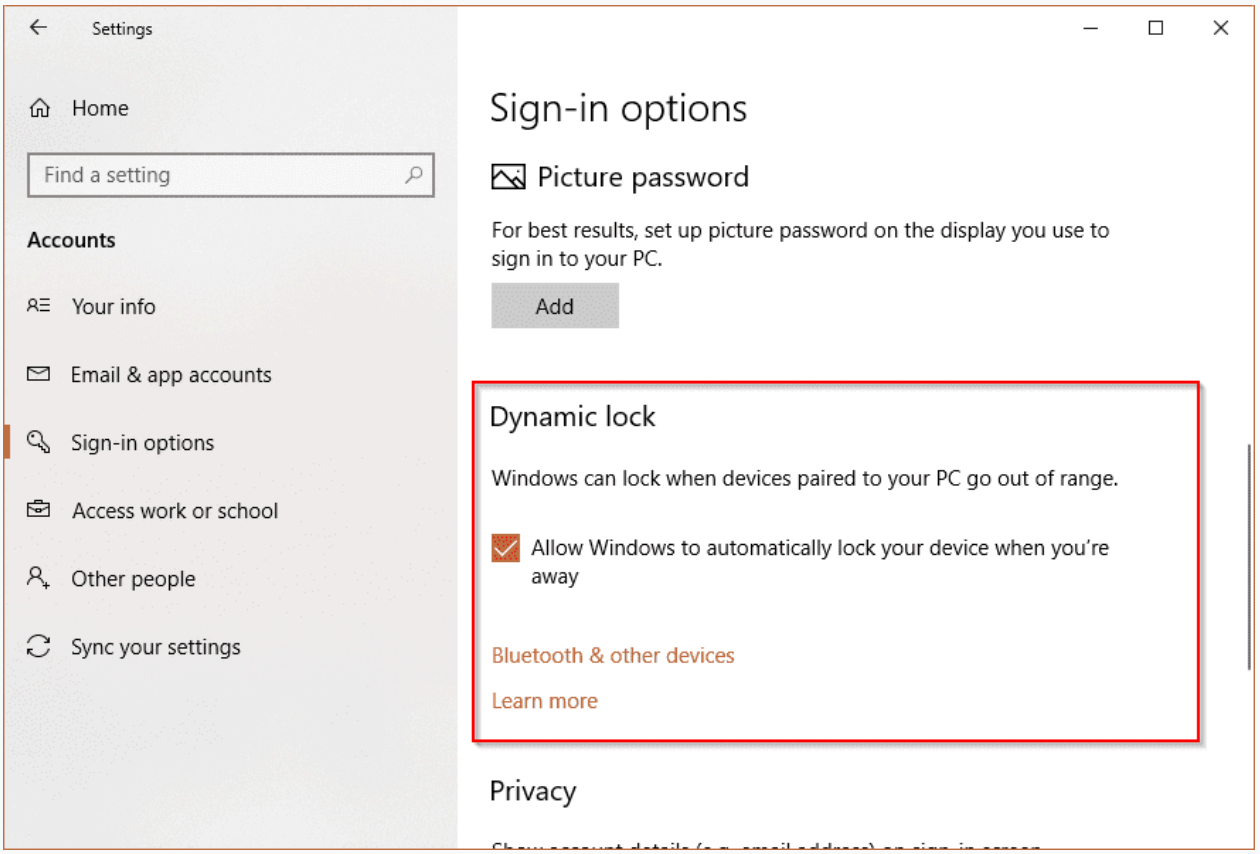
A. Facial recognition

B. A smartwatch that is Bluetooth-enabled

C. A PIN

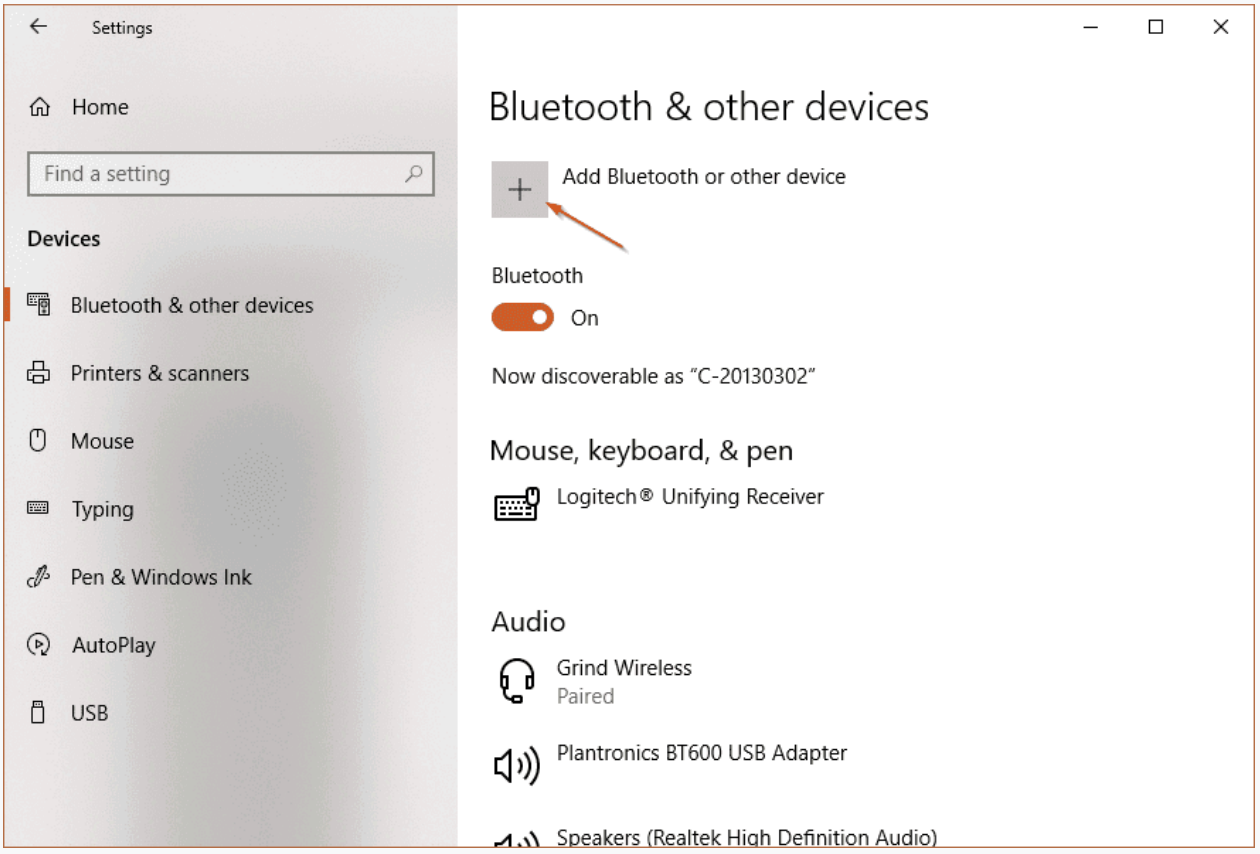
D. A USB key

**Suggested 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 ɔ€Add Bluetooth or other devicesɔ€ 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

*Community vote distribution*

AC (94%) 6%

**Derrickdrx** Highly Voted 2 years, 4 months 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 22 times

**FlailingLimbs** 2 years, 3 months ago

Agreed.

upvoted 3 times

**Contactfornitish** Most Recent 1 year, 2 months ago

Selected Answer: AB

Just open the dynamic lock related policy and check the particular gpo setting XML details. It would make it clear.
<rule schemaVersion="1.0"> <signal type="Bluetooth" scenario="Dynamic Lock" classOfDevice="512" rssiMin="-10" rssiMaxDelta="-10"/> </rule>

upvoted 1 times

**Contactfornitish** 1 year, 2 months ago

On the second thought, yes dynamic lock would not help you in sign in but rather lock unlock so we can stick to pin and face

upvoted 1 times

**OG_Diablo** 1 year, 5 months ago

Selected Answer: AC

A and C are correct.
Dynamic Lock with a Bluetooth device only locks the device; you cannot sign-in with it.
However, when setting up biometrics to unlock, you also set up a backup PIN. So you can always sign-in with PIN when WHfB is configured.

upvoted 2 times

**Badr_123** 1 year, 6 months ago

Selected Answer: AC

Chat GPT

The two valid methods a user can use to sign in, based on the given configuration, are:

A. Facial recognition (using the camera for Windows Hello)
C. A PIN (personal identification number)

By enabling the "use biometric" setting and "use Windows Hello for Business" setting in the Windows Hello for Business Group Policy, the user can utilize facial recognition as one of the authentication methods. This is possible due to the computers having cameras that support Windows Hello for Business.

Additionally, the "use Windows Hello for Business" setting allows the user to set up and use a PIN as an alternative sign-in method.

Therefore, the correct answers are A. Facial recognition and C. A PIN.

upvoted 1 times

**VMLaza** 1 year, 10 months ago

Selected Answer: AC

Correct Answers are AC

upvoted 1 times

**jt2214** 1 year, 11 months ago

I got this question on MD-100, It's A and C.

upvoted 1 times

**aleexoo** 1 year, 12 months ago

Selected Answer: AC

Correct Answers are AC:
Biometrics allow to sign-in using Facial recognition and PIN to use in case of failures (stated in the GPO)

Dynamic lock can only lock the device, it does not allow to sign-in.

upvoted 1 times

**snoopie104** 2 years ago

Selected Answer: AC

I agree wit Derrrickdrx

upvoted 1 times

**Graz** 2 years ago

Selected Answer: AC

Dynamic Lock only locks your machine when you are away. It doesn't unlock it when you come back.

The device unlock setting is also left unconfigured. I would agree with AC

There was a similar question regarding dynamic lock on the MD-100 Dump that everyone in the comments thought was wrong but turned out to be right. Wouldn't surprise me if this is the case. Thanks Microsoft!

upvoted 2 times

**drhousedk** 2 years ago

Selected Answer: AC

AC for sure, Dynamic Lock isn't exactly unlocking.

upvoted 1 times

**Meebler** 2 years ago

AC,

Options A and C: Facial recognition and a PIN, are valid methods that a user can use to sign in based on the configuration of the Windows Hello for Business Group Policy settings shown in the exhibit.

The exhibit shows that facial recognition is enabled as a sign-in method, which means that users can use the camera on their computer to sign in using facial recognition. The exhibit also shows that the use of a PIN is allowed, which means that users can use a PIN to sign in to their computer.

Option B: A smartwatch that is Bluetooth-enabled, is not a valid method for signing in based on the configuration shown in the exhibit. The exhibit does not mention the use of smartwatches or other Bluetooth-enabled devices as a sign-in method.

Option D: A USB key, is also not a valid method for signing in based on the configuration shown in the exhibit. The exhibit does not mention the use of USB keys as a sign-in method.

Therefore, the valid methods for signing in based on the configuration shown in the exhibit are facial recognition and a PIN.

upvoted 2 times

**devilcried** 2 years, 2 months ago

Selected Answer: AC

Does not unlock with "a smartwatch that is Bluetooth-enabled" . So A, C

upvoted 2 times

**KiwE** 2 years, 2 months ago

The answer here is pin and facial. Your computer will just LOCK upon leaving; when you return with your bluetooth watch (or smarthphone) it will NOT unlock automatically. If you google it; it's one of the complaints about the method.

upvoted 2 times

**raduM** 2 years, 2 months ago

two valid modes to sign in. dynamic lock just locks the computer when you step away from it, it does not sign you in. so the answer is c

upvoted 1 times

**daye** 2 years, 2 months ago

Selected Answer: AC

I agree with AC, also when you configure Windows Hello for Business you are required to stablish at least a PIN a part from a biometric option

https://learn.microsoft.com/en-us/windows/security/identity-protection/hello-for-business/hello-overview#how-windows-hello-for-business-works-key-points

upvoted 3 times

**cbjorn8931** 2 years, 3 months 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** 2 years, 3 months ago

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

upvoted 2 times

**RickyBee** 2 years, 3 months ago

Selected Answer: AC

Agree i

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.

**Suggested 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

*Community vote distribution*
AE (100%)

**[Removed]** 1 year, 4 months ago
A and E. A GPT patition and UEFI are required
upvoted 1 times

**Setryx** 1 year, 7 months ago
my question is this: UEFI is already running in BIOS , why should we choose E?
upvoted 1 times

**mathyvarnan** 1 year, 8 months ago
Chat GPT said B and E
To ensure that the computers can use Secure Boot after upgrading to Windows 10, you should perform the following two actions:

B. Enable the TPM chip - Secure Boot requires a TPM chip to store and protect encryption keys used for secure boot process.

E. Convert the firmware from BIOS to UEFI - Secure Boot requires UEFI firmware to enable and enforce security policies during the boot process.

Therefore, options B and E are correct. Options A, C, and D are not required for enabling Secure Boot.
upvoted 1 times

**mathyvarnan** 1 year, 8 months ago
Chat GPT said A and E
To ensure that the computers can use Secure Boot after upgrading to Windows 10, you should perform the following two actions:

B. Enable the TPM chip - Secure Boot requires a TPM chip to store and protect encryption keys used for secure boot process.

E. Convert the firmware from BIOS to UEFI - Secure Boot requires UEFI firmware to enable and enforce security policies during the boot process.

Therefore, options B and E are correct. Options A, C, and D are not required for enabling Secure Boot.

upvoted 1 times

**Hatsapatsa** 2 years ago

**Selected Answer: AE**

This question was on MD-100 exam and AE were correct.

upvoted 1 times

**snoopie104** 2 years, 2 months ago

**Selected Answer: AE**

I think this is correct.

upvoted 1 times

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).

**Suggested 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

*Community vote distribution*


**Mendel** Highly Voted 5 years, 3 months 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 35 times

**Sortjuh** 5 years, 2 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

**PESK** 5 years, 2 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** 4 years, 11 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** 4 years, 5 months ago
"You need to automatically register all the existing computers to Azure AD"
So they aren't enrolled just yet.
upvoted 8 times

**egdeeptha** 3 years, 6 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** 2 years, 8 months 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 4 times

**CvdK** 4 years, 1 month 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 3 times

**CvdK** 4 years, 1 month ago
So D is the correct answer!
upvoted 9 times

**MZONDERL** 2 years, 11 months ago
Azure AD–registered is not the same as Azure AD Joined...
upvoted 2 times

**Dnyc** 1 year, 10 months ago
You cannot be joined to AD and Azure AD at the same time. In hybrid join scenario as stated, you join AD, and register with Azure AD.
upvoted 1 times

**jojolabubu** Highly Voted 4 years, 2 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 14 times

**mikl** 3 years ago
Thats not how you minimize administrative effort - answer is D.
upvoted 2 times

**RodrigoT** 2 years, 9 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** 2 years, 8 months 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 5 times

**Amir1909** Most Recent 11 months, 4 weeks ago
D is correct
upvoted 1 times

**Contactfornitish** 1 year, 2 months ago
Selected Answer: D
A. An Autodiscover address record.
Not relevant, nowhere mentioned in auto-pilot requirements

B. A Windows AutoPilot deployment profile.
How you deploy the profile if the device is NOT ENROLLED in Intune yet?

C. An Autodiscover service connection point (SCP).
Yes! this step is required for case, whenever no AD

D. A Group Policy object (GPO).
For Hybrid joined device, when enrollment is not done yet, easiest option is GPO since it's managed by AD
https://learn.microsoft.com/en-us/windows/client-management/enroll-a-windows-10-device-automatically-using-group-policy
upvoted 1 times

**lannythewizard** 1 year, 8 months ago
Selected Answer: D
I think D. Crux of this question is with least administrative effort. It mentions devices are joined to Active Directory, so you can use a GPO in this case. If they were Azure AD joined, GPO obviously wouldn't be an option, but since they are you can use a GPO to enroll into MDM automatically
upvoted 1 times

**zm9** 1 year, 9 months ago
The question mentions that: A hybrid Microsoft Azure Active Directory (Azure AD) and Microsoft Intune are already implemented >> This means devices are already registered in the Azure AD
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

The second request is to enroll the computers in Intune >> there are two ways (B and D)
The third request is to minimize administrative effort >> Answer D is has the less administrative effort
upvoted 2 times

**Titus42** 1 year, 10 months ago
B People need to keep in mind you don't need to touch these 2000 machines individually, your provider can just give you a csv. file with all of the information needed to upload right into the cloud.
upvoted 1 times

**An1m4_** 1 year, 10 months ago
Selected Answer: D
D, GPOs allow to enroll your Hybrid devices in AAD and Intune easily and with minimal effort
upvoted 2 times

**Meebler** 2 years ago
B,

Option A: An Autodiscover address record, is not relevant in this scenario. Autodiscover is a feature in Microsoft Exchange that allows clients to automatically discover and configure their Exchange server connection settings. It is not related to registering and enrolling devices in Azure AD and Intune.

Option C: An Autodiscover service connection point (SCP), is also not relevant in this scenario. An SCP is an Active Directory object that allows clients to locate the Autodiscover service for their domain. It is not related to registering and enrolling devices in Azure AD and Intune.

Option D: A Group Policy object (GPO), is also not relevant in this scenario. Group Policy is a feature in Windows that allows you to configure and manage settings and policies for computers and users in a domain. While Group Policy can be used to configure various settings on devices, it is not specifically designed for registering and enrolling devices in Azure AD and Intune.

Therefore, the solution that minimizes administrative effort in this scenario is to use a Windows AutoPilot deployment profile.

upvoted 2 times

**Graz** 2 years ago

There's the practical real life way to tackle these scenarios and then there is the Microsoft way. With old questions with a ton of debate that the mods don't switch, that typically the answer Microsoft is looking for (even if it is ass backwards).

upvoted 1 times

**gigiscula** 2 years ago

Guys, the answer is D.
A - I don't even consider it
It's said "You implement hybrid Microsoft Azure Active Directory (Azure AD) and Microsoft Intune." So you have configured Azure AD Connect for Hybrid mode and SCP it's automatically created on Active Directory. So C it's out.
B - If completely resetting 2000 machines is considered a minimum effort I challenge anyone to propose it to a customer. Also, Windows Autopilot only works the first time you start your PC.
Only D remains, which is in any case the only viable and correct solution

upvoted 1 times

**DDHP7** 2 years, 1 month ago

the key words is " hybrid Microsoft Azure Active Directory " which mean it has AD and AAD, therefore, auto-enroll AD PCs to Intune would be D use GPO, which I have done in my last job

upvoted 2 times

**Deric** 2 years, 4 months 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 years, 5 months ago

B shopuld be correct

upvoted 1 times

**Harold** 2 years, 8 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 2 times

**MR_Eliot** 2 years, 8 months ago

**Selected Answer: C**

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

upvoted 2 times

**Cisco** 2 years, 8 months 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

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 | |

**Suggested 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 ג€" Notify the user before downloading the update. Users choose to download and install updates.
* Auto install at maintenance time ג€" 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 ג€" 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 4 years 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 13 times

**RodrigoT** 2 years, 9 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 2 times

**ThomasDehottay** Highly Voted 3 years, 7 months ago
This question should be updated. Delivery Optimization is now set by a configuration profile.
upvoted 8 times

**Tomtom11** Most Recent 3 years, 9 months ago

https://docs.microsoft.com/en-us/mem/intune/configuration/delivery-optimization-settings
upvoted 2 times

**PESK** 5 years, 2 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** 5 years, 2 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 31 times

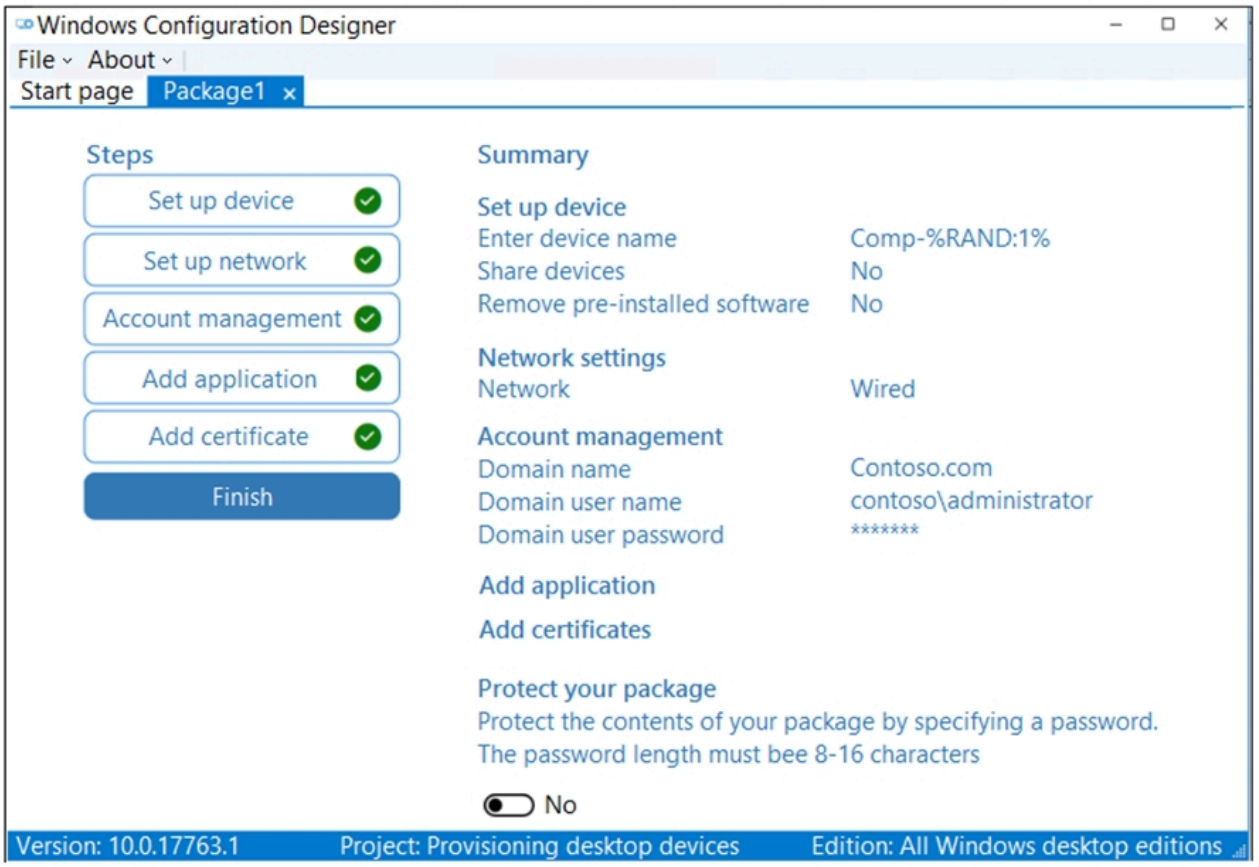
**PESK** 5 years, 2 months ago

Thanks for the clarification. I'm over-thinking it as usual.
upvoted 9 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

**Suggested Answer:** *B*

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

*Community vote distribution*

B (100%)

**Merma** Highly Voted 3 years, 7 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

**AyoR32** Most Recent 2 years ago

This question sounds like another :

Question #6Topic 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

2 similar questions and 2 different answers...

Which answer is officially correct for Microsoft during a certification exam ?

upvoted 1 times

**Antimus** 2 years, 1 month ago

Another READ THE QUESTION question, I got stuck on how many times an account can join a machine to the domain and went down a rabbit hole

upvoted 1 times

**MaxMink** 2 years, 5 months ago

**Selected Answer: B**

Right!

upvoted 1 times

**AL99** 2 years, 9 months ago

Answer :10 device

upvoted 1 times

**Hulisanimellla** 2 years, 9 months ago

**Selected Answer: B**

ANSWER IS CORRECT

upvoted 1 times

**PersoDaniels** 3 years, 6 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** 3 years, 6 months ago

Answer is D

upvoted 2 times

**Mujja** 3 years, 6 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** 3 years, 5 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 3 times

**AVR31** 2 years, 8 months ago

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

upvoted 1 times

**Perycles** 3 years, 7 months ago

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

upvoted 2 times

Question #12 *Topic 2*

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

**Suggested 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 4 years, 1 month ago
Tested this today. Answer is ok:
- Wifi password remain
- App1 removed
- VPN removed
upvoted 67 times

**RodrigoT** 2 years, 8 months ago
Thank you for really testing.
upvoted 4 times

**Lomak** Highly Voted 4 years, 4 months 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

**Amir1909** Most Recent 11 months, 4 weeks ago
Correct
upvoted 1 times

**NoursBear** 1 year, 2 months ago
https://learn.microsoft.com/en-us/autopilot/tutorial/reset/autopilot-reset-overview
upvoted 1 times

**NKG123** 3 years, 1 month ago
Shut your mouth instead of saying wrong statements
upvoted 7 times

**sbmkhize** 3 years, 3 months ago
The answer does not look to be right BUT it is right....
upvoted 2 times

**uns_uns** 3 years, 9 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 13 times

**forExamCert2023** 2 years, 10 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** 2 years, 9 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 3 times

**67_sbc** 4 years, 1 month 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** 2 years, 9 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 4 times

**MaxMink** 2 years, 5 months 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** 4 years, 2 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** 4 years, 2 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** 4 years, 2 months ago

This question answer is correct: https://docs.microsoft.com/en-us/mem/autopilot/windows-autopilot-reset

upvoted 2 times

**MD0000** 4 years, 2 months ago

there is no specific mention of VPN status after reset on the referenced link

upvoted 1 times

**loganharris** 4 years, 3 months ago

VPN connection will be retained and the credentials will be cached rest is correct

upvoted 1 times

**MD0000** 4 years, 2 months ago

source please

upvoted 2 times

**Mujja** 3 years, 6 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** 4 years, 4 months ago

Why Wi-Fi connection will not removed?

upvoted 3 times

**Mujja** 3 years, 6 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** 3 years, 9 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

**Suggested 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

**zm9** 1 year, 9 months ago
The question is either NOT correct OR old because of the updates to Intune

The purpose of the reset operation is to reset the computers to run Windows 10 Enterprise with the latest update
NONE of the answers is correct according to the references mentioned in the answer

The Wipe action will do this:
The Wipe action restores a device to its factory default settings

The Fresh start action will do this:
If you do not retain user data, the device will be restored to the default OOBE

NONE of the actions will reset the computers to run Windows 10 Enterprise with the latest update
upvoted 2 times

**ExamTopics1_EIS** 1 year, 9 months ago
Fresh Start: 3 Only - Wipe: 1, 2, and 3 (dig for this, you'll find more). The Fresh Start device action removes any apps that are installed on a PC running Windows 10, version 1709 or later
upvoted 1 times

**baniraaisukurimu** 1 year, 11 months ago
I think for both options it's computer 3 only. Fresh start doesn't install the feature update either.
upvoted 1 times

**mikekrt** 2 years, 1 month ago
Fresh start: 2-3 and wipe only 3. The wipe option will not update a computer, so only the computer with the latest updates already installed will be up to date
upvoted 2 times

**xian05** 2 years ago
Confirmation that the fresh start updates the computer automatically and a reset "Resets the operating system to its default state and settings."

https://www.petervanderwoude.nl/post/factory-reset-fresh-start-autopilot-reset-so-many-options/
upvoted 1 times

**zm9** 1 year, 9 months ago

It is on .. July 16, 2018

The updates in Microsoft website are in 2023

upvoted 1 times

**Deric** 2 years, 3 months ago

The answer is correct.

upvoted 4 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

**Suggested 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/

*Community vote distribution*
A (100%)

**Santosh4u** Highly Voted 4 years, 11 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 29 times

**Dave4187** Highly Voted 4 years, 7 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 2 years, 11 months ago

A. Computer2 and Computer4 only
upvoted 2 times

**washandr** 2 years, 11 months 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** 2 years, 11 months ago
Ignore the above. Apparently you can update w7 directly to w10
upvoted 6 times

**mikl** 3 years 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** 3 years 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** 3 years ago
A. Computer2 and Computer4 only
upvoted 1 times

**3citech** 3 years, 1 month 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** 3 years, 1 month 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** 3 years, 3 months 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** 2 years, 8 months 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** 3 years, 7 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** 4 years 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** 4 years 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** 3 years, 4 months 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** 4 years, 1 month 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** 4 years, 1 month ago
Comp 2 and Comp 4
upvoted 2 times

**Jammer** 4 years, 2 months ago
Dave4187 got it right. Bit locker will just be suspended during the upgrade. A is correct.
upvoted 2 times

**RobbieH** 4 years, 3 months 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

**Suggested 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/

*Community vote distribution*
A (100%)

**Perycles** Highly Voted 3 years, 7 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** 2 years, 8 months ago
The same question appeared on Page 1 Question #9.
upvoted 1 times

**Amir1909** Most Recent 1 year ago
A is correct
upvoted 1 times

**mikl** 3 years ago
Selected Answer: A
A. Device configuration

Agree!
upvoted 4 times

**b3arb0yb1m** 3 years ago
A. Device configuration
upvoted 2 times

**Harisasikumar92** 3 years, 2 months 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** 2 years, 3 months 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 2 times

**tf444** 3 years, 2 months 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** 2 years, 9 months ago
Dude, if you open Intune from the Azure portal you'll be redirected to Endpoint. You are overthinking, relax man.
upvoted 8 times

**Jvp21** 3 years, 6 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

**Suggested 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

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

**jairojunior_br** Highly Voted 4 years, 10 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 19 times

**Syed7** 3 years, 7 months ago
so your answer is A -> Yes ???
upvoted 4 times

**Anthony_2770** 3 years, 10 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** 3 years, 10 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** 3 years, 10 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

**Morwen** 2 years, 3 months 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

**snabelkabel** Highly Voted 4 years, 12 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

**MrPocketRocket** Most Recent 1 year, 10 months ago
Answer is Yes, that is one way to prevent the video drivers from being updated automatically by Windows Update. By using the Group Policy object (GPO) and configuring the Prevent installation of devices using drivers that match these device setup classes setting, you can block the installation of specific device drivers based on their device GUID.

To find the device GUID for your video driver, you can follow these steps:

Open the Device Manager by right-clicking on the Start menu button and selecting Device Manager.
Find your video driver under the Display adapters section.
Right-click on the video driver and select Properties.
Go to the Details tab and select Device instance path from the drop-down menu.
The device GUID should be displayed in the Value field.

Once you have the device GUID, you can use it to configure the Prevent installation of devices using drivers that match these device setup classes setting in the GPO to prevent Windows Update from updating the video driver automatically.
upvoted 1 times

**Meebler** 2 years ago
A,

This solution would meet the goal of preventing the video drivers from being updated automatically by using Windows Update. By enabling the Prevent installation of devices using drivers that match these device setup classes setting in a Group Policy object and specifying the device GUID, you can prevent the specified devices from being updated or installed through Windows Update. This can be useful in situations where specialized hardware or software is in use and you want to ensure that updates do not cause compatibility issues or disrupt the functioning of the system.
upvoted 2 times

**Dedutch** 2 years, 5 months ago
I've done this before for network drivers that have caused issues.
upvoted 1 times

**MitchF** 2 years, 5 months 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** 2 years, 6 months ago
The question is 'updated automatically' not 'installed'. That GPO would prevent any installation, even manual.
upvoted 1 times

**MR_Eliot** 2 years, 8 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** 2 years, 9 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** 2 years, 9 months 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** 2 years, 9 months ago

Answer A:Yes

upvoted 1 times

**PiPe** 2 years, 11 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 8 times

**Santeria** 2 years, 11 months ago

Selected Answer: A

If you specify the GUID, it's correct!

upvoted 1 times

**tf444** 3 years, 3 months 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 3 times

**auton** 3 years, 2 months 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** 3 years, 4 months 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** 3 years, 5 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** 3 years, 6 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

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

**Suggested Answer:** *B*
Reference:
https://www.stigviewer.com/stig/microsoft_windows_server_2012_member_server/2013-07-25/finding/WN12-CC-000024

*Community vote distribution*
B (100%)

**Perycles** Highly Voted 3 years, 7 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

**MvdH81Rijswijk** Most Recent 1 year, 6 months ago
“You need to prevent the video drivers from being updated automatically by using >>>>>Windows Update.<<<<<”:

GPO:
Open the Start menu, search for gpedit.msc, and select the first result that appears. This will open the Local Group Policy Editor.
Use the left pane to navigate to Computer Configuration > Administrative Templates > Windows Components > Windows Update > Manage updates offered from Windows Update.
Double-click the Do not include drivers with Windows Updates policy on your right.

This way you disable the driver update only via WinUpdates. So answer B, NO
upvoted 2 times

**daye** 2 years, 3 months 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** 2 years, 3 months ago
nevermind I was thinking in a WUFB GPO rather than a W10 setting
upvoted 1 times

**MR_Eliot** 2 years, 8 months ago
Selected Answer: B
It's B
upvoted 2 times

**mclovin** 3 years, 4 months ago
duh! ofc it's NO
upvoted 4 times

**dinjo** 4 years, 9 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

**Suggested 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

*Community vote distribution*
A (100%)

**riel_gesh** Highly Voted 4 years, 10 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 22 times

**muzzag** Highly Voted 4 years, 10 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 12 times

**Meebler** Most Recent 2 years ago
A,

This solution meets the goal of preventing the video drivers from being updated automatically by using Windows Update. By enabling the Specify search order for device driver source locations setting and selecting Do not search Windows Update, you can prevent Windows from searching for device driver updates on Windows Update. This will ensure that the video drivers are not updated automatically through Windows Update.
upvoted 1 times

**MR_Eliot** 2 years, 8 months ago
Selected Answer: A
A = correct
upvoted 1 times

**Moderator** 2 years, 9 months ago
Selected Answer: A

And again, a bit overdone but it does do it's job:
https://gpsearch.azurewebsites.net/#183
upvoted 3 times

**franto** 2 years, 10 months 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** 3 years, 7 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** 3 years, 7 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 9 times

**RodrigoT** 2 years, 9 months ago
Apparently it works.
upvoted 3 times

**GohanF2** 3 years, 8 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** 3 years, 8 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** 3 years, 8 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** 3 years 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** 3 years, 10 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** 3 years, 10 months ago

This is exactly what the question is looking for: How to keep getting driver updates from Windows Update.

upvoted 1 times

**vinnyct** 4 years ago

it's A

http://woshub.com/how-to-turn-off-automatic-driver-updates-in-windows-10/

upvoted 5 times

**hawkens** 4 years, 1 month 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

**Suggested 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

*Community vote distribution*
B (100%)

**Perycles** Highly Voted 3 years, 7 months ago
B seems to be correct : "NOTIFY FOR Install" doesn't match with the question "Automatically installed".
upvoted 9 times

**Cristyy** Most Recent 1 year, 2 months ago
Selected Answer: B
B seems to be correct
upvoted 1 times

**franto** 2 years, 10 months 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 3 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

**Suggested 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

*Community vote distribution*
A (100%)

**MidCities** Highly Voted 5 years, 2 months ago
Retract the above. Yes, the answer should be A.
upvoted 15 times

**GrayRant27** Most Recent 2 years, 3 months ago
Correct answer A!
upvoted 2 times

**MitchF** 2 years, 5 months 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 2 times

**Hulisanimellla** 2 years, 9 months ago
Selected Answer: A
AGREE ON A
upvoted 1 times

**mikl** 3 years ago
Agree on A.
upvoted 1 times

**Perycles** 3 years, 7 months ago
Agree for A.
upvoted 2 time

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

**Suggested 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 4 years, 3 months 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 29 times

**mikl** 3 years ago
Agree.
upvoted 2 times

**MikeMatt2020** Highly Voted 3 years, 8 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 9 times

**GrayRant27** Most Recent 2 years, 3 months 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** 4 years, 8 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

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

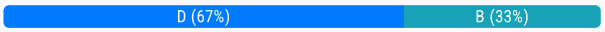
B. Join Azure Active Directory (Azure AD)

C. Create an event subscription

D. Install the Microsoft Monitoring Agent

**Suggested 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

*Community vote distribution*




**Mike_Row** Highly Voted 4 years, 9 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** 2 years, 8 months ago
And this question appeared on Page 1 Question #10. Same answer, install MMA.
upvoted 2 times

**RodrigoT** 2 years, 8 months ago
Commercial ID is to monitor Windows Updates with Update Compliance. Another story.
upvoted 7 times

**riel_gesh** Highly Voted 4 years, 10 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

**Amir1909** Most Recent 11 months, 4 weeks ago
Correct
upvoted 1 times

**AymanShawky** 1 year, 5 months ago
i think i can join to azure AD and can use Log Analytics to query events
upvoted 1 times

**wafa2022** 1 year, 5 months ago
The correct answer is D. Install the Microsoft Monitoring Agent.

To enable Log Analytics to query events from Computer1, you need to install the Microsoft Monitoring Agent on the computer. The Microsoft Monitoring Agent allows you to collect and send data from the computer to the Log Analytics workspace.

Option A (Configure the commercial ID) is not relevant to configuring Log Analytics for querying events from Computer1.

Option B (Join Azure Active Directory) is not necessary for this scenario. Joining Azure Active Directory is typically done for managing user identities and access control.

Option C (Create an event subscription) is not the correct action in this case. Creating an event subscription is used for forwarding events to another destination, not for configuring Log Analytics on a local computer.

Therefore, the correct action to enable Log Analytics querying on Computer1 is to install the Microsoft Monitoring Agent (option D).
upvoted 2 times

**JePe** 1 year, 8 months ago
Checked with Chap gpt and answer D makes sense and works when only in a workgroup.
upvoted 1 times

**Brandon_Marlin** 1 year, 10 months ago
**Selected Answer: D**
To ensure that you can use Log Analytics to query events from Computer1, you should install the Microsoft Monitoring Agent on Computer1.

The Microsoft Monitoring Agent is a lightweight agent that can be installed on Windows computers to collect data and send it to Log Analytics. It enables the monitoring of the performance and health of Windows computers, including the collection of event logs, performance counters, and custom logs.
upvoted 1 times

**AliNadheer** 1 year, 10 months ago
**Selected Answer: B**
i think answer should be B, based on the Prerequisites of azure monitoring agent:

-The machine must be running Windows client OS version 10 RS4 or higher.
-To download the installer, the machine should have C++ Redistributable version 2015) or higher
-The machine must be domain joined to an Azure AD tenant (AADj or Hybrid AADj machines), which enables the agent to fetch Azure AD device tokens used to authenticate and fetch data collection rules from Azure.
You may need tenant admin permissions on the Azure AD tenant.
The device must have access to the following HTTPS endpoints:
and etc..
reference: https://learn.microsoft.com/en-us/azure/azure-monitor/agents/azure-monitor-agent-windows-client
hope i'm not missing something here
upvoted 1 times

**Titus42** 1 year, 10 months ago
Domain Joined and joined to AAD are two different things
upvoted 1 times

**OG_Diablo** 1 year, 5 months ago
You are right, but that is Microsoft's error when writing the doc.
The article does state quite clearly that the device needs to be AAD-joined or hybrid AAD-joined.
So while D seems correct, B is a prerequisite of D.
upvoted 1 times

**N0peasaurus** 2 years, 6 months ago
D:
D
https://docs.microsoft.com/en-us/azure/azure-monitor/agents/log-analytics-agent
upvoted 1 times

**MR_Eliot** 2 years, 8 months ago
**Selected Answer: D**
D = Correct
upvoted 1 times

**Perycles** 3 years, 7 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** 2 years, 9 months 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** 2 years, 8 months ago
Paragraph 2, I mean.
upvoted 2 times

**Balena** 3 years, 10 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** 4 years, 4 months ago
Just to add - Not for making query
upvoted 1 times

**aronutics** 4 years, 4 months ago
it is Install the Microsoft Monitoring Agent, you need commercial ID to enrol computer in windows analytics
upvoted 6 times

**AnoniMouse** 3 years, 7 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

**Suggested 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

*Community vote distribution*
B (100%)

**MR_Eliot** 2 years, 8 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)

**Suggested 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

*Community vote distribution*
A (100%)

**riel_gesh** Highly Voted 4 years, 10 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** 3 years, 3 months ago
not true, with i: migApp you can keep user application.
upvoted 1 times

**JimmyC** 2 years, 1 month ago
Sorry tf444, but you are incorrect. Migapp.xml include application *settings*, it does not install apps. USMT does not have the ability to install apps.
upvoted 2 times

**LauLauLauw** Highly Voted 4 years, 9 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 2 years, 8 months ago
Selected Answer: A
A is the fastest and easiest way to upgrade from Windows 8.1 to Windows 10.
upvoted 3 times

**b3arb0yb1m** 3 years ago
A. an in-place upgrade
upvoted 1 times

**Mujja** 3 years, 6 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** 3 years, 8 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** 3 years, 7 months ago

Windows 10 pro could be updated to Win 10 ENT after the inplaceUpgrade (with intune for example).

upvoted 1 times

**letters1234** 2 years, 10 months 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** 3 years, 7 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 4 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

**Suggested 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/

*Community vote distribution*
C (100%)

**riel_gesh** Highly Voted 4 years, 10 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 27 times

**Perycles** Highly Voted 3 years, 7 months ago
Answer is correct.
upvoted 7 times

**Amir1909** Most Recent 11 months, 4 weeks ago
Correct
upvoted 1 times

**MR_Eliot** 2 years, 8 months ago
Selected Answer: C
C => Correct!
upvoted 1 times

**b3arb0yb1m** 3 years ago
C. SetupConfig.ini
upvoted 2 times

Question #26 *Topic 2*

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. | ○ | ○ |

**Suggested 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 3 years, 8 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 65 times

**IrvSus** 3 years, 8 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** 3 years, 7 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 5 times

**letters1234** 2 years, 10 months 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** 3 years, 8 months ago
I agree
upvoted 1 times

**Layer8** 3 years, 7 months ago
but wouldn't the GPO being set to "disabled" override the intune setting then?
upvoted 4 times

**RodrigoT** 2 years, 9 months 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 6 times

**Jimbob77** 3 years, 7 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

**Percyles** Highly Voted 3 years, 7 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 32 times

**RodrigoT** 2 years, 8 months ago
Thank you for really testing.
upvoted 4 times

**aleexoo** Most Recent 1 year, 12 months ago
YES, NO, YES
Local Policy win over MDM and disabled setting act like "not configured"
upvoted 1 times

**Graz** 2 years ago
If it has been a year and a half and the mods haven't corrected it, the given answer is probably correct although I would have went with yes no yes
upvoted 2 times

**raduM** 2 years, 2 months ago
GPO wins over MDM so i would say yes no no
upvoted 1 times

**TonySuccess** 2 years, 3 months ago

Feel like it should specify Local GPO, as that is misleading.

upvoted 1 times

**coelho4cc** 2 years, 6 months 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 2 times

**Gulshan85** 2 years, 6 months ago

No, Yes, No

The above is the correct answer.

https://docs.microsoft.com/en-us/mem/intune/fundamentals/scope-tags

upvoted 4 times

**AngelusNL** 2 years, 2 months ago

Scope Tags are only used to control acces for Admins and have NOTHING to do with update rings being applied, this is the wrong answer

upvoted 4 times

**AVR31** 2 years, 8 months ago

Answer should be corrected. It is YES-NO-YES. For reasons very well explained by other users.

upvoted 1 times

**Dedutch** 2 years, 5 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 2 times

**Dedutch** 2 years, 5 months ago

No. Scope tag not applied.

upvoted 1 times

**AngelusNL** 2 years, 2 months ago

Scope Tags are only used to control acces for Admins and have NOTHING to do with update rings being applied, this is the wrong answer

upvoted 1 times

**Solaris2002** 2 years, 10 months 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 3 times

**ChrisThrelfall** 2 years, 10 months 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 4 times

**b3arb0yb1m** 3 years ago

Yes

No

Yes

upvoted 4 times

**encxorblood** 3 years, 1 month ago

Answer is correct. GPO in a workgroup? Only intune is the solution and the scope tag ist important.

upvoted 2 times

**letters1234** 2 years, 10 months ago

"Local" Group Policy Object - still accessed by GPedit.msc where it shows both domain and local policies set.

upvoted 1 times

**mikl** 3 years ago

I was wondering the exact same - GPO settings cant apply to devices in workgroup.

upvoted 2 times

**ANDREVOX** 3 years, 1 month 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** 3 years, 7 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 14 times

**camino** 2 years, 10 months ago

Tags are just for RBAC and have nothing to do with assigning a policies

upvoted 4 times

**[Removed]** 2 years, 10 months ago

Correct: https://docs.microsoft.com/en-us/mem/intune/fundamentals/scope-tags

upvoted 2 times

**DaZa5** 2 years, 2 months ago

As described in the link: "https://learn.microsoft.com/en-us/mem/intune/protect/windows-10-update-rings" Windows update rings support scope tags. You can use scope tags with update rings to help you filter and manage sets of configurations that you use.

upvoted 3 times

**ceskil** 2 years, 9 months 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** 3 years, 7 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** 3 years, 7 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 9 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

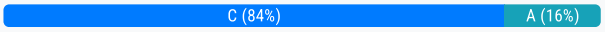
B. any computer in the domain

C. the computers in SubnetA only

D. any computer on the network

**Suggested 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

*Community vote distribution*




**nolancl** Highly Voted 5 years, 3 months 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 27 times

**Layer8** 3 years, 7 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

**ExamTopics1_EIS** 1 year, 9 months ago
Not how networking works. Subnets mandate use of GATEWAY which goes back to router/smart switches and routes to another subnet. So, nope.
upvoted 1 times

**distortion** 2 years, 11 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 3 times

**MZONDERL** Highly Voted 2 years, 11 months 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 13 times

**RodrigoT** 2 years, 8 months ago
You got it my friend! Same subnet only, by default.
upvoted 6 times

**Dedutch** 2 years, 5 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 2 times

**[Removed]** Most Recent 1 year, 4 months ago

A the default is peer to peer behind the same NAT.

upvoted 1 times

**wafa2022** 1 year, 5 months ago

D. any computer on the network.

Since Delivery Optimization is enabled and there is no specific restriction mentioned regarding update sources, Computer1 will download updates from any computer on the network. Delivery Optimization utilizes peer-to-peer sharing, allowing Windows 10 computers to download updates from other computers on the same local network or from the internet. Therefore, Computer1 will download updates from any computer on the network, not limited to a specific site or subnet.

upvoted 1 times

**flavio2** 1 year, 7 months ago

Same subnet only brow.

To communicate different subnets you will need at least a Routing table

upvoted 1 times

**ExamTopics1_EIS** 1 year, 9 months ago

Selected Answer: A

Never specified any changes. Default is used. Same subnet only. 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 1 times

**Topupjay** 1 year, 10 months ago

How to Enable Delivery Optimization in Windows 10 or 11?
Delivery Optimization is enabled in all Windows 10 (build 1511 and newer) and Windows 11 versions. By default, it is allowed to get files from the computers in the current local network (LAN) only.

Reference link: https://woshub.com/using-windows-update-delivery-optimization/

upvoted 1 times

**Meebler** 2 years ago

C,

By default, Delivery Optimization is configured to download updates from other devices on the local network, as well as from Microsoft servers. This means that Computer1 will download updates from other computers in SubnetA, as well as from Microsoft servers. It will not download updates from computers in other sites or subnets.

Therefore, the correct answer is C: the computers in SubnetA only.

upvoted 1 times

**JimmyC** 2 years, 1 month ago

Selected Answer: A

In my opinion, you would expect a site to be a location which shares an external IP, and where the subnets are typically able to inter-communicate freely. By that logic, and the rules of the default LAN Mode which are referenced in other comments here - the answer would be A.

upvoted 2 times

**DDHP7** 2 years, 1 month ago

The answer is C it's LAN only not domain

upvoted 1 times

**raduM** 2 years, 1 month ago

not enough information what kind of question is this?

upvoted 1 times

**snoopie104** 2 years, 2 months ago

Selected Answer: C

I think C is the right answer

upvoted 1 times

**Alejack** 2 years, 6 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 2 times

**MR_Eliot** 2 years, 8 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** 3 years ago

A. the computers in Site1 only.

upvoted 1 times

**Ka1Nn** 3 years, 4 months 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** 3 years ago

So ; A. the computers in Site1 only ?

upvoted 1 times

**forummj** 3 years, 5 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

Question #28 *Topic 2*

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.

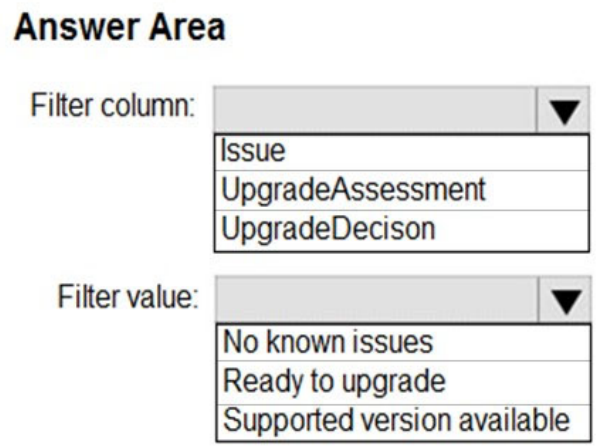
From Upgrade Readiness, you open a table view of the applications.

You need to filter the view to show only applications that can run successfully on Windows 10.

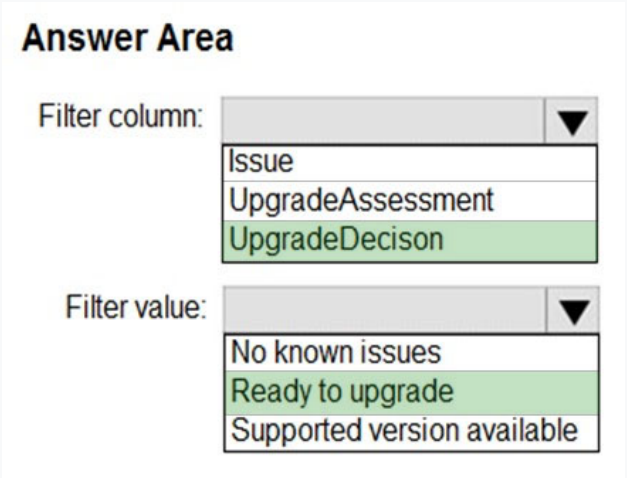
How should you configure the filter in Upgrade Readiness? To answer, select the appropriate options in the answer area.

NOTE: Each correct selection is worth one point.

Hot Area:




**Suggested 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 3 years, 3 months ago

can't believe this is a question, how irrelevant.

upvoted 12 times

**Perycles** Highly Voted 3 years, 7 months ago

correct answer. Another good link : https://www.anoopcnair.com/windows-10-upgrade-readiness/

upvoted 7 times

**Cristyy** Most Recent 1 year, 8 months ago

Why ready to upgrade and not supported version available ?

upvoted 1 times

**RodrigoT** 2 years, 9 months 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** 2 years, 3 months ago

Also it's deprecated

upvoted 1 times

**Timmi** 3 years, 11 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 |

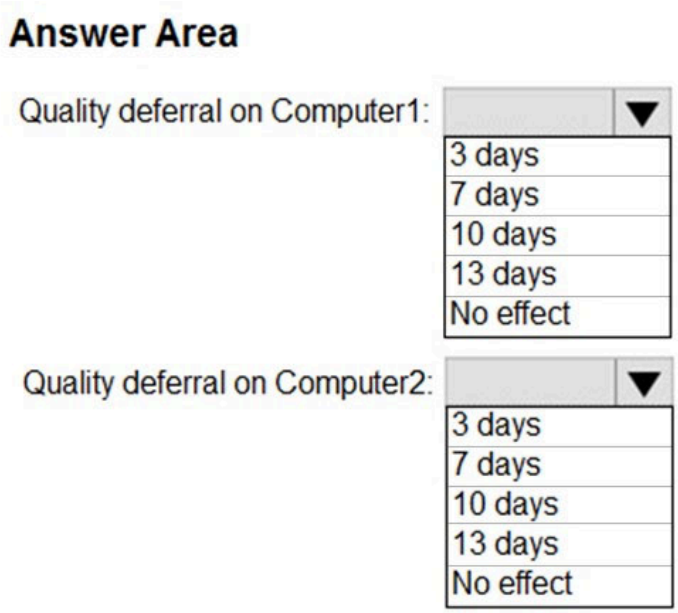
You assign the update rings as shown in the following table.

| Name | Include | Exclude |
|---|---|---|
| Ring1 | Group1 | Group2 |
| Ring2 | Group2 | Group1 |

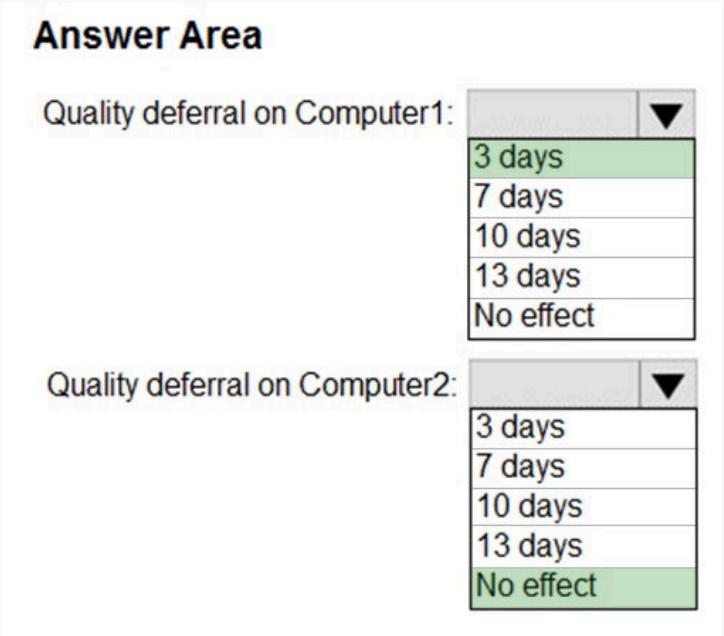
What is the effect of the configurations on Computer1 and Computer2? To answer, select the appropriate options in the answer area.

NOTE: Each correct selection is worth one point.

Hot Area:




**Suggested 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 4 years, 9 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 74 times

**mikl** 3 years ago
Thanks for clarifying!
upvoted 1 times

**RodrigoT** 2 years, 8 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 4 times

**nolancl** Highly Voted 5 years, 3 months 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** 5 years, 1 month ago
True, Even through the basic group permissions.
upvoted 1 times

**steven1** 4 years, 10 months ago
That's not how policies work, one always take precedence over the other.
upvoted 3 times

**DJM** 4 years, 1 month ago
I tested this myself in a lab, this is the correct answer.
upvoted 8 times

**Johan99** 4 years, 1 month ago
So the the given answer is correct?
upvoted 1 times

**DJM** 4 years, 1 month ago
No, I meant nolancl's comment is correct, the answer is:

Computer 1: 3 Days
Computer 2: No Effect
upvoted 16 times

**Amir1909** Most Recent 1 year ago
Correct
upvoted 1 times

**jt2214** 1 year, 10 months ago
this was a good one.
upvoted 1 times

**Altheus** 2 years, 3 months ago

3 Days and no effect.

Exclude always beats include.

upvoted 3 times

**moobdoob** 2 years, 11 months ago

Comp 1 - 3 Days

Comp 2 - No Effect

upvoted 5 times

**handsofthelp** 3 years, 1 month 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** 2 years, 8 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 2 times

**tf444** 3 years, 2 months 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** 2 years, 8 months ago

But Ring1 applies in Group1(include) and Group2(exclude). So, if exclusion overrides inclusion then Computer2 is not in any ring.

upvoted 2 times

**Ouianonymous** 3 years, 7 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** 2 years, 8 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 years, 5 months 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 years, 5 months 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** 3 years, 7 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 years, 6 months ago

This ^.

I had to look over it several times, to get it and come to the same conclusion.

upvoted 1 times

**Koenvld** 3 years, 9 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** 4 years, 1 month 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** 4 years, 2 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** 4 years, 4 months 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** 4 years, 4 months 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** 4 years, 5 months ago

Intune will check Exclude first, then Include. So answer will be 3 and 10.

upvoted 1 times

**DJM** 4 years, 1 month ago

I tested it, it is 3 days / No Effect

upvoted 3 times

**gigimail3332** 4 years, 8 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

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

**Suggested 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

*Community vote distribution*
C (100%)

**h3nk13** Highly Voted 4 years, 10 months ago
MDT can be used to inplace upgrade, but if would be a lot more work. So provisioning package is best.
upvoted 16 times

**Amir1909** Most Recent 11 months, 4 weeks ago
Correct
upvoted 1 times

**Mage10** 2 years, 3 months ago
Selected Answer: C
C since all users apps will be retained
upvoted 1 times

**MR_Eliot** 2 years, 8 months ago
Selected Answer: C
C seems to be right.
upvoted 1 times

**b3arb0yb1m** 3 years ago
C. a Windows Configuration Designer provisioning package
upvoted 3 times

**justabasicuser** 3 years, 5 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** 3 years, 7 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 3 times

**RodrigoT** 2 years, 9 months ago

MDT would not retain applications installed by the users. Answer is C.

upvoted 1 times

**Nisaj** 3 years, 10 months ago

if this answer is correct, can we use provisioning package to upgrade windows edition?

upvoted 1 times

**vinnyct** 4 years ago

It's C

upvoted 3 times

**goyelVishal** 4 years, 8 months ago

Why not Autopilot?

upvoted 1 times

**Perycles** 3 years, 7 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 4 times

**PrimeSki** 4 years, 5 months ago

Autopilot on a device would wipe current apps the user wants to retain.

upvoted 11 times

**mikl** 3 years 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

**Suggested 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

*Community vote distribution*
B (100%)

**Perycles** Highly Voted 3 years, 7 months ago
10 by default with the availability to defer to 365 days max by GPO (windows update for business GPo).
upvoted 6 times

**vinnyct** Highly Voted 4 years 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

**jt2214** Most Recent 1 year, 11 months ago
easy peasy. I wish they were all this way.
upvoted 2 times

**mikl** 3 years ago
Selected Answer: B
B. 10 is correct.

Previous it was 30 days.
upvoted 4 times

**Merma** 3 years, 8 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*

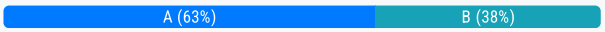
Note: This question is part of a series of questions that present the same scenario. Each question in the series contains a unique solution that might meet the stated goals. Some question sets might have more than one correct solution, while others might not have a correct solution.
After you answer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

**Suggested 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

*Community vote distribution*




**Santosh4u** Highly Voted 4 years, 11 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** 4 years, 4 months 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** 3 years, 5 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** Highly Voted 2 years, 10 months ago
Selected Answer: A
Whilst this method is quite extreme, it does fulfill its purpose.
upvoted 5 times

**Meebler** Most Recent 2 years ago
A,

This solution meets the goal of preventing video drivers from being updated automatically by using Windows Update. By enabling the "Do not include drivers with Windows Updates" setting in a Group Policy object (GPO), you can prevent drivers from being included in Windows Updates that are installed on the computers in the research department. This will prevent the video drivers from being updated automatically on these computers.
upvoted 1 times

**lykeP** 2 years, 11 months 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** 2 years, 11 months 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 16 times

**TonySuccess** 2 years, 3 months ago
Exactly, forget all logic. This is an MS Exam and they love to f with your head.
upvoted 5 times

**mikl** 3 years 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** 3 years, 2 months ago
Yes, enabling the policy result:
Enable this policy to not include drivers with Windows quality updates.
upvoted 1 times

**tf444** 3 years, 3 months ago
Lol, the reference link is so unrelated to the question.
upvoted 1 times

**Sironin** 3 years, 5 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** 3 years, 5 months ago
The question is just asking if it meets the goal. Not if it's the best practice
upvoted 1 times

**Perycles** 3 years, 7 months ago
Comparing with other previous questions for this scenario, this is the best answer. SO answer is correct.
upvoted 3 times

**ExamStudy101** 3 years, 5 months ago
"Some question sets might have more than one correct solution, while others might not have a correct solution."
upvoted 1 times

**GohanF2** 3 years, 8 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** 4 years ago
It's Yes

http://woshub.com/how-to-turn-off-automatic-driver-updates-in-windows-10/
upvoted 1 times

**SaiVR** 4 years, 6 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** 4 years, 8 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.

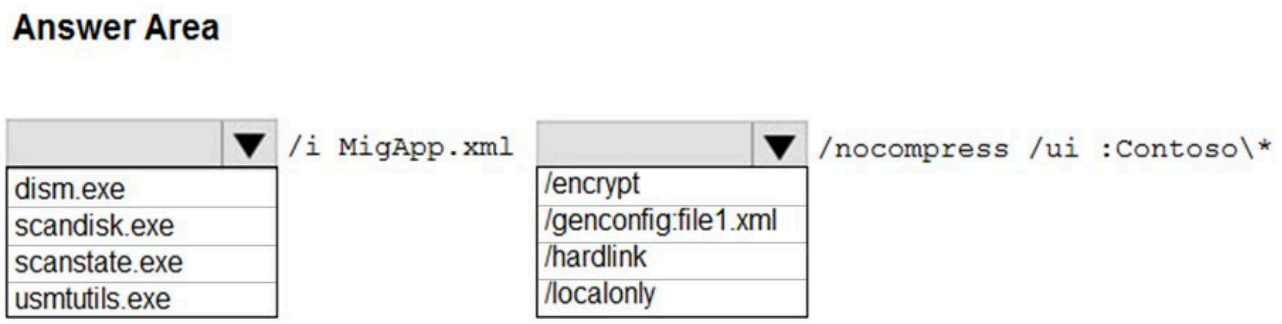
You plan to refresh the operating system of the computers to Windows 10.

You need to retain the personalization settings to applications before you refresh the computers. The solution must minimize network bandwidth and network storage space.

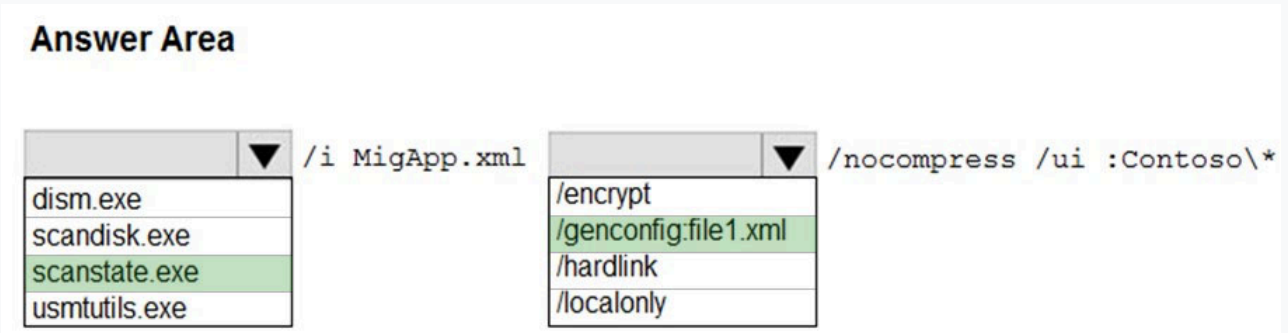
Which command should you run on the computers? To answer, select the appropriate options in the answer area.

NOTE: Each correct selection is worth one point.

Hot Area:




**Suggested 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 5 years, 4 months ago

I would choose "Hardlink"

upvoted 25 times

**PESK** 5 years, 2 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** 4 years, 12 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** 3 years, 10 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** 3 years, 7 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 3 years, 7 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 13 times

**RodrigoT** 2 years, 9 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 6 times

**dlast** Most Recent 1 year, 7 months ago
/Genconfig parameter doens't work together with /ui see https://learn.microsoft.com/en-us/windows/deployment/usmt/usmt-scanstate-syntax#incompatible-command-line-options

Should be /hardlink
upvoted 1 times

**rajpatel007** 2 years, 8 months ago
2nd answer is incorrect
upvoted 1 times

**rajpatel007** 2 years, 8 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** 3 years, 3 months 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** 3 years, 3 months 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** 3 years, 7 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** 3 years, 7 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** 3 years, 8 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** 3 years, 8 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** 3 years, 9 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** 3 years, 10 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** 3 years, 9 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** 3 years, 10 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** 3 years, 10 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** 3 years, 12 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** 3 years, 10 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** 4 years, 2 months ago

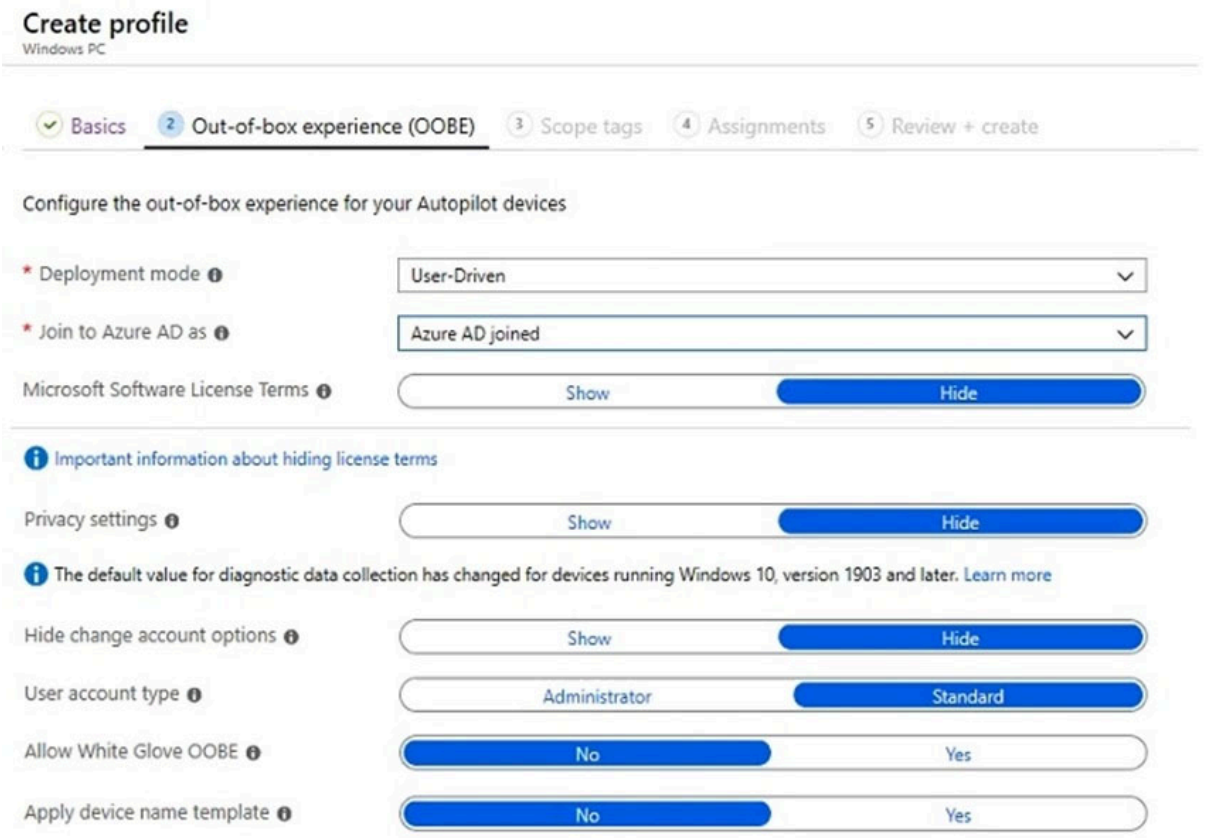
scanstate.exe, hardlink. https://docs.microsoft.com/en-us/windows/deployment/usmt/usmt-hard-link-migration-store A hard-link migration store enables you to perform an in-place migration where all user state is maintained on the computer while the old operating system is removed and the new operating 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

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:

## Answer Area

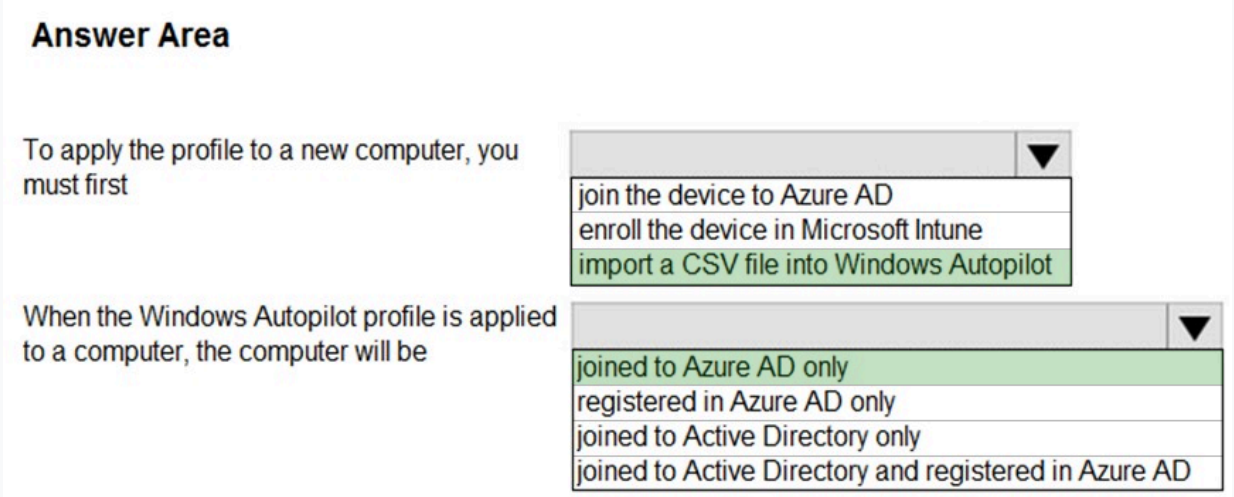
To apply the profile to a new computer, you must first

- join the device to Azure AD
- enroll the device in Microsoft Intune
- import a CSV file into Windows Autopilot

When the Windows Autopilot profile is applied to a computer, the computer will be

- joined to Azure AD only
- registered in Azure AD only
- joined to Active Directory only
- joined to Active Directory and registered in Azure AD

**Suggested 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 3 years, 8 months ago
I would lean towards "CSV" and Azure Ad Joined Only.
upvoted 62 times

**larry_cse20** 3 years, 8 months ago
me too,
upvoted 6 times

**Wilf32** 3 years, 8 months ago
I also agree with this.
upvoted 6 times

**mikl** 3 years ago
I agree.
upvoted 1 times

**Solaris2002** 2 years, 11 months 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** 2 years, 9 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 5 times

**MitchF** 2 years, 5 months 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 3 years, 8 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 10 times

**Mujja** 3 years, 6 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** 3 years, 7 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

**raduM** 2 years, 2 months ago

on autopilot the device is always joind
upvoted 1 times

**Amir1909** Most Recent 11 months, 4 weeks ago

Correct
upvoted 1 times

**jt2214** 1 year, 11 months ago

this is correct. This is how we do it in our organization. Import the hash in intune and join it to Azure AD.
upvoted 1 times

**okkies** 1 year, 11 months ago

as administrator of an hybrid enviorment with autopilot setup.
i can confirm the answers are correct.

the devices are not added to local AD
upvoted 1 times

**Nen0** 3 years, 1 month 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** 3 years, 2 months 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** 2 years, 10 months 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** 3 years, 3 months 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** 3 years, 5 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** 3 years, 7 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** 3 years, 7 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** 3 years, 6 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** 3 years, 7 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** 2 years, 11 months 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** 2 years, 6 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** 3 years, 7 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** 3 years, 7 months ago
totaly wrong,
upvoted 2 times

**densyo** 3 years, 7 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

Question #35 *Topic 2*

DRAG DROP -

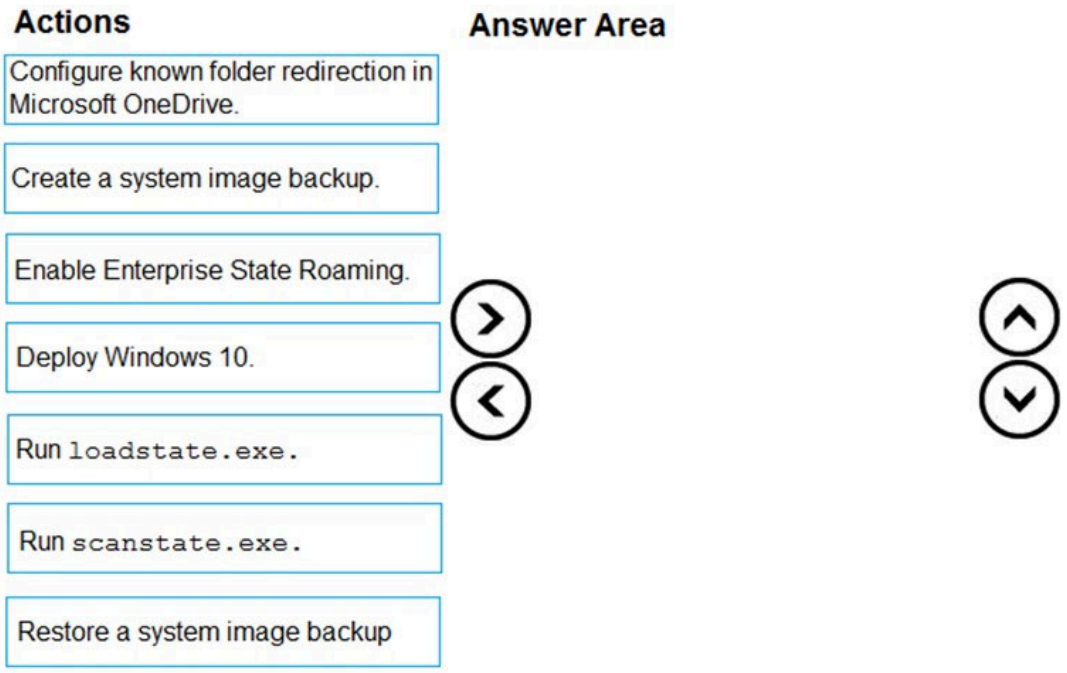
You have 100 computers that run Windows 8.1.

You plan to deploy Windows 10 to the computers by performing a wipe and load installation.

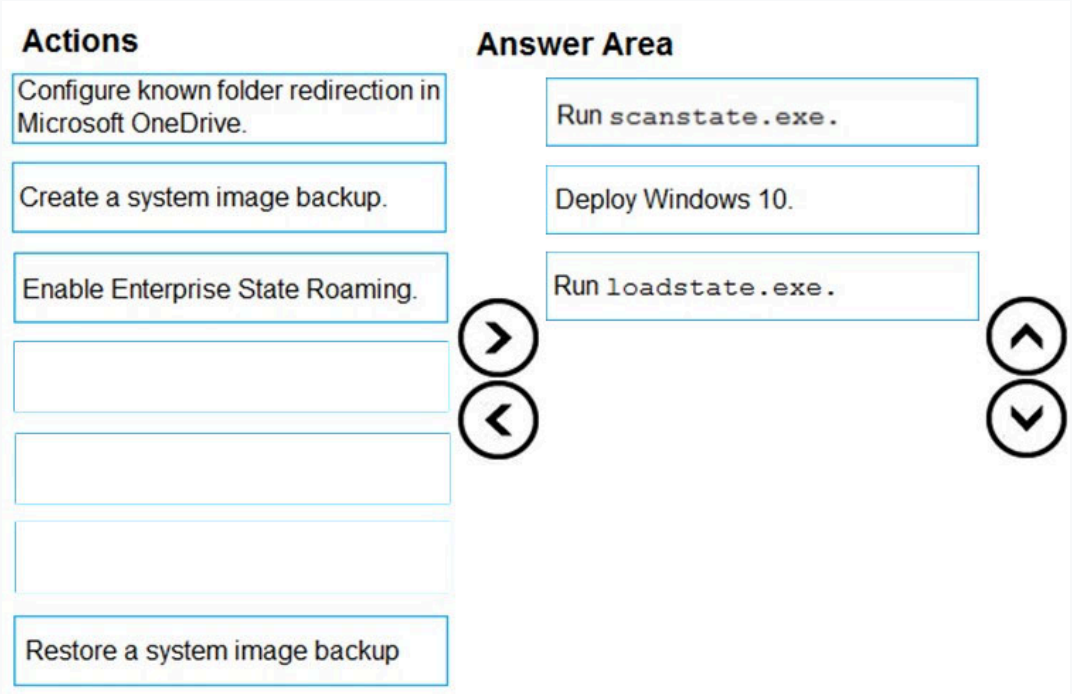
You need to recommend a method to retain the user settings and the user data.

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:




**Suggested 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 3 years, 7 months ago
gotta love a straightforward question
upvoted 27 times

**Merma** Highly Voted 3 years, 8 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 7 times

**raduM** Most Recent 2 years, 5 months ago
correct
upvoted 1 times

**BAbdalla** 3 years, 2 months ago
It seems good
upvoted 1 times

**Perycles** 3 years, 7 months ago
answers are correct.
upvoted 6 times

**goape** 4 years, 4 months 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 6 times

**goape** 4 years, 4 months ago
Actually, nevermind. Of course it's not avail in win 8.1
upvoted 9 times

**Mujja** 3 years, 6 months ago
It was a nice idea though.
upvoted 3 times

**Jvp21** 3 years, 7 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 2 times

**mikl** 3 years ago

I was thinking the exact same - but you got the point before me :)

upvoted 1 times

Question #36 *Topic 2*

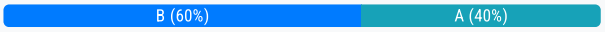
Note: This question is part of a series of questions that present the same scenario. Each question in the series contains a unique solution that might meet the stated goals. Some question sets might have more than one correct solution, while others might not have a correct solution.
After you answer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

**Suggested 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

*Community vote distribution*




**Jonnaz** Highly Voted 3 years, 6 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 16 times

**MostWare_certificering** Most Recent 1 year, 9 months ago
Yes, performing a local Windows Autopilot Reset will reset the device to its original state and the next user, User2, will be prompted to select the language setting and agree to the license agreement during the initial setup process. This will provide a fresh start for the new user and ensure that the device is properly configured for their use.

upvoted 1 times

**Meebler** 2 years ago

B,

This solution does not meet the goal. Performing a local Windows Autopilot Reset will reset the device to its original factory settings, which will remove all user data, applications, and settings, including the language and license agreement selections. This will require User2 to go through the initial setup process again, including selecting the language and agreeing to the license agreement. To meet the goal of ensuring that User2 is prompted to select the language setting and agree to the license agreement, you should use the Windows Autopilot deployment process to re-enroll the device under User2's account. This will retain the existing configuration and settings on the device, while prompting User2 to select the language setting and agree to the license agreement during the initial setup process.

upvoted 1 times

**asturmark** 2 years, 3 months 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** 2 years, 3 months 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 years, 5 months 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** 2 years, 6 months 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 4 times

**MR_Eliot** 2 years, 8 months ago

**Selected Answer: B**

When using Local AutoPilot Reset, after reset you will be presented with the login screen (no OOBE).

upvoted 3 times

**Skorne** 3 years, 1 month 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** 3 years, 1 month 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** 2 years, 9 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 2 times

**daonga** 3 years, 4 months 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** 2 years, 9 months ago
Did it ask also to select the language? No. So, B.
upvoted 4 times

**Angarali** 3 years, 5 months ago
Answer is No
upvoted 1 times

**justabasicuser** 3 years, 5 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 4 times

**jibutoms** 3 years, 6 months ago
"local" Windows Autopilot Reset prompts me to choose "Option B"
upvoted 1 times

**Perycles** 3 years, 7 months ago
after testing, autolpilot reset is the good way , so answer is A:YES
upvoted 2 times

**Perycles** 3 years, 7 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** 3 years, 7 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** 3 years, 7 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** 3 years, 8 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

**Suggested 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

*Community vote distribution*
B (100%)

**Merma** Highly Voted 3 years, 7 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

**ExamTopics1_EIS** Most Recent 1 year, 9 months ago
Wow, they actually had EMAIL the ppkg in the answer. You would think that they would use OneDrive and maybe have the share link emailed instead?
upvoted 1 times

**moobdoob** 2 years, 11 months ago
Selected Answer: B
Correct answer: B
upvoted 3 times

**b3arb0yb1m** 3 years ago
B. Create a provisioning package (.ppkg) file and email the file to the user
upvoted 2 times

**Perycles** 3 years, 7 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

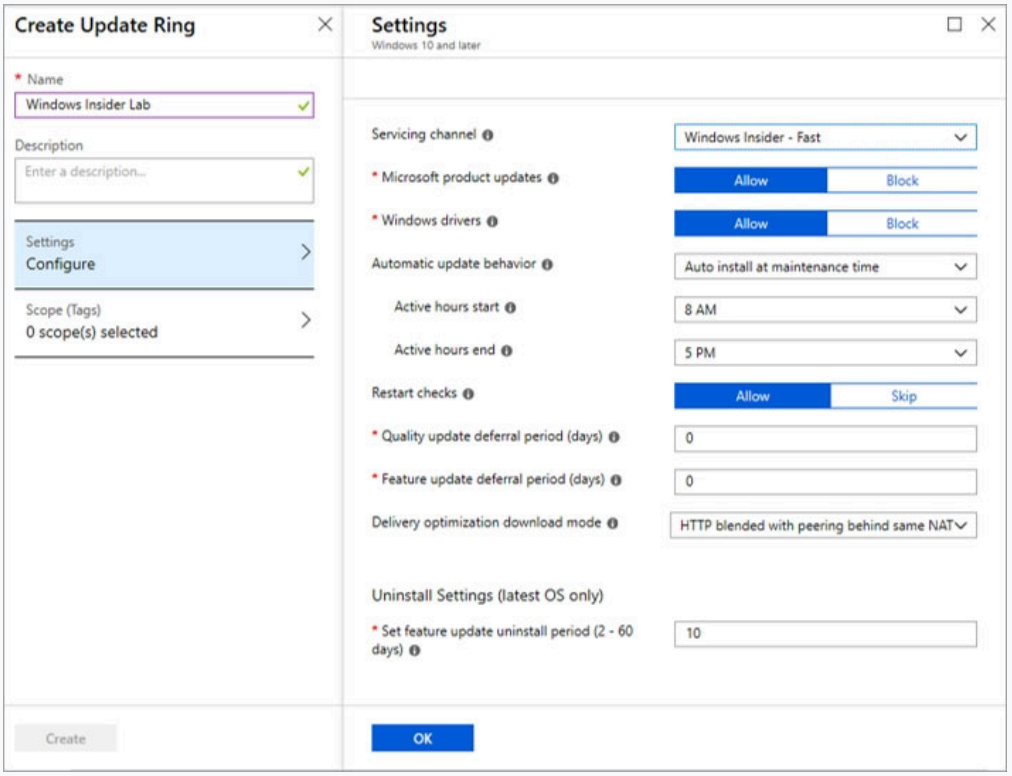
B. an app configuration policy

C. a custom device configuration profile

D. a Windows 10 update ring

E. a device restrictions device configuration profile

**Suggested 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

**3dk1** 1 year, 7 months ago
The answer looks good to me.

I can definitely say D is correct, C also makes sense. Keep in mind that you are not creating a restriction, but rather editing the option out.
upvoted 1 times

**Cristyy** 1 year, 8 months ago
I do not understand... Why C. and D. and not A. and E. ?

upvoted 1 times

**Natsumiko** 1 year, 7 months ago

I checked A and E and none of them contain settings to configure Windows Insider update settings. App policies are also irrelevant here, so the given answer must be correct.

upvoted 1 times

**JimmyC** 2 years, 1 month ago

I'm not sure what the custom device configuration profile would be for... but I did go through the options under the Device Restrictions template, and I don't see anything that would be relevant here (unless you want to remove access to all update options in the Settings app).

upvoted 2 times

**bitjos** 2 years ago

custom OMA-URI

https://learn.microsoft.com/en-us/windows/client-management/mdm/policy-csp-system#system-allowbuildpreview

upvoted 3 times

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

**Suggested 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

*Community vote distribution*
C (100%)

**Anthony_2770** Highly Voted 3 years, 11 months ago
Answer is correct. Refer to the supplied link.
upvoted 22 times

**Dnyc** 1 year, 10 months ago
Question/answer is defunct now, see adamc157 post. You no longer have to create and assign the config manager client, but you do still have to specify the parameters.
upvoted 1 times

**adamc157** Most Recent 2 years, 1 month ago
You no longer need to create and assign an Intune app to install the Configuration Manager client. The Intune enrollment policy automatically installs the Configuration Manager client as a first-party app. The device gets the client content from the Configuration Manager cloud management gateway (CMG), so you don't need to provide and manage the client content in Intune. For more information, see How to enroll with Autopilot.

https://learn.microsoft.com/en-us/mem/configmgr/comanage/how-to-prepare-Win10
upvoted 3 times

**MR_Eliot** 2 years, 8 months ago
Selected Answer: C
C => Correct!
upvoted 1 times

**ercluff** 3 years, 4 months 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** 2 years, 9 months 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** 2 years, 9 months 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** 3 years, 7 months ago

yes it's correct .Configuration manager client program has to be add into intune and then deploy and devices.

upvoted 4 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

**Suggested 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 4 years 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 12 times

**RodrigoT** 2 years, 9 months 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 3 years ago
C. a device collection in Endpoint Configuration Manager
upvoted 2 times

**Perycles** 3 years, 7 months ago
C of course, when configuring "intune pilot" under SCCM, we have to specific a collection.
upvoted 1 times

**Anthony_2770** 3 years, 11 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** 3 years, 11 months ago

Configuration Manager device collection

upvoted 8 times

Question #41 *Topic 2*

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.

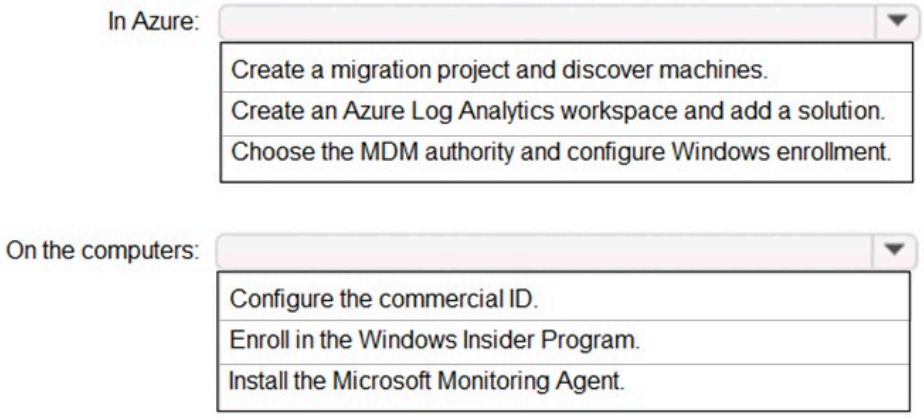
You need to generate an Upgrade Readiness report for the computers.

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

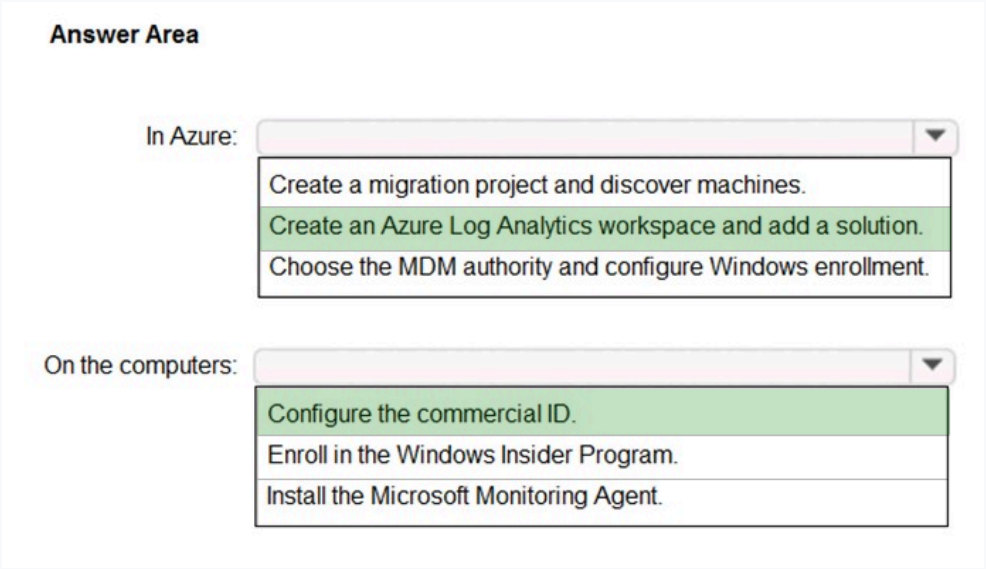
NOTE: Each correct selection is worth one point.

Hot Area:

**Answer Area**




**Suggested Answer:**




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 3 years, 8 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 29 times

**Moorebid** 3 years, 7 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** 3 years ago

I agree.

upvoted 1 times

**RodrigoT** 2 years, 8 months 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 3 years, 7 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 16 times

**Jimbob77** 3 years, 7 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** 2 years, 8 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 3 times

**Dedutch** Most Recent 2 years, 5 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** 2 years, 8 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 3 times

**lykeP** 2 years, 11 months 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** 3 years, 1 month 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** 3 years ago
You configure commercial ID on configuration manager and not on computers.
upvoted 2 times

**RodrigoT** 2 years, 9 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** 2 years, 8 months ago
The answer provided is correct:
https://docs.microsoft.com/en-us/windows/deployment/update/update-compliance-using
upvoted 2 times

**Sizz** 3 years, 4 months 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 4 times

**Perycles** 3 years, 7 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** 3 years, 7 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** 3 years ago
The best explanation I can see here
upvoted 1 times

**MikeMatt2020** 3 years, 7 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** 3 years, 7 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 7 times

**Anna_Peters** 3 years, 8 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

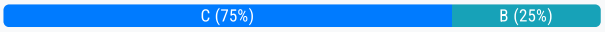
B. The Microsoft SharePoint Migration Tool

C. Enterprise State Roaming

D. Roaming user profiles

**Suggested 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

*Community vote distribution*




**Justin0020** Highly Voted 4 years, 3 months ago
C is correct. D is not correct, because Roaming profiles does not work with Azure-AD only.
upvoted 15 times

**AliNadheer** Most Recent 1 year, 10 months ago
Selected Answer: C
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. For devices that use on-premises Active Directory, the IT admin must Configure hybrid Azure Active Directory joined devices.
reference: https://learn.microsoft.com/en-us/azure/active-directory/devices/enterprise-state-roaming-enable
upvoted 1 times

**okkies** 1 year, 11 months ago
Selected Answer: C
C is correct. D is not correct, because Roaming profiles does not work with Azure-AD only.
upvoted 1 times

**raduM** 2 years, 4 months ago
c is correct
upvoted 1 times

**ZzeezZ** 2 years, 5 months ago
Selected Answer: B
No, only applies to packages on removable media
upvoted 1 times

**MR_Eliot** 2 years, 8 months ago
Selected Answer: C
C is Correct!
upvoted 1 times

**mikl** 3 years ago
C. Enterprise State Roaming is correct!
upvoted 1 times

**b3arb0yb1m** 3 years ago
C. Enterprise State Roaming
upvoted 1 times

**Harrysa** 3 years, 8 months ago

X-man - I guess because the setup is primarily Azure AD enterprise state roaming is a perfect fit

upvoted 1 times

**Tomtom11** 3 years, 8 months ago

https://docs.microsoft.com/en-us/azure/active-directory/devices/enterprise-state-roaming-faqs

upvoted 2 times

**MD4439** 3 years, 9 months ago

c is correct

upvoted 1 times

**X_man** 4 years, 4 months 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

**Suggested 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

*Community vote distribution*
B (100%)

**mlleremallqui** Highly Voted 4 years, 4 months 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

**jojolabubu** Highly Voted 4 years, 3 months 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 20 times

**wafa2022** Most Recent 1 year, 5 months ago
B. No

The solution provided does not meet the goal. The correct steps to apply a provisioning package in Windows 10 are as follows:

Copy the provisioning package (Package1) to a location accessible by Computer1 (e.g., a shared folder or a removable storage device).
On Computer1, navigate to the folder where Package1 is located (in this case, C:\Folder1).
Double-click on Package1 to initiate the provisioning process.
Follow the prompts and provide any necessary credentials or permissions to complete the provisioning.
Using the Settings app and selecting "Access work or school" and "Add or remove a provisioning package" does not directly apply the package to the computer. It opens a menu to manage installed provisioning packages but does not initiate the provisioning process itself.
upvoted 1 times

**Kock** 1 year, 6 months ago
Um pacote de provisionamento contém configurações ou configurações específicas e recursos que podem ser fornecidos por meio de "mídia removível" ou "baixados para o dispositivo".
https://learn.microsoft.com/es-es/windows/configuration/provisioning-packages/provisioning-how-it-works
upvoted 1 times

**JePe** 1 year, 9 months ago

I have inserted the question in CHATGPT and he replied:
Yes, the solution mentioned will meet the goal of applying Package1 to Computer1.

By selecting "Access work or school" from the Settings app and then choosing "Add or remove a provisioning package," you can easily apply the saved Package1 to the computer. The provisioning package will contain instructions for configuring settings, installing apps, and other tasks to prepare the computer for use in an organization.

Note that before applying the provisioning package, you should ensure that it is compatible with the Windows 10 version running on Computer1 and that any required dependencies are already installed.
upvoted 3 times

**Titus42** 1 year, 10 months ago
Guys you do realize its completely possible to have a folder on a USB drive called C:\Folder1 right?
upvoted 1 times

**Brandon_Marlin** 1 year, 10 months ago
Selected Answer: B
Chiming in also to say "No" since the folder is on the C:/ and not a USB drive, the answer to this question is no
upvoted 1 times

**AliNadheer** 1 year, 10 months ago
No, from "access work or school account>add or remove provisioning package" you will only be able to add provisioning packages from removable media.
so i would navigate to the path and install it from there
upvoted 1 times

**Meebler** 1 year, 11 months ago
B. No.

The steps you described in the solution for applying a provisioning package to a Windows 10 computer is incorrect. To apply a provisioning package to a Windows 10 computer, you can use the Windows Configuration Designer tool or the DISM command-line tool.
You can use the Windows Configuration Designer to create or modify provisioning packages, and then you can use the DISM command-line tool to apply the provisioning package to a Windows 10 computer.
Using the command line you can use the following command :
DISM /online /apply-provisioningPackage /packagepath:c:\folder1\package1.ppkg

It is important to note that provisioning packages are used to configure Windows 10 devices in a corporate environment, usually for mass deployment and it's not a feature that is commonly used on personal computers.
upvoted 2 times

**aleexoo** 1 year, 12 months ago
Selected Answer: B
It's B (False), this option only support Provisioning package from a Removal Media: https://learn.microsoft.com/en-us/windows/configuration/provisioning-packages/provisioning-apply-package#windows-settings
upvoted 2 times

**AyoR32** 2 years ago
B is for me the good answer to this question, but what is the official version for Microsoft during a certification exam?
upvoted 1 times

**mikekrt** 2 years, 1 month ago
Selected Answer: B
This method to add a provisioning package is valid, however, you will not be able to select a provisioning package from the c:\folder1 location, ONLY from a USB drive or an SD Card!
upvoted 2 times

**cbjorn8931** 2 years, 1 month ago
It is A (Yes): Stop trying to confuse people... A is one way to add a provisioning package is through Access work/school. It was even demonstrated through CBT nuggets training.
upvoted 1 times

**cbjorn8931** 2 years, 1 month ago
Insert the USB drive, then navigate to Settings > Accounts > Access work or school > Add or remove a provisioning package > Add a package.

upvoted 1 times

**rendog** 2 years ago

No it is B since the question clearly states that "you save a provisioning package named Package1 to a folder named C:\Folder1," meaning this ppkg is saved to the C drive and not a USB!

While it is possible to change the system drive letter to something other than C (unadvisable to do so), I'm sure Microsoft is implying the folder is located on the system drive, thus making the method mentioned in the question invalid.

upvoted 1 times

**geggio** 2 years, 3 months ago

y

https://learn.microsoft.com/en-us/windows/configuration/provisioning-packages/provisioning-apply-package

upvoted 1 times

**Russ_A7x** 2 years, 5 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 4 times

**bounce_united** 2 years, 6 months ago

**Selected Answer: B**

In settings, needs removable media

upvoted 4 times

**MR_Eliot** 2 years, 8 months ago

**Selected Answer: B**

Answer is B. You only can select *.ppkg files from removeable-devices.

upvoted 6 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

**Suggested 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

*Community vote distribution*
A (100%)

**vnod007** Highly Voted 4 years, 1 month ago
Double clicking should work:
https://youtu.be/UU6l7-CMSRc
upvoted 23 times

**RodrigoT** 2 years, 9 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 4 years, 4 months 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

**Darkfire** Most Recent 1 year, 3 months ago
Selected Answer: A
Should be A

Apply Directly
https://learn.microsoft.com/en-us/windows/configuration/provisioning-packages/provisioning-apply-package
upvoted 1 times

**aleexoo** 1 year, 12 months ago
Selected Answer: A
It's A (True), see documentation https://learn.microsoft.com/en-us/windows/configuration/provisioning-packages/provisioning-apply-package#apply-directly
upvoted 1 times

**AyoR32** 2 years ago

A works but what is the official version for Microsoft during a certification exam?

upvoted 1 times

**cbjorn8931** 2 years, 1 month ago

Yes, this is another way to apply the provisioning package via email and double-click on the file.

upvoted 1 times

**zdiddy** 2 years, 5 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 years, 5 months ago

Selected Answer: A

Yes, it will work

upvoted 2 times

**MR_Eliot** 2 years, 8 months ago

Selected Answer: A

A is correct.

upvoted 2 times

**Angarali** 2 years, 8 months ago

Selected Answer: A

YES YES YES

upvoted 2 times

**moobdoob** 2 years, 11 months ago

Double clicking works, answer is YES.

upvoted 5 times

**IykeP** 2 years, 11 months ago

Selected Answer: A

A is the correct Answer, double clicking will work.

upvoted 3 times

**Ferrix** 3 years ago

Tested in Lab, doble click is working! The Answer is YES

upvoted 2 times

**TAndrasSF** 3 years 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** 3 years, 1 month ago

Yes . mouse click or add in account from medium

upvoted 1 times

**BAbdalla** 3 years, 2 months ago

Double click works! The Correct awnser is A.Yes

upvoted 2 times

**encxorblood** 3 years, 3 months ago

Yes. Tested.

upvoted 3 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

**Suggested 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

*Community vote distribution*
B (100%)

**jojolabubu** Highly Voted 4 years, 3 months 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 23 times

**ZzeezZ** Most Recent 2 years, 5 months ago
Selected Answer: B
Answer is No, but the explanation provided is incorrect
upvoted 1 times

**moobdoob** 2 years, 11 months ago
Answer is NO.
upvoted 2 times

**Merma** 3 years, 7 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.

**Suggested 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 ıâ€" 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

*Community vote distribution*
D (100%)

**Parzival** Highly Voted 5 years, 1 month 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 21 times

**Perycles** Highly Voted 3 years, 7 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 2 years, 8 months ago

Selected Answer: D

D is the correct answer

upvoted 2 times

**larteyotoo** 3 years ago

D is correct

upvoted 3 times

**mikl** 3 years ago

Selected Answer: D

Correct answer.

D. From Software updates, view the Per update ring deployment state.

upvoted 1 times

**b3arb0yb1m** 3 years ago

D. From Software updates, view the Per update ring deployment state.

upvoted 1 times

**encxorblood** 3 years, 3 months 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** 3 years, 7 months ago

A is the correct answer. I have just verified myself right now

upvoted 2 times

**AnoniMouse** 3 years, 7 months ago

Apparently I was wrong! The answer provided is correct

upvoted 7 times

**Merma** 3 years, 8 months ago

D. is correct. Another helpful link:

https://docs.microsoft.com/en-us/mem/intune/fundamentals/reports

upvoted 3 times

**AzZnLuVaBol** 3 years, 10 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** 3 years, 11 months ago

This practice questions is only 40% valid. I failed this exam earlier.

upvoted 3 times

**cankayahmet** 3 years, 11 months ago

Have you check discussions because some given answers are not correct.

upvoted 14 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

**Suggested 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

*Community vote distribution*

B (100%)

**Perycles** Highly Voted 3 years, 7 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 3 years, 8 months ago

Answer B is correct.

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

upvoted 5 times

**AnoniMouse** 3 years, 7 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 3 times

**Amir1909** Most Recent 11 months, 4 weeks ago

Correct

upvoted 1 times

**jt2214** 1 year, 10 months ago

Selected Answer: B

Although not ideal with 4GB of RAM. B is the answer.

upvoted 1 times

**MR_Eliot** 2 years, 8 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** 3 years 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** 3 years ago

B. Device3 only

upvoted 1 times

**RamazanInce** 3 years, 3 months 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** 3 years, 8 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

Question #48 *Topic 2*

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. | ○ | ○ |

**Suggested 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 3 years, 7 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 30 times

**Merma** 3 years, 7 months ago
You're correct the answer should be YYN.
upvoted 3 times

**Wilf32** 3 years, 7 months ago
I agree, if i get this question on the exam i will answer YYN
upvoted 3 times

**RodrigoT** 2 years, 9 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

**Solaris2002** 3 years, 3 months 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 8 times

**FleurJ** 3 years, 5 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 6 times

**handsofthelp** Highly Voted 3 years 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 6 times

**Raxon** Most Recent 1 year, 10 months ago
There is no in-place upgrade path from Windows 8.1 Home, Pro or Enterprise to Windows 10 Enterprise. Enterprise versions are licensed independently. That's why BOX 3 is a NO
upvoted 2 times

**N0peasaurus** 2 years, 6 months 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** 2 years, 8 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** 2 years, 8 months ago
Yes
Yes
No
upvoted 1 times

**erwiense** 2 years, 11 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** 2 years, 11 months ago
YES, YES, NO
upvoted 1 times

**MZONDERL** 2 years, 11 months 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** 2 years, 9 months ago
But the license is applied directly to User2. So, for me Y Y N.
upvoted 1 times

**lykeP** 2 years, 11 months 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

**lykeP** 2 years, 11 months 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 2 times

**IykeP** 2 years, 11 months 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** 2 years, 9 months ago

But the license is applied directly to User2. So, for me Y Y N.

upvoted 1 times

**b3arb0yb1m** 3 years ago

Yes

Yes - because there is Azure sync.

No

upvoted 2 times

**jorlloen** 3 years, 4 months 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** 3 years, 7 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** 3 years, 7 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** 3 years, 7 months ago

Answers are correct as User 2 is not in Azure

upvoted 1 times

**mikl** 3 years ago

But there are sync in place?

upvoted 1 times

**Tomtom11** 3 years, 7 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** 3 years, 7 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

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

**Suggested 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 3 years, 8 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 21 times

**Perycles** Highly Voted 3 years, 7 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** 2 years, 8 months 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 2 years, 11 months ago

Given answer is correct.

upvoted 3 times

**angelize** 3 years, 6 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 7 times

**RodrigoT** 2 years, 8 months 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

**Suggested 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.

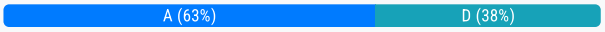
They are treated as a whole system and are, therefore, commonly ɹ€upgradedɹ€ by building and validating a new system, turning off the old device, and replacing it with the new, certified device

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

*Community vote distribution*




**BLYBOI** Highly Voted 4 years, 1 month 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 24 times

**skalolaz** 2 years, 5 months 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 4 times

**neobahamutk** Highly Voted 2 years, 5 months 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 6 times

**TonySuccess** 2 years, 4 months 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

**Deric** 2 years, 3 months 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

**Raxon** Most Recent 1 year, 10 months ago

The question asked: "Which operating systems support update rings?"
Which would be the following:
Windows 10/11 Pro.
Windows 10/11 Enterprise.
Windows 10/11 Team - for Surface Hub devices.
Windows Holographic for Business. ...
Windows 10/11 Enterprise LTSC - While LTSC is supported, the following ring controls are not supported for LTSC:

While there are ring controls are not supported for LTSC:
This is not the question that was asked.
upvoted 1 times

**Meebler** 1 year, 11 months ago
A,

Windows 10 Pro, Windows 10 Enterprise, and Windows 10 Enterprise LTSC only.

Update rings are a feature of Microsoft Intune that allows you to control the deployment of Windows updates on client computers. Update rings are only available for Windows 10 Pro, Windows 10 Enterprise, and Windows 10 Enterprise LTSC. Windows 8.1 does not support update rings. When you create an update ring, you can specify the group of devices that you want to include in the ring, and you can also specify the branch of Windows updates that you want to use (e.g. Current Branch, Current Branch for Business, Long-term Servicing Branch). This allows you to control the pace of updates and test updates before deploying them to all devices.
upvoted 2 times

**Meebler** 1 year, 11 months ago
I apologize , Windows 10 Enterprise LTSC does not support update rings.
Windows 10 LTSC (Long-Term Servicing Channel) is a specialized version of Windows 10 designed for devices that have specific long-term support needs. LTSC releases are designed to be stable, secure, and predictable, with a 10-year lifecycle. Because of this focus on stability, LTSC releases do not include many of the features and updates that are available in other versions of Windows 10, including the ability to use update rings.

So the correct answer would be:
D. Windows 10 Pro and Windows 10 Enterprise only.
upvoted 2 times

**aleexoo** 1 year, 12 months ago
Selected Answer: A
Right Answer: A
Windows 10 Enterprise LTSC is as well supported with limited features: https://docs.microsoft.com/en-us/windows/deployment/windows-autopilot/self-deploying
upvoted 1 times

**djgqil** 1 year, 9 months ago
A can't be correct as it includes 8.1
upvoted 1 times

**Graz** 2 years ago
Flawed Question

LTCS is supported, but at a limited capacity at a limited capacity. See below

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.

Old question, probably won't be on updated exam but fresh documentation says its supported, not sure if it was when the question was written.
upvoted 1 times

**Cycubxl** 2 years ago
Selected Answer: A
LTSC is also support by update ring
upvoted 1 times

**cbjorn8931** 2 years, 2 months ago

Microsoft Intune supports Windows 10 Enterprise LTSC 2019 and later. However, Windows 10 update rings device profiles don't support LTSC releases. For installing software updates, use the policy configuration service provider (CSP), Windows Server Update Services (WSUS), or Microsoft Endpoint Configuration Manager.

upvoted 1 times

**cbjorn8931** 2 years, 2 months ago

https://learn.microsoft.com/en-us/windows/whats-new/ltsc/whats-new-windows-10-2019

upvoted 1 times

**anu21** 2 years, 6 months 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** 2 years, 8 months ago

**Selected Answer: D**

D is indeed correct.

upvoted 2 times

**moobdoob** 2 years, 11 months ago

My vote is D

upvoted 2 times

**mikl** 3 years 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 4 times

**neobahamutk** 2 years, 5 months ago

Windows 10/11 Enterprise LTSC is suported too.
https://docs.microsoft.com/en-us/mem/intune/protect/windows-10-update-rings

upvoted 3 times

**b3arb0yb1m** 3 years ago

D. Windows 10 Pro and Windows 10 Enterprise only

upvoted 1 times

**Perycles** 3 years, 7 months ago

answers are correct

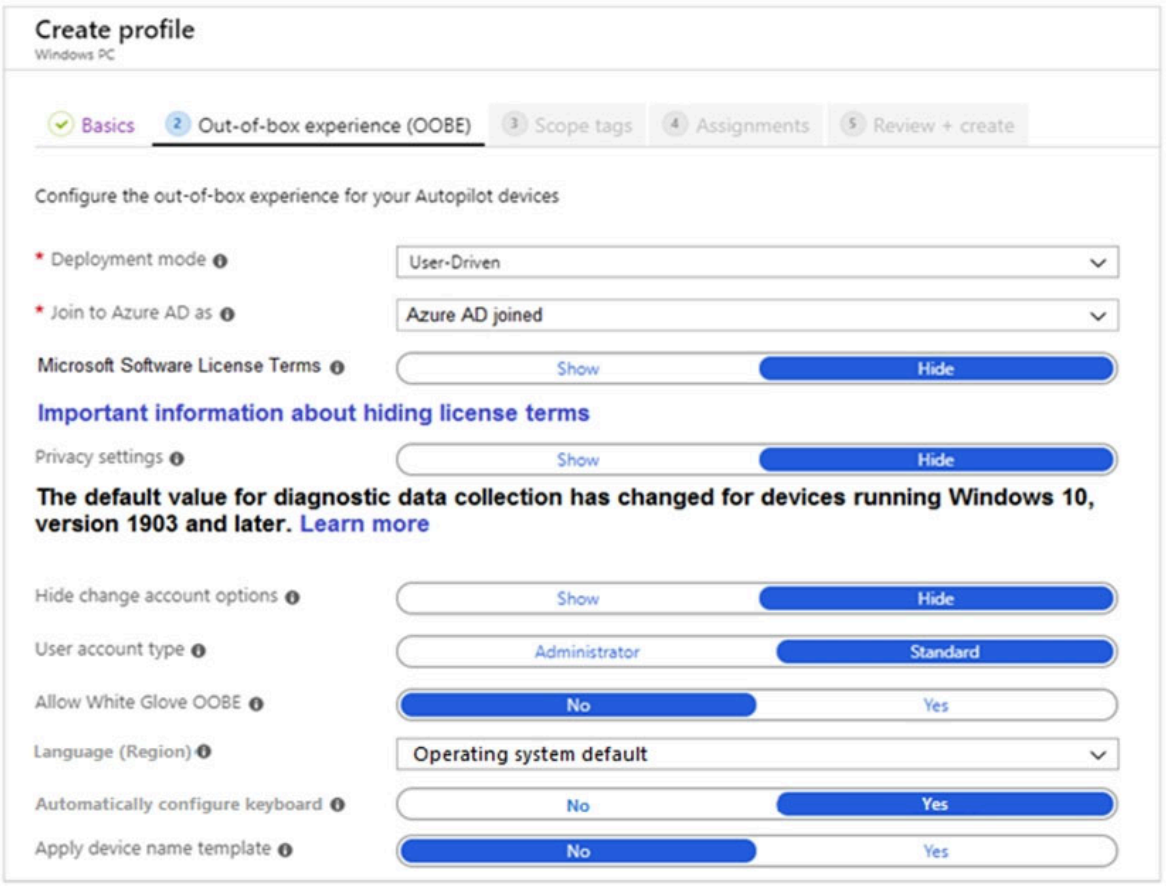
upvoted 5 times

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**

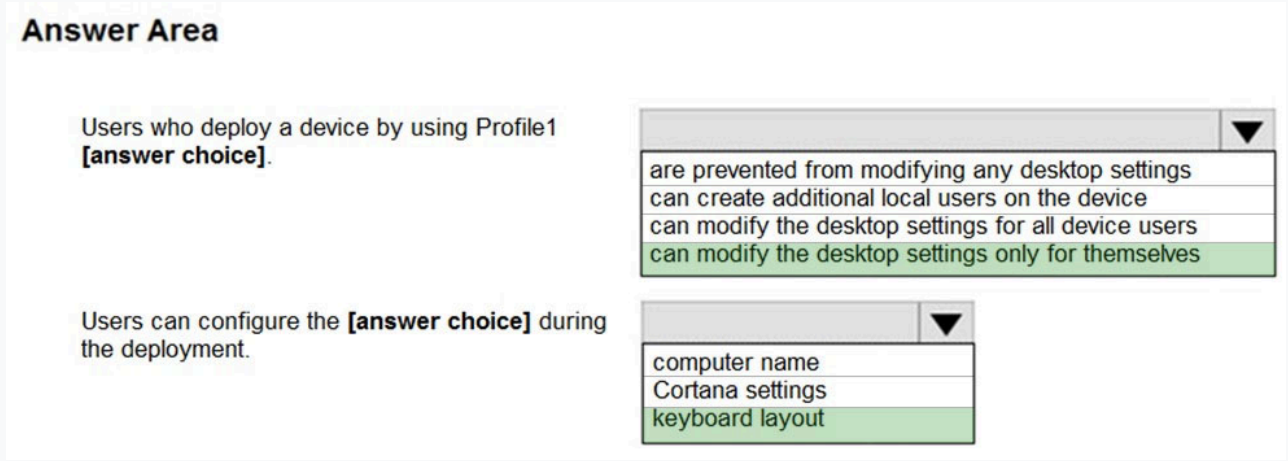
Users who deploy a device by using Profile1 **[answer choice]**.

- 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

**Suggested Answer:**




Reference:
https://www.microsoftpressstore.com/articles/article.aspx?p=2453566

**ANDREVOX** Highly Voted 3 years, 2 months 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 22 times

**mikl** 3 years ago

I totally agree.
upvoted 1 times

**[Removed]** 2 years, 9 months 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** 2 years, 9 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** 2 years, 9 months 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 2 times

**moobdoob** Highly Voted 2 years, 11 months ago

My answer will be:
1. Can modify desktop settings only for themselves.
2. Computer name
upvoted 11 times

**Angarali** 2 years, 8 months 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 6 times

**NZS** 2 years, 8 months ago

Alright, explain your reasoning. How would they change the keyboard settings if it's managed by the Autopilot profile?

upvoted 6 times

**Antimus** 2 years, 1 month ago

Well standard users can't change the computer name and there's no prompt during OOBE to set the computer name, so it gets even more complicated. Why not Cortana?

upvoted 1 times

**Darkfire** Most Recent 1 year, 3 months ago

Answer is correct.

See explination of ANDREVOX

upvoted 1 times

**[Removed]** 1 year, 12 months ago

Automatically configure keyboard*: If a Language (Region) is selected, choose Yes to skip the keyboard selection page. This option is available in all Deployment modes starting with Windows 10 version 2004.

Maybe because the language region is not selected (default) is why the keyboard layout is able to be configured by the user even though it is ticked 'yes'. Might be wrong, any thoughts?

upvoted 1 times

**AK4U_111** 2 years, 2 months ago

I have yet to encounter a situation where a user, admin or not, can name the computer in the OOBE/Setup process. Also, it'd be a good idea to test and see if a user can still add another keyboard layout when the "Automatically configure keyboard" setting is set to yes, because then it would mean that the answer for the second part of the question is indeed "keyboard layout"

upvoted 1 times

**isatemelci** 2 years, 3 months 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** 2 years, 8 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 2 times

**b3arb0yb1m** 3 years, 1 month 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 3 times

**b3arb0yb1m** 3 years, 1 month ago

Skip Cortana is on (and greyed) by default when creating a profile.

upvoted 1 times

**RodrigoT** 2 years, 9 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** 3 years, 2 months 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** 3 years, 2 months ago

Or is it because of the standard account? Someone please help me with the correct answer

upvoted 1 times

**anzer123** 3 years, 2 months ago

Should be computer name

upvoted 3 times

**mikl** 3 years 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)

**Suggested 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/

*Community vote distribution*
C (100%)

**Anthony_2770** Highly Voted 3 years, 11 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** 3 years ago
Agree!
upvoted 1 times

**Darkfire** Most Recent 1 year, 3 months ago
Selected Answer: C
C = correct

Keywords: Answer file & C. Windows System Image Manager (Windows SIM)
upvoted 1 times

**AliNadheer** 1 year, 10 months ago
Selected Answer: C
i use SIM allot to customize the answer file for my WIM. its the only correct answer here.
upvoted 1 times

**[Removed]** 2 years, 3 months ago
This was a question in my MD-100 exam which I wrote 12 days ago.
upvoted 1 times

**MR_Eliot** 2 years, 8 months ago
Selected Answer: C
C is correct.
upvoted 1 times

**cor_** 2 years, 9 months ago
Selected Answer: C
C. Windows SIM can create unattended.xml, also known as 'answer file'
upvoted 1 times

**RodrigoT** 2 years, 9 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 6 times

**FlailingLimbs** 2 years, 3 months ago
Thanks for the breakdown with reasons why the others were not the right answer.
upvoted 2 times

**moobdoob** 2 years, 11 months ago
Given answer is correct.
upvoted 2 times

**mikl** 3 years ago
**Selected Answer: C**
C. Windows System Image Manager (Windows SIM)
upvoted 3 times

**mikl** 3 years 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** 3 years ago
C. Windows System Image Manager (Windows SIM)
upvoted 1 times

**Perycles** 3 years, 7 months ago
Answer is C
upvoted 2 times

**Timmi** 3 years, 12 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.

**Suggested 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

*Community vote distribution*
C (100%)

**vinnyct** Highly Voted 4 years ago
It's C
upvoted 12 times

**pogap64757** Highly Voted 2 years, 11 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 8 times

**Meebler** Most Recent 1 year, 11 months 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.

The User State Migration Tool (USMT) is a command-line tool that can be used to migrate user profiles between computers. USMT is included in the Windows Assessment and Deployment Kit (ADK) and can be used to migrate data and settings from Windows 8.1 to Windows 10. The process involves running scanstate.exe on the Windows 8.1 computer to create a migration store, and then running loadstate.exe on the Windows 10 computer to apply the migration store.
This method is more effective as it's designed for migrating user profiles between different versions of Windows.
Roaming user profiles and Folder redirection are not designed for migration between different versions of Windows.
upvoted 1 times

**MR_Eliot** 2 years, 8 months ago
Selected Answer: C
C is correct.
upvoted 1 times

**moobdoob** 2 years, 11 months ago

Correct answer is C.

scanstate.exe on each user
Upgrade OS
loadstate.exe on each user
upvoted 2 times

**mikl** 3 years 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** 3 years 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** 3 years, 7 months ago
For sure is correct.
upvoted 3 times

**Layer8** 3 years, 7 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** 3 years, 10 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

**Suggested 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 3 years, 10 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 42 times

**TrustMebro** 3 years ago
Thank you for always giving the answers and confirmations !
upvoted 2 times

**RodrigoT** 2 years, 8 months ago
And here is the proof:
https://docs.microsoft.com/en-us/mem/configmgr/desktop-analytics/about-deployment-plans#readiness-rules
upvoted 5 times

**Perycles** Highly Voted 3 years, 7 months ago
C : desktop analytics for sure.
upvoted 6 times

**ShanePh** Most Recent 1 year, 10 months ago
Hasn't desktop analytics been deprecated?
upvoted 2 times

**Saint3118** 1 year, 5 months ago
yes boss
upvoted 2 times

**b3arb0yb1m** 3 years ago
C. Deployment plans in Desktop Analytics
upvoted 2 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

**Suggested Answer:** *A*
Windows 10 supports a ג€Rollbackג€ 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

*Community vote distribution*


**Merma** Highly Voted 3 years, 8 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 5 times

**jt2214** Most Recent 1 year, 10 months ago
Selected Answer: A
A fo Sho
upvoted 1 times

**Meebler** 1 year, 11 months ago
it is possible to downgrade from Windows 10 to Windows 8.1 by using the recovery options in the Settings app.
The process involves going to the Settings app, then Update & Security > Recovery. Under Go back to Windows 8.1, you will find the option to go back to the previous version of Windows. This option is only available for a limited time after upgrading to Windows 10.

It's important to note that downgrading to Windows 8.1 will require you to reinstall any applications that are not compatible with Windows 8.1 and it's also important to backup all your files and data before performing the downgrade, as the process will delete all the data.
Also, when you downgrade to Windows 8.1, you will no longer receive security updates and other benefits that come with Windows 10.
upvoted 1 times

**KiwE** 2 years, 4 months ago
Threadlink isn't working as of now for the answer
upvoted 1 times

**mikl** 3 years 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

**DJHASH786** 3 years, 9 months ago

From the Settings App, you then goto UPDATE AND SECURITY and then click Recovery... Answer is incomplete ..

upvoted 4 times

**Slammer900** 3 years, 8 months ago

so is it still yes then?

upvoted 2 times

**petir** 3 years, 8 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** 3 years, 7 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

**Suggested 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

*Community vote distribution*
A (100%)

**Perycles** Highly Voted 3 years, 7 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 23 times

**Fourbell** Highly Voted 3 years, 5 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

**giobos** Most Recent 1 year, 6 months ago
Tested today on my HyperV env, Resp: A TESTED !!!
upvoted 1 times

**Meebler** 1 year, 11 months ago
B, No

Downgrading from Windows 10 to Windows 8.1 is not a straightforward process and it's not supported by Microsoft. Windows 10 is designed to be an upgrade from Windows 8.1 and it's not possible to downgrade the operating system by using the Windows Recovery Environment (Windows RE) or the Advanced options.

To downgrade to Windows 8.1, you would need to perform a clean installation of the operating system. This would require you to have a Windows 8.1 installation media and a product key. You would also need to backup all your data and programs, because during the process all data will be

deleted.

It is also important to note that it's not always a good idea to downgrade the operating system, as it may lead to compatibility issues with new hardware and software and security risks.

upvoted 2 times

**MitchF** 2 years, 5 months 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** 2 years, 8 months ago

Selected Answer: A

Answer is A.

upvoted 1 times

**NZS** 2 years, 8 months ago

The answer is definitely YES

upvoted 1 times

**Moderator** 2 years, 9 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** 2 years, 9 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.

NO

upvoted 1 times

**mayleni** 2 years, 11 months ago

Selected Answer: A

Tested and answer is yes

upvoted 5 times

**moobdoob** 2 years, 11 months ago

Selected Answer: A

Tested this in lab enviroment, answer is YES.

upvoted 5 times

**mikl** 3 years ago

Answer is yes.

https://www.thewindowsclub.com/uninstall-latest-quality-or-feature-update

upvoted 2 times

**rovert94** 3 years, 1 month ago

Selected Answer: A

I think the answer is yes

upvoted 4 times

**BLYBOI** 3 years, 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.

upvoted 2 times

**Merma** 3 years, 8 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** 3 years, 8 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** 3 years, 8 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** 3 years, 7 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

Question #57 *Topic 2*

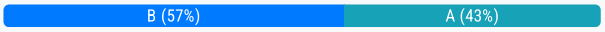
Note: This question is part of a series of questions that present the same scenario. Each question in the series contains a unique solution that might meet the stated goals. Some question sets might have more than one correct solution, while others might not have a correct solution.
After you answer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

**Suggested 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

*Community vote distribution*




**Hatsapatsa** 1 year, 12 months ago

**Selected Answer: B**

The path is not correct for Windows 10. (If it was W11 then yes)

upvoted 1 times

**raduM** 2 years, 1 month ago

you need to go to seetings recovery, go back. There is no option to go back under advanced features

upvoted 1 times

**Whatsamattr81** 2 years, 6 months 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** 2 years, 10 months ago

**Selected Answer: A**

Answer is (at least partially) correct when using Windows 11. Settings -> Windows Update -> Advanced Options -> Recovery -> Go Back

upvoted 3 times

**RodrigoT** 2 years, 8 months ago

The exam is about Windows 10, not Windows 11.

upvoted 6 times

**blitzyx** 2 years, 11 months 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** 2 years, 11 months ago

Answer is no.

upvoted 1 times

**mikl** 3 years ago

Answer is no - you can't uninstall from Windows Update.

upvoted 1 times

**rovert94** 3 years, 1 month ago

**Selected Answer: B**

The answer is NO because you would go under Settings > Update & Security > Recovery, NOT Windows Update.

upvoted 3 times

**MikeMatt2020** 3 years, 7 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** 3 years, 3 months ago

Yes, that is what the q is asking "setting up"!

Hello!!!!

upvoted 1 times

**lucidgreen** 3 years, 11 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:

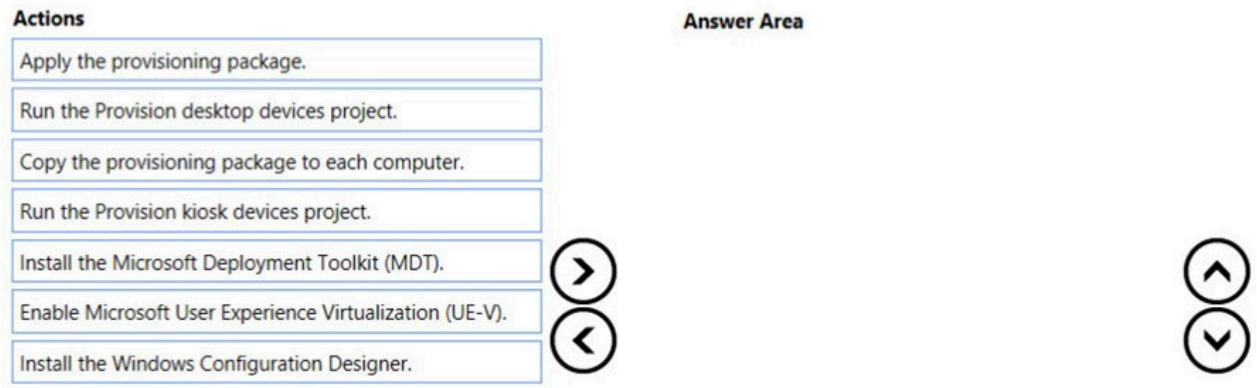
✑ Run an interactive app.

✑ Automatically sign in by using a local user account.

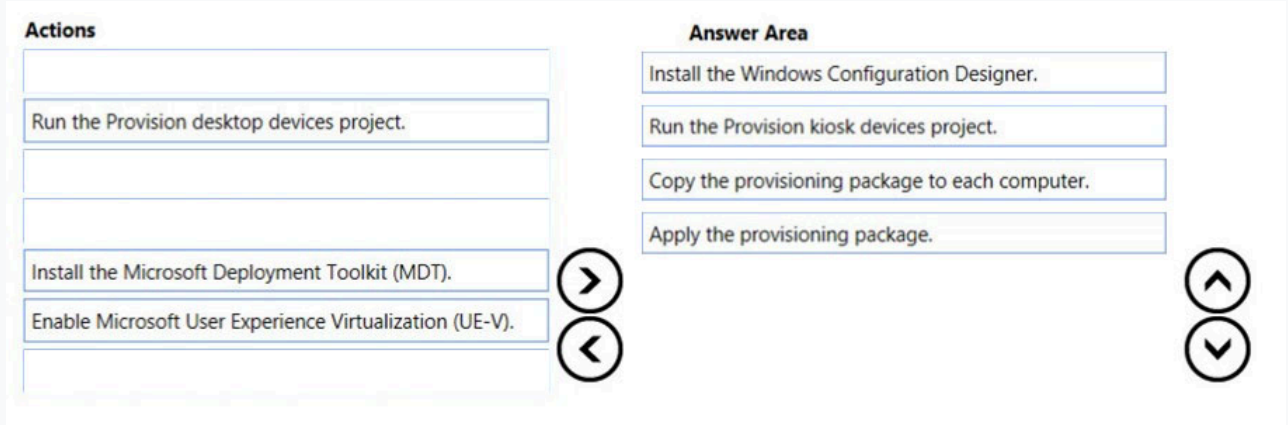
✑ Prevent users from accessing the desktop and running other applications.

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:




**Suggested 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

**Percyles** Highly Voted 3 years, 7 months ago

all is right :)

upvoted 11 times

**Merma** Highly Voted 3 years, 7 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

**AliNadheer** Most Recent 1 year, 10 months ago
answer is correct, i did this i did this in LAB during the class for the course and applied this two weeks ago where i readied provisioning packages for kiosks
upvoted 1 times

**moobdoob** 2 years, 11 months ago
Answer is correct.
upvoted 3 times

**Cowok** 3 years, 7 months ago
Seems it correct
upvoted 4 times

Question #59 *Topic 2*

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 | ○ | ○ |

**Suggested 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 3 years, 8 months ago

No, Yes, Yes,

https://support.microsoft.com/en-us/windows/go-back-to-windows-8-1-40e2d7dc-f640-b0e5-56e1-b41a27e28533

upvoted 42 times

**Evilcoocie** Highly Voted 3 years, 6 months ago

Isnt it:

NO (more than 10 days ago)

NO ( deleted everything)

YES ( within 10 days & kept all files)

upvoted 37 times

**Dbomb** 3 years 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** 2 years, 9 months 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** 2 years, 4 months ago
And? Have you tested?
upvoted 2 times

**Cycubxl** 1 year, 11 months ago
I've tested on my VM win10
if you reset without keeping data, the windows.old won't be created. Even after choosing " Remove everything -> Change settings -> No (just remove your files, This is quicker, but less secure)
so for my NNY
upvoted 2 times

**daonga** 3 years, 3 months 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 17 times

**rej0088** 3 years, 3 months ago
None = Fresh Install , you cannot revert back to anything as Windows.old will not exist, so its NO NO YES
upvoted 5 times

**NKG123** 3 years ago
Start by reading all the question including the context…
upvoted 4 times

**jcgm1990** 2 years, 6 months ago
At least read the question right, where does it say fresh install???
upvoted 2 times

**giobos** Most Recent 1 year, 6 months ago
NO
NO ( deleted everything, tested on my lab today)
YES
upvoted 2 times

**VMLaza** 1 year, 10 months ago
NO
NO ( deleted everything, windows.old won't be created)
YES
upvoted 1 times

**TonySuccess** 2 years, 3 months ago
No, Yes, Yes.

Please ignore people posting answers that are not correct.
upvoted 3 times

**raduM** 2 years, 5 months 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 years, 5 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** 2 years, 7 months 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** 2 years, 11 months 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** 2 years, 9 months 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** 3 years 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** 3 years, 1 month ago
Correct answer is "No, Yes, Yes". System rollback availability lasts for 10 days.
upvoted 3 times

**ANDREVOX** 3 years, 2 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** 3 years ago
What an imagination !!!
upvoted 1 times

**mikl** 3 years ago
What ?
upvoted 1 times

**RodrigoT** 2 years, 8 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** 3 years, 3 months 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** 2 years, 9 months ago

Why not the second computer? Only the user data was not saved during the in place upgrade.

upvoted 1 times

**RodrigoT** 2 years, 8 months ago

And your link is just about rollback feature updates, not Windows version.

upvoted 1 times

**Rick_C137** 3 years, 6 months ago

Anyone know why Computer1 would be a "Yes" based on the question and info provided in it?

upvoted 1 times

**RodrigoT** 2 years, 9 months 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** 3 years, 7 months ago

10 days max to rollback : NO, YES, YES

upvoted 4 times

**Vizsgazo1** 3 years, 7 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** 3 years, 7 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** 2 years, 8 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

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

**Suggested 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 3 years, 7 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** 3 years ago
Agree!
upvoted 1 times

**moobdoob** Most Recent 2 years, 11 months 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

**Suggested 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 3 years, 7 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 2 years, 11 months ago
Answer is NO.
upvoted 2 times

**john909** 3 years, 2 months 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

**Suggested 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 3 years, 7 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 3 years, 7 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 2 years, 11 months 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.

**Suggested 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

*Community vote distribution*
A (100%)

**ThreeDay** Highly Voted 3 years, 3 months ago
I see nobody said this yet but A is correct
upvoted 21 times

**BrentOn** 2 years, 9 months ago
I see nobody has confirmed what you said yet, A is correct
upvoted 8 times

**RodrigoT** 2 years, 9 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 22 times

**MR_Eliot** 2 years, 8 months ago
I see nobody had voted the answer is A, so I did.
upvoted 8 times

**Perycles** Highly Voted 3 years, 7 months ago
A is correct
upvoted 7 times

**thewavyman** Most Recent 1 year, 4 months ago
This has been deprecated - I would not sweat this question if you got it wrong.
upvoted 1 times

**shaolin_monk** 2 years, 5 months ago
A: (Click Sync to get the apps you've purchased from the Microsoft Store into Intune).
upvoted 1 times

**MR_Eliot** 2 years, 8 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** 2 years, 8 months 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** 2 years, 12 months ago

Tenant Admin -> Connector and token -> MSfB -> Enable sync

upvoted 5 times

**moobdoob** 2 years, 11 months ago

Great success!

upvoted 2 times

**Nome2025** 3 years, 7 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.

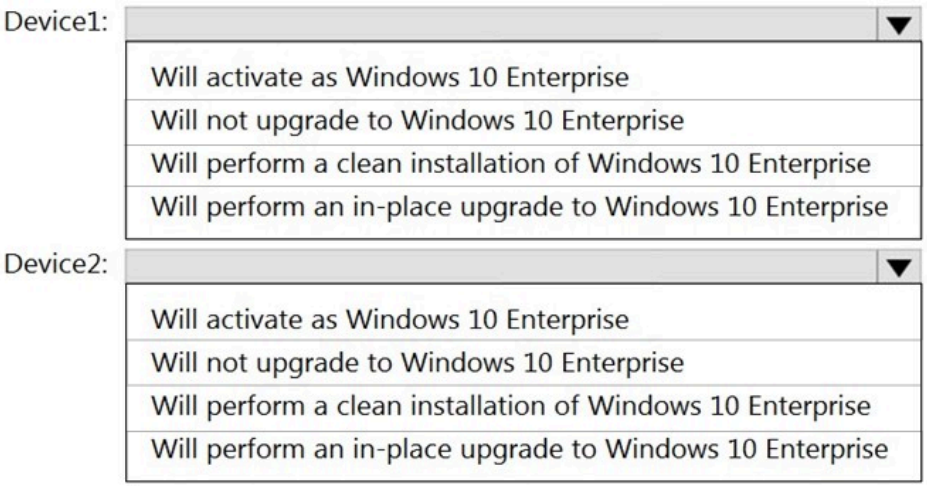
You need to identify what will occur when User1 next signs in to the devices.

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.

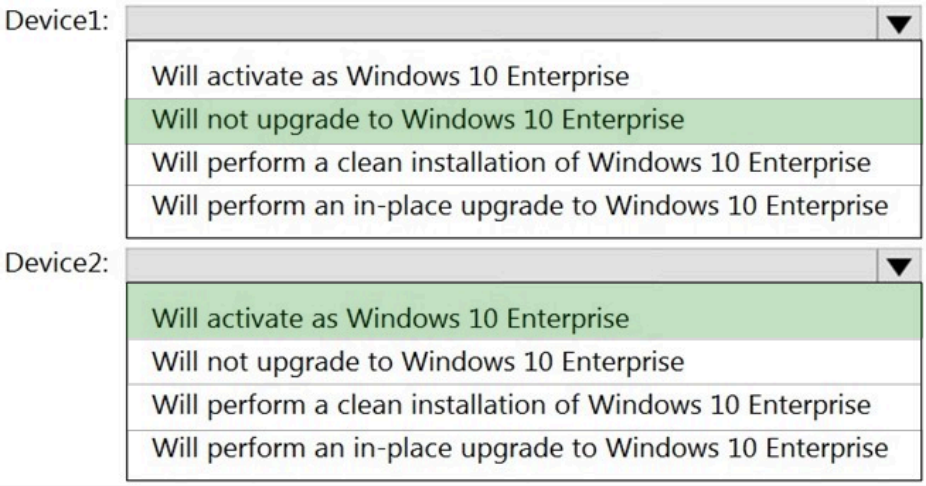
Hot Area:

**Answer Area**




**Suggested 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 3 years, 7 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 68 times

**moobdoob** 2 years, 11 months ago
Agreed. Correct answer above.
upvoted 1 times

**mikl** 3 years ago
Agree!
upvoted 1 times

**AzureLearner01** 2 years, 6 months 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 3 years, 6 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

**Amir1909** Most Recent 11 months, 4 weeks ago
Correct
upvoted 1 times

**jonny_sins** 1 year, 10 months ago
Overthinking this question - tested this in my lab and the provided answers are correct.
upvoted 1 times

**Rob69420** 2 years, 6 months 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** 2 years, 6 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** 3 years 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 4 times

**[Removed]** 3 years, 2 months 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** 2 years, 7 months 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** 3 years, 3 months ago
this is the reason i read the comments, im sure this answer was entered wrong on purpose
upvoted 1 times

**BAbdalla** 3 years, 3 months 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** 2 years, 9 months ago
That's what I'm talking about. Thanks for the lab.
upvoted 4 times

**RodrigoT** 2 years, 9 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** 3 years, 5 months 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** 3 years, 6 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** 3 years, 5 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** 3 years, 6 months ago
Subscription Activation Windows 10 Subscription Activation allows you to automatically 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** 3 years, 6 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** 3 years, 6 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** 3 years, 6 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** 3 years, 7 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

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.

**Suggested 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

*Community vote distribution*
B (100%)

**Perycles** Highly Voted 3 years, 7 months ago
of course B : in place upgarde is the recommended way by microsoft in this case.
upvoted 11 times

**jt2214** Most Recent 1 year, 10 months ago
Selected Answer: B
B is the way. :)
upvoted 1 times

**NZS** 2 years, 8 months ago
B. Also, MDT can be used to do in-place upgrades.
upvoted 1 times

**Angarali** 2 years, 8 months ago
Selected Answer: B
B. Perform an in-place upgrade of Windows 8.1 to Windows 10.
upvoted 2 times

**RodrigoT** 2 years, 9 months 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** 2 years, 11 months ago
In place upgrade is correct.
upvoted 2 times

**mikl** 3 years ago

**Selected Answer: B**

B. Perform an in-place upgrade of Windows 8.1 to Windows 10.

upvoted 2 times

**BAbdalla** 3 years, 2 months ago

Why not option A (Refresh to Windows10 and use USMT)?

upvoted 1 times

**AVP_Riga** 3 years, 2 months ago

Faster(cheaper) and "The installation must retain the user files, settings, and supported applications."

upvoted 3 times

**mikl** 3 years 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

**Harv717** 1 year, 6 months ago

A cannot be used because applications won't be retained.

upvoted 1 times

**RodrigoT** 2 years, 9 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 3 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?

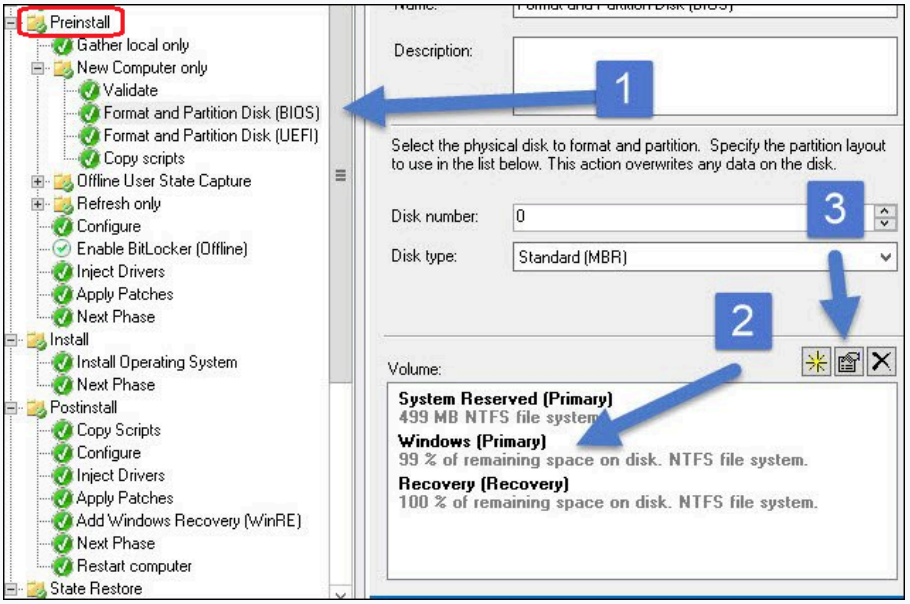
A. Preinstall

B. State Restore

C. Initialization

D. Postinstall

**Suggested 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/

**BRoald** 2 years, 2 months ago
Pre-Install of course, the other answers dont make sense
upvoted 3 times

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.

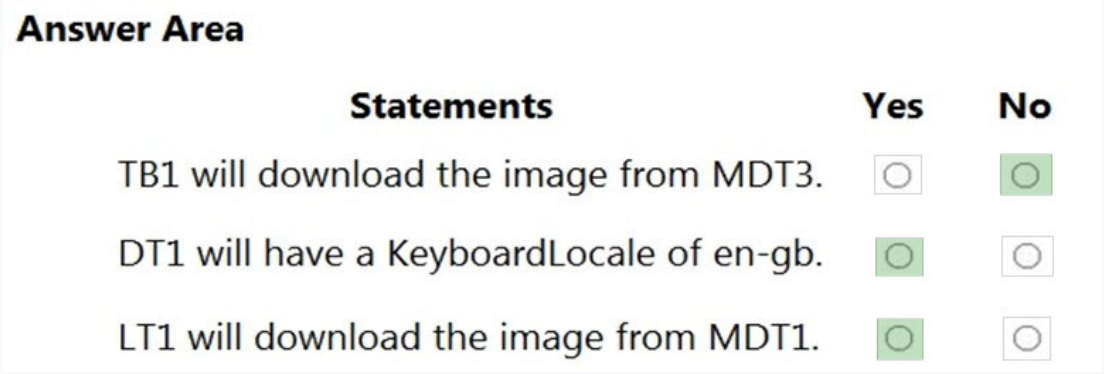
NOTE: Each correct selection is worth one point.

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. | ○ | ○ |

**Suggested Answer:**




Reference:
https://docs.microsoft.com/en-us/windows/deployment/deploy-windows-mdt/build-a-distributed-environment-for-windows-10-deployment

**Perycles** Highly Voted 3 years, 7 months ago
all is correct.
upvoted 19 times

**[Removed]** 3 years, 6 months ago
can you please elaborate on why the 1st is yes?
upvoted 3 times

**AVP_Riga** 3 years, 2 months ago
Because device has x.2.2.x IP address which didn't mention in first DefaultGateway table.
upvoted 1 times

**RodrigoT** 2 years, 9 months ago
So, how can TB1 comunicate if it's in a different subnet of all three MDTs?
upvoted 3 times

**NZS** 2 years, 8 months 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

**DaZa5** 2 years, 1 month ago
10.X.X.X is a private IP. What do you mean with the outside world?
upvoted 1 times

**ercluff** Highly Voted 3 years, 4 months 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 17 times

**RodrigoT** 2 years, 9 months 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 6 times

**veteran_tech** 2 years, 9 months ago
Agree, N Y Y as TB1 is on a different subnet and would therefore access the default GW.
upvoted 1 times

**RodrigoT** 2 years, 8 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

**Amir1909** Most Recent 11 months, 4 weeks ago

Yes
Yes
Yes
upvoted 1 times

**dlast** 1 year, 7 months ago

All should be YES
1:) There is no IP condition matched and there for the default section below in the ini file is process, which will give MDT3
2:) Loction London is used
3:) Location New York is used
upvoted 1 times

**TonySuccess** 2 years, 3 months ago

Nobody going to say it, okay I will. What a joke of a question.
upvoted 6 times

**silver_bullet666** 2 years, 6 months 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** 2 years, 11 months 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** 2 years, 11 months 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** 2 years, 11 months 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** 2 years, 11 months ago
YES, YES, YES
upvoted 2 times

**ANDREVOX** 3 years, 2 months 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** 3 years, 2 months 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

**[Removed]** 3 years, 2 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** 2 years, 8 months 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** 3 years, 3 months ago
NYY there is no 10.2.2.x network...
upvoted 7 times

**Ka1Nn** 3 years, 4 months 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** 3 years, 6 months ago
N Y Y is correct. TB1 will take the Deployroot from [Default] section , ie. \\MDT3
upvoted 5 times

**DPivc** 3 years, 6 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** 3 years, 6 months ago

N Y Y is the correct answer

upvoted 4 times

**cloudnothings** 3 years, 7 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** 3 years, 6 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** 3 years, 6 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

**Suggested 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

*Community vote distribution*
C (100%)

**Jimbob77** Highly Voted 3 years, 7 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 22 times

**Darkfire** Most Recent 1 year, 3 months ago
Selected Answer: C
C is correct

Keywords are: securely wipe and decommission + User State Migration Tool = Standard Client Replace Task Sequence.
upvoted 1 times

**moobdoob** 2 years, 11 months 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**

Compatibility insights:
- Device1 only
- Device1 and Device2 only
- Device3 and Device4 only
- Device1, Device2, Device3, and Device4

App usage insights:
- Device1 only
- Device1 and Device2 only
- Device3 and Device4 only
- Device1, Device2, Device3, and Device4

**Suggested Answer:**

**Answer Area**

Compatibility insights:
- Device1 only
- **Device1 and Device2 only**
- Device3 and Device4 only
- Device1, Device2, Device3, and Device4

App usage insights:
- Device1 only
- Device1 and Device2 only
- Device3 and Device4 only
- **Device1, Device2, Device3, and Device4**

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 3 years, 7 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 26 times

**ozoz** 3 years, 5 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** 3 years, 4 months ago
It talks about Compatibility insight, not Application insight... App Usage is all devices .. So the answer is correct
upvoted 10 times

**[Removed]** 3 years, 2 months ago
Confusing question - Application Insights is not part of Desktop Analytics...
upvoted 5 times

**RodrigoT** 2 years, 8 months ago
You "plan" to implement Desktop Analytics.
upvoted 2 times

**lykeP** Highly Voted 2 years, 11 months 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 16 times

**RodrigoT** 2 years, 9 months 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 15 times

**cjanim03** Most Recent 2 years, 10 months 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** 2 years, 10 months 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 5 times

**RodrigoT** 2 years, 8 months ago
So, until there the question is still valid.
upvoted 1 times

**moobdoob** 2 years, 11 months ago
Compatibility Insights: Device 1 & 2 only
App usage insights: Device 1
upvoted 1 times

**HellRaver80** 3 years, 1 month 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

Question #70 *Topic 2*

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.

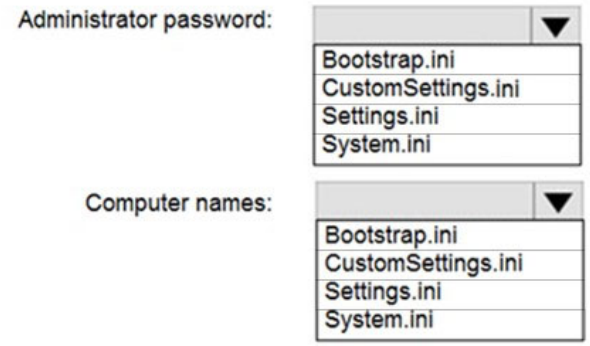
The solution must NOT replace the existing WinPE image.

Which file should you modify for each requirement? To answer, select the appropriate options in the answer area.

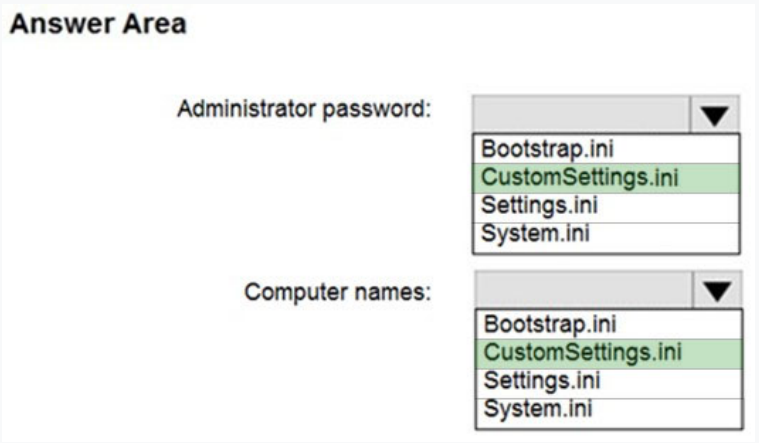
NOTE: Each correct selection is worth one point.

Hot Area:

**Answer Area**




**Suggested Answer:**




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

**Amir1909** 11 months, 3 weeks ago

Correct

upvoted 1 times

**jenraed** 2 years, 1 month ago

Answers are correct. From the links:

SkipAdminPassword=YES is an option in CustomSettings.ini
OSDComputerName=%ComputerName% is also an option in CustomSettings.ini

upvoted 1 times

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

**Suggested 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 3 years, 4 months ago
agreed
upvoted 7 times

**moobdoob** Most Recent 2 years, 11 months ago
Good answer.
upvoted 2 times

**mikl** 3 years 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** 3 years, 6 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

**Suggested 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 3 years, 5 months ago
answer look correct
upvoted 6 times

**Amir1909** Most Recent 11 months, 4 weeks ago
B is correct
upvoted 1 times

**RodrigoT** 2 years, 9 months ago
Check step 5 of the provided link under: Create the selection profiles for boot image drivers.
upvoted 3 times

**moobdoob** 2 years, 11 months 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

**Suggested Answer:** *A*

Discovery method: Use Active Directory Domain Services (AD DS)

Credentials required ɔ€" 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 3 years, 5 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 16 times

**Bradobrey** Highly Voted 3 years, 5 months ago

Ok. May be user 1 or user3, but principle of least privilege- user3.

upvoted 6 times

**RodrigoT** 2 years, 9 months ago

Exactly

upvoted 2 times

**tf444** Most Recent 3 years, 2 months ago

Why not user 4?

upvoted 1 times

**tf444** 3 years, 2 months ago

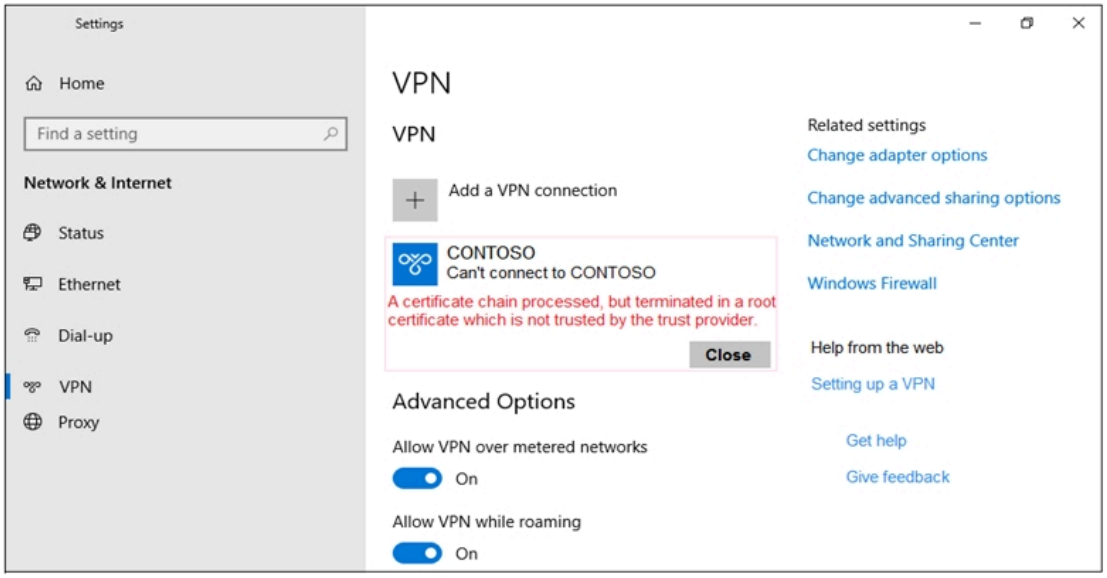
Got it ,the user must be a member of the local Administrators group.

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

**Suggested 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

*Community vote distribution*

C (100%)

**badguytoo** Highly Voted 3 years, 4 months ago

I think should install the root certificate....

upvoted 15 times

**AVP_Riga** 3 years, 3 months ago

It will work, but I assume it isn't a best practice...

upvoted 2 times

**PiPe** Highly Voted 2 years, 11 months 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** 2 years, 8 months ago

Thank you for the link.

upvoted 1 times

**PHSmiffy** Most Recent 2 years, 9 months ago

C is the correct answer. Generating certs from your root CA is bad practice
upvoted 1 times

**cor_** 2 years, 9 months ago
See answer from PiPe.
upvoted 1 times

**Marle** 2 years, 12 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** 3 years, 1 month 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** 3 years, 4 months 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** 3 years, 4 months 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

Question #75 *Topic 2*

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 | ○ | ○ |

**Suggested 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 3 years, 5 months ago

no, yes, yes

upvoted 9 times

**RodrigoT** 2 years, 8 months 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 4 times

**RodrigoT** 2 years, 8 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 3 years, 5 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 9 times

**daonga** 3 years, 4 months ago

So if I understand correctly, the Update ring applies to all devices regardless? Then this is YYY?

upvoted 5 times

**AVP_Riga** 3 years, 3 months ago

NYY, personal device isn't property of company...

upvoted 7 times

**[Removed]** 3 years, 2 months 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** 2 years, 9 months 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 5 times

**Angarali** 2 years, 8 months ago

the answer is N Y Y, the device will be marked as non compliant, until updated by owner

upvoted 1 times

**RodrigoT** 2 years, 8 months 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 10 times

**keenehteek** 3 years, 4 months 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

**Cristyy** Most Recent 1 year, 3 months ago
I do not understand why not YNY ?
upvoted 1 times

**Meebler** 1 year, 11 months ago
NYN,

A. The Active Hours of Device 1 are not affected by the update ring settings because it is not part of the Group1 which is excluded in the assignments of the update ring. As per the given information, Device1 is part of the Group1 but it is excluded in the assignments of the update ring so the active hours of Device1 which is 10am to 6pm will not be affected.
B. The Active Hours of Device 2 are from 9am to 5pm, as specified in the table, but since it is not part of the Group1, it will be affected by the update ring settings. And the update ring setting specified active hours start at 8 am and end at 8 pm so the active hours of device2 will be 8am to 8pm.
C. The Active Hours of Device 3 are not affected by the update ring settings because it is not part of the Group1 which is excluded in the assignments of the update ring. As per the given information, Device3 is part of the Group1 but it is excluded in the assignments of the update ring so the active hours of Device3 which is 10am to 6pm will not be affected
upvoted 2 times

**AK4U_111** 2 years, 2 months ago
So the fact the User1 is a memebr of Group1 doesn't matter at all here?
upvoted 1 times

**KiwE** 2 years, 2 months ago
No because it's a personal device
upvoted 1 times

**PiPe** 2 years, 11 months 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 8 times

**PiPe** 2 years, 11 months ago
Correction typo: *(case 4 & 7 on the below URL)
upvoted 2 times

**RodrigoT** 2 years, 9 months 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

**syougun200x** 1 year, 6 months ago
Probably some change made on intune? could not find the "user exclusion is not supported" said on the article.
https://docs.microsoft.com/en-us/mem/intune/configuration/device-profile-assign#exclude-groups-from-a-profile-assignment

I tested with my tenant and the profile was created excluding some users without an error.
upvoted 1 times

**rovert94** 2 years, 11 months 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** 2 years, 9 months 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** 3 years, 5 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

**Suggested 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

*Community vote distribution*


**examkiller321** Highly Voted 3 years, 2 months 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 24 times

**coppermine** 2 years, 11 months 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** 3 years ago
Tricky question.
upvoted 3 times

**ShanePh** 1 year, 10 months ago
very helpful thank you.
upvoted 1 times

**verifedtomic** Highly Voted 3 years, 3 months 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

**RodrigoT** 2 years, 9 months ago
If you do this you will wipe and install Win 10, not upgrade.
upvoted 4 times

**AVP_Riga** 3 years, 2 months ago

Yes, if you start it from windows, but question about "You start Computer1 from the Windows 10 installation media".

upvoted 5 times

**jt2214** Most Recent 1 year, 10 months ago

This one was tricky. Answer is correct

upvoted 1 times

**Tanderson2491** 2 years, 9 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 2 times

**moobdoob** 2 years, 11 months 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 2 times

**handsofthelp** 3 years ago

Is correct. You can start Computer 1 from installation media, but will not be able to install.

upvoted 1 times

**Jeff8989** 3 years, 3 months ago

Answer is not correct.

upvoted 4 times

**Tanderson2491** 2 years, 9 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

**Suggested 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

*Community vote distribution*


**verifedtomic** Highly Voted 3 years, 3 months ago
This is correct. Answer is No. User licenses don't have any effect on in-place upgrade.
upvoted 5 times

**Muhaymin** Most Recent 1 year, 5 months ago
B is correct
upvoted 1 times

**Cisco** 2 years, 8 months 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** 2 years, 8 months ago
Only from Windows 10 Pro to Windows 10 Enterprise
upvoted 1 times

**mikl** 3 years 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

**Suggested 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

*Community vote distribution*
A (100%)

**kalmann** Highly Voted 3 years, 3 months ago
Answer A is correct.
upvoted 5 times

**jt2214** Most Recent 1 year, 10 months ago
Selected Answer: A
A all the way
upvoted 1 times

**Tanderson2491** 2 years, 9 months ago
Selected Answer: A
Answer is correct
upvoted 1 times

**moobdoob** 2 years, 11 months ago
A is correct.
upvoted 1 times

**Anderp** 2 years, 11 months ago
Selected Answer: A
A is correct
upvoted 1 times

**mikl** 3 years ago
A is correct.
upvoted 1 times

Question #79 *Topic 2*

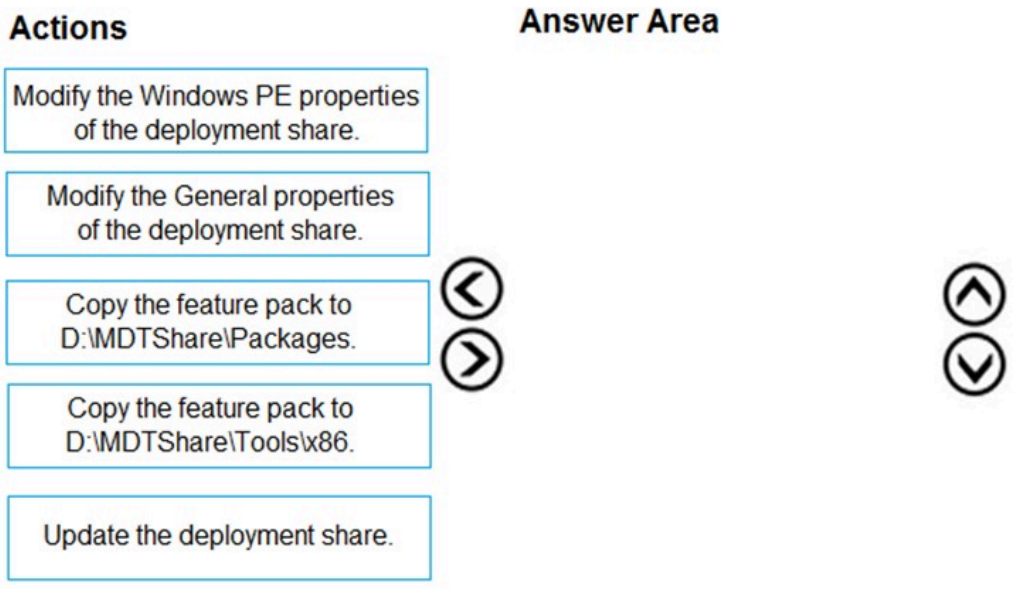
DRAG DROP -

You have a Microsoft Deployment Toolkit (MDT) deployment share that has a path of D:\MDTShare.

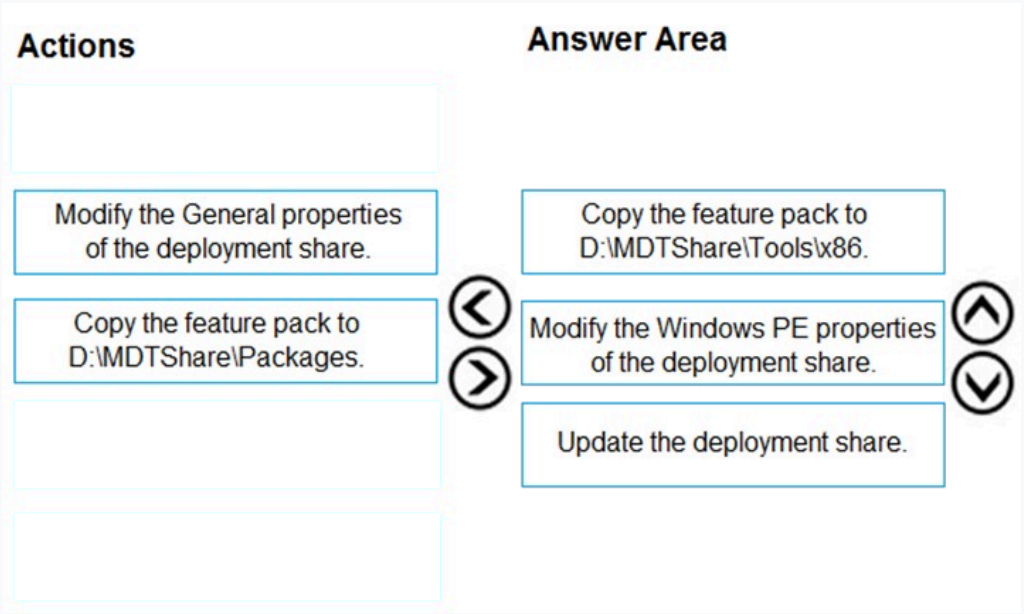
You need to add a feature pack to the boot image.

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:




**Suggested 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.

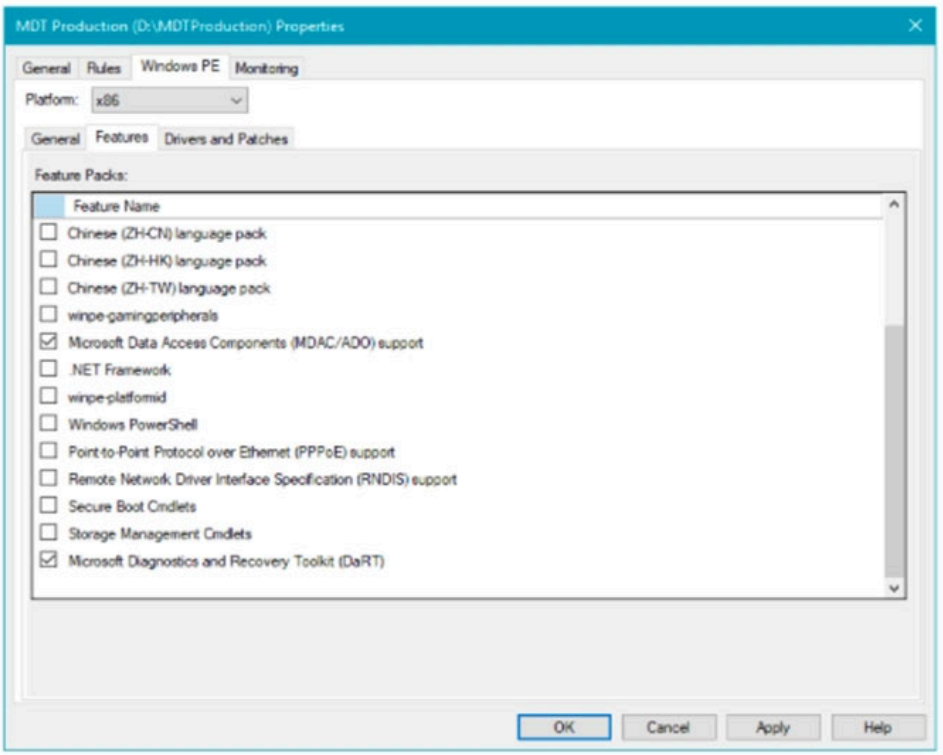
1. Copy the CAB files to the deployment share: MDTShare\Tools\x86

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

**Amir1909** 11 months, 3 weeks ago

Correct

upvoted 1 times

**Meebler** 1 year, 11 months ago

Step 1: Copying the feature pack to the appropriate location is correct. The location you have specified (D:\MDTShare\Tools\x86) is where the MDT tools and files are stored, so it is a logical location for the feature pack.

Step 2: Modifying the Windows PE properties of the deployment share is also correct. You will need to specify that the DaRT feature pack should be included in the boot image by editing the appropriate settings in the MDT Deployment Workbench.

Step 3: Updating the deployment share is the final step, in which the new settings you have specified in step 2 will be applied to create the updated boot image. This is a necessary step to include the DaRT feature pack in the boot image.

It is important to note that you should always test your changes before deploying it to production.

upvoted 3 times

**Fuzm4n** 2 years, 1 month ago

Looks right. Example uses x86 but you have to copy it to x64 also if you want to add it to the x64 tab.

https://learn.microsoft.com/en-us/windows/deployment/deploy-windows-mdt/deploy-a-windows-10-image-using-mdt

upvoted 1 times

HOTSPOT -

You create a Windows Autopilot deployment profile.

You need to configure the profile settings to meet the following requirements:

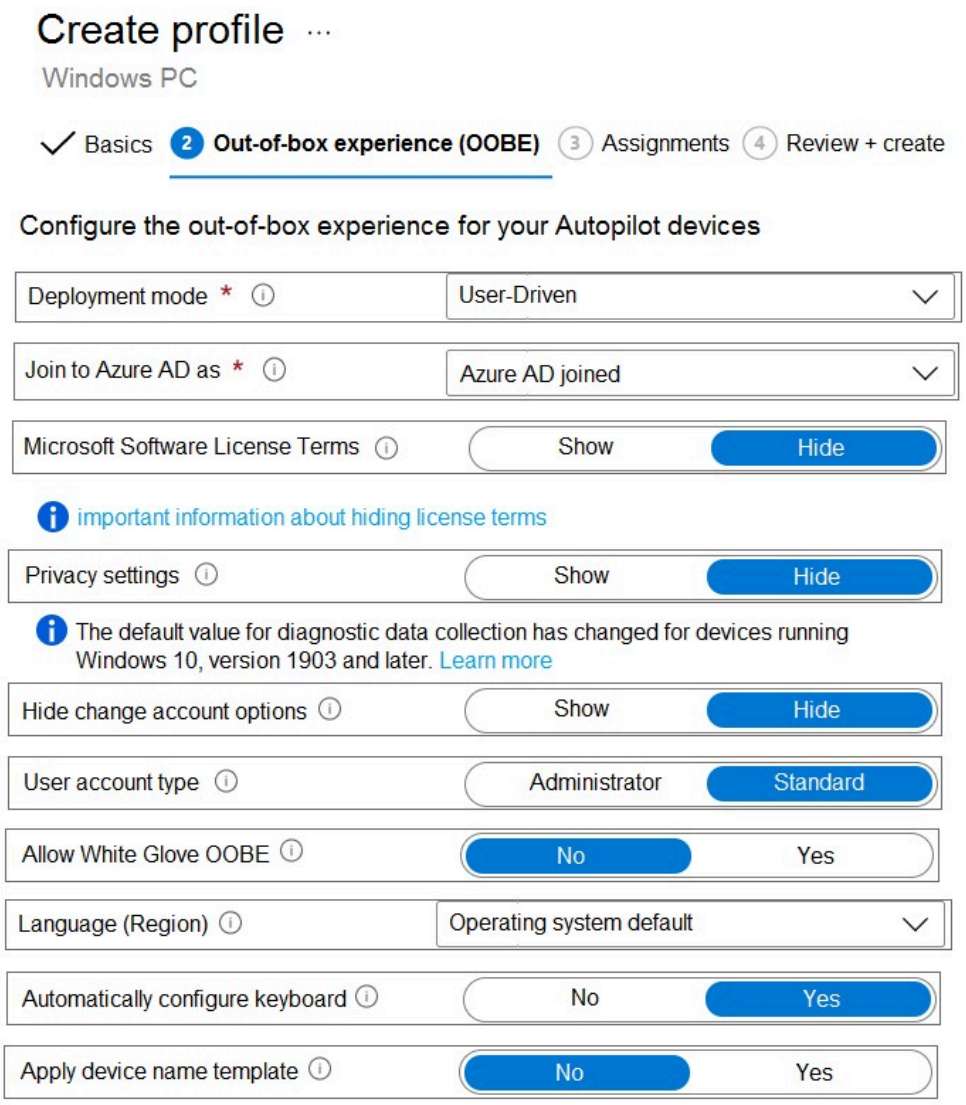
- ✑ Automatically enroll new devices and provision system apps without requiring end-user authentication.
- ✑ Include the hardware serial number in the computer name.

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

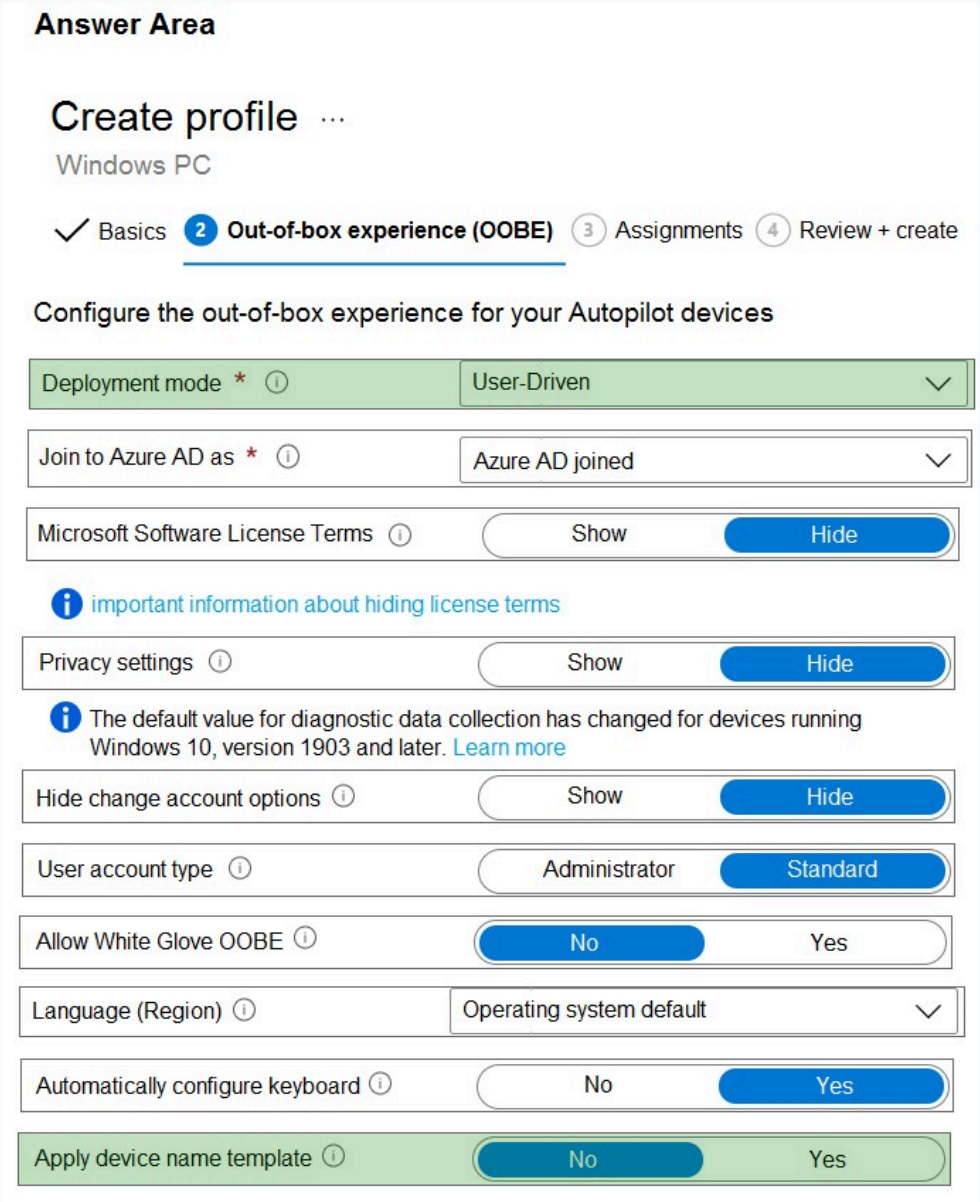
NOTE: Each correct selection is worth one point.

Hot Area:

**Answer Area**



**Suggested Answer:**




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

**BRoald** Highly Voted 2 years, 3 months 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 5 times

**daye** 2 years, 2 months ago

self deployment doesn't require user authentication either and also enroll and install system apps so technically you can use both methods based on this requirement.

Whiteglove / PreProvisioning is basically to delegate providers (Dell, HP, Lenovo, etc) to run the autopilot process and reduce the IT process. So, I guess this question would have several options :)
upvoted 4 times

**BRoald** 2 years, 2 months ago
Yes youre right i read the question different now i look back at it. Forget my answer but you can pre-provision with WhiteGlove so you dont need user authentication :)
upvoted 1 times

**TonySuccess** Highly Voted 2 years, 3 months ago
Mods please correct this, we are paying bro
upvoted 5 times

**USRobotics** 1 year, 4 months ago
is not correct?
upvoted 1 times

**Amir1909** Most Recent 11 months, 4 weeks ago
Correct
upvoted 1 times

**USRobotics** 1 year, 4 months ago
From what i searched the correct answer should be white-glove now called "pre-provisioning mode".
Please fix the answer
upvoted 1 times

**vanr2000** 1 year, 6 months ago
The answers are correct, if you use White Glove, which is called now pre-provision, these are the two scenarios to use it, and both of them the user intervein:

Windows Autopilot for pre-provisioned deployment supports two distinct scenarios:

- User-driven deployments with Azure AD join. The device is joined to an Azure AD tenant.
- User-driven deployments with hybrid Azure AD join. The device is joined to an on-premises Active Directory domain and separately registered with Azure AD.
upvoted 2 times

**Chombo08** 1 year, 7 months ago
User Driven requires end user authentication. White Glove on the other hand, don't. I would say White Glove and Apply Device name Template
upvoted 1 times

**KiwE** 2 years, 2 months ago
Self deploying seems correct say setting up a Kiosk and what app(s)to use automated
https://learn.microsoft.com/en-us/mem/autopilot/self-deploying
upvoted 2 times

**bensrayan** 2 years, 3 months ago
- Allow white Glove (provision system APPS without requiring....)
- Apply Device name
upvoted 2 times

**rockhound** 2 years, 3 months ago
Correct
upvoted 2 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

**Suggested 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

*Community vote distribution*

B (100%)

**RodrigoT** 2 years, 9 months ago

Selected Answer: B

B. NO is correct

upvoted 2 times

**ercluff** 3 years 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 4 times

**TrustMebro** 3 years 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

**Suggested Answer:** *B*
Instead run the Windows 10 Readiness scenario.
Reference:
https://www.techielass.com/using-maps-azure-readiness/

*Community vote distribution*
B (100%)

**ANDREVOX** Highly Voted 3 years, 2 months ago
Answer is Correct.
You should collect inventory data and run the Windows 10 Readiness scenario (Not the Windows 8.1 Readiness scenario).
upvoted 16 times

**wafa2022** Most Recent 1 year, 5 months ago
Answer is A : YES
upvoted 1 times

**Shalen** 1 year, 11 months ago
The answer is B see question 84 , the same question
upvoted 1 times

**AK4U_111** 2 years, 2 months ago
NO is correct. See Question #62 on page 11.

From the Microsoft Assessment and Planning Toolkit, you collect inventory data and run the Windows 10 Readiness scenario.
upvoted 1 times

**MR_Eliot** 2 years, 8 months ago
Selected Answer: B
B is the answer.
upvoted 1 times

**moobdoob** 2 years, 11 months ago
NOTE: Windows 8.1 readiness scenario, therefore answer is NO.
upvoted 3 times

**Will_1_AM** 3 years, 2 months 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.

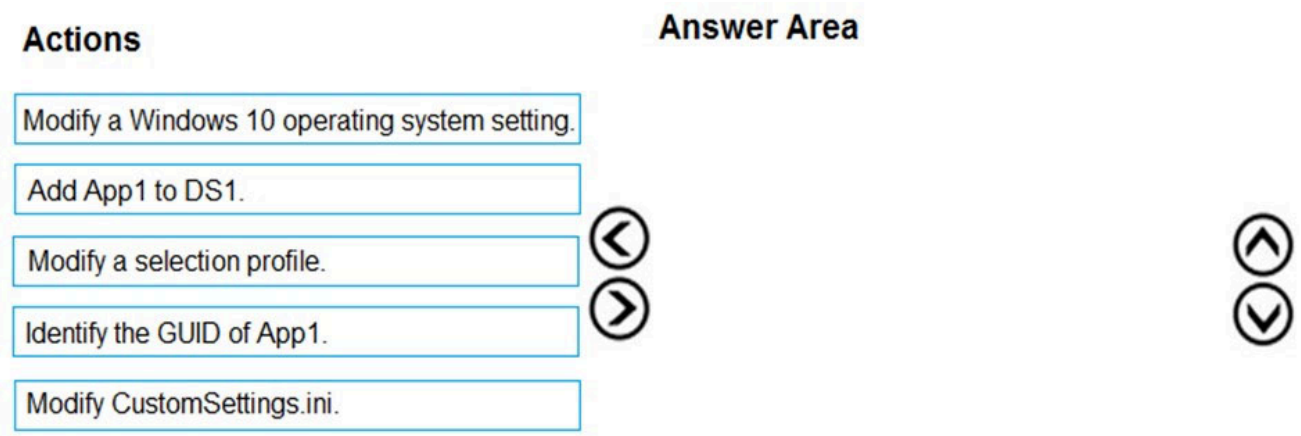
You import a Windows 10 image to DS1.

You have an executable installer for an application named App1.

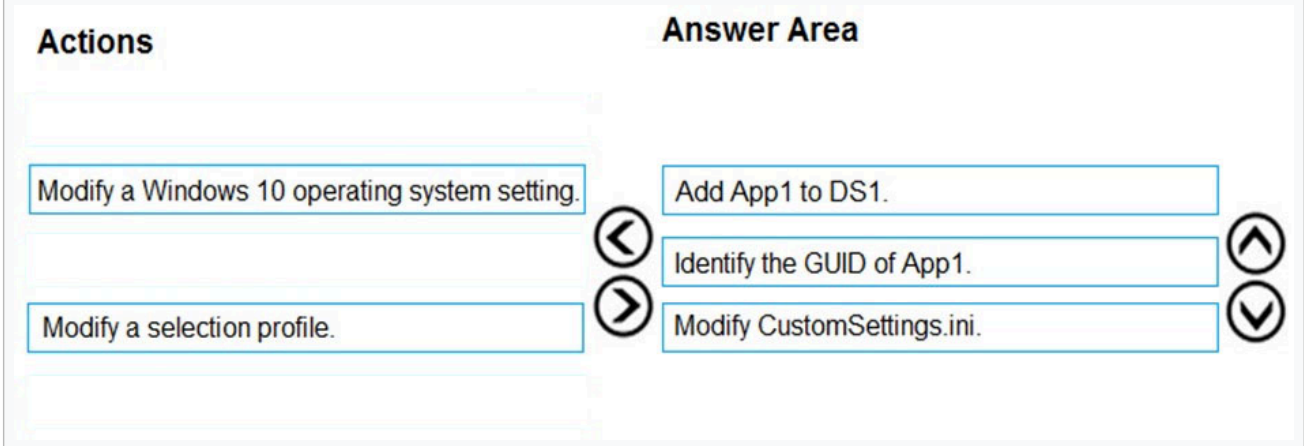
You need to ensure that App1 will be installed for all the task sequences that deploy the image.

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:




**Suggested 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 3 years, 3 months ago

1. Add App to DS1, Identify the GUIS of App1, Modify CS.ini

upvoted 24 times

**handsofthelp** 3 years, 1 month ago

I have the same opinion.

upvoted 1 times

**forummj** 2 years, 11 months 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 7 times

**RodrigoT** 2 years, 9 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 2 times

**RodrigoT** 2 years, 8 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 3 times

**RodrigoT** 2 years, 8 months ago

And selection profiles is usually for drivers. To mach drivers with device models.

upvoted 1 times

**tcmaggio** Highly Voted 3 years, 3 months 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

**Amir1909** Most Recent 11 months, 4 weeks ago

Correct

upvoted 1 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)

**Suggested 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-Vэ„¢, 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

*Community vote distribution*
A (100%)

**BAbdalla** Highly Voted 3 years, 2 months ago
Correct. Option A (MAP).
upvoted 5 times

**Beng_ali** Most Recent 2 years, 10 months 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)

**Suggested 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 3 years, 2 months ago
Option B (MAP) is Correct.
upvoted 6 times

**mrjeet** Most Recent 2 years ago
If all the questions were this easy :) B is correct
upvoted 1 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. | ○ | ○ |

**Suggested 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 3 years, 3 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 22 times

**[Removed]** 3 years, 2 months 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** 3 years, 2 months 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** 2 years, 10 months 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** 2 years, 9 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 4 times

**RodrigoT** 2 years, 8 months 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 5 times

**Goofer** Highly Voted 3 years, 1 month 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 15 times

**RodrigoT** 2 years, 8 months ago
Perfect simple answer 
upvoted 2 times

**AyoR32** Most Recent 1 year, 12 months ago
I'm not agree withe the first aswer: "Device 1 will install feature update twice a year"
The Device1 is under the Policy 1 that control monthly updates and not feature updates.
upvoted 1 times

**daye** 2 years, 2 months ago
Nowadays this question is pretty old since W10 only has 1 feature update every year... but based on this "old scenario" it would be correct. :)
upvoted 2 times

**MR_Eliot** 2 years, 8 months ago
Omar86 is right. Correct answer is Y,N,N
upvoted 1 times

**PiPe** 2 years, 11 months 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** 2 years, 8 months ago
Check my second comment above and you will understand.
upvoted 1 times

**a92876** 2 years, 11 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** 2 years, 11 months 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

**Suggested 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** Highly Voted 3 years 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 5 times

**MR_Eliot** 2 years, 8 months ago
I agree.
upvoted 1 times

HOTSPOT -

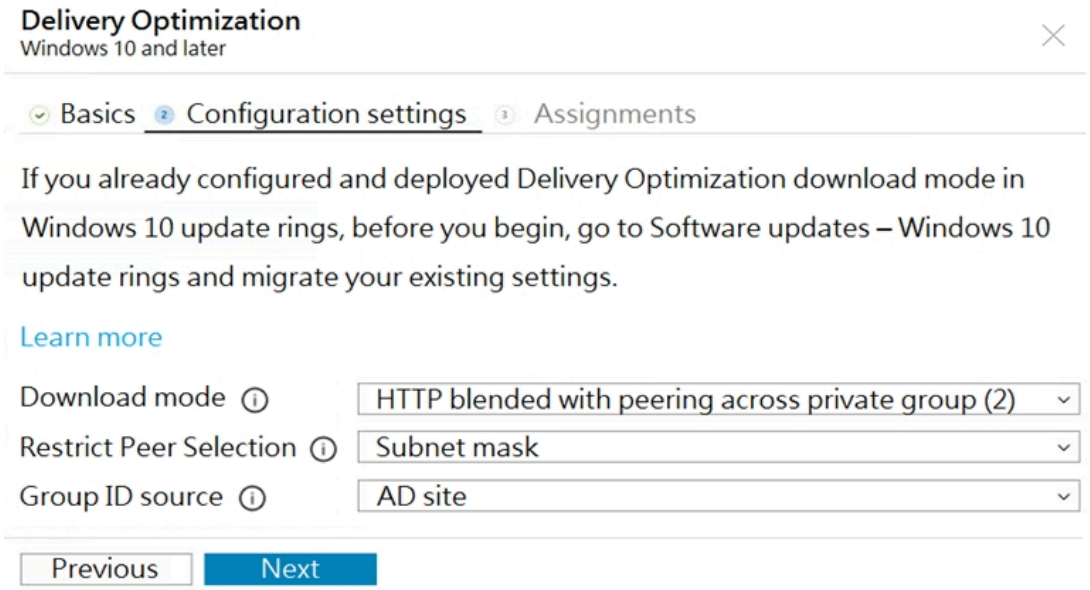
Your network contains an on-premises Active Directory domain that contains the locations shown in the following table.

| 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:

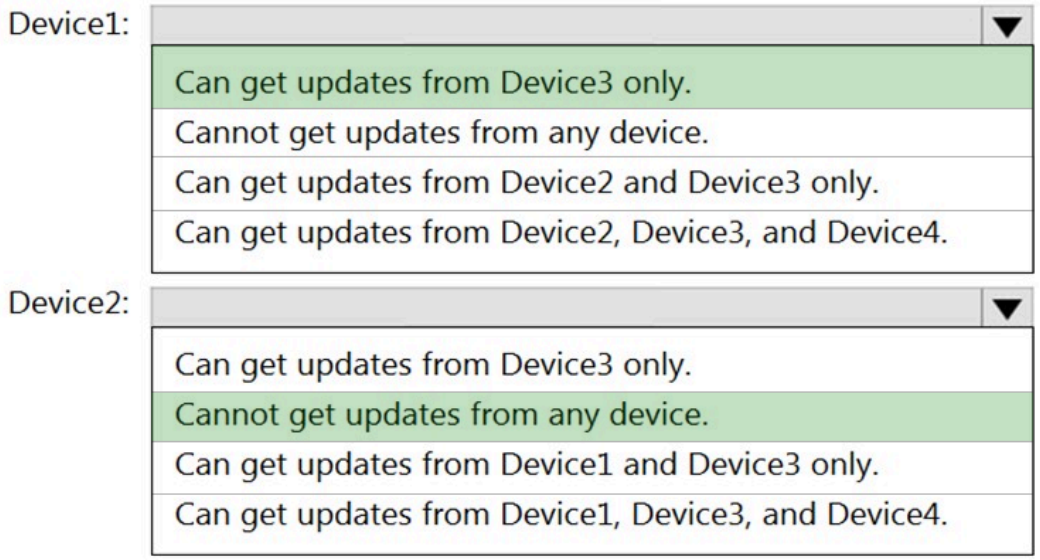
- Can get updates from Device3 only.
- Cannot get updates from any device.
- Can get updates from Device2 and Device3 only.
- Can get updates from Device2, Device3, and Device4.

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.

**Suggested Answer:**

**Answer Area**




Reference:
https://garvis.ca/2021/06/01/delivery-optimization-know-your-options/

**czara6** Highly Voted 3 years, 3 months ago
Device 1: only from Device 3
Device 2: cannot get updates from any device
upvoted 27 times

**NorthBlueEdd** 2 years, 9 months ago
This is correct. If logically answering the question.
upvoted 1 times

**musiman** 3 years 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** 2 years, 9 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 3 times

**Nerovats74** 2 years, 3 months ago
Restrict Peer Selection is set to subnetmask, so answer is correct
upvoted 4 times

**Nerovats74** 2 years, 2 months ago
No, RdrigoT is right, if HTTP blended with peering behind the same NAT was selected answer would have correct.
upvoted 1 times

**blueninja** 3 years, 2 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** 3 years 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** 3 years, 2 months 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** 2 years, 9 months 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

**PiPe** Highly Voted 2 years, 11 months 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 8 times

**AVR31** 2 years, 8 months ago
Yes, since peer selection is restricted to network mask, this is the correct answer.
upvoted 2 times

**Amir1909** Most Recent 11 months, 3 weeks ago
Correct
upvoted 1 times

**Iannythewizard** 1 year, 8 months ago
HTTP Blended with peering across private group means that computers in the same AD DS site, or same domain, can talk to each other. Also mentions doing this by subnet mask. All Devices have /16 CIDR networks, so subnet mask for ALL is 255.255.0.0

After that, the only differentiator is the two sites. All devices in Site 1 can talk to each other. Device 4 Cannot because it's in Site 2.

Answer is Device 1 can talk to 2 and 3, and device 2 can talk to 1 and 3

RodrigoT is correct
upvoted 1 times

**Raxon** 1 year, 9 months ago
Device1:
Can get updates from Device2 and Device3 only.

Device2:
Can get updates from Device1 and Device3 only.

Restrict Peer Selection: Subnet mask
Group ID source: AD site

The devices can get updates from the devices within their respective sites and subnets, but not from Device4 as it belongs to a different site.

Devices 1 - 3 IP are Class A & Site 1 - Because we're not provided with additional information, we must assume the IP are on the same Subnet Mask.

Device 4 IP is Class B & Site 2 - Different Subnet Mask and Site.

upvoted 3 times

**randdrick** 2 years, 8 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

**cbjorn8931** 2 years, 2 months ago

How's are device 1 and 3 on the same subnet ? Device 1 is on a /16 subnet mask and Device 3 is on a /24 mask? Where did you get that they are on the same network ? https://ipinfo.io/ips/10.10.1.0/24

upvoted 1 times

**Graz** 2 years ago

The first two octets match.
"10.10.x.x" Device 1 and 3 are on the same subnet both are /16 subnet masks

upvoted 1 times

**Raxon** 1 year, 10 months ago

First 3 Devices are Class A IP addresses. Default Subnet Masks 255.0.0.0

While is not uncommon for devices to have different Subnet Masks. The question doesn't provide us with the Subnet masks for the individual devices. We then must assume they're set to default.

The last Device is on Class B which would be 255.255.0.0

upvoted 1 times

**lannythewizard** 1 year, 8 months ago

Class A are 255.0.0.0 if there isn't CIDR notation. There is though, and all networks are a /16, so subnet mask for all of them is 255.255.0.0

upvoted 1 times

**MR_Eliot** 2 years, 8 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

**cbjorn8931** 2 years, 2 months ago

This is correct! Device 3 is on the subnet /24 which not listed I. Means it cannot communicate effectively with other devices

upvoted 1 times

**cbjorn8931** 2 years, 2 months ago

And it doesn't belong to site 1 or site 2

upvoted 1 times

**moobdoob** 2 years, 11 months 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

**cbjorn8931** 2 years, 2 months ago

Device 3 is not on the same subnet

upvoted 1 times

**Graz** 2 years ago

yes it is. 10.10.x.x /16 for both device 1 and device 3. Not sure where you are seeing /24 for device 3?

upvoted 1 times

**forummj** 2 years, 11 months 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 4 times

**LoganBundrant91** 3 years ago

So who's correct?

upvoted 7 times

**RodrigoT** 2 years, 9 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

**Goofer** 3 years, 1 month 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 4 times

**lijk_manson** 3 years, 2 months 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.

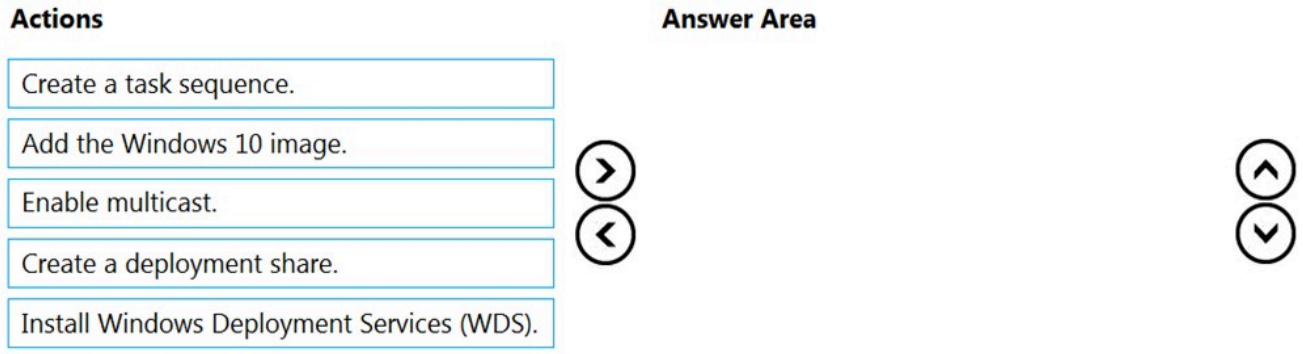
You install the Microsoft Deployment Toolkit (MDT) on a server.

You have a custom image of Windows 10.

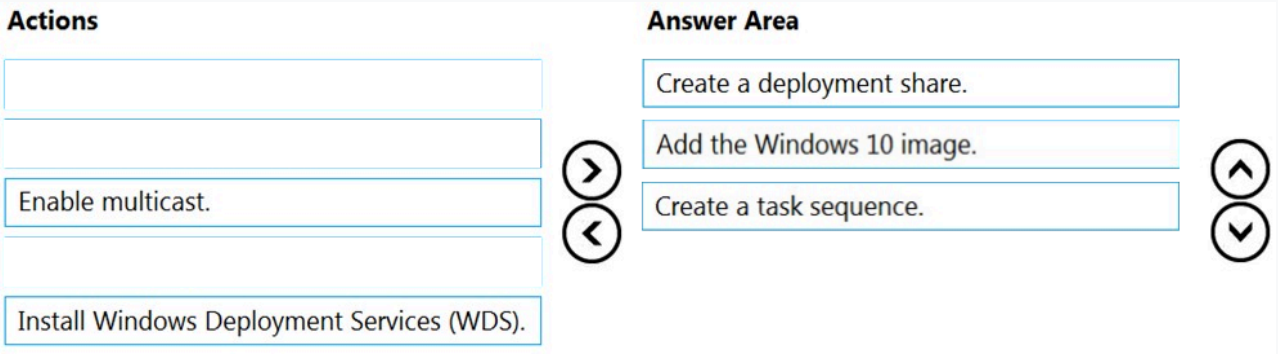
You need to deploy the image to 100 devices by using MDT.

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:




**Suggested 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 2 years, 12 months ago

The given answer is correct.

upvoted 8 times

**RodrigoT** 2 years, 9 months ago

I agree.

upvoted 1 times

**TaboloDude** Highly Voted 3 years ago

@b3arb0yb1m

What are you talking about? Those options aren't even available in the answer?

upvoted 5 times

**Amir1909** Most Recent 11 months, 4 weeks ago

Correct

upvoted 1 times

**AVR31** 2 years, 8 months 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** 2 years, 8 months ago

Totally wrong, sorry. WDS is a very old way to wipe and load static images. Welcome to MDT.
upvoted 3 times

**AliNadheer** 1 year, 10 months ago

at first this is what i thought, this setup works for PXE deployment i have it implemented in my organization, but reading the question it doesn't specify we need to use PXE.
so your typical 1- create deployment share, 2- add windows 10 image, 3- create task sequence. should work
upvoted 1 times

**b3arb0yb1m** 3 years, 1 month 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

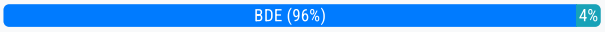
E. desktop theme settings

**Suggested 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 ɔ€" desktop theme, taskbar settings, etc.
Internet Explorer settings ɔ€" recently opened tabs, favorites, etc.
(C) Edge browser settings ɔ€" favorites, reading list
(D) Passwords ɔ€" Internet passwords, Wi-Fi profiles, etc.
Language preferences ɔ€" keyboard layouts, system language, dateand time, etc.
Ease of access ɔ€" high contrast theme, Narrator, Magnifier, etc.
Other Windows settings ɔ€" 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/

*Community vote distribution*




**fvibes** Highly Voted 3 years 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 12 times

**RodrigoT** 2 years, 9 months ago

The word Chromium is there just to confuse you. Microsoft Edge is "based" in the Chromium project. CDE is correct.
upvoted 8 times

**veteran_tech** 2 years, 9 months ago

Agreed, sticking with CDE
upvoted 3 times

**chosenw0w** 1 year, 11 months ago

Microsoft Edge is a cross-platform application with an expanded scope for syncing user data across all their devices and is no longer a part of Azure AD Enterprise State Roaming.
upvoted 1 times

**lykeP** Highly Voted 2 years, 11 months ago

Selected Answer: BDE

Correct Answer is BDE
upvoted 5 times

**golijat** Most Recent 1 year, 3 months ago

Selected Answer: BCE

A. Microsoft Teams settings: No, Microsoft Teams settings are not synced through Enterprise State Roaming.

B. Mouse settings: Yes, system settings such as mouse settings, keyboard settings, and more are synced.

C. Microsoft Edge Chromium settings: Yes, browser settings are included in the sync.

D. Internet passwords: No, Internet passwords are not synced through Enterprise State Roaming. Passwords saved in the browser may sync as part of the browser's own sync capabilities.

E. Desktop theme settings: Yes, user preferences like desktop theme settings are also synced.

So, the correct answers would be B, C, and E.

upvoted 1 times

**Topupjay** 1 year, 10 months ago

Specifically stated.....

Note

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.

Reference link: https://learn.microsoft.com/en-us/azure/active-directory/devices/enterprise-state-roaming-enable

upvoted 1 times

**bitjos** 2 years ago

BCDE ;)

https://learn.microsoft.com/en-us/azure/active-directory/devices/enterprise-state-roaming-windows-settings-reference

upvoted 2 times

**DDHP7** 2 years ago

found this info https://itconnect.uw.edu/tools-services-support/it-systems-infrastructure/msinf/aad/device/esr/

upvoted 1 times

**Fedexxx92** 2 years, 1 month ago

Final Answer: BDE

Microsoft Edge is a cross-platform application with an expanded scope for syncing user data across all their devices and is no longer a part of Azure AD Enterprise State Roaming. However, Microsoft Edge will fulfill the data protection promises of ESR, such as the ability to bring your own key. For more information, see Microsoft Edge and Enterprise State Roaming.

https://learn.microsoft.com/en-us/deployedge/microsoft-edge-enterprise-sync#microsoft-edge-and-enterprise-state-roaming-esr

upvoted 2 times

**MR_Eliot** 2 years, 8 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** 2 years, 8 months 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** 2 years, 8 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 4 times

**Moderator** 2 years, 9 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 2 times

**Garito** 2 years, 10 months ago
Selected Answer: BDE
Chromium settings not supported
upvoted 3 times

**RodrigoT** 2 years, 9 months ago
The word Chromium is there just to confuse you. Microsoft Edge is "based" in the Chromium project. CDE is correct.
upvoted 4 times

**Deric** 2 years, 3 months 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** 2 years, 10 months ago
https://docs.microsoft.com/en-us/azure/active-directory/devices/enterprise-state-roaming-windows-settings-reference
BCE
upvoted 2 times

**moobdoob** 2 years, 11 months ago
Selected Answer: BDE
Correct
upvoted 3 times

**NKG123** 3 years 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** 3 years, 1 month 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** 3 years, 1 month 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** 3 years ago
B, D, and E. Not C. Your reference clearly states it does not include Edge Chromium browser.
upvoted 1 times

**Will_1_AM** 3 years, 2 months ago
Correct. Internet password is included. https://docs.microsoft.com/en-us/azure/active-directory/devices/enterprise-state-roaming-faqs
upvoted 1 times

**[Removed]** 3 years, 2 months 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]** 3 years, 2 months ago
Sorry I meant also B, mouse settings, should be right: "Other Windows settings, such as mouse settings."
upvoted 1 times

**Anon1212** 2 years, 11 months ago
BDE, If exploder or edge were mentioned than perhaps CDE.
upvoted 1 times

Question #91 *Topic 2*

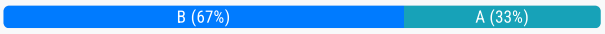
Note: This question is part of a series of questions that present the same scenario. Each question in the series contains a unique solution that might meet the stated goals. Some question sets might have more than one correct solution, while others might not have a correct solution.
After you answer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

**Suggested 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

*Community vote distribution*




**PESK** Highly Voted 5 years, 2 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** 2 years, 8 months 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 2 times

**JohnxLarusso** Highly Voted 5 years, 1 month 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

**cbjorn8931** Most Recent 2 years, 2 months ago
Answer: A Yes, by conducting a Windows autopilot reset, it will bring back to business-ready so that the next user can login in and be prompted to select their OOB settings -> https://learn.microsoft.com/en-us/mem/autopilot/windows-autopilot-reset
upvoted 2 times

**OG_Diablo** 1 year, 5 months ago
"business-ready", yes. But it will not result in OOBE. The keyboard settings etc. are all set during the reset. The new user is simply presented with a sign-in screen (not OOBE).
upvoted 1 times

**JN_311** 2 years, 5 months ago
Selected Answer: A
Answer A, done it many times
upvoted 2 times

**4Shawsy** 2 years, 11 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** 3 years 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** 3 years 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 4 times

**Moderator** 3 years 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** 3 years, 6 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** 3 years, 6 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 2 times

**Jeffoort** 3 years, 9 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** 3 years, 9 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** 4 years, 1 month 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** 4 years, 3 months 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** 3 years ago
Depends on how you have configured your Autopilot deployment profiles : https://docs.microsoft.com/en-us/mem/autopilot/profiles
upvoted 1 times

**loganharris** 4 years, 4 months 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** 4 years, 11 months ago
Definitely B as Windows Autopilot Reset process automatically retains information from the existing device including LANGUAGE.
upvoted 12 times

**nolancl** 5 years, 3 months ago
Correct answer is A and the document you linked supports that. Device has already been configured once.
upvoted 11 times

**Parzival** 5 years, 1 month ago
I agree I have read it twice.
upvoted 2 times

**Cronus1610** 3 years, 8 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 4 times

Question #92 *Topic 2*

HOTSPOT -

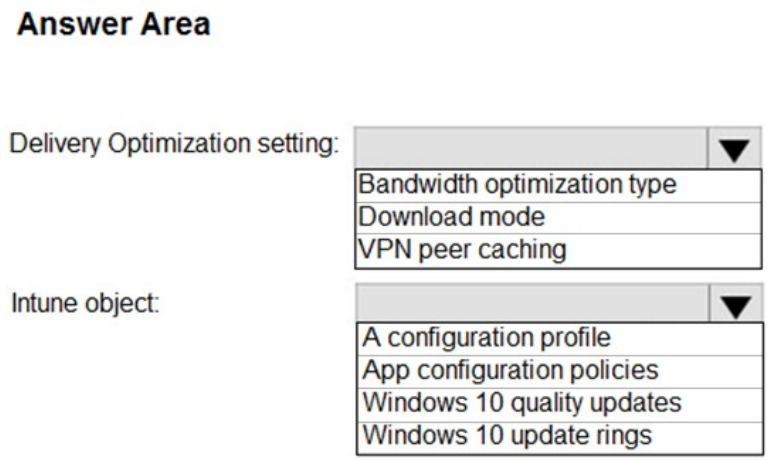
You have 100 Windows 10 devices enrolled in Microsoft Intune.

You need to configure the devices to retrieve Windows updates from the internet and from other computers on a local network.

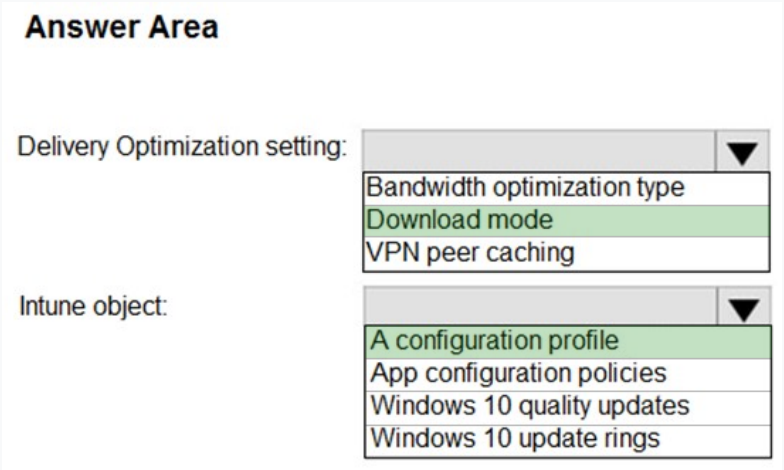
Which Delivery Optimization setting should you configure, and which type of Intune object should you create? To answer, select the appropriate options in the answer area.

NOTE: Each correct selection is worth one point.

Hot Area:




**Suggested 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

**Amir1909** 11 months, 4 weeks ago

Correct

upvoted 1 times

**Hatsapatsa** 1 year, 12 months ago

I think correct.

Download mode dictates which download sources clients are allowed to use when downloading Windows updates in addition to Windows Update servers.

https://learn.microsoft.com/en-us/windows/deployment/do/waas-delivery-optimization-reference

upvoted 1 times

**MR_Eliot** 2 years, 8 months ago

Provided answer is correct.

upvoted 1 times

Question #93 *Topic 2*

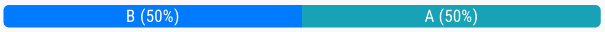
Note: This question is part of a series of questions that present the same scenario. Each question in the series contains a unique solution that might meet the stated goals. Some question sets might have more than one correct solution, while others might not have a correct solution.
After you answer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

**Suggested 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

*Community vote distribution*




**Mike666** Highly Voted 5 years ago
A is correct, as the following link describes
https://docs.microsoft.com/en-us/windows/deployment/windows-autopilot/user-driven
upvoted 17 times

**ercluff** 3 years, 4 months 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 5 years, 3 months 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 11 times

**lucidgreen** 3 years, 10 months ago
The question says user-driven.
upvoted 6 times

**ercluff** 3 years, 4 months 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 2 times

**NeilSays** Most Recent 11 months, 2 weeks ago

tested this at my home lab and it doesn't work. Answer is no

upvoted 1 times

**vanr2000** 1 year, 6 months ago

Selected Answer: B

: "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

**e635466** 1 year, 7 months ago

Selected Answer: A

Answer: A

All is explained here: https://learn.microsoft.com/en-us/mem/autopilot/user-driven

upvoted 1 times

**Anon1212** 3 years 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 4 times

**Moderator** 3 years 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** 3 years, 1 month 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** 3 years, 7 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** 3 years, 7 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** 3 years, 8 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** 3 years, 9 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** 3 years, 10 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** 3 years, 5 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 4 times

**hawkens** 3 years, 10 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** 3 years, 10 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** 3 years, 10 months ago
Do you mean "It does not get the used device in a state ready for the next user."
upvoted 1 times

**mfalkjunk** 3 years, 10 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** 3 years, 11 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** 3 years, 11 months ago
ok so after reading the 3 scenarios for this question this one probably seems the most likely..
upvoted 1 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

**Suggested 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

*Community vote distribution*
C (100%)

**Darkfire** 1 year, 3 months ago
Selected Answer: C
Defenitely C
upvoted 1 times

**Titus42** 1 year, 10 months ago
No where does it mention AD, only AAD therefore traditional GPO for roaming profiles would not be possible.
upvoted 2 times

**Shalen** 1 year, 11 months ago
C is Correct
upvoted 1 times

**CODENAME_KND** 1 year, 11 months ago
Selected Answer: C
Correct
upvoted 1 times

**NEv187** 2 years ago
Selected Answer: C
C Is correct
upvoted 2 times

**asdffail99** 2 years ago
Selected Answer: C
correct answer is C
upvoted 3 times

**M4rcintheD4rk** 2 years, 2 months ago
Selected Answer: C
ESR is the correct answer --> C
upvoted 1 times

**Henkjanarie** 2 years, 3 months ago

Selected Answer: C

Enterprise State Roaming is the correct answer - Azure AD.

upvoted 2 times

**Deric** 2 years, 3 months ago

Selected Answer: C

C - Enterprise State Roaming. This is Azure AD, not AD.

upvoted 1 times

**thuba_TD** 2 years, 3 months ago

Selected Answer: C

correct answer is C

upvoted 2 times

**MR_Eliot** 2 years, 8 months ago

Selected Answer: C

Correct answer is C

upvoted 2 times

**mathlete1083** 2 years, 8 months ago

Selected Answer: C

C for the win!

upvoted 2 times

**AVR31** 2 years, 8 months ago

Selected Answer: C

That would be C, Enterprise State Roaming.

upvoted 2 times

**RodrigoT** 2 years, 8 months ago

Wrong link and wrong answer. The correct is C. ESR.

upvoted 3 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

**Suggested 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

*Community vote distribution*
C (100%)

**Amir1909** 11 months, 4 weeks ago
Correct
upvoted 1 times

**USRobotics** 1 year, 4 months ago
**Selected Answer: C**
From Intune admin center -> iOS/iPadOS apps -> Add -> App Type: Line-of-business app
the menù provide this information:
1. Android (APK)
2. iOS (IPA)
3. macOS (.pkg)
4. Windows (.msi, .appx, .appxbundle, .msix, and .msixbundle)
upvoted 1 times

**rendog** 2 years, 1 month ago
LOB app file extrnsions:
WIN - .msi, .appx, .appxbundle, .msix, & .msixbundle
iOS - .ipa
Android - .apk
MacOS - .pkg

https://learn.microsoft.com/en-us/mem/intune/apps/apps-add
upvoted 4 times

**raduM** 2 years, 4 months ago
i stand corrected ios sorry. ipa is correct
upvoted 1 times

**raduM** 2 years, 4 months ago
https://docs.microsoft.com/en-us/mem/intune/apps/lob-apps-windows
appx all the way
upvoted 1 times

**neobahamutk** 2 years, 4 months 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 -

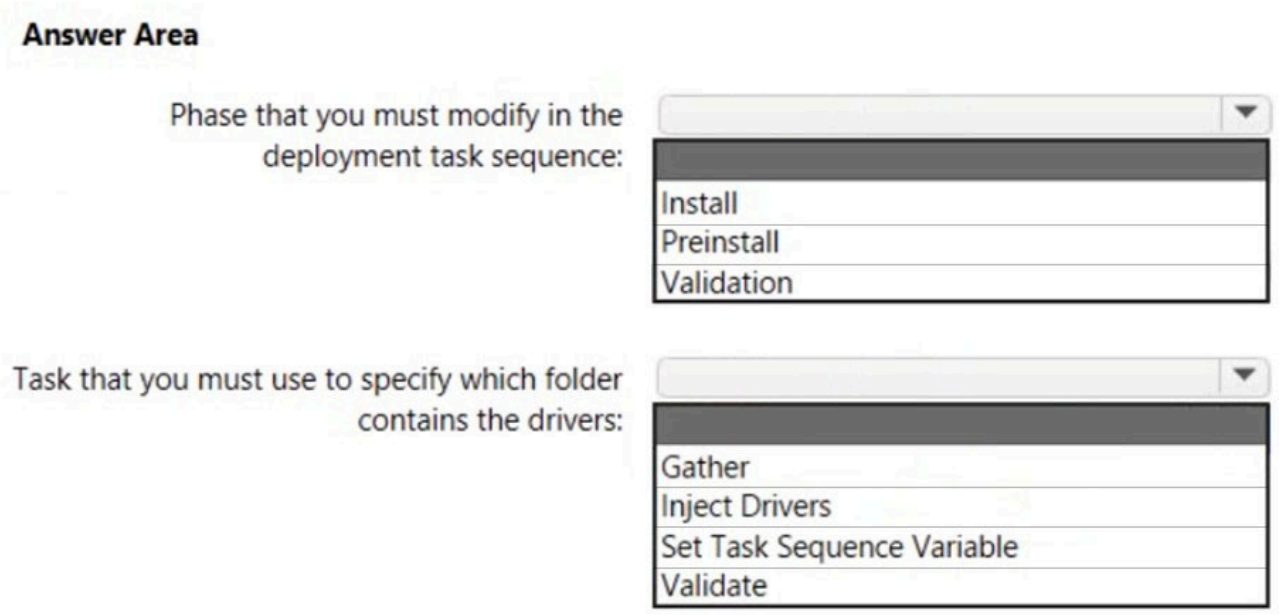
You manage a Microsoft Deployment Toolkit (MDT) deployment share named DS1. DS1 contains an Out-of-Box Drivers folder named Windows 10 x64 that has subfolders in the format of {make name}\{model name}.

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.

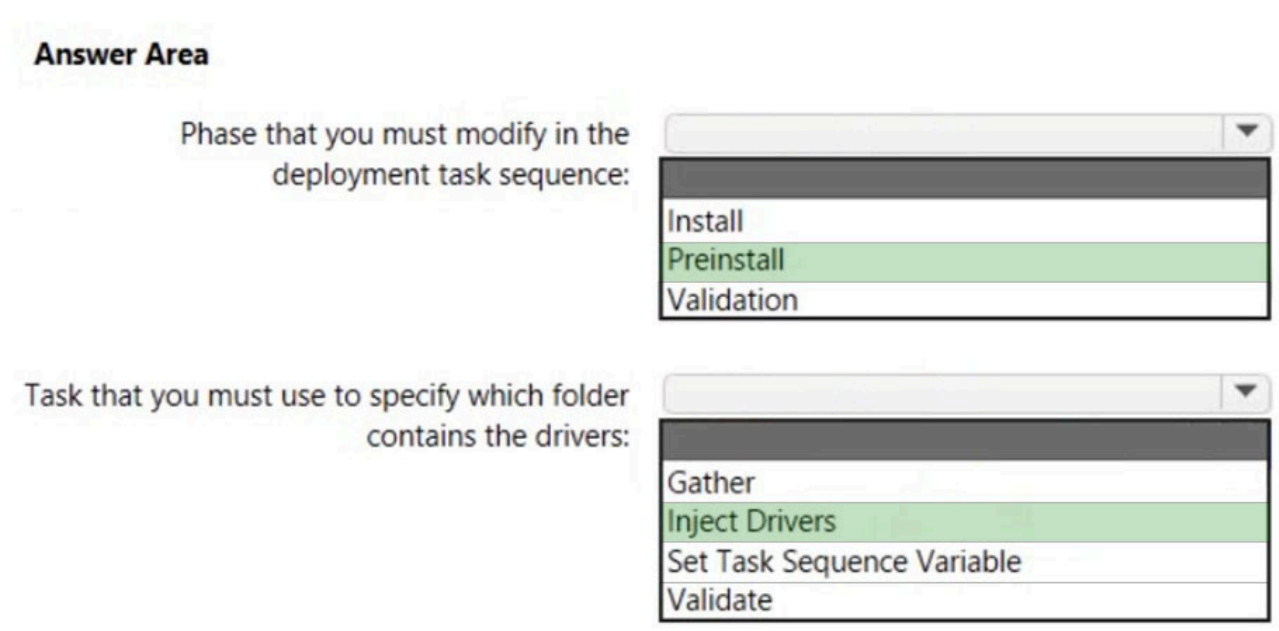
What should you do? To answer, select the appropriate options in the answer area.

NOTE: Each correct selection is worth one point.

Hot Area:




**Suggested 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

**Amir1909** 11 months, 3 weeks ago
-Preinstall
-Set Task Sequence Variable
upvoted 1 times

**Fuzm4n** 2 years, 1 month ago
Preinstall
Set Task Sequence Variable

https://learn.microsoft.com/en-us/windows/deployment/deploy-windows-mdt/deploy-a-windows-10-image-using-mdt
upvoted 1 times

**_Phiphi_** 2 years, 2 months ago
To select drivers according to the manufacturer and model, but without using profiles, use the variable "DriverGroup001" (https://learn.microsoft.com/en-us/windows/deployment/deploy-windows-mdt/deploy-a-windows-10-image-using-mdt). It is therefore necessary to create a variable before modifying 'Inject drivers'
upvoted 4 times

**daye** 2 years, 2 months ago
Should be Install not PreInstall, you are installing drivers after OS not beforehand
upvoted 3 times

**KiwE** 2 years, 2 months ago
Wrong: https://ememeye.wordpress.com/2013/01/14/injecting-drivers-based-on-target-computer-model/
upvoted 3 times

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.

**Suggested 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

*Community vote distribution*

B (100%)

**NoursBear** 12 months ago
This is talking about Powershell Support not drivers
upvoted 1 times

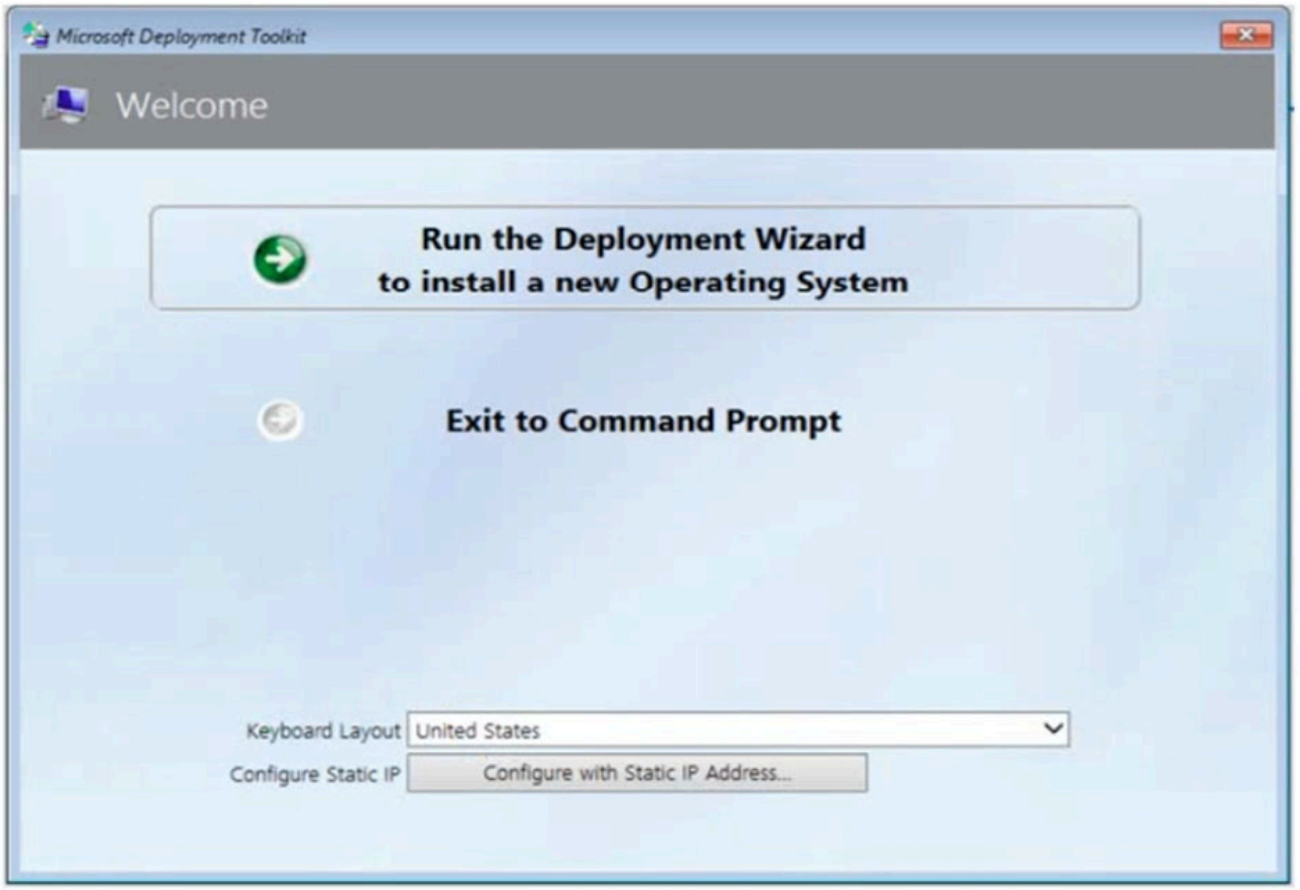
**jenraed** 2 years, 2 months ago
**Selected Answer: B**
I know this is from a forum and thus not official, but it appears the answer is correct:
B. From the Deployment Shares node, update the deployment share.

https://www.reddit.com/r/sysadmin/comments/9b916j/mdt_boot_image_best_way_to_update/
"Go to Windows PE and select the Drivers and Patches Tab and make sure you are targeting the correct platform (x86 or x64).
Select the Selection Profile you created for the PE drivers, apply your changes and update your deployment share."
upvoted 4 times

DRAG DROP -

You have a Microsoft Deployment Toolkit (MDT) server named MDT1.

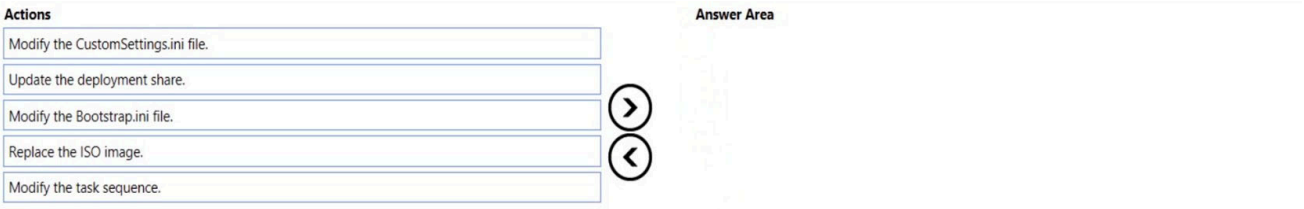
When computers start from the LiteTouchPE_x64.iso image and connect to MDT1, the welcome screen appears as shown in the following exhibit.



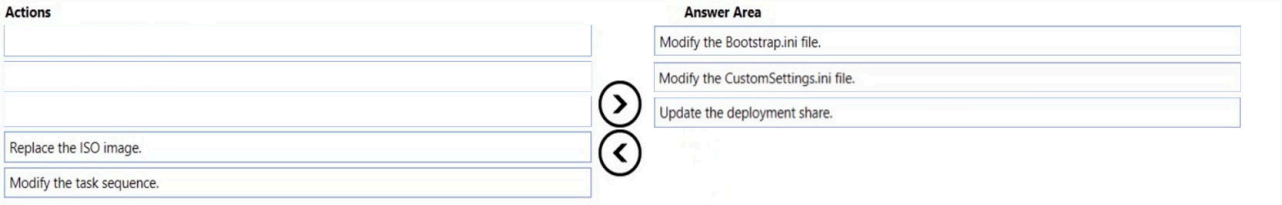

You need to prevent the welcome screen from appearing when the computers connect to MDT1.

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:




**Suggested 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

**ubiquituz** 12 months ago
nnmnmbmnvbmnv fxfccgh
upvoted 1 times

**JustJoeyhere** 1 year, 7 months ago
It is not required to add the SkipBDDWelcome=yes in customsettings.ini. Adding it to Bootstrap.ini is sufficient to hide it from the task sequence.

However, the question states that you have to select 3 answers and the other given answers are wrong hence why this answer is correct based on how the question is asked.
upvoted 1 times

**rockhound** 2 years, 3 months ago
Correct
upvoted 3 times

**Fuzm4n** 2 years, 1 month ago
Agreed.

https://www.itsupportguides.com/knowledge-base/configmgr-sccm/customising-bootstrapini-in-mdt/
upvoted 2 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:

**Answer Area**

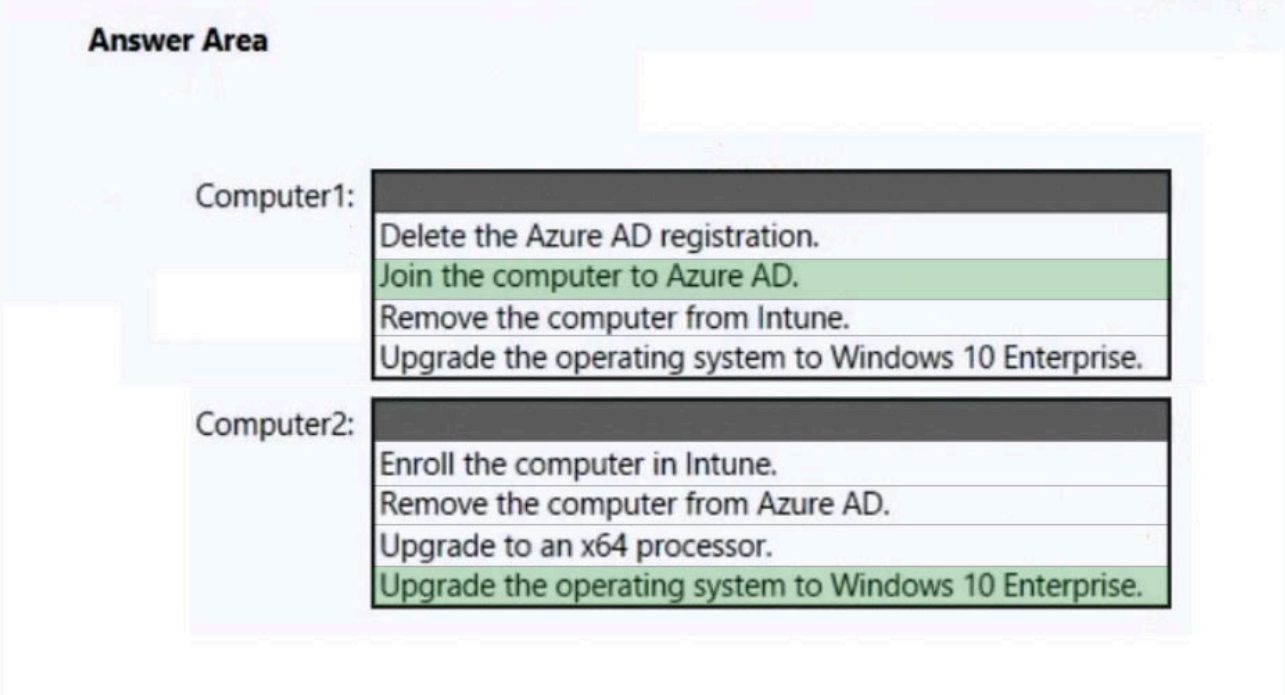
Computer1:

| |
|---|
| Delete the Azure AD registration. |
| Join the computer to Azure AD. |
| Remove the computer from Intune. |
| Upgrade the operating system to Windows 10 Enterprise. |

Computer2:

| |
|---|
| Enroll the computer in Intune. |
| Remove the computer from Azure AD. |
| Upgrade to an x64 processor. |
| Upgrade the operating system to Windows 10 Enterprise. |

**Suggested 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

**NoursBear** 12 months ago
I believe there is no correct answer for Computer 1, it needs a deployment profile, the info is probably wrong
upvoted 1 times

**e635466** 1 year, 7 months ago
Computer 1
Existing Intune devices only need to have a a new deployment profile
Can't find anything about being AD registered that could form an issue
https://www.anoopcnair.com/repurpose-existing-devices-windows-autopilot/

Computer 2 has to be upgraded. See link below for supported.
https://learn.microsoft.com/en-us/mem/autopilot/software-requirements
upvoted 2 times

**TonySuccess** 2 years, 3 months 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 4 times

**jenraed** 2 years, 3 months 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 3 times

**raduM** 2 years, 1 month ago
yes but they also need to be enrolled in intune so...
upvoted 4 times

**asturmark** 2 years, 3 months 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 4 times

**syougun200x** 2 years, 2 months ago

Something wrong with the table on the Q maybe? Com2 has to be MDM joined and Win 10 upgraded both.

upvoted 1 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**

On Server1:

- Import the Deployment Image Servicing and Management (DISM) PowerShell module.
- Import the WindowsAutopilotIntune Windows PowerShell module.
- Install the Windows Assessment and Deployment Kit (Windows ADK).
- Install the Windows Deployment Services server role.

Add to the MDT deployment share:

- Windows 10 image and package only
- Windows 10 image and task sequence only
- Windows 10 image only
- Windows 10 image, task sequence, and package

**Suggested Answer:**

**Answer Area**

On Server1:

- Import the Deployment Image Servicing and Management (DISM) PowerShell module.
- Import the WindowsAutopilotIntune Windows PowerShell module.
- Install the Windows Assessment and Deployment Kit (Windows ADK).
- Install the Windows Deployment Services server role.

Add to the MDT deployment share:

- Windows 10 image and package only
- Windows 10 image and task sequence only
- Windows 10 image only
- Windows 10 image, task sequence, and package

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** Highly Voted 2 years, 3 months ago

My picks:
-install ADK
-windows 10 image and task sequence only
upvoted 10 times

**Deric** 2 years, 3 months 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 6 times

**rendog** 2 years ago

I agree since it does state MDT is already installed (which means ADK is already installed). After doing some reading on the subject I think adding the WDS role and using this in conjunction with MDT would make the most sense for deploying WIN 10 to a group of computers (although the client computers would need to have PXE-enabled network cards for this to work so they can boot from the image specified in the WDS server options).

Steps to accompish this:
1) https://petri.com/deploy-windows-10-using-mdt-wds-part-1-create-mdt-deployment-share/
2) https://petri.com/deploy-windows-10-using-mdt-wds-part-2-install-wds-boot-pxe-client/
3) https://petri.com/deploy-windows-10-using-mdt-wds-part-3-deploy-windows-10-pxe-enabled-boot-client/
upvoted 1 times

**Meebler** 1 year, 11 months ago

In general, if you have a smaller environment and you only need to deploy Windows 10 to a limited number of computers, the ADK is a good choice. But if you have a larger environment with a significant number of computers to manage, WDS is a better choice as it provides more advanced features such as multicast deployment, PXE boot, and remote installation.
upvoted 1 times

**Amir1909** Most Recent 11 months, 4 weeks ago

- (Windows ADK)
- Windows 10 image and task sequence only
upvoted 1 times

**dlast** 1 year, 6 months ago

According to https://learn.microsoft.com/en-us/windows/deployment/deploy-windows-mdt/prepare-for-windows-deployment-with-mdt both WDS and ADK are required. Which makes this an riddle instead of question. My pick is ADK because WDS is for PXE boot which doesn't do in-place upgrades.
upvoted 1 times

**USRobotics** 1 year, 4 months ago

I agree with you. Have we any proof that the choice is correct?
upvoted 1 times

**e635466** 1 year, 7 months ago

If they now run the Windows 8.1 image then the ADK should be updates anyway. My pick

- Install ADK
- Win10 image and task sequence only

Nowhere on this site is WDS mentioned. WDS is specific to install computers over the network with PXE boot.
upvoted 1 times

**e635466** 1 year, 7 months ago

Sorry, It's a shame you can't change you comments. Here is the link:
https://learn.microsoft.com/en-us/windows/deployment/deploy-windows-mdt/upgrade-to-windows-10-with-the-microsoft-deployment-toolkit
upvoted 1 times

**Fuzm4n** 2 years, 1 month ago

WDS is for PXE booting. You can use a WinPE USB stick for MDT.

Install ADK

Win 10 image and task sequence

upvoted 2 times

**_Phiphi_** 2 years, 2 months ago

I agree with Bensrayan. It is necessary to update the ADK which is mandatory and which is related to the version of Windows to deploy

upvoted 1 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

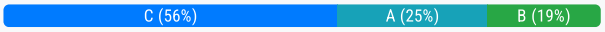
B. Subscription Activation

C. Microsoft Deployment Toolkit (MDT) and a default image of Windows 10 Enterprise

D. Windows Autopilot

**Suggested Answer:** *B*

*Community vote distribution*




**dlast** 1 year, 6 months ago

**Selected Answer: C**

C is the correct answer. Upgrade can only be done with a default image and not with a custom image, which is mentioned in A. Subscription activation only work from Windows 10 Pro to Windows 10 Enterprise. Autopilot doesn't support in-place upgrade.

upvoted 1 times

**e635466** 1 year, 7 months ago

**Selected Answer: C**

A: Setting up a SCCM environment doesn't seem like "minimize adminstrative effort" and the custom image is nonsens
B: You can't upgrade from Windows 8.1 to Windows 10 using a subscription activation -> https://learn.microsoft.com/en-us/windows/deployment/windows-10-subscription-activation
C: MDT does the job -> CORRECT ANSWER
D: Windows Autopilot only does a reimage of the device -> https://learn.microsoft.com/en-us/mem/autopilot/existing-devices

upvoted 1 times

**CODENAME_KND** 1 year, 9 months ago

**Selected Answer: C**

Correct

upvoted 1 times

**Brandon_Marlin** 1 year, 10 months ago

**Selected Answer: A**

ChatGPT thinks it's A
This is because an in-place upgrade is not supported when upgrading from Windows 8.1 Pro to Windows 10 Enterprise, so a custom image of Windows 10 Enterprise is needed. Subscription Activation is not a method for upgrading Windows, and MDT with a default image is not recommended for an in-place upgrade. Windows Autopilot is also not recommended for an in-place upgrade.

upvoted 1 times

**Raxon** 1 year, 10 months ago

**Selected Answer: C**

B. Subscription Activation ???
Correct me if I'm wrong but would that not step up a 8.1 Pro to Enterprise...

The question stated: You need to upgrade the computers to Windows 10 Enterprise by using an in-place upgrade.

Answer:
C. Microsoft Deployment Toolkit (MDT) and a default image of Windows 10 Enterprise

upvoted 1 times

**jt2214** 1 year, 10 months ago

**Selected Answer: C**

I'm voting for C

upvoted 1 times

**Meebler** 1 year, 11 months ago

The best solution to minimize administrative effort while upgrading 25 computers that run Windows 8.1 Pro to Windows 10 Enterprise by using an in-place upgrade is to use Windows Autopilot.

Windows Autopilot is a service provided by Microsoft Intune, which is included in Microsoft 365 E5 subscription. It allows you to reset, repurpose, and recover devices, as well as to perform a Windows Out-of-Box Experience (OOBE) and an in-place upgrade to Windows 10. With Windows Autopilot, you can easily enroll new Windows devices into Intune, configure settings, and automatically install business apps and data.

upvoted 1 times

**Meebler** 1 year, 11 months ago

Using Microsoft Endpoint Configuration Manager and a custom image of Windows 10 Enterprise would be more complex, as it would require a significant amount of administrative effort to create and manage the custom image, and to deploy it to the computers.

Subscription Activation is used to activate Windows 10 Enterprise on the devices, it doesn't perform the in-place upgrade.

Using the Microsoft Deployment Toolkit (MDT) and a default image of Windows 10 Enterprise would also be more complex, as it would require a significant amount of administrative effort to create and manage the deployment share, and to deploy the image to the computers.

upvoted 1 times

**ya12** 1 year, 11 months ago

Windows Autopilot upgrade only edition but not version. Custom image add migrate user date to share and back after update. In-place upgrate - only MDT.

upvoted 1 times

**dja12** 1 year, 3 months ago

Autopilot only works on Windows 10 devices, known in Azure AD.

upvoted 1 times

**Graz** 2 years ago

I Know this question is regarding upgrading from 8.1 to 10 but i found this interesting

"Subscription activation is available for qualifying devices running Windows 10 or Windows 11. You can't use subscription activation to upgrade from Windows 10 to Windows 11"

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

I can't find anything that confirms you can even do an inplace upgrade from 8.1 to 10 via a subscription activation.

upvoted 2 times

**Fuzm4n** 2 years, 1 month ago

This exam is for managing MODERN desktops. MECM is not it. I vote C.

upvoted 2 times

**raduM** 2 years, 2 months ago

subscription activation works only to go from pro to enterprise. cannot be used for in place upgrade. threfore c is the correct answer

upvoted 4 times

**AK4U_111** 2 years, 2 months ago

In-place upgrade from Windows 8.1 Pro top windows 10 Enterprise is possibler according to the link provided by AngelusNL. Therefore i also vote on C as the correct answer.

upvoted 3 times

**AngelusNL** 2 years, 2 months ago

Right Answer is C: See here https://learn.microsoft.com/en-us/windows/deployment/deploy-windows-mdt/upgrade-to-windows-10-with-the-microsoft-deployment-toolkit

upvoted 2 times

**AngelusNL** 2 years, 2 months ago

Right Answer is C: See here https://learn.microsoft.com/en-us/windows/deployment/deploy-windows-mdt/upgrade-to-windows-10-with-the-microsoft-deployment-toolkit

upvoted 2 times

**Feyenoord** 2 years, 2 months ago

Selected Answer: C

The least effort is C.
A is way to much effort.
B is only possible to upgrade from pro to Enterprise etc.
D doenst support in place upgrade.

So its C
upvoted 4 times

**syougun200x** 2 years, 2 months ago

It looks like Subs activation to me.

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

Earlier versions of Windows
If devices are running Windows 7, more steps are required. A wipe-and-load approach still works, but it can be easier to upgrade from Windows 7 Pro directly to Windows 10 Enterprise edition. This path is supported, and completes the move in one step. This method also works for devices with Windows 8.1 Pro.
upvoted 2 times

**Deric** 2 years, 3 months 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** 2 years, 3 months 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

**Graz** 2 years ago

Why no to C? According to this link, you Perform an Inplace Upgrade using MDT and using a deafault image is the least amount of effort.

https://learn.microsoft.com/en-us/windows/deployment/deploy-windows-mdt/upgrade-to-windows-10-with-the-microsoft-deployment-toolkit
upvoted 2 times

**thuba_TD** 2 years, 3 months ago

Selected Answer: B

answer is correct B
https://docs.microsoft.com/en-us/windows/deployment/windows-10-subscription-activation
upvoted 3 times

**TonySuccess** 2 years, 3 months 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** 2 years, 3 months 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

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**

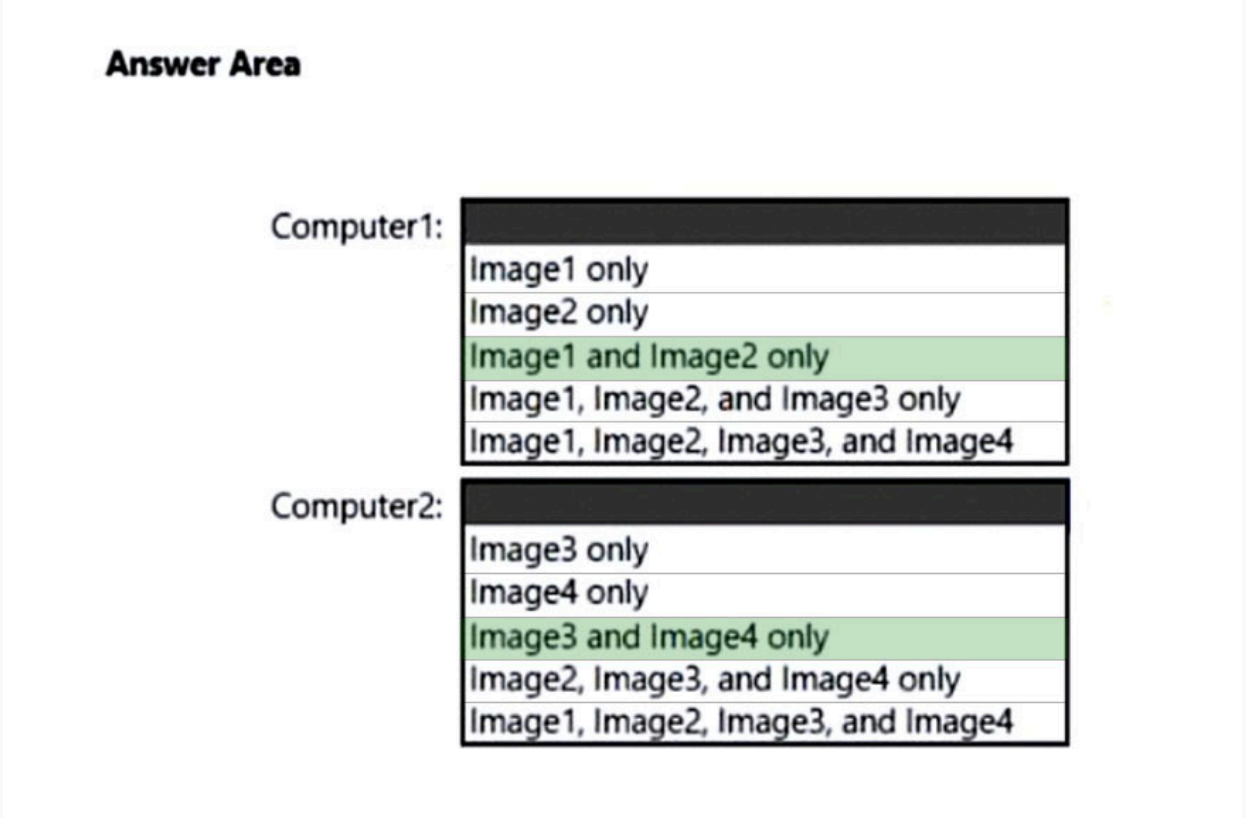
Computer1:

- 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

**Suggested 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

**_Phiphi_** Highly Voted 2 years, 2 months ago
Cannot Upgrade from x86 to x64 and cannot UPGRADE with custom image (https://learn.microsoft.com/en-us/windows/deployment/windows-10-deployment-scenarios)
- Image 2 only
- Image 4 only
upvoted 19 times

**raduM** 2 years, 2 months ago
correct image 2 and image 4
upvoted 2 times

**raduM** 2 years, 2 months ago
https://learn.microsoft.com/en-us/windows/deployment/deploy-windows-mdt/upgrade-to-windows-10-with-the-microsoft-deployment-toolkit
i stand corrected. you cannot use a custom image for in place upgrade.
upvoted 1 times

**raduM** 2 years, 2 months ago
"Because existing applications are preserved through the process, the upgrade process uses the standard Windows installation media image (Install.wim); custom images are not needed and cannot be used because the upgrade process is unable to deal with conflicts between apps in the old and new operating system. (For example, Contoso Timecard 1.0 in Windows 7 and Contoso Timecard 3.0 in the Windows 10 image.)"

although on the x86 image you do not have any applications installed so no conflicts can appear. thus a valid for the x86 a solotuion might be image 3 and 4. But i nerver saw somebody do an in-place upgrade like this
upvoted 2 times

**SR1991** 1 year, 6 months ago

Correct anwser, https://learn.microsoft.com/en-us/windows/deployment/deploy-windows-mdt/upgrade-to-windows-10-with-the-microsoft-deployment-toolkit

upvoted 1 times

**AK4U_111** Most Recent 2 years, 2 months ago

Answer is correct. Cannot upgrade from x86 to x64.

upvoted 1 times

**AK4U_111** 2 years, 2 months ago

After some research, I have to with -Phiphi on this one

upvoted 1 times

**neobahamutk** 2 years, 3 months ago

Correct.

upvoted 1 times

**rockhound** 2 years, 3 months 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:

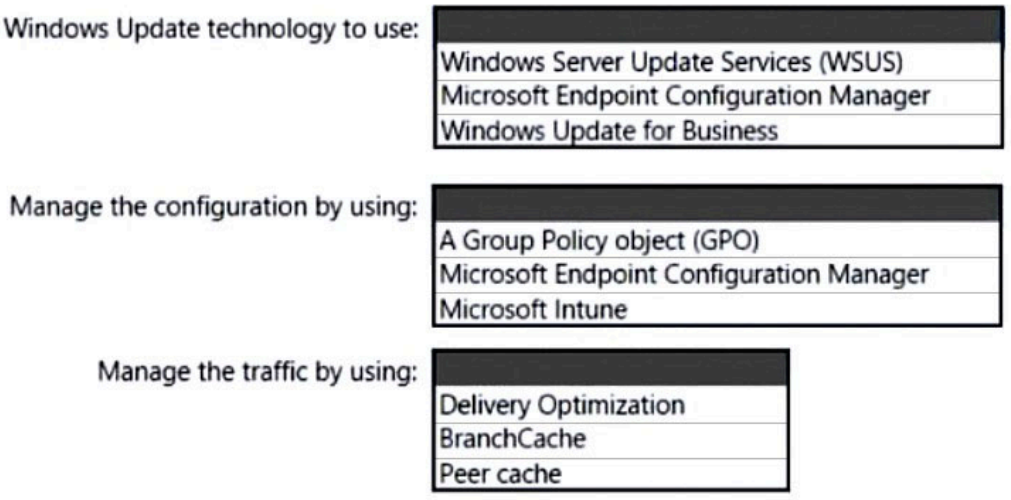
- ✑ The configuration must be managed from a central location.
- ✑ Internet traffic must be minimized.
- ✑ Costs must be minimized.

How should you configure Windows Update? To answer, select the appropriate options in the answer area.

NOTE: Each correct selection is worth one point.

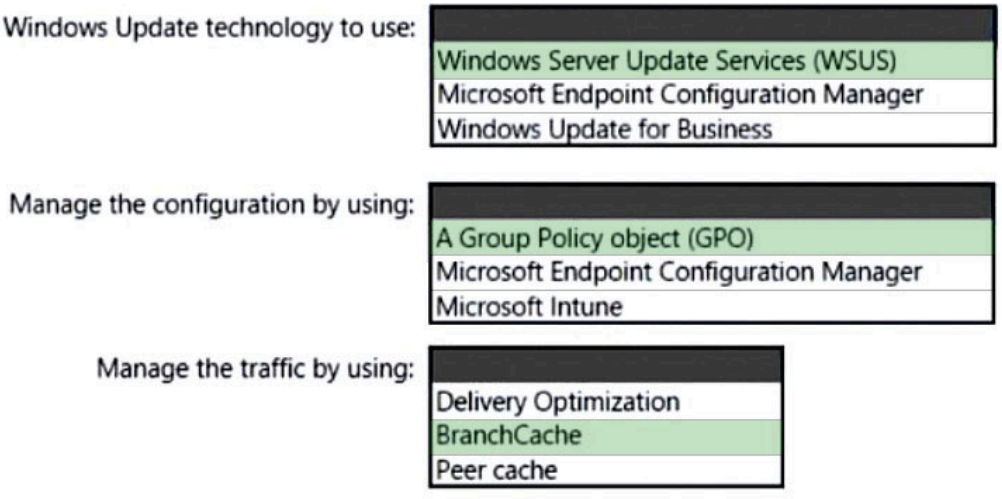
Hot Area:

**Answer Area**




**Suggested Answer:**

**Answer Area**




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 2 years, 4 months ago
device is joined to azure ad not to activtive directory. so solution is update for business, intune, delivery optimization
upvoted 36 times

**rockhound** 2 years, 3 months ago
correct
upvoted 2 times

**bensrayan** Highly Voted 2 years, 3 months ago
The answer given is wrong.. ! so should be :
- windows update for business and not WSUS (there is no server!)
- intune
-delivery optimization
upvoted 18 times

**Amir1909** Most Recent 12 months ago
Windows update for Business
Microsoft Intune
Delivery Optimization
upvoted 1 times

**thewavyman** 1 year, 4 months ago
My jaw dropped when I saw this.. this is just pathetic. Great site but sheesh, this is horrible.
No servers = No WSUS
upvoted 1 times

**junior6995** 1 year, 8 months ago
This type of question aged pretty bad, in mid 2023 I will go for:

- Windows Update for Business
- Intune
- Delivery Optimization
upvoted 6 times

**venkat284** 1 year, 9 months ago
ITS CLEARLY MENTIONED NO SERVERS SO ANSWERS ARE WRONG
upvoted 1 times

**ExamTopics1_EIS** 1 year, 9 months ago
Can we say the answers are a 'SOUP SANDWICH' - worthless. NO SERVERS was stated... COST... so, update for business, Intune, Delivery... simple.
upvoted 1 times

**Titus42** 1 year, 10 months ago
Who is allowing this to even be on here, there are no servers!! NM no mention of local AD, this is just terrible.

upvoted 1 times

**Meebler** 1 year, 11 months ago

Update for Busines, Intune, Delivery Optimization

In general, Windows Update for Business is considered to be a more cost-effective solution as it is built into Windows 10 and does not require any additional infrastructure or licenses. It allows for easy management of updates and enables IT administrators to delay or pause updates for a specific period of time.

On the other hand, WSUS requires a Windows Server to be set up and configured to manage updates. It also requires additional infrastructure and resources, such as storage and network bandwidth, as well as ongoing maintenance and management. Additionally, WSUS requires an additional license if you have a Windows Server that is not covered by Software Assurance.

In summary, Windows Update for Business is a less expensive solution, as it does not require additional infrastructure or licenses, while WSUS is more expensive as it requires additional infrastructure and ongoing maintenance and management.

upvoted 2 times

**AyoR32** 1 year, 12 months ago

Are these the official answers or is it a mistake on the part of the person who updated the questions on this site?

upvoted 1 times

**Graz** 2 years ago

Another lousy answer

upvoted 1 times

**AyoR32** 1 year, 12 months ago

Are these the official answers or is it a mistake on the part of the person who updated the questions on this site?

upvoted 1 times

**DDHP7** 2 years ago

Is this a trick questions giving out wrong answers

upvoted 2 times

**devilcried** 2 years, 1 month ago

I will go for:
- windows update for business
- intune
-delivery optimization
No AD, no centralized GPO management, so you have to update the local security policy of every client with no centralized way. With Windows for Bussiness and Intune you have the centralized way. With Delivery Optimization you can comply with "Internet traffic must be minimized" (There is configuration profile to Intune for that)

upvoted 2 times

**raduM** 2 years, 2 months ago

also for wsus you would require servers so...

upvoted 2 times

**Vileita** 2 years, 2 months ago

I think that we should focus on "Internet traffic must be minimized". That's why it's not Windows update for business. I'm just guessing.

upvoted 1 times

**AK4U_111** 2 years, 2 months ago

ADDS is not mentioned here so WSUS is out of the question. As for #2, isn't intune a part of the Microsoft Endpoint Configuration Manager? As for #3 i would say Delivery Optimization.

upvoted 2 times

**Altheus** 2 years, 2 months ago

This scenario doesn't have servers so how exactly are we supposed to deploy wsus?

upvoted 2 times

**DaZa5** 2 years, 1 month ago

Wrong. AD is not mandatory to configure WSUS. You can use local Group Policy settings to set a client windows 10 as WSUS server without the need of a domain. How can you minimize the cost and internet traffic with your solution? The provided answers are corrects.

https://learn.microsoft.com/en-us/answers/questions/65486/wsus-without-active-directory.html

upvoted 1 times

**[Removed]** 1 year, 6 months ago

Server is required for WSUS https://learn.microsoft.com/en-us/windows-server/administration/windows-server-update-services/plan/plan-your-wsus-deployment#11-review-considerations-and-system-requirements

upvoted 1 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

**Suggested Answer:** *A*
Reference:
https://docs.microsoft.com/en-us/windows/deployment/windows-deployment-scenarios-and-tools

*Community vote distribution*
B (100%)

**raduM** Highly Voted 2 years, 4 months ago
i think the answer is no. you cannot do in place upgrade with wds
upvoted 6 times

**bensrayan** 2 years, 3 months ago
Correct!
upvoted 1 times

**AngelusNL** 2 years, 2 months ago
You can do an In-Place Upgrade with WDS but not when you start it from PXE
https://learn.microsoft.com/en-us/windows/deployment/deploy-windows-mdt/upgrade-to-windows-10-with-the-microsoft-deployment-toolkit
upvoted 1 times

**raduM** 2 years, 2 months ago
ok. so where in this article do you see wds? becasue it is not specified in this article
upvoted 1 times

**dlast** Most Recent 1 year, 7 months ago
Selected Answer: B
No WDS is only for clean install.
upvoted 1 times

**JePe** 1 year, 8 months ago
No, this solution does not meet the goal. Adding Windows 10 startup and install images to a WDS server and initiating the Windows 10 installation using PXE boot will result in a clean install of Windows 10 on the computer.

To perform a Windows 10 in-place upgrade on Computer1, you need to use the Windows 10 installation media, such as a DVD or USB drive, to upgrade the existing Windows 8.1 installation on the computer. You can either download the Windows 10 ISO file from Microsoft's website or use the Media Creation Tool to create the installation media.

Once you have the installation media, you can insert the DVD or USB drive into the computer, run the setup.exe file, and select the option to upgrade the existing installation of Windows. This will perform an in-place upgrade of Windows 8.1 to Windows 10, preserving all user data, settings, and installed applications.
upvoted 2 times

**jt2214** 1 year, 10 months ago

Selected Answer: B

No In place upgrade from PXE

upvoted 1 times

**Shalen** 1 year, 10 months ago

Selected Answer: B

you doing an in-place upgrade, this can't be done via PXE

upvoted 2 times

**AyoR32** 1 year, 12 months ago

Are these the official answers or is it a mistake on the part of the person who updated the questions on this site?

upvoted 1 times

**cbjorn8931** 2 years, 1 month ago

Using WDS with PXE is a image file in which custom images are not used for in-place upgrades. So the answer is B

upvoted 1 times

**geggio** 2 years, 2 months ago

wrong. for me no

upvoted 2 times

**DaZa5** 2 years, 2 months ago

Correct. The "in-place upgrade" isn't just the media creation tool of Microsoft.

upvoted 1 times

**Fuzm4n** 2 years, 1 month ago

Bro, did you fail the test? All the comments I read from you are wrong.

upvoted 3 times

**DaZa5** 2 years, 1 month ago

Bro, all your answer is only your opinion without any prove. Motivate your reason please or your comment is useless.

upvoted 1 times

**JB_** 1 year, 11 months ago

so you did fail

upvoted 1 times

**DaZa5** 2 years, 1 month ago

The answer is wrong but only because you can't start a WDS in-place upgrade from PXE as AngelusNL said. You can do an In-Place Upgrade with WDS.

https://learn.microsoft.com/en-us/windows/deployment/deploy-windows-mdt/upgrade-to-windows-10-with-the-microsoft-deployment-toolkit

upvoted 1 times

**Deric** 2 years, 3 months ago

Selected Answer: B

Correct answer is B

upvoted 1 times

**geggio** 2 years, 3 months 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

**Suggested 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

*Community vote distribution*


**daye** Highly Voted 2 years, 2 months ago
guys, are you sure is it able to run an In Place Upgrade from PXE? I guess the answer is NO. This procedure may be right if you run the setup.exe from network share directly from OS rather than PXE.
upvoted 13 times

**AngelusNL** 2 years, 2 months ago
Exactly, the crux here is starting from PXE
upvoted 4 times

**xian05** 2 years ago
It's starting from Windows PE (WinPE), not PXE.
Doesn't that change the answer to Yes?
upvoted 1 times

**DaZa5** 2 years, 2 months ago
I agree. This is not the right process.
upvoted 4 times

**sbermejor** Most Recent 1 year ago
YES
You can do it booting the computer from WinPE O.S. and from the command prompt running the windows exe file on the shared resourse.
https://www.youtube.com/watch?v=itNNACsk5nY
upvoted 1 times

**3dk1** 1 year, 7 months ago
Selected Answer: B
It's No - the only way to do an in-place upgrade from 8.1 to 10 is by running setup.exe from the booted 8.1 client. You cannot do it in a preboot environment (even if you are selecting setup.exe from a network share).
upvoted 2 times

**dlast** 1 year, 7 months ago
Selected Answer: B
Answer is correct silly to run setup.exe from WinPE and Microsoft doesn't support running it even from a network share (which technically would work when you run it from the Windows 8.1 Windows environment). This question was also in MD-100

upvoted 1 times

**ExamTopics1_EIS** 1 year, 9 months ago

**Selected Answer: A**

No... you run it from withing 8.1... not pxe boot.

upvoted 1 times

**jt2214** 1 year, 10 months ago

**Selected Answer: B**

I vote B.

upvoted 1 times

**JimmyC** 2 years, 1 month ago

**Selected Answer: B**

Come on, you can't run setup.exe via PXE, that is silly

upvoted 4 times

**xian05** 2 years ago

It's starting from Windows PE (WinPE), not PXE.

Doesn't that change the answer to Yes?

upvoted 1 times

**Fuzm4n** 2 years, 1 month ago

daye and cbjorn8931 is right. Can't do it from PE or PXE. Run the setup.exe from the OS.

Answer is No.

upvoted 3 times

**xian05** 2 years ago

Windows PE supports the following:

Networking, including connecting to file servers using TCP/IP and NetBIOS over TCP/IP via LAN.

https://learn.microsoft.com/en-us/windows-hardware/manufacture/desktop/winpe-intro?view=windows-11

upvoted 1 times

**cbjorn8931** 2 years, 1 month ago

Correct! You can't run in-place upgrade through PXE or PE environment. Windows PE is used for system restore and troubleshooting the pc for boot errors and etc. There are no options for in place upgrade.

upvoted 1 times

**xian05** 2 years ago

Windows PE supports the following:

Networking, including connecting to file servers using TCP/IP and NetBIOS over TCP/IP via LAN.

https://learn.microsoft.com/en-us/windows-hardware/manufacture/desktop/winpe-intro?view=windows-11

upvoted 1 times

**TonySuccess** 2 years, 3 months ago

**Selected Answer: A**

Mod please sort these questions out

upvoted 3 times

**RADYN** 2 years, 3 months ago

**Selected Answer: A**

A for me

upvoted 2 times

**Deric** 2 years, 3 months ago

**Selected Answer: A**

A is correct.

upvoted 2 times

**thuba_TD** 2 years, 3 months ago

**Selected Answer: A**

a is the correct answer.

upvoted 1 times

**raduM** 2 years, 4 months 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?

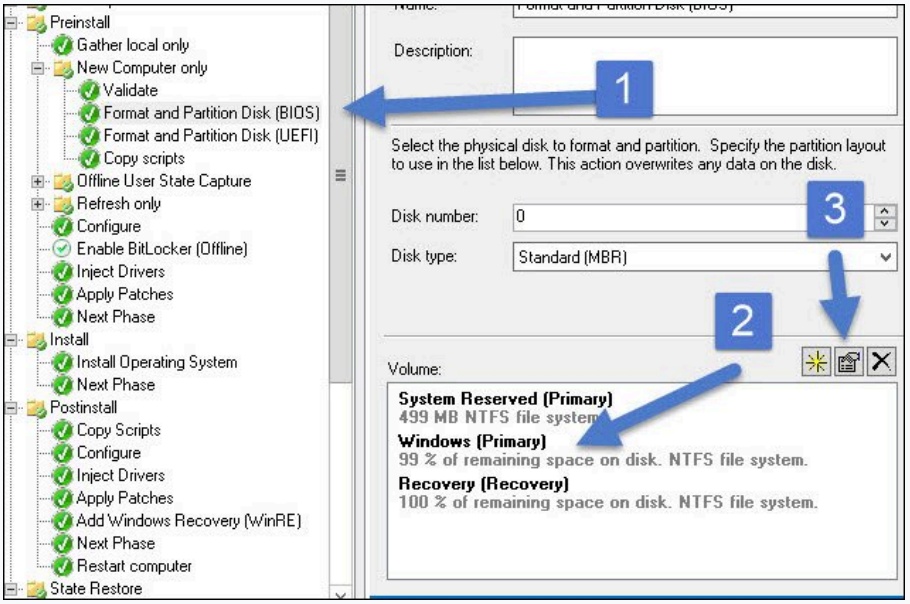
A. Initialization

B. Install

C. PostInstall

D. Preinstall

**Suggested 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/

*Community vote distribution*
D (100%)

**Amir1909** 11 months, 4 weeks ago
Correct
upvoted 1 times

**DaZa5** 2 years, 1 month ago
**Selected Answer: D**
Correct
upvoted 1 times

**Fuzm4n** 2 years, 1 month ago
**Selected Answer: D**
Answer provided is correct.
upvoted 1 times

**neobahamutk** 2 years, 3 months ago

Correct.

upvoted 2 times

**Deric** 2 years, 3 months ago

Agreed.

upvoted 1 times

Question #107 *Topic 2*

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<br>Read: Group1 |
| Image3 | x86 | Full control: Administrators, WDSServer<br>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). | ○ | ○ |

**Suggested 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.

**AliNadheer** Highly Voted 1 year, 10 months ago
this is the same question as in MD-100 Question #: 39 Topic #: 4
the answer there is No for all, i tend to agree with that. because of permission issues, wds has no permission on image 2 and user 1&2 need read and write.
upvoted 5 times

**NoursBear** Most Recent 12 months ago
According to Microsoft, the WDSServer group needs to have full control permissions on the folder that contains the images as well as its subfolders.
upvoted 1 times

**NoursBear** 12 months ago
furthermore, there is only a x86 boot image, so for x64 that is out of the window
upvoted 1 times

**SR1991** 1 year, 6 months ago
I think all is no.
1. Not part of the group
2. Can not download 64 bit from 32 bit.
3. Could if the premission was set on change en not on read.
upvoted 1 times

**dlast** 1 year, 7 months ago
Should by NO, NO, NO, because there is not x64 boot image only x86. It will require the boot files from the x64 boot image to be able to perform a pxe boot. See also same question for MD-100 https://www.examtopics.com/discussions/microsoft/view/64514-exam-md-100-topic-4-question-39-discussion/
upvoted 2 times

**Dnyc** 1 year, 10 months ago
N, N, Y
1: N because no permission to share, and x86 boot image (cannot install 64 bit OS from 32 bit WinPE)
2: N (cannot install 64 bit OS from 32 bit WinPE)
3: Y (booted to x86 winPE and installing x86 image which is allowed on 64 bit hardware)
upvoted 2 times

**TheRealKobeVH** 1 year, 10 months ago
It is N - Y - Y
1 = N - User 1 doesn't have access to image 1
2 = Y - User has access and is correct architecture
3 = Y - x86 (a 32-bit system) installs on x64 CPU architecture without a problem.
upvoted 1 times

**grammetje84** 1 year, 11 months ago
To my knowledge, applying an x64 image with an x86 boot image is impossible. x64 boot image you can only apply x64 images and x86 boot image only x86 images. So, N/N/Y.
upvoted 2 times

**BRoald** 2 years ago
1 = N - User 1 does not have access to Image 1
2 = Y - User 1 does have access to image 2 (user 1 = group 1 and group 1 is member off image 2)
3 = Y - User 2 is member of Image 3

Am i correct?
upvoted 1 times

**Fuzm4n** 2 years, 1 month ago
I'm going to go N, N, Y. Users don't have access to Image 1, WDSServer group does not have access to Image 2, and although not ideal, an x86 image should work on an x64 machine.
upvoted 2 times

**rendog** 2 years, 1 month ago

Agreed

upvoted 1 times

**AK4U_111** 2 years, 2 months ago

If the reason that Q1 is N is because neither Group1 nor Group 2 have access to this image, wouldn't this apply to the Q2+3 and the answer would be be N/N/N? Since group 1+2 only have read permissions for Image2+3?

Thanks in advance. Any help is greatly appreciated!

upvoted 3 times

**raduM** 2 years, 2 months ago

normaly if it is shared with read user can also execute if ntfs is not modified.

upvoted 1 times

**SR1991** 1 year, 6 months ago

You are wrong. You need the change premission for that.

upvoted 1 times

**DragonSlayer848** 2 years, 4 months ago

Shouldn't it be No Yes No? x86 version will not work on a 64bit computer right>

upvoted 3 times

**raduM** 2 years, 4 months ago

wrong. 32 bit works on 64 bit. the other way around it does not work

upvoted 5 times

**Deric** 2 years, 3 months ago

It will work, it's just not ideal / wise. It will install fine though.

upvoted 1 times

HOTSPOT -

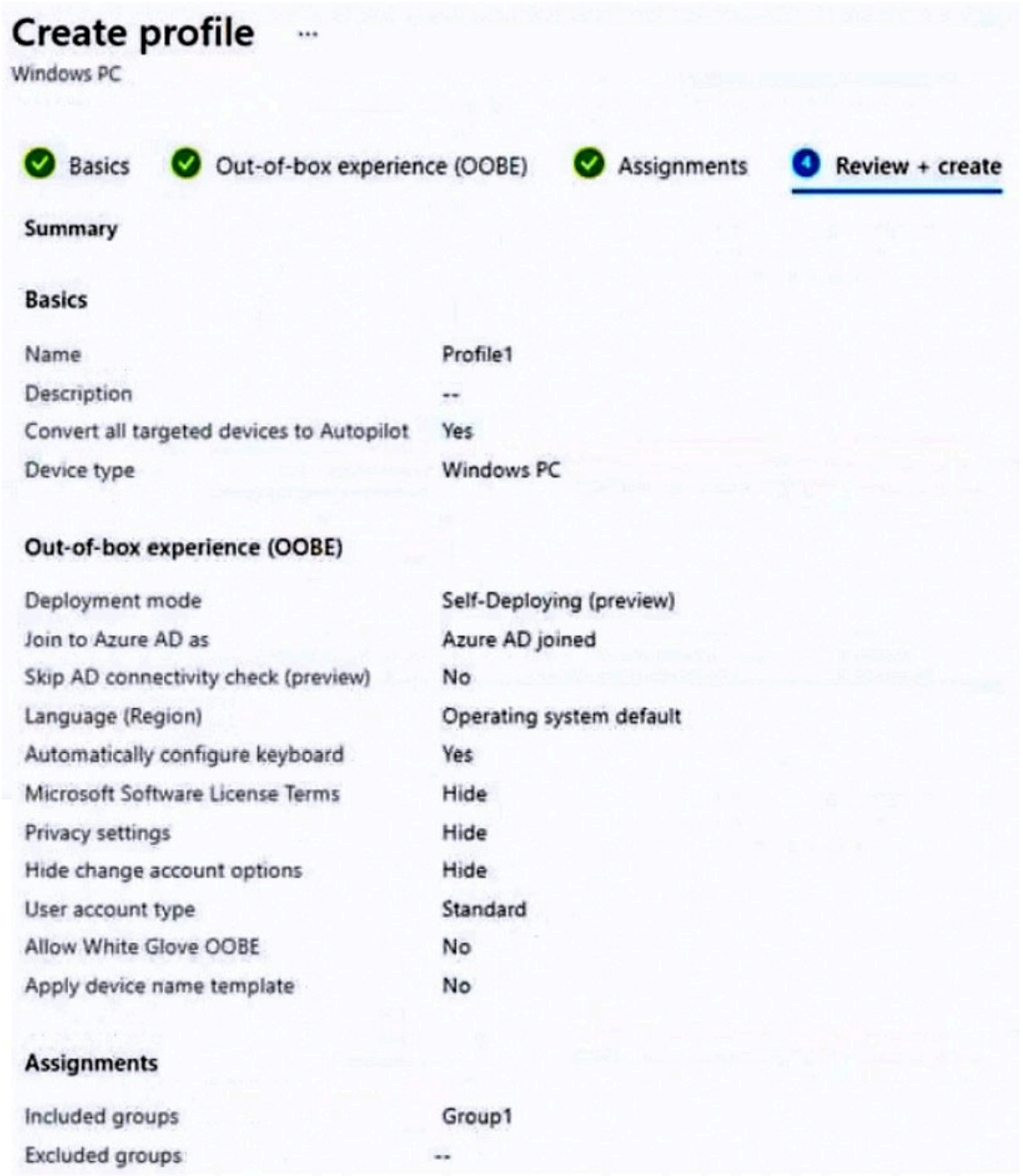
You have an Azure Active Directory (Azure AD) tenant named contoso.com that contains the devices shown in the following table.

| 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 | ○ | ○ |

**Suggested 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

**Amir1909** 11 months, 4 weeks ago

Correct

upvoted 1 times

**RAJKPB** 1 year, 4 months ago

Its Self Deploying mode, So only enrolled to Intune can Convert the device as Autopilot and run Profile so NNY
upvoted 1 times

**Feyenoord** 2 years, 1 month ago
Nested groups are not supported. Windows 8.1 is not supported. So for me its, N, N, Y
upvoted 2 times

**_Phiphi_** 2 years, 2 months ago
I think it's no for everything, because the mode is 'self-deploying' and the keyboard is on 'Yes'. So no OOBE except for Wifi.
(https://learn.microsoft.com/en-us/mem/autopilot/self-deploying)
upvoted 1 times

**daye** 2 years, 2 months ago
Guys, IMHO, forgot about the nested groups. One requirement to run Autopilot is register it as Autopilot devices with its hash id. Nowadays, it can be done as well with the "convert all targeted devices in Autopilot devices" within the configuration profile, and this setting is enabled but the device must be enrolled in the MDM, so:

1. NO, because it's W8.1 and the device is not currently enrolled therefore is not registered as Autopilot Device
2. NO, because is not currently enrolled, therefore is not registered as Autopilot Device
3. YES, because it's a W10 and it will registered as Autopilot Device.

1. N. Because it's W8.1 and it cannot be applied as autopilot directly and also
upvoted 2 times

**Mage10** 2 years, 3 months 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 2 times

**geggio** 2 years, 3 months ago
no
y
y
upvoted 2 times

**bensrayan** 2 years, 3 months 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
upvoted 4 times

**asturmark** 2 years, 3 months ago
I think the correct answer is:
1. Yes, it will be deployed (Azure AD join is not a requirement, is something Autopilot does)
2. No, because is a nested group
3. Yes
upvoted 1 times

**AK4U_111** 2 years, 2 months ago
Windows 8.1 is not supported by Autopilot
upvoted 3 times

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

**Suggested 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

*Community vote distribution*
A (100%)

**Amir1909** 11 months, 4 weeks ago
Correct
upvoted 1 times

**JMF04** 1 year, 11 months ago
**Selected Answer: A**
Correct A
upvoted 1 times

**Deric** 2 years, 3 months ago
**Selected Answer: A**
Correct, A
upvoted 1 times

**raduM** 2 years, 4 months 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:

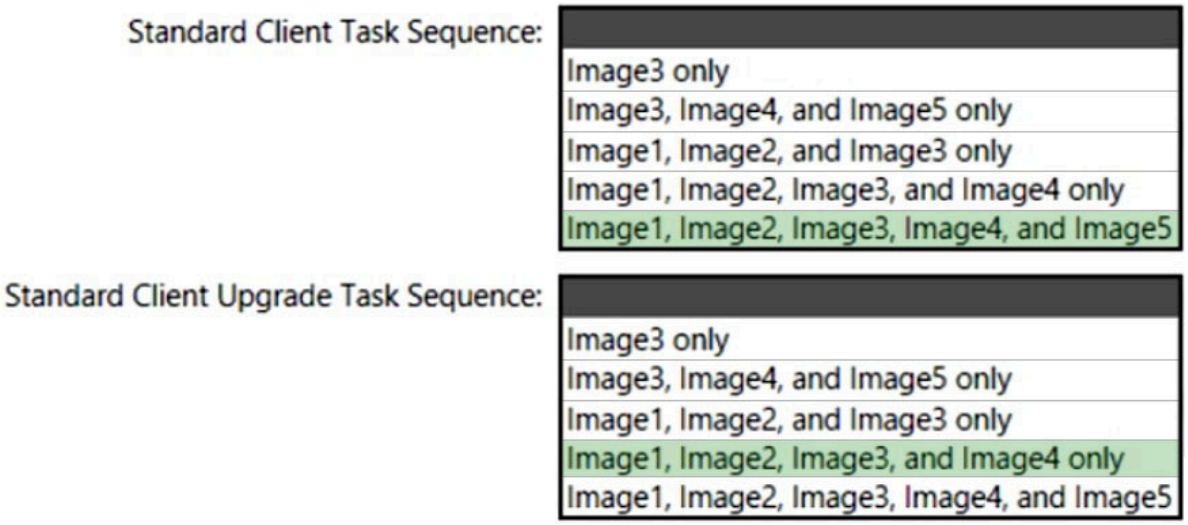
- Image3 only
- Image3, Image4, and Image5 only
- Image1, Image2, and Image3 only
- Image1, Image2, Image3, and Image4 only
- Image1, Image2, Image3, Image4, and Image5

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

**Suggested Answer:**

**Answer Area**




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

**Amir1909** 11 months, 4 weeks ago
- image1,2,3,4 and 5
- image1,2 and 3 only
upvoted 1 times

**Fedexxx92** 2 years, 1 month ago
You can't use a custom image, even if it has no additional applications installed:

In-place upgrade differs from computer refresh in that you can't use a custom image to perform the in-place upgrade. In this article, we'll add a default Windows 10 image to the production deployment share specifically to perform an in-place upgrade.

https://learn.microsoft.com/en-us/windows/deployment/deploy-windows-mdt/upgrade-to-windows-10-with-the-microsoft-deployment-toolkit
upvoted 4 times

**Fedexxx92** 2 years, 1 month ago
So the answer:
Standard Client Task Sequence: Image1,Image2, Image3, Image4 and Image5
Standard Client Upgrade Task Sequence: Image1,Image2 and Image3 only
upvoted 9 times

**DaZa5** 2 years, 1 month ago
Why are you talking about In-Place Upgrade? I don't see the reference on the question.
Below, in the link, I can see different paragraph about standard and in-place upgrade.
Can you help me to understand your opinion?

https://learn.microsoft.com/en-us/windows/deployment/deploy-windows-mdt/deploy-a-windows-10-image-using-mdt
upvoted 1 times

**JN_311** 2 years, 1 month ago

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.
Check under Task Sequence Templates: https://learn.microsoft.com/en-us/windows/deployment/deploy-windows-mdt/get-started-with-the-microsoft-deployment-toolkit
upvoted 2 times

**Hkayak** 2 years, 1 month ago

First one is correct, but the second one should only be image 1, 2 and 3 because you can't upgrade using custom image.
upvoted 3 times

Question #111 *Topic 2*

You have a Windows 10 device named Computer1 enrolled in Microsoft Intune.

You need to configure Computer1 as a public workstation that will run a single customer-facing, full-screen application.

Which template should you use to create a configuration profile for Computer1 in the Microsoft Endpoint Manager admin center?

A. Kiosk

B. Device restrictions

C. Shared multi-user device

D. Endpoint protection

**Suggested Answer:** *A*

*Community vote distribution*

A (100%)

**AliNadheer** 1 year, 10 months ago

**Selected Answer: A**

what a difficult question..

upvoted 2 times

**3dk1** 1 year, 7 months ago

my head hurt after answering this question

upvoted 1 times

Question #112 *Topic 2*

HOTSPOT
-

You have a Microsoft Deployment Toolkit (MDT) solution that is used to manage Windows 10 deployment tasks.

MDT contains the operating system images shown in the following table.

| Name | Description |
|---|---|
| Image1.wim | Custom-built Windows 10 image that has preinstalled custom apps |
| Image2.wim | Custom-built Windows 10 image without apps |
| Install.wim | Default Windows 10 image |

You need to perform a Windows 10 in-place upgrade on several computers that run Windows 8.1.

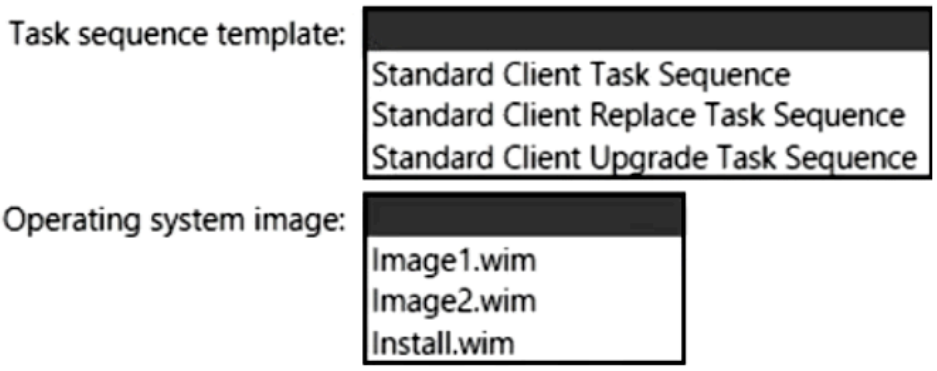
From the Deployment Workbench, you open the New Task Sequence Wizard.

You need to identify which task sequence template and which operating system image to use for the task sequence. The solution must minimize administrative effort.

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

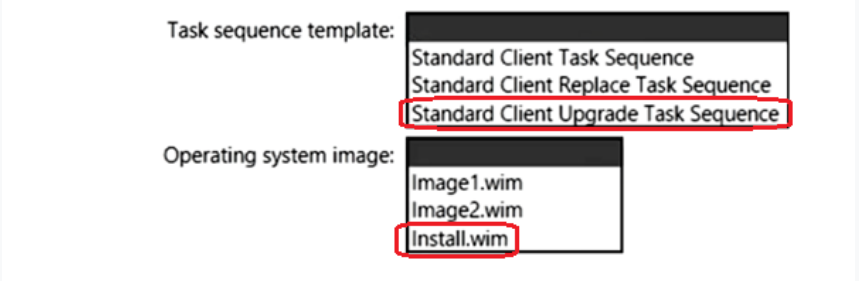
NOTE: Each correct selection is worth one point.

**Answer Area**




**Suggested Answer:**

**Answer Area**



**Amir1909** 11 months, 4 weeks ago

Correct

upvoted 1 times

**JustJoeyhere** 1 year, 7 months ago

Answer is correct. You can't perform an upgrade with custom images.

upvoted 1 times

**Hatsapatsa** 1 year, 11 months ago

Seems correct, can't upgrade with Custom image.

upvoted 4 times

Question #113 *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. From Windows 8.1 on Computer1, you run setup.exe from the network share.

Does this meet the goal?

A. Yes

B. No

**Suggested Answer:** *B*

*Community vote distribution*

A (75%) B (25%)

**SR1991** 1 year, 5 months ago

My anwser is no, if you want to do it from a sbare, it May not be part of Azure

https://learn.microsoft.com/en-us/windows-server/get-started/perform-in-place-upgrade

upvoted 1 times

**dlast** 1 year, 6 months ago

**Selected Answer: B**

This is technically possible but Microsoft wants you to choose MDT in these series of questions. Which MDT there is more flexibility to use tools as scanste and loadstate to keep your user configuration.

upvoted 1 times

**jester123** 1 year, 9 months ago

**Selected Answer: A**

If you launch setup.exe from a share it will mount on the local PC and run

upvoted 1 times

**dawnbringer69** 1 year, 9 months ago

**Selected Answer: A**

As per MD-100 Question 39 Topic 4
From Official MS course : "Upgrade
After evaluating your computer requirements, and backing up your data and personal settings, you are ready to perform the actual upgrade. To perform the upgrade, run the Windows 10 installation program (setup.exe) from the product DVD, removable media, or a network share." so answer is YES.

I have personally done this several times in my work environment. It is verified.

upvoted 2 times

**jt2214** 1 year, 10 months ago

looks correct based on the link
https://learn.microsoft.com/en-us/windows/deployment/deploy-windows-mdt/upgrade-to-windows-10-with-the-microsoft-deployment-toolkit
upvoted 1 times

**jonny_sins** 1 year, 10 months ago
Correct, you need to mount the .exe to the computer then run the set.exe.
upvoted 1 times

**Pcservices** 1 year, 10 months ago
Answer is A
upvoted 4 times

**Afsan** 1 year, 11 months ago
Answer is correct.
Microsoft only uses these two options to perform an in-place upgrade.

Using the MDT toolkit;
https://docs.microsoft.com/en-us/windows/deployment/deploy-windows-mdt/upgrade-to-windows-10-with-the-microsoft-deployment-toolkit

Using SSCM:
https://docs.microsoft.com/en-us/windows/deployment/deploy-windows-cm/upgrade-to-windows-10-with-configuration-manager
upvoted 2 times

Question #114 *Topic 2*

You have a Microsoft 365 subscription that includes Microsoft Intune.

You plan to use Windows Autopilot to deploy Windows 11 devices.

You need to meet the following requirements during Autopilot provisioning:

• Display the app and profile configuration progress.
• Block users from using the devices until all apps and profiles are installed.

What should you configure?

A. an app configuration policy

B. an enrollment device platform restriction

C. an app protection policy

D. an enrollment status page

**Suggested Answer:** *A*

*Community vote distribution*

D (100%)

**Windows311** Highly Voted 1 year, 9 months ago

Selected Answer: D

Correct answer is Enrollment status page.
https://learn.microsoft.com/en-us/mem/intune/enrollment/windows-enrollment-status
Options "Show app and profile configuration progress" and "Block device use until these required apps are installed if they are assigned to the user/device"

upvoted 8 times

**Cheekypoo** 1 year, 9 months ago

Agree, D

upvoted 2 times

**Amir1909** Most Recent 11 months, 3 weeks ago

D is correct

upvoted 1 times

**MAPH61** 1 year, 6 months ago

To meet the given requirements during Autopilot provisioning for Windows 11 devices, you should configure option D, an enrollment status page.

An enrollment status page allows you to display the app and profile configuration progress to users during the provisioning process. It provides real-time updates and notifications about the installation progress.

Additionally, the enrollment status page can be configured to block users from using the devices until all apps and profiles are installed, ensuring that the provisioning process completes before granting access to the device.

Therefore, the correct option is D, an enrollment status page.

upvoted 1 times

**j_sebastian_88** 1 year, 6 months ago

Selected Answer: D

As @Windows311 states, ESP or Enrollment Status Page, shows the progress of several steps in the autopilot deployment proces. When activating the ESP, you can manually specify which apps need to be installed completely before your users can use the device. So D is the one and only correct answer in this case.

upvoted 1 times

**lannythewizard** 1 year, 7 months ago

**Selected Answer: D**

By default Autopilot blocks users from using the device until the configuration process is complete. You don't need to block them from using it. There fore the enrollment status page will show the status.

upvoted 1 times

HOTSPOT
-

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** |

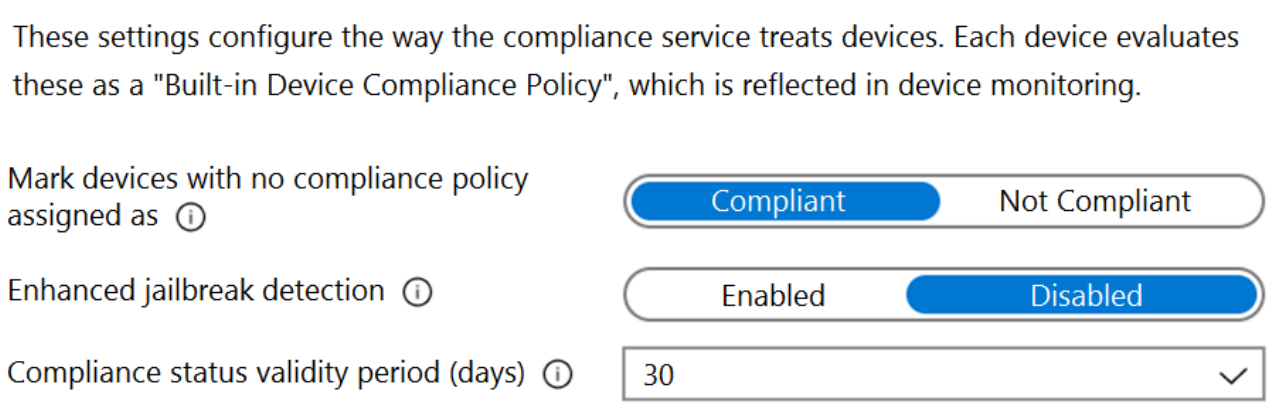
All the Azure AD joined devices have an executable file named C:\AppA.exe and a folder named D:\Folder1.

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:
o 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:
o Name: Boundary1
o Network boundary: 192.168.1.0/24
o Scope tags: Tag1
o Assignments:

- Included groups: Group1, Group2
• Deploy two VPN configuration profiles named Connection1 and Connection2 that will have the following settings:
o Name: Connection1
o Connection name: VPN1
o Connection type: L2TP
o Assignments:
- Included groups: Group1, Group2, GroupA
- Excluded groups: --
o Name: Connection2
o Connection name: VPN2
o Connection type: IKEv2
o 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.

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

NOTE: Each correct selection is worth one point.

**Answer Area**

| Statements | Yes | No |
|---|---|---|
| If User1 joins a Windows 10 device to Azure AD, the device will be enrolled in Intune automatically. | ○ | ○ |
| If User2 joins a Windows 10 device to Azure AD, the device will be enrolled in Intune automatically. | ○ | ○ |
| If User3 joins a Windows 10 device to Azure AD, the device will be enrolled in Intune automatically. | ○ | ○ |

**Suggested Answer:**

**Answer Area**

| Statements | Yes | No |
|---|---|---|
| If User1 joins a Windows 10 device to Azure AD, the device will be enrolled in Intune automatically. | ○ | ● |
| If User2 joins a Windows 10 device to Azure AD, the device will be enrolled in Intune automatically. | ● | ○ |
| If User3 joins a Windows 10 device to Azure AD, the device will be enrolled in Intune automatically. | ○ | ● |

**NoursBear** 12 months ago

I think it's NNN, none of the users have the Deployment Profile assigned. The confusion for User 2 is the menton of the "joined Device Local Administrators" group, this is assigned to all computers after joining, you don't use this role to enroll computers. That was probably the trick

upvoted 2 times

**NSA_Poker** 9 months ago

Correct. Logging into a domain doesn't enroll the device into Intune to allow machine configuration. Enrollment requires the deviceID to be uploaded @ the Intune Admin Center.

upvoted 1 times

**USRobotics** 1 year, 4 months ago

is it correct?

upvoted 1 times

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.

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 an XLSX file and upload the file from the Device settings in Microsoft Store for Business.

B. Extract the serial number of each computer to an XML file and upload the file from the Microsoft Endpoint Manager admin center.

C. Generalize the computers and configure the Device settings from the Azure Active Directory admin center.

D. Extract the hardware ID information of each computer to a CSV file and upload the file from the Devices settings in Microsoft Store for Business.

**Suggested Answer:** *D*

**USRobotics** 1 year, 4 months ago
Hardware ID is no more requested. You need to provide the hardware hashes
https://learn.microsoft.com/en-us/education/windows/tutorial-school-deployment/enroll-autopilot
upvoted 1 times

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 |

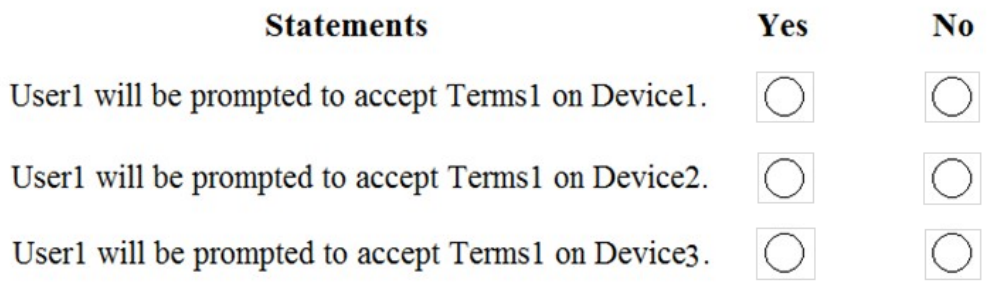
On September 5, 2019, you create and enforce a terms of use (ToU) in contoso.com. The ToU has the following settings:

- ✑ 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:




**Suggested Answer:**


Reference:

https://docs.microsoft.com/en-us/azure/active-directory/conditional-access/terms-of-use#frequently-asked-questions

**Perycles** Highly Voted 3 years, 6 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 18 times

**Angarali** 2 years, 8 months 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** 2 years, 9 months 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 3 times

**poepvlekje** 1 year, 6 months ago

Device 2+3 are AAD registered so they will automatically login to Azure, hence triggering the TOU, Device 1 requires a login which is not specified in the question, so the answer is correct: N Y Y.

upvoted 1 times

**Tomtom11** Highly Voted 3 years, 7 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** 3 years, 1 month 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** 3 years, 1 month ago

Hahaha you can register a device in a single azure tenant.

upvoted 2 times

**NoursBear** Most Recent 11 months, 4 weeks ago

Per-device terms of use

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're accessing from. The end user's device must be registered in Microsoft Entra ID. When the device is registered, the device ID is used to enforce the terms of use policy on each device. Their experience is dependent on permissions to join devices and the platform or software used. For more information, see device identity in Microsoft Entra ID.

https://learn.microsoft.com/en-us/entra/identity/conditional-access/terms-of-use

upvoted 1 times

**raduM** 2 years, 1 month ago

just tested. as soon as you try to access corporate ressources i am prompted to register the device and afterwards to consent the ToU. Therefore answer is YYY

upvoted 2 times

**rendog** 2 years ago

Im wondering if that would mean yes or no since that would not be dependednt if user1 actually registers the device or not. Very confused as to what Microsoft wants from us here so I guess i'll just go with YYY and hope this one doesn't show up on the exam...

upvoted 1 times

**Angarali** 2 years, 8 months 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** 2 years, 9 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** 2 years, 9 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** 2 years, 11 months ago
Answer is: NO, YES, YES
upvoted 3 times

**moobdoob** 2 years, 11 months ago
N - Device is not registered in AzureAD
Y - registered in AzureAD
Y - registered in AzureAD
upvoted 3 times

**RodrigoT** 2 years, 9 months 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 3 times

**Goofer** 3 years, 1 month ago
N - Device is not registered in AzureAD
Y - registered in AzureAD
Y - registered in AzureAD
upvoted 2 times

**BLYBOI** 3 years, 7 months ago
I think Y,Y,Y, because the question says User1 will be prompted TOU?
upvoted 3 times

**Danohav** 3 years, 7 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** 3 years, 7 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** 3 years, 7 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** 3 years, 8 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** 3 years, 7 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** 3 years, 7 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** 3 years, 8 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** 3 years, 8 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** 3 years, 6 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** 3 years, 8 months ago

i think first one should be no

upvoted 2 times

**Layer8** 3 years, 7 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 |

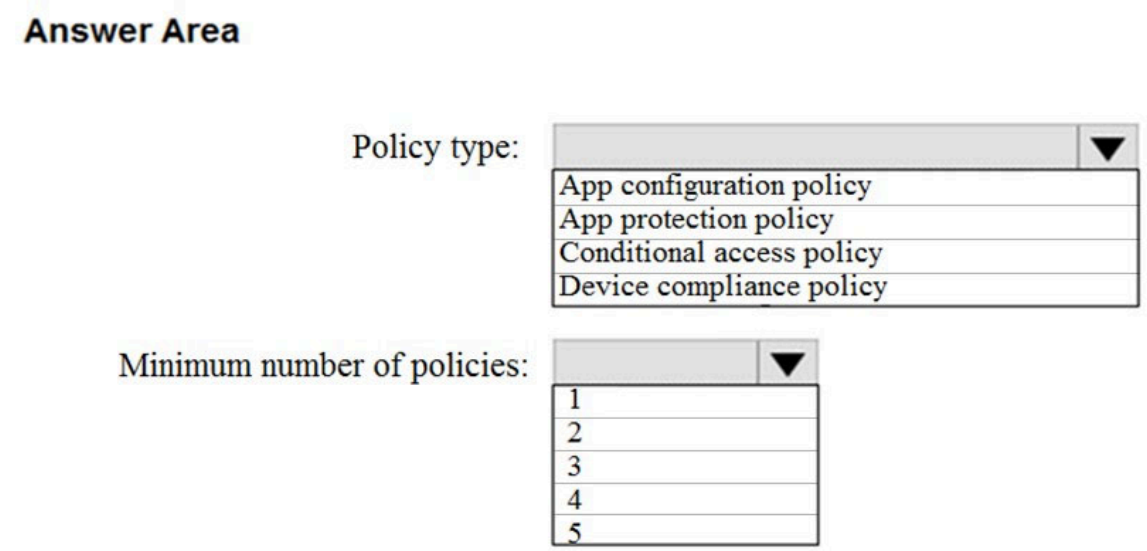
All devices contain an app named App1 and are enrolled in Microsoft Intune.

You need to prevent users from copying data from App1 and pasting the data into other apps.

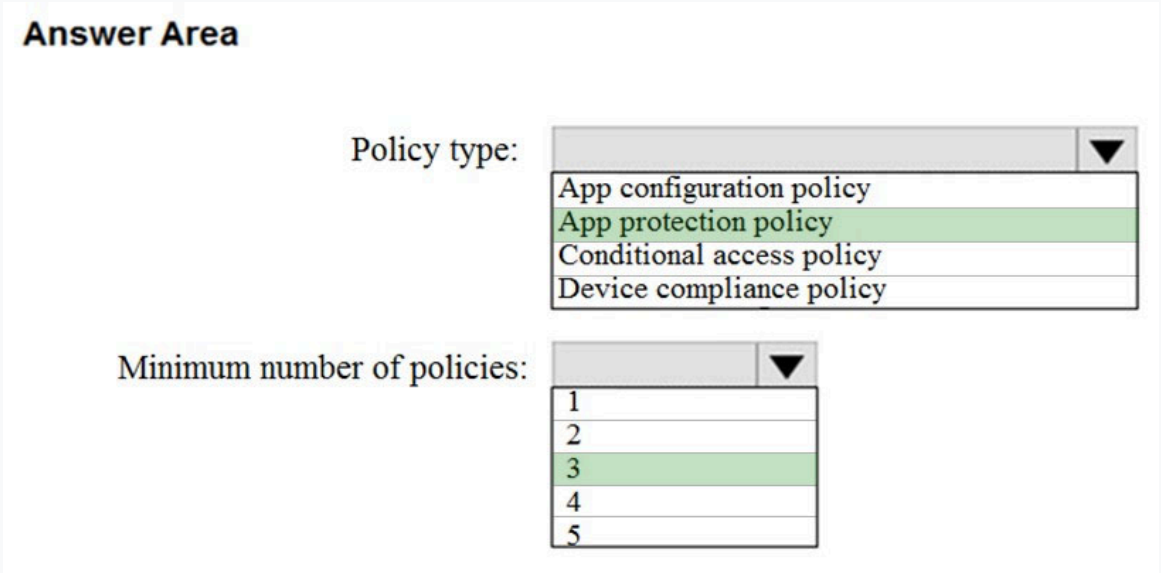
Which type of policy and how many policies should you create in Intune? To answer, select the appropriate options in the answer area.

NOTE: Each correct selection is worth one point.

Hot Area:




**Suggested Answer:**




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 3 years, 6 months ago

when creating Apps Protection Policy , you have 3 choice possible : IOS, ANDROID , WINDOWS. SO 3 policies necessary.

upvoted 14 times

**mikl** 3 years ago
I agree.
upvoted 1 times

**Amir1909** Most Recent 12 months ago
Correct
upvoted 1 times

**raduM** 2 years, 1 month ago
4 is now history. you can stay at 3 b ecause the is no more wip for not enrolled devices
upvoted 1 times

**raduM** 2 years, 2 months ago
4 policies for windows you have 2 with enrolment and without enrolment. If you choose without enrloment for windows the policies will apply only to unenrolled devices if you choose with enrolment it will apply only to the enrolled devices
upvoted 1 times

**Altheus** 2 years, 2 months ago
One policy for each type of device - reading the question is important.
upvoted 1 times

**us3r** 3 years ago
applies also for ms-101.
upvoted 2 times

**lijk_manson** 3 years, 1 month 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 2 times

**lijk_manson** 3 years, 1 month ago
You need to follow the table, so yes it is 3 not 4
upvoted 1 times

**RodrigoT** 2 years, 9 months 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** 2 years, 8 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

**raduM** 2 years, 1 month ago
you are so wrong mate. i can't believe this. please test it in the enviroment if you have any
upvoted 1 times

**Angarali** 3 years, 5 months ago
Answer is correct

https://docs.microsoft.com/en-us/microsoft-365/business/protection-settings-for-windows-10-devices
upvoted 4 times

**GohanF2** 3 years, 7 months ago
the answer is correct
upvoted 1 times

**Layer8** 3 years, 7 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** 3 years, 8 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** 3 years, 7 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** 3 years, 8 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** 3 years, 8 months ago

Correct, but then it should be 2 policies - 1 for iOS, 1 for Android

upvoted 6 times

**Moorebid** 3 years, 7 months ago

The correct answer is 3, one for each platform (Windows, Android, iOS).

upvoted 3 times

**IrvSus** 3 years, 8 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

**Suggested 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 4 years ago
I will get them to use Chrome or Firefox.
upvoted 28 times

**asturmark** 2 years, 3 months ago
Or Brave :)
upvoted 3 times

**Anthony_2770** Highly Voted 3 years, 11 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

**Yeuri** Most Recent 2 years, 1 month ago
Non of the previous answers Right now is just called, Internet Explorer mode on Edge.
upvoted 2 times

**NZS** 2 years, 8 months ago
Enterprise Mode... but IE is gone from both Windows 10 and 11 now
upvoted 3 times

**letters1234** 2 years, 10 months 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** 3 years ago
Enterprise Mode is the solution.
upvoted 2 times

**Perycles** 3 years, 6 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** 4 years ago

It's B

upvoted 2 times

**lijk_manson** 4 years, 1 month 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)

**Suggested 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

*Community vote distribution*
D (100%)

**Mendel** Highly Voted 5 years, 3 months 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 25 times

**nolancl** 5 years, 3 months 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** 4 years, 9 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** 3 years ago
Exactly.
upvoted 1 times

**DUSHIWORLD** Highly Voted 4 years, 10 months ago
Answer is D!
upvoted 13 times

**AliNadheer** Most Recent 1 year, 10 months ago
Selected Answer: D
This is the full list of all possible device attributes that can be used:

accountEnabled
displayName
deviceOSType
deviceOSVersion
deviceCategory
deviceManufacturer
deviceModel

deviceOwnership
domainName
enrollmentProfileName
isRooted
managementType
organizationalUnit
deviceId
objectId
upvoted 1 times

**cbjorn8931** 2 years, 1 month ago
The link that is provided states that the answer is C: but they are saying D? My guess was C Device category within Intune. Within Intune Device Category you can create groups to filter devices.
upvoted 1 times

**raduM** 2 years, 2 months ago
D all the way
upvoted 1 times

**gotrekk** 2 years, 4 months ago
Selected Answer: D
Dynamic groups
upvoted 1 times

**raduM** 2 years, 4 months ago
i would also go with dynamic groups here
upvoted 1 times

**mikl** 3 years ago
Selected Answer: D
D. Groups that have dynamic membership rules in Microsoft Azure Active Directory (Azure AD) is correct.
upvoted 3 times

**Perycles** 3 years, 6 months ago
D is the good answer, by using "deviceOSversion" setting, whith can type the version of the desired OS.
upvoted 2 times

**Tomtom11** 3 years, 7 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 3 times

**BLYBOI** 3 years, 7 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** 3 years, 8 months ago
Correct aswer is D
upvoted 4 times

**slaoui** 3 years, 8 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** 3 years, 8 months ago
Disregard my comment, it was meant for the previous question
upvoted 1 times

**Tomtom11** 3 years, 9 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** 4 years 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** 4 years 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** 4 years, 1 month ago

https://docs.microsoft.com/nl-nl/azure/active-directory/devices/device-management-azure-portal
its B

upvoted 1 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

**Suggested 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/

*Community vote distribution*
D (100%)

**Tomtom11** Highly Voted 3 years, 9 months ago
Answer D = Windows | Configuration profiles - Edition upgrade and mode switch
upvoted 14 times

**Amir1909** Most Recent 11 months, 4 weeks ago
Correct
upvoted 1 times

**jt2214** 1 year, 10 months ago
When in doubt Device Configuration :P
upvoted 1 times

**AliNadheer** 1 year, 10 months ago
Selected Answer: D
(configuration profiles -> then select Template -> Edition upgrade)
upvoted 1 times

**AK4U_111** 2 years, 2 months ago
Answer is correct - Device Configuration Policy
upvoted 1 times

**mikl** 3 years ago
D. A device configuration profile is correct
upvoted 1 times

**john909** 3 years, 2 months ago
Yes, D (configuration profiles -> then select Template -> Edition upgrade)
upvoted 3 times

**AzZnLuVaBol** 3 years, 10 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?

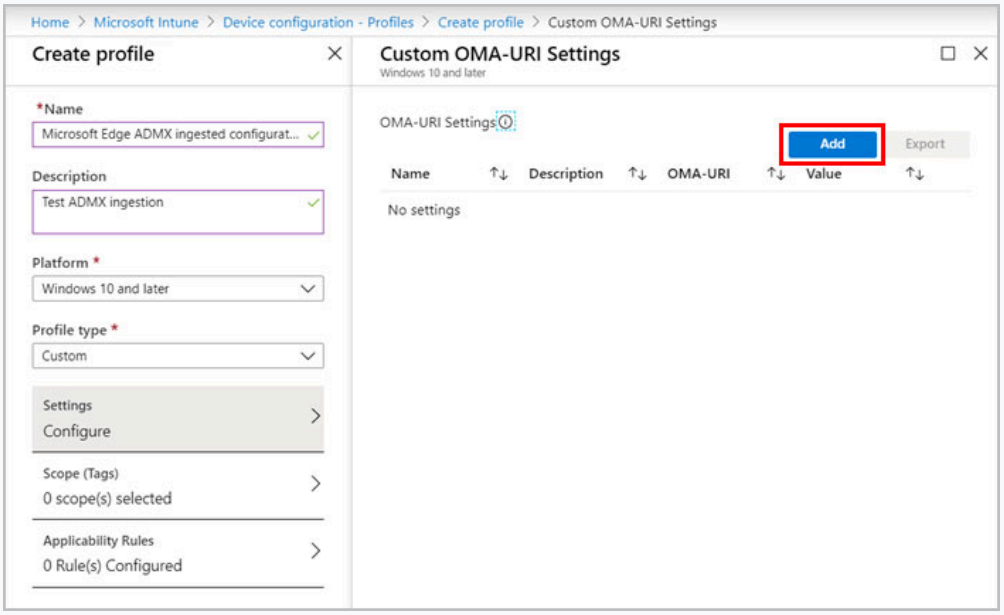
A. Identity protection

B. Custom

C. Device restrictions

D. Device restrictions (Windows 10 Team)

**Suggested 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

**AyoR32** 2 years ago
The new feature is : "Imported Administrative templates (Preview)"
Why is it not purposed ? This question was updated on december 6th...
upvoted 2 times

**osxzvkwpfcfxobqjby** 1 year, 6 months ago
Microsoft is not clear about that... :(

"While most questions cover features that are General Availability (GA), the exam may contain questions on Preview features if those features

are commonly used."

https://learn.microsoft.com/en-us/certifications/frequently-asked-questions

upvoted 1 times

**daye** 2 years, 2 months ago

It's correct but currently there is a new feature when it can be uploaded directly

https://learn.microsoft.com/en-us/mem/intune/configuration/administrative-templates-import-custom

upvoted 3 times

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. | ○ | ○ |

**Suggested 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 3 years, 8 months ago

looks right, had to pay attention to enrollment state

upvoted 18 times

**RodrigoT** 2 years, 9 months 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 6 times

**RodrigoT** 2 years, 9 months 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 9 times

**RodrigoT** 2 years, 9 months ago
"because the device1 is enrolled" I meant.
upvoted 1 times

**51007** 2 years, 7 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 6 times

**MitchF** 2 years, 5 months 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 2 times

**Merma** Highly Voted 3 years, 7 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** 2 years, 8 months ago
When an app protection policy is created for Windows 10 "without enrollment" it will be applied anyway by MAM.
upvoted 3 times

**NoursBear** Most Recent 11 months, 4 weeks ago
Could it just be, why the second option is No, because "MAM policies don't support multiple users on the same device" ? So User 1 is the first user of this device, then the policy won't work when getting on Device 1 as well. Just a thought. Another one of those tricky questions
upvoted 1 times

**AliNadheer** 1 year, 10 months ago
guys, reading the comments here is i feel things have been lost in translation, for user2 on device1 we all agree that apps will be protected regardless of enrollment, but the question has two policies for each scenario so in my opinion policy1 wont take effect but perhaps policy3 will. that's why the answer is Y, N ,Y.
appreciate your thoughts about this because i am confused.

upvoted 1 times

**raduM** 2 years, 1 month ago

no more without enrollment

upvoted 1 times

**raduM** 2 years, 2 months ago

Yes no yes. get your facts straight. without enrollment applies to devices that are not enrolled and with enrollment applies to the devices that are enrolled

upvoted 1 times

**AK4U_111** 2 years, 2 months ago

Are Policy3+4 there just to try and throw us off? It seems they dont have anything to do with the question/answer

upvoted 1 times

**BRoald** 2 years, 3 months 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 years, 3 months 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** 2 years, 6 months ago

Answer is Y Y Y

upvoted 3 times

**Whatsamattr81** 2 years, 6 months 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** 3 years 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** 3 years ago

You are wrong. When you create it you specify with or without enrollment.

upvoted 1 times

**RodrigoT** 2 years, 9 months 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 3 times

**tf444** 3 years, 2 months 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** 2 years, 9 months ago

so Yes No No or Yes No Yes

upvoted 3 times

**Layer8** 3 years, 7 months ago

App protection policies should effect regardless of intune enrollment then?

upvoted 1 times

**NKG123** 3 years ago

You are wrong. You can chose to apply on an unmanaged device!

upvoted 1 times

**Pleebb** 3 years, 5 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

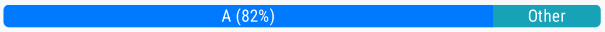
B. File1.docx, the screen saver settings, the desktop background, and the default save location for Word

C. File1.docx only

D. File1.docx, the desktop background, and the default save location for Word only

**Suggested 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

*Community vote distribution*




**Y2** Highly Voted 2 years, 9 months ago
Why are there SOO many wrong anwer in MD-101 past papers. i have never seen anything like this
upvoted 12 times

**Brent0n** 2 years, 9 months ago
IKR, really forces you to actually try understand things because no one can be trusted.
upvoted 9 times

**Technik** Highly Voted 3 years, 7 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

**[Removed]** 3 years, 2 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** 2 years, 10 months 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 5 times

**Raxon** Most Recent 1 year, 10 months ago

Why use roaming profiles and folder redirection?
User profiles allow multiple users to share a Windows system and still maintain their own preferences. You can set your background to chartreuse without affecting anyone else who uses the machine. Folder redirection allows you to use Windows as you are used to, but to have files saved on the Desktop and My Documents, follow you around to each workstation. Some of the things you can set that are stored in your profile and redirected folders include:

Wallpaper
Screen saver
Display properties - colors, fonts and sizes
Shortcuts on the desktop
Whether to display or not to display web content
A personalized Taskbar
Desktop Toolbars
Settings for some applications

Answer: B. File1.docx, the screen saver settings, the desktop background, and the default save location for Word

The default location of Word is MY DOCUMENT.
upvoted 2 times

**Deezal** 1 year, 11 months ago

Selected Answer: A

Labbed it and answer is A. file and desktop background
upvoted 5 times

**raduM** 2 years, 1 month ago

after testing this in my lab i can tell you the answer is file and desktop
upvoted 4 times

**JN_311** 2 years, 1 month ago

Selected Answer: A

Answer A
upvoted 2 times

**Fuzm4n** 2 years, 1 month ago

C.

A copy of the current custom desktop background image is stored in appdata\roaming but not the ntuser.dat which actually tells windows to use that desktop image.
upvoted 1 times

**raduM** 2 years, 2 months ago

c is the answer
upvoted 1 times

**raduM** 2 years, 3 months ago

the answer should be c
upvoted 2 times

**raduM** 2 years, 4 months ago

Selected Answer: C

c should be correct
upvoted 1 times

**raduM** 2 years, 4 months 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** 2 years, 6 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** 2 years, 6 months 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** 2 years, 6 months 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** 2 years, 7 months ago

A is the answer.

Default save location for MS Word is the Documents folder.

upvoted 1 times

**MR_Eliot** 2 years, 8 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** 2 years, 8 months 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

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.

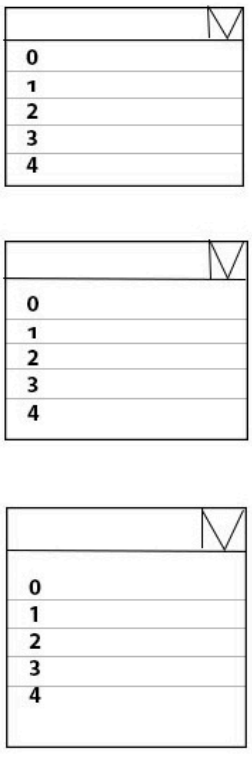
Hot Area:

**Answer Area**

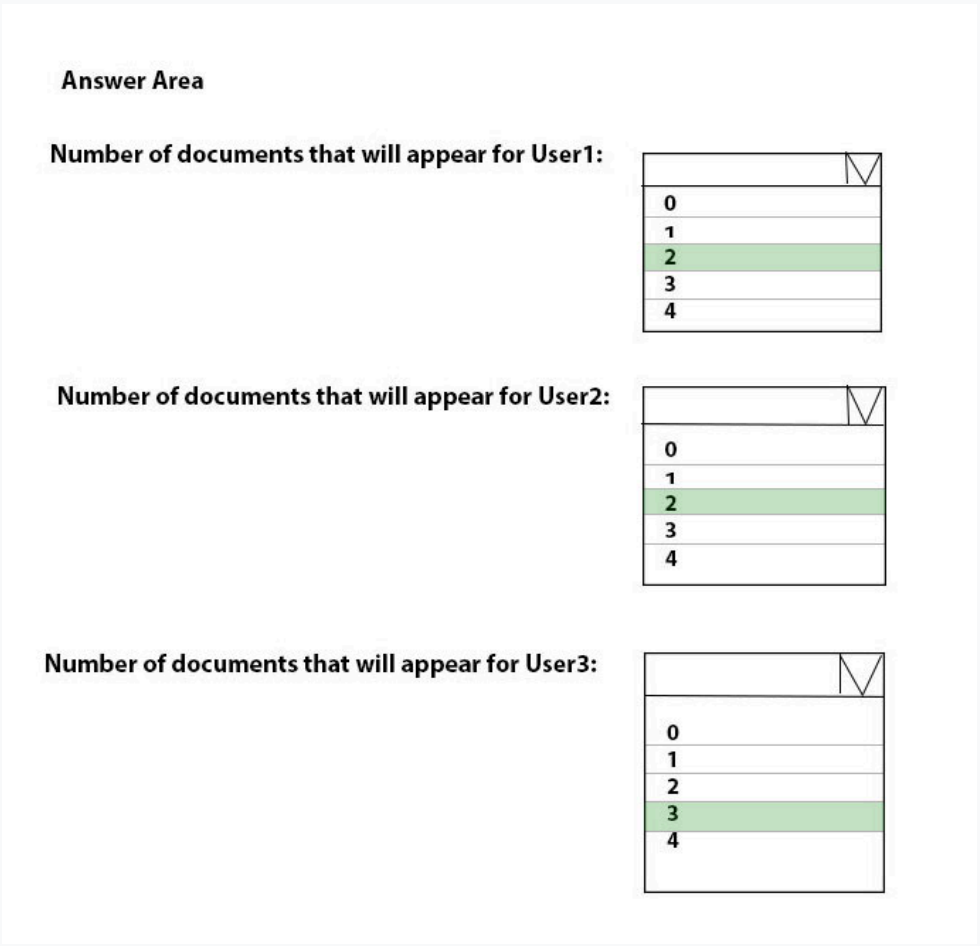
**Number of documents that will appear for User1:**

**Number of documents that will appear for User2:**

**Number of documents that will appear for User3:**



**Suggested Answer:**




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 4 years, 10 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 77 times

**RodrigoT** 2 years, 9 months 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 2 times

**RodrigoT** 2 years, 8 months 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 27 times

**StefanSteg** 2 years, 1 month ago
User2 Only gets only 2 files if its also member of the Users group. The table in the questions says "user2 is member of the Replicator group". so User2 won't be able to log in. When User2 is also member of the users group, it gets 2 files. i just tested.
upvoted 1 times

**Mendel** Highly Voted 5 years, 3 months 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 26 times

**stepient** 4 years, 4 months ago
User3 won't see File4, because Guest setttings and files are not saved. I just tested it i lab.
upvoted 13 times

**RodrigoT** 2 years, 8 months ago
Wrong, User3 KEEPS the files that he created before. Tested in a Win10 Pro 21H2.
upvoted 1 times

**mistrzkungfu** 4 years, 11 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** 4 years, 10 months ago
User 3 is an existing user, so it won't get file 3.
upvoted 3 times

**Saldi** 4 years, 8 months ago
Every time a guest user logs in, they will be treated as new.
upvoted 10 times

**RodrigoT** 2 years, 9 months 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 4 times

**Anthony_2770** 3 years, 11 months ago
User 3 is a guest and will not get File4
upvoted 6 times

**PinkyK** 2 years, 7 months 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** 3 years, 3 months ago
not true, it keeps all the 3 files.
upvoted 1 times

**bassfunk** Most Recent 1 year, 5 months ago
Based on the information laid out in the question, the answer is 2,0,2. User2 is not stated to be a member of a group that can login. It is also stated that User2 has never logged in. If it's wrong then its MS fault for wording it in this way. We answer questions based on the information given to us. We can't be expected to make baseless assumptions. Answer is 2,0,2.

upvoted 1 times

**Nokobungo** 1 year, 5 months ago

This question was on the MD-100 exam I took a few days ago.

upvoted 1 times

**GabrielN** 1 year, 9 months ago

If I understand correctly, the answer to User3 depends if User3 signed in for the first time or not, right?

If we assumed User3 signed in for the first time after the files are created, he'll get File2 and 3, then create File4. Since no files will be lost on logout, User3 will have 3 files on its desktop.

But if we assume User3 DID sign in previously, at any moment, then they would only get File2 on sign-in, and create File4, totalling 2 files when they sign in again.

Honestly, this question is kinda dubious. It doesnt specify if User3 has signed in before or not, and knowing Microsoft, it could go both ways

upvoted 1 times

**JN_311** 2 years, 1 month ago

Final Answer - 2, 0, 2

The Replicator Group, cannot logon locally, it has no default user rights, so User2 has 0 files

https://learn.microsoft.com/en-us/previous-versions/windows/it-pro/windows-server-2008-r2-and-2008/cc771990(v=ws.10)

upvoted 2 times

**raduM** 2 years, 1 month ago

2 2 2

just tested in the lab

upvoted 1 times

**Altheus** 2 years, 1 month ago

This is a sneaky one, you get the contents of the default desktop when a new desktop is created - i.e. when a new user signs in.

Because User 1 already exists he doesn't get to see the file in the default desktop.

upvoted 1 times

**AK4U_111** 2 years, 2 months ago

Correct me if i'm wrong, but a normal user which is a member of the Guests group, is actually not a normal guest user. A normal guest user would log in using "Guest" and then the profile will be new every time he logs in. But User3 which is a part of the Guests group would still have the file which he created on the desktop when he logs back in, then i would say that the given answer is correct.

upvoted 1 times

**Jnorris** 2 years, 4 months 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** 2 years, 4 months ago

3-2-2 should be correct

upvoted 1 times

**Whatsamattr81** 2 years, 6 months 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** 2 years, 6 months 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

**Brent0n** 2 years, 9 months ago

Beginning to wonder if these answers are pulled out of a hat.

upvoted 1 times

**jage01** 2 years, 10 months 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 4 times

**coppermine** 2 years, 11 months 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** 2 years, 9 months 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

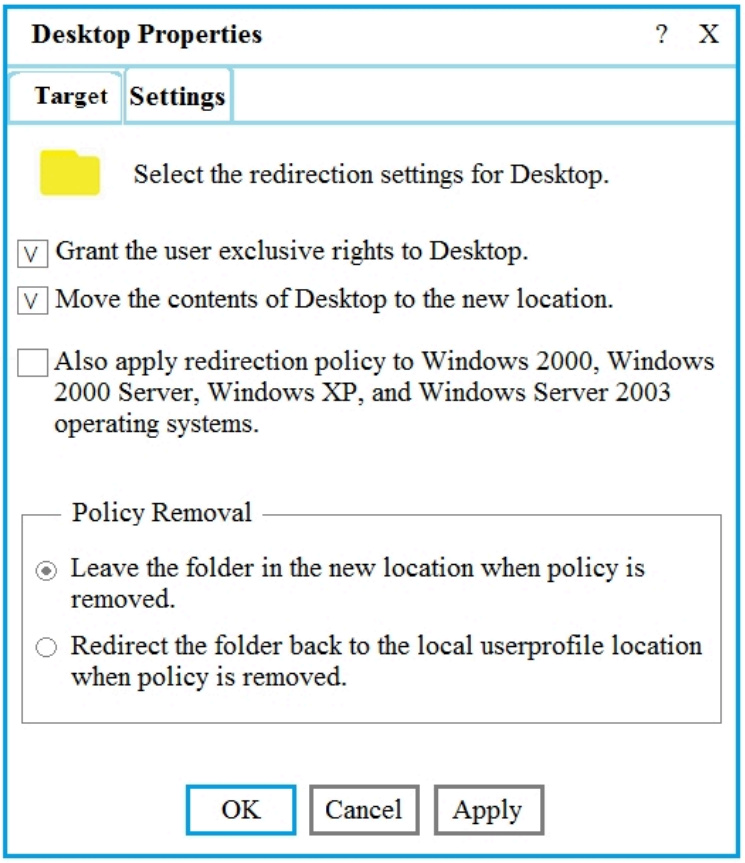
**jage01** 2 years, 12 months ago

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

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.

**Suggested Answer:** *AB*
Reference:
https://docs.microsoft.com/en-us/onedrive/redirect-known-folders

*Community vote distribution*
BC (55%) AB (45%)

**nolancl** Highly Voted 5 years, 3 months 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 42 times

**thesystem** 5 years ago
Agreed, I think it should also be BC.
upvoted 5 times

**DUSHIWORLD** 4 years, 10 months ago
Correct
upvoted 2 times

**Layer8** 3 years, 7 months ago
if it's anything, it's BC
upvoted 3 times

**RodrigoT** Highly Voted 2 years, 8 months 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 9 times

**ken2ut** 2 years, 7 months 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

**Bart_Hofstede** Most Recent 1 year, 3 months ago
I'd say AB is correct. Microsoft wants you to leave the data on the network and use migration manager to copy.

https://learn.microsoft.com/en-us/sharepoint/redirect-known-folders

If folders have been redirected to a network file share:

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.

Note

If Migration Manager will create the Documents, Pictures, or Desktop folders, ensure that Preserve file share permissions is not selected when performing the migration.

Disable the Window Folder Redirection Group Policy and make sure to leave the folder and contents on the network file share.

Enable Known Folder Move 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 1 times

**devilcried** 1 year, 10 months ago
Selected Answer: BC
I have implement this to a customer of mine. B , C are the right answers.
upvoted 1 times

**AK4U_111** 2 years, 2 months ago
How can C be correct if the question says "when you implement known folder redirection"m so how can the solution be to disable folder redirection?
upvoted 1 times

**Deezal** 1 year, 11 months ago

Folder redirection and Known Folder Redirection are different things

upvoted 1 times

**gotrekk** 2 years, 4 months ago

Selected Answer: BC

Change the policy and disabile redirection

upvoted 2 times

**MitchF** 2 years, 5 months 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 years, 5 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 2 times

**silver_bullet666** 2 years, 6 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** 2 years, 6 months 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

**Adhikari123** 2 years, 8 months ago

Selected Answer: BC

This is the answer

upvoted 1 times

**Adhikari123** 2 years, 9 months ago

Selected Answer: BC

B and C

upvoted 1 times

**Harold** 2 years, 9 months ago

Selected Answer: BC

Agree with the other explanations.

upvoted 1 times

**rj_client** 2 years, 10 months 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** 2 years, 11 months 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** 3 years, 2 months 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** 3 years, 8 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** 3 years, 11 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** 3 years, 11 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

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

**Suggested 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 3 years, 2 months ago

Looks ok
Check also https://docs.microsoft.com/en-us/mem/intune/protect/actions-for-noncompliance
upvoted 9 times

**Amir1909** Most Recent 11 months, 4 weeks ago
Correct
upvoted 1 times

**Thinkin** 1 year, 4 months ago
Answers are Conditional Access for both
remotely locked option only available for iOS and Android devices not for Windows. The question here is about windows 10.
upvoted 2 times

**AK4U_111** 2 years, 2 months ago
Correct me if i'm wrong, but a normal user which is a member of the Guests group, is actually not a normal guest user. A normal guest user would log in using "Guest" and then the profile will be new every time he logs in. But User3 which is a part of the Guests group would still have the file which he created on the desktop when he logs back in, then i would say that the given answer is correct.
upvoted 1 times

**AK4U_111** 2 years, 2 months ago
Sorry replied to wrong question
upvoted 1 times

**chapinoli** 2 years, 11 months 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 2 times

**pogap64757** 2 years, 11 months 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** 2 years, 9 months 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 3 times

**RodrigoT** 2 years, 8 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** 2 years, 11 months ago
correct
upvoted 1 times

**Moderator** 2 years, 11 months ago
Correct answers.
upvoted 1 times

**mikl** 3 years ago
I agree.

upvoted 1 times

Question #12 *Topic 3*

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.

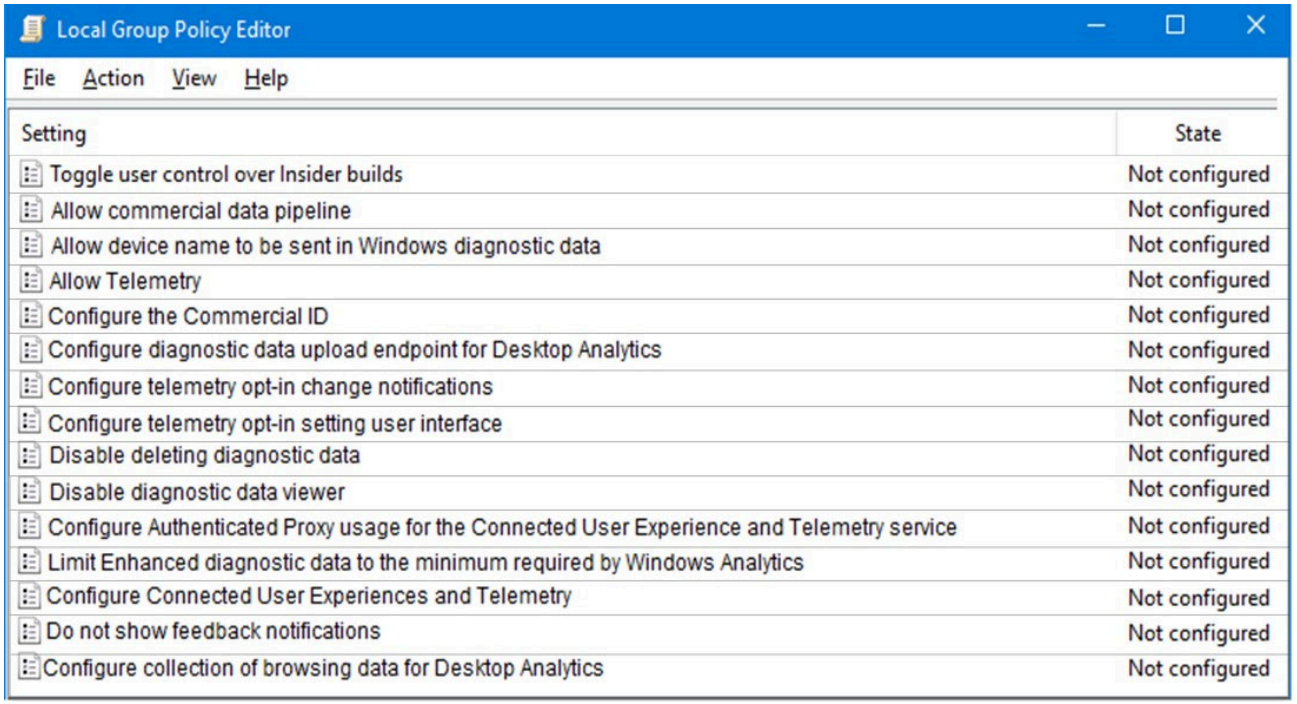
You create the required resources in Azure.

You need to configure the computers to send enhanced Update Compliance data.

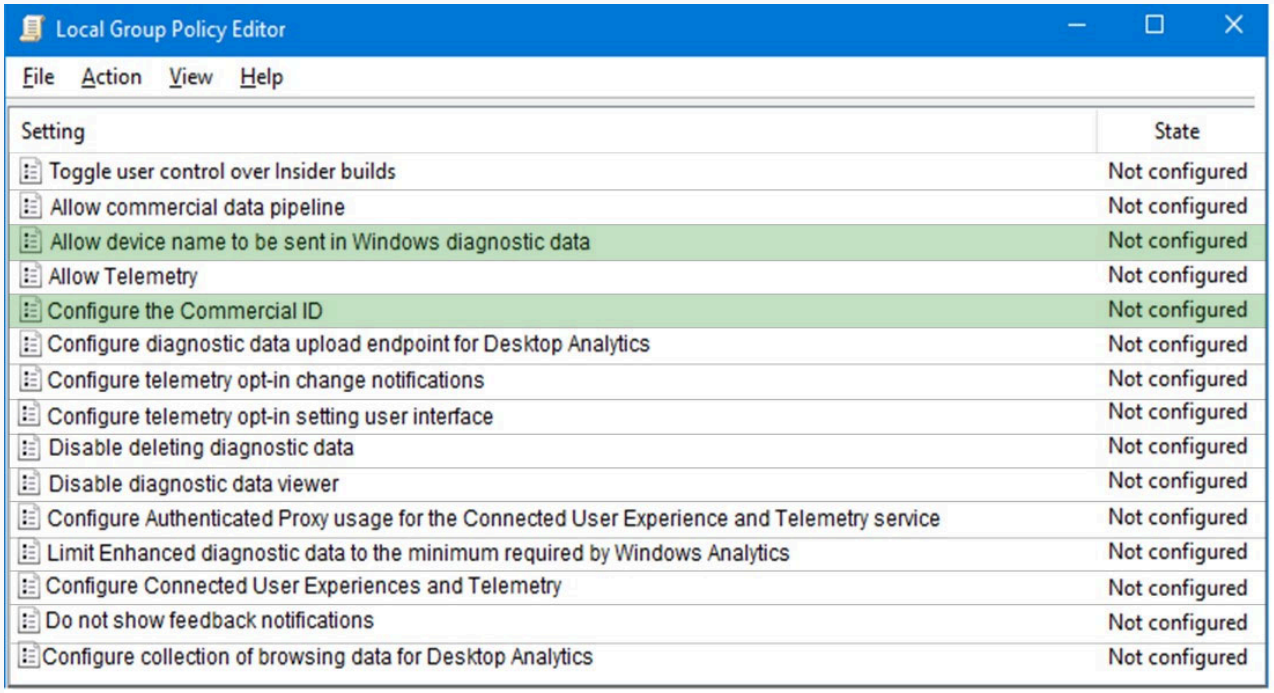
Which two Group Policy settings should you configure? To answer, select the appropriate settings in the answer area.

NOTE: Each correct selection is worth one point.

Hot Area:




**Suggested 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 3 years, 8 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 12 times

**raduM** Most Recent 2 years, 4 months ago
configure commercial id and allow telemetry
upvoted 2 times

**silver_bullet666** 2 years, 5 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** 2 years, 6 months 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** 2 years, 7 months 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** 2 years, 11 months 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** 2 years, 11 months ago
Commercial ID + Telemetry is what im going with.
upvoted 4 times

**forummj** 2 years, 11 months 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** 3 years, 1 month 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%20col
upvoted 2 times

**Perycles** 3 years, 6 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** 3 years, 8 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 2 times

**Poncho25** 3 years, 7 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** 3 years, 8 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** 3 years, 7 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** 3 years, 7 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 2 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 |

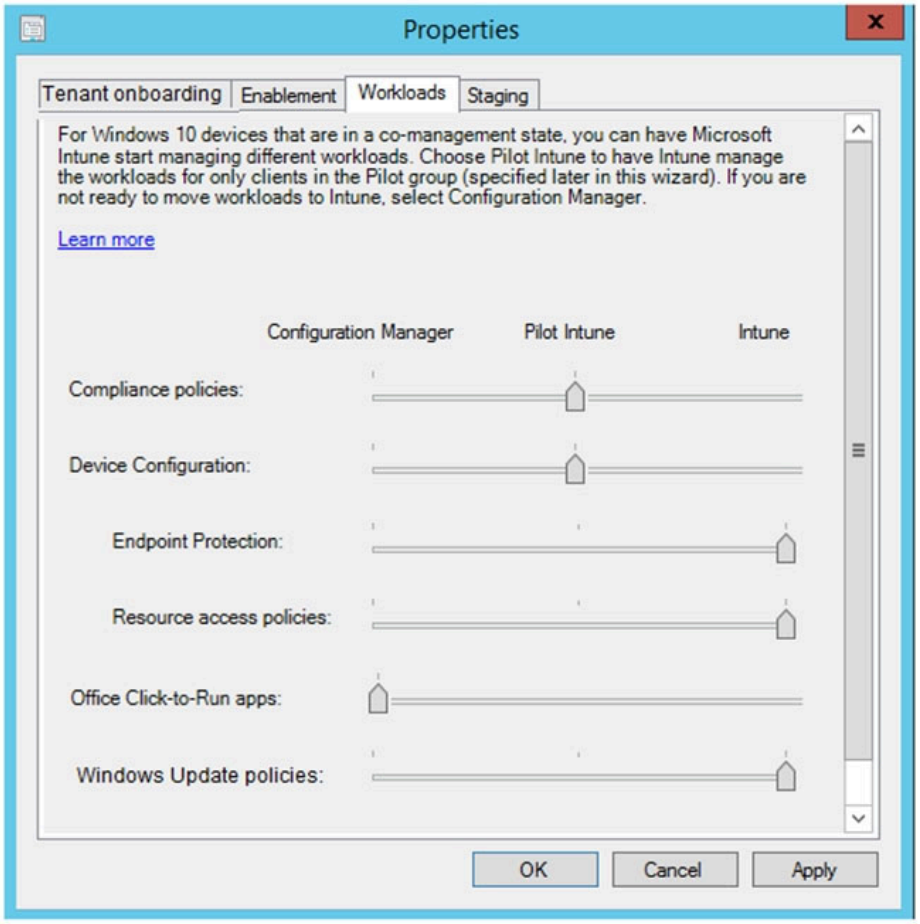
In Configuration Manager, you enable co-management and configure the following settings:

- 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. | ○ | ○ |

**Suggested 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 3 years, 6 months ago
No,No,Yes see Anonimouse explains, it's correct.
upvoted 23 times

**asdaa** Highly Voted 3 years, 2 months 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 8 times

**RodrigoT** 2 years, 9 months 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 3 times

**RodrigoT** 2 years, 9 months 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 5 times

**raduM** Most Recent 2 years, 4 months ago
No No Yes. Given answer is wrong
upvoted 1 times

**MitchF** 2 years, 5 months 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** 2 years, 4 months ago
device 2 is not comanaged because you set the auto enrollment just for collection 1
upvoted 2 times

**Merma** 3 years, 7 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** 3 years, 7 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 38 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)

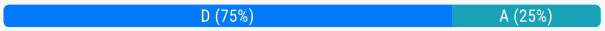
B. Settings

C. Applicability Rules

D. Assignments

**Suggested 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

*Community vote distribution*




**[Removed]** Highly Voted 3 years, 2 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 14 times

**ercluff** 3 years ago
Didn't you mean "assignments" as the only correct answer?
upvoted 6 times

**Amir1909** Most Recent 12 months ago
Correct
upvoted 1 times

**CODENAME_KND** 1 year, 11 months ago
Selected Answer: D
Correct
upvoted 1 times

**raduM** 2 years, 1 month ago
ok you modify assigments but you also need to create a new group. so i would go with d here
upvoted 1 times

**randdrick** 2 years, 8 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** 2 years, 11 months 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 2 times

**b3arb0yb1m** 3 years ago
C. Applicability Rules
upvoted 1 times

**CARO54** 3 years 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** 3 years, 1 month ago
D is correct. Include or Exclude Devices in assigment.
upvoted 2 times

**DogeZaemon** 3 years, 2 months 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** 2 years, 8 months ago
you're confused..
upvoted 2 times

**[Removed]** 3 years, 2 months ago
Tags limit Administrators view,
upvoted 4 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

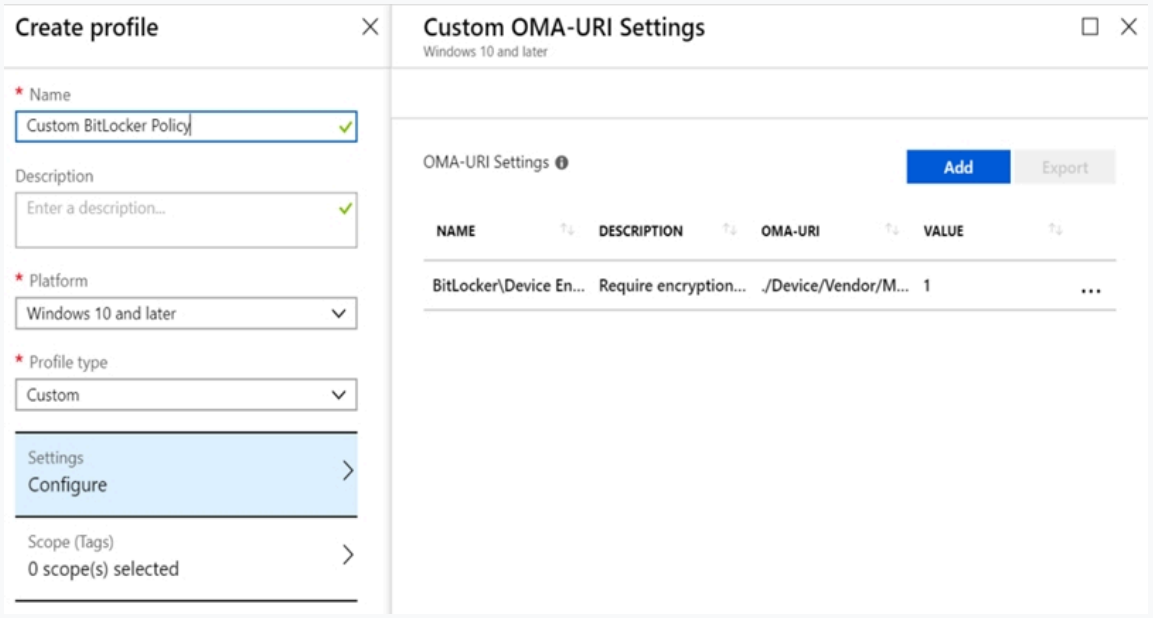
D. Device restrictions

**Suggested 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/

*Community vote distribution*

D (88%) 13%

**Amir1909** 11 months, 4 weeks ago

D is correct

upvoted 1 times

**CODENAME_KND** 1 year, 9 months ago

**Selected Answer: D**

Device Restrictions is correct

upvoted 1 times

**ya12** 1 year, 11 months ago

**Selected Answer: A**

Custom, beacose device restrictions - "Number of sign-in failures before wiping device" but this not "Lockoutbadcount"

upvoted 1 times

**devilcried** 2 years, 1 month ago

**Selected Answer: D**

These days device restrictions

upvoted 1 times

**Horhe** 2 years, 2 months ago

**Selected Answer: D**

As per Pedro488: https://learn.microsoft.com/en-us/mem/intune/configuration/device-restrictions-windows-10#password

upvoted 1 times

**daye** 2 years, 2 months ago

**Selected Answer: D**

old answer, nowadays should be created as device restrictions

upvoted 1 times

**Pedro488** 2 years, 3 months ago

**Selected Answer: D**

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

upvoted 3 times

**asturmark** 2 years, 3 months ago

The answer should be ¨device restrictions¨. From there you have the options for password complexity

upvoted 2 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

**Suggested Answer:** *A*
Reference:
https://docs.microsoft.com/en-us/windows/configuration/kiosk-single-app

*Community vote distribution*
A (100%)

**Dong1999** Highly Voted 3 years, 5 months ago
Answer is correct
upvoted 7 times

**MR_Eliot** Most Recent 2 years, 8 months ago
Selected Answer: A
Kiosk is the answer.
upvoted 1 times

**mikl** 3 years 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

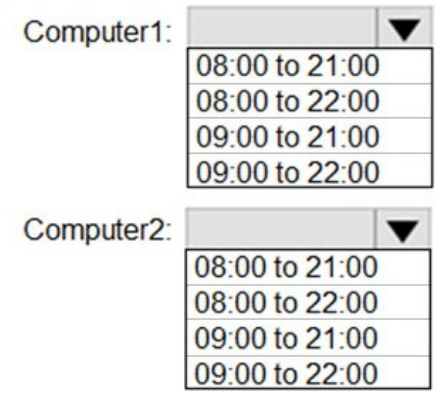
You assign Profile to Group1.

How are the active hours configured on Computer1 and Computer2? To answer, select the appropriate options in the answer area.

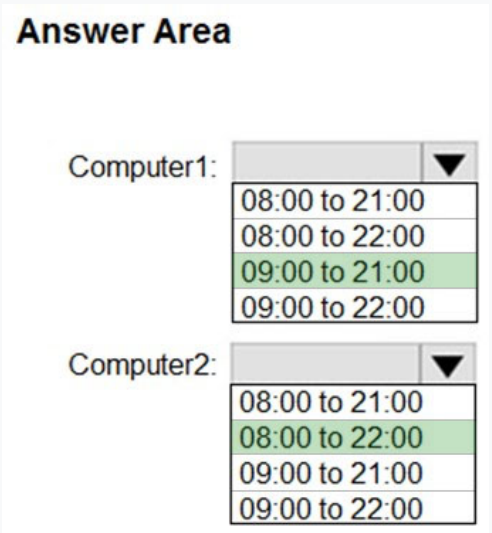
NOTE: Each correct selection is worth one point.

Hot Area:

**Answer Area**




**Suggested Answer:**




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 3 years, 6 months ago
if all questions could be like this one :)
Answer is correct/
upvoted 27 times

**RodrigoT** 2 years, 9 months ago
Two points easy peasy.
upvoted 4 times

**AliNadheer** Most Recent 1 year, 10 months ago
correct
If set to 1 then any MDM policy that is set that has an equivalent GP policy will result in GP service blocking the setting of the policy by GP MMC. Setting the value to 0 (zero) or deleting the policy will remove the GP policy blocks restore the saved GP policie
reference: https://learn.microsoft.com/en-us/windows/client-management/mdm/policy-csp-controlpolicyconflict
upvoted 1 times

**raduM** 2 years, 4 months ago
if it all would be that easy
upvoted 1 times

**Anon1212** 2 years, 10 months ago
Literally the easiest question on this test <~
upvoted 4 times

**krisbla** 2 years, 10 months 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** 2 years, 11 months ago
hehe...straight forward one...
upvoted 1 times

**mikl** 3 years ago
I agree.
upvoted 1 times

**lollo1234** 3 years, 7 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.

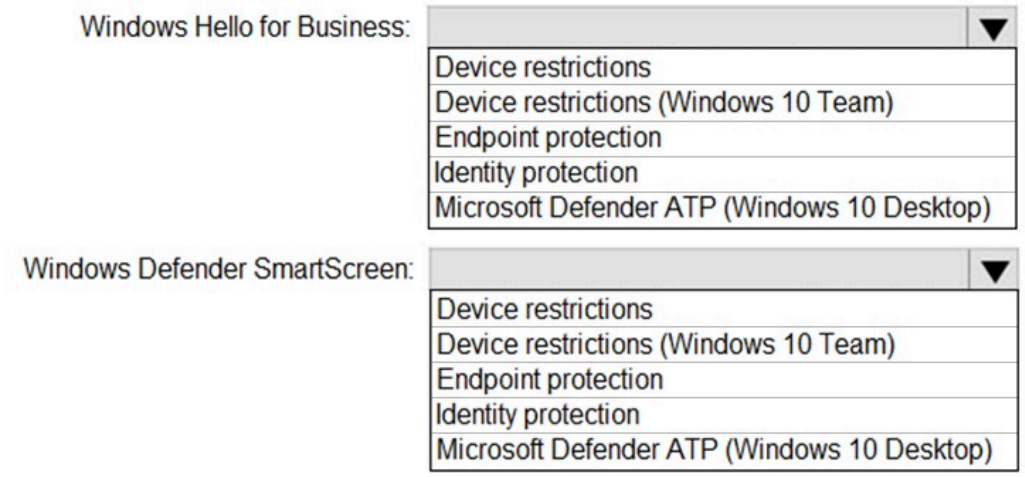
✑ Configure Microsoft Defender SmartScreen to block users from running unverified files.

Which profile types should you configure? To answer, select the appropriate options in the answer area.

NOTE: Each correct selection is worth one point.

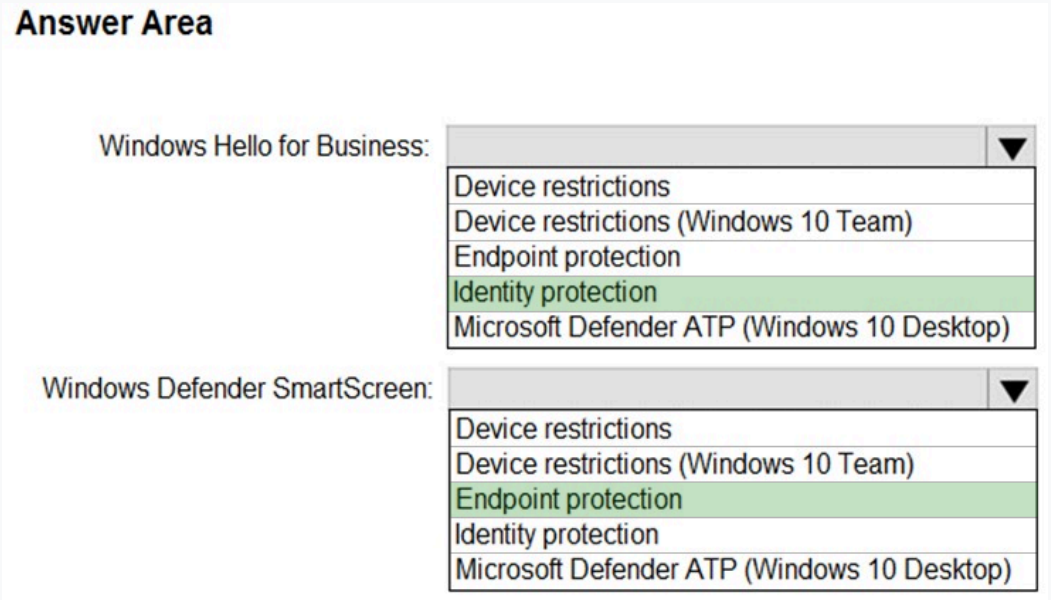
Hot Area:

**Answer Area**




**Suggested 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 3 years, 6 months ago

answers are correct.

upvoted 11 times

**MikeMatt2020** Highly Voted 3 years, 7 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** 3 years, 7 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** 2 years, 9 months 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 8 times

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).

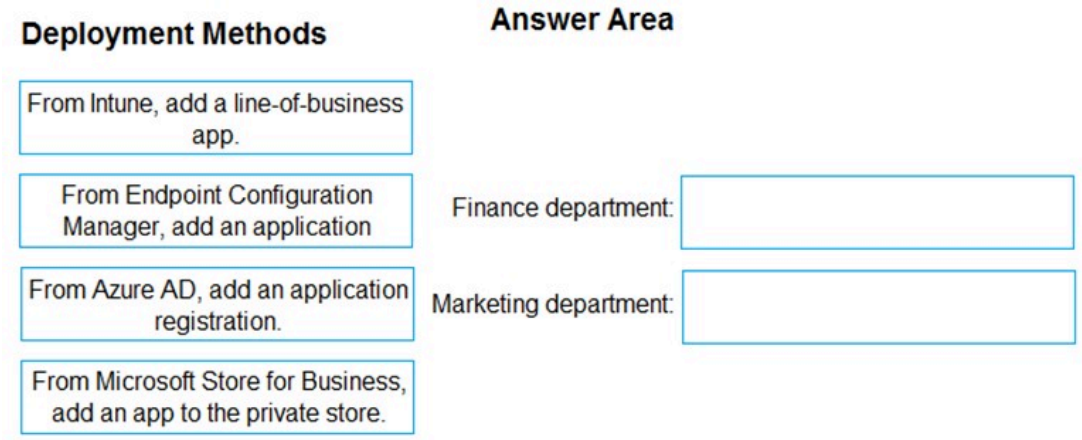
You purchase an application named App1 that uses an MSI package.

You need to install App1 on the finance department computers and the marketing department computers.

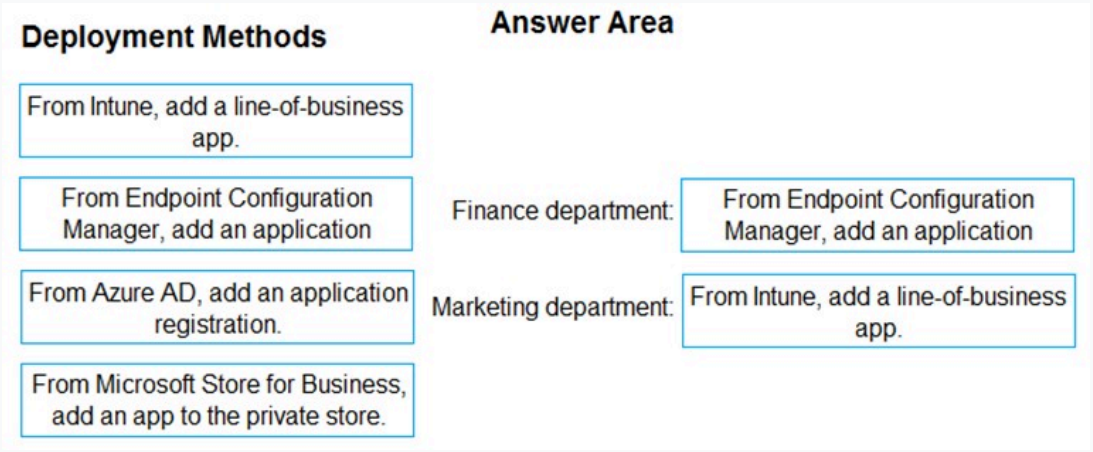
How should you deploy App1 to each department? To answer, drag the appropriate deployment methods to the correct departments. Each deployment method may be used once, more than once, or not at all. You may need to drag the split bat between panes or scroll to view content.

NOTE: Each correct selection is worth one point.

Select and Place:




**Suggested 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 3 years, 1 month ago
For MECM answer is correct!
upvoted 6 times

**Gaskonader** Most Recent 1 year, 3 months ago
Feels like a trick question.
upvoted 1 times

**mrjeet** 2 years ago
Easy peasy
upvoted 1 times

**USRobotics** 1 year, 4 months ago
Lemon squeeze
upvoted 1 times

**RodrigoT** 2 years, 9 months ago
Correct answer. Two easy points.
upvoted 4 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.

**Suggested 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 3 years, 7 months ago
Correct:

I believe this can be found under "Reports" > "Device Compliance"
upvoted 10 times

**Perycles** 3 years, 6 months ago
you're right
upvoted 4 times

**chalitha** Most Recent 3 years, 6 months ago
https://docs.microsoft.com/en-us/mem/intune/fundamentals/tutorial-walkthrough-endpoint-manager
upvoted 1 times

**Merma** 3 years, 7 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:

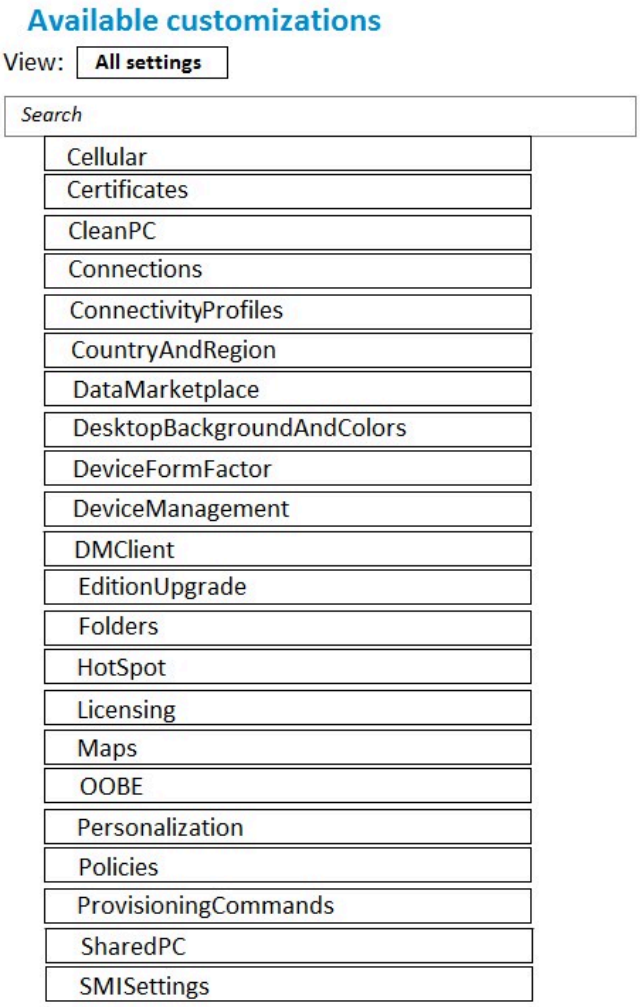
✑ Remove the Microsoft News and the Xbox Microsoft Store apps.

✑ Add a VPN connection to the corporate network.

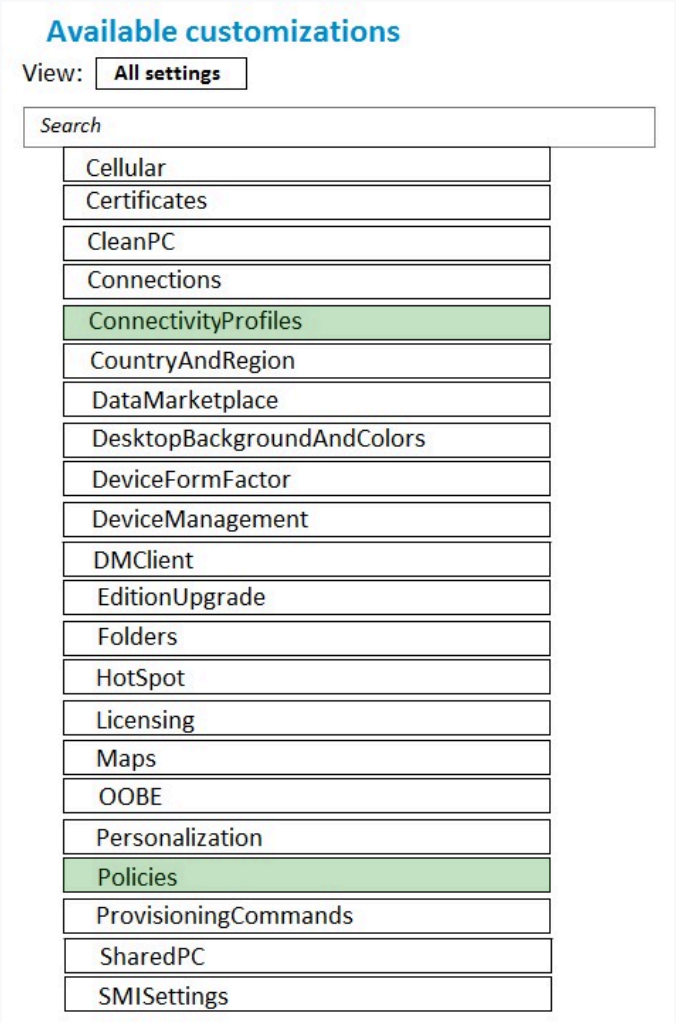
Which two customizations should you configure? To answer, select the appropriate customizations in the answer area.

NOTE: Each correct selection is worth one point.

Hot Area:



**Suggested 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 4 years, 6 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 32 times

**nolancl** Highly Voted 5 years, 3 months ago
Missing half the available customizations. UniversalAppUninstall should be an options and is the correct method to Remove the desired apps.
upvoted 20 times

**LauLauLauw** 4 years, 9 months ago
You are correct, checked it in a lab environment
upvoted 8 times

**lannythewizard** Most Recent 1 year, 8 months ago

App uninstall could be done with OOBE, but not sure if this question is saying this would be done during an initial setup, or applied to already setup machines, which would make a difference. The ConnectivityProfiles is for sure right for VPN though.
upvoted 1 times

**silver_bullet666** 2 years, 6 months 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** 3 years, 1 month 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** 3 years, 6 months ago
just checked under ICD : answer are : ConnectivityProfile and UniversaleAppUninstall
upvoted 2 times

**Perycles** 3 years, 6 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** 3 years, 8 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** 3 years, 10 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** 4 years, 6 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

**Suggested 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 4 years 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 3 years, 6 months ago
Conditional Access
-Access Control
-Require app protection policy
-ToU
upvoted 2 times

**Perycles** 3 years, 6 months ago
A is correct.
upvoted 3 times

**bertik** 3 years, 7 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** 3 years, 7 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** 3 years, 8 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** 3 years, 7 months ago
How to deploy Terms of Use in Azure Active Directory - https://www.youtube.com/watch?v=N4vgqHO2tgY
upvoted 1 times

**marz** 3 years, 10 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** 3 years, 11 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** 3 years, 11 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. | ○ | ○ |

**Suggested 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 3 years, 6 months ago

NO,YES,NO : be carrefull , most restrectived so bigger password lenght applied.

upvoted 42 times

**mikl** 3 years ago

I agree.

upvoted 2 times

**RodrigoT** 2 years, 8 months ago

Agreed. Answer provided is correct.

upvoted 6 times

**Merma** Highly Voted 3 years, 7 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 17 times

**RodrigoT** 2 years, 9 months ago

Good explanation, the bigger password applies because is the more restrictive.

upvoted 4 times

**Altheus** Most Recent 2 years, 1 month ago

The explanation is wrong about device 2, policy 2 and 4 apply to android and the most restrictive will apply.

upvoted 1 times

**AK4U_111** 2 years, 2 months ago

Answer is correct NO/YES/NO

This part of the given explanation is wrong:

"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."

Profile 2 & 4 are Android

upvoted 1 times

**gotrekk** 2 years, 4 months ago

No yes no

upvoted 2 times

**TonySuccess** 2 years, 3 months ago

Agreed

upvoted 1 times

**Nome2025** 3 years, 7 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 2 times

**Nome2025** 3 years, 7 months ago

they saying must have 6, so i think its a NO then.

upvoted 2 times

**Tomtom11** 3 years, 7 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** 3 years, 7 months ago

The correct answer is No, Yes, Yes

upvoted 1 times

**MikeMatt2020** 3 years, 7 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** 3 years ago
True !
upvoted 1 times

**Technik** 3 years, 8 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** 3 years, 8 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** 3 years, 8 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** 3 years, 8 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

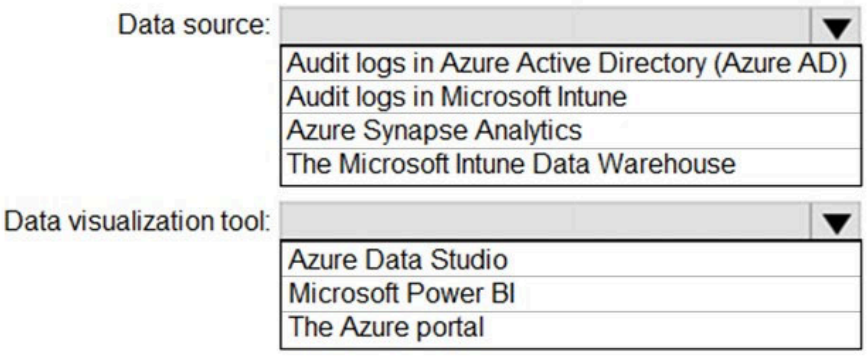
You need to recommend a data source and a data visualization tool for the design.

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

NOTE: Each correct selection is worth one point.

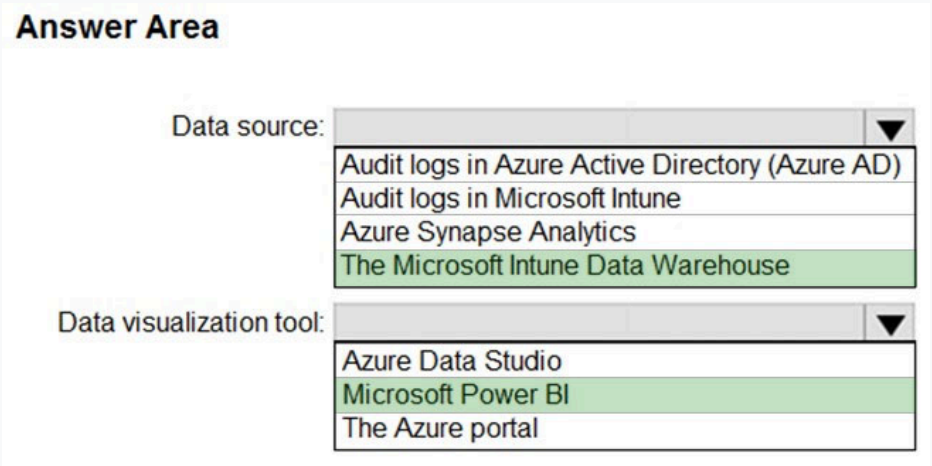
Hot Area:

**Answer Area**




**Suggested 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 3 years, 7 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 15 times

**Perycles** Highly Voted 3 years, 6 months ago
answer are correct.
upvoted 7 times

**jonny_sins** Most Recent 1 year, 10 months ago
Johnny sins approves these answers - look correct to me
upvoted 1 times

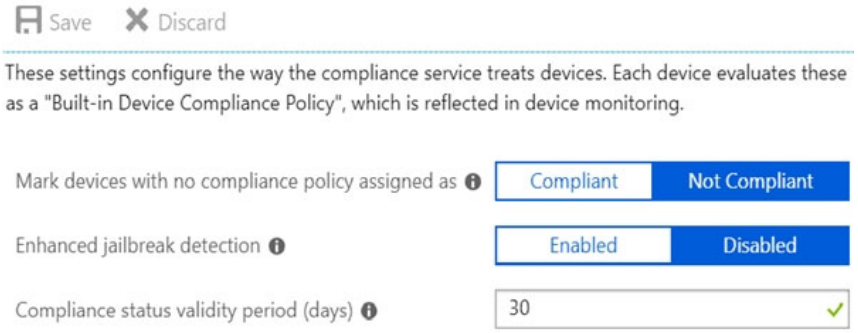
**mrjeet** 2 years ago
Correct!
upvoted 1 times

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.



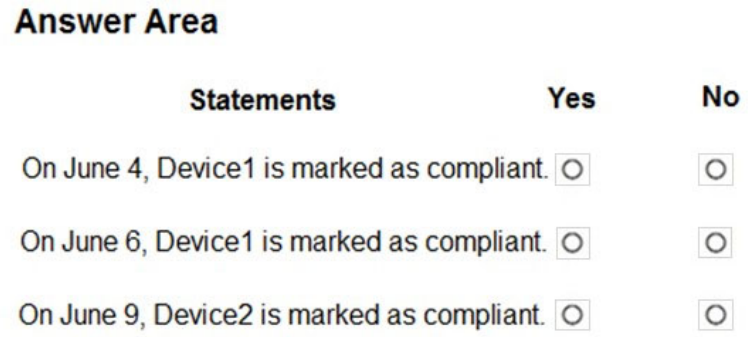

On June 1, you enroll Windows 10 devices in Intune as shown in the following table.

| 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:




**Suggested 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 3 years, 7 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 26 times

**LordCaine** 3 years, 3 months 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** 3 years, 3 months 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 18 times

**john909** 3 years, 2 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** 2 years, 11 months 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

**smart008** 10 months, 3 weeks ago

The Policy is for Windows 8.1 or later which means the policy will implement on windows 10 and 11 too.

upvoted 1 times

**Gonch** Highly Voted 3 years, 7 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** 3 years, 7 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** 2 years, 9 months 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 6 times

**smart008** Most Recent 10 months, 3 weeks ago

Box 1: Yes
Device 1 is not compliant as bit locker is not enabled but is still in grace period which is 5 days. This means the device is yet compliant and still have 1 day to show non-compliant status.
Box 2: No
Device 1 is not compliant because the BitLocker is not enabled and the grace period is also over which was 5 days.
Box 3: No
Group 2 (device2) has two policies assigned, Policy 2 with grace period 7 days and Policy 3 with grace period 10 days. Under Policy 3, the device is not compliant due to lack of encryption but is till in grace period which is 10 days. However, under Policy 2, the device is not compliant due to BitLocker not configured but the grace period is over which was 7 days.
Please correct me if I'm wrong

upvoted 1 times

**smart008** 10 months, 3 weeks ago

Apologies for incorrect interpretation:

Box 1: Yes
Device 1 is not compliant as bit locker is not enabled but is still in grace period which is 5 days. This means the device is yet compliant and still have 1 day to show non-compliant status.
Box 2: No
Device 1 is not compliant because the BitLocker is not enabled and the grace period is also over which was 5 days.
Box 3: Yes
Group 2 (device2) has two policies assigned, Policy 2 with grace period 7 days and no encryption required and Policy 3 with grace period 10 days. Under Policy 2, the device is compliant as BitLocker is not configured (not required) even though the grace period is over which was 7 days. Under Policy 3, the device is not compliant due to lack of encryption but is till in grace period which is 10 days. So device 2 is compliant in both cases.
Please correct me if I'm wrong

upvoted 2 times

**Amir1909** 11 months, 4 weeks ago

Yes
No
Yes
upvoted 1 times

**Altheus** 2 years, 2 months ago
This question contradicts itselt, answer A is marked as non-compliant even though it is in the grace period. Answer C is marked as compliant because it is in the grace period.
upvoted 1 times

**raduM** 2 years, 3 months ago
no no no. it will be in grace period not compliant
upvoted 3 times

**raduM** 2 years, 4 months ago
the correct answer is no, no,no. the devices will be in grace period and not compliant.just tested this fyi. :)
upvoted 2 times

**gotrekk** 2 years, 4 months ago
NNN.. i agree with others
upvoted 1 times

**CARO54** 2 years, 12 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** 3 years, 1 month 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** 2 years, 9 months ago
Policy1 is just for Windows 8 and Device1 is a Windows 10. So, Policy1 doesn't apply.
upvoted 1 times

**bensrayan** 2 years, 3 months ago
Policy1 is for Windows 8 AND LATER !
upvoted 2 times

**Perycles** 3 years, 6 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** 3 years, 7 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** 3 years, 6 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** 3 years, 6 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** 3 years, 6 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** 3 years, 7 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** 3 years, 7 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** 3 years, 7 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** 3 years, 8 months ago
No
No
Yes
upvoted 4 times

**RodrigoT** 2 years, 9 months 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** 3 years, 8 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** 3 years, 8 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

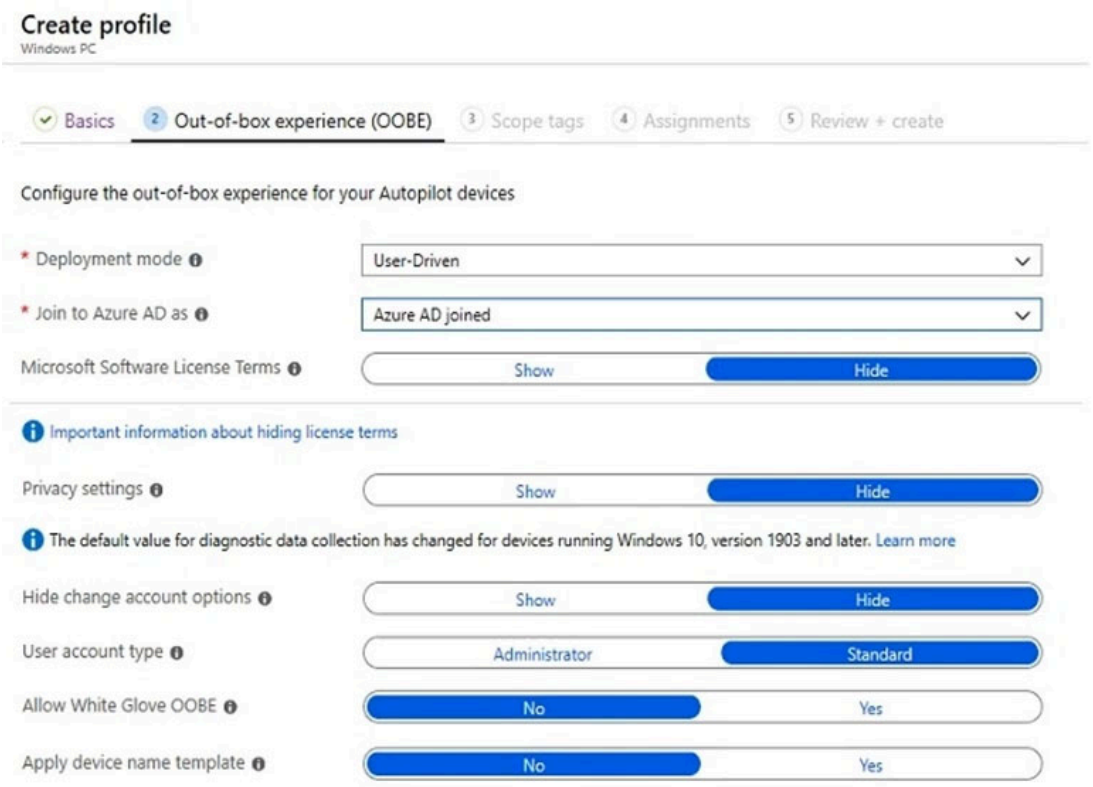
**RodrigoT** 2 years, 9 months ago

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.

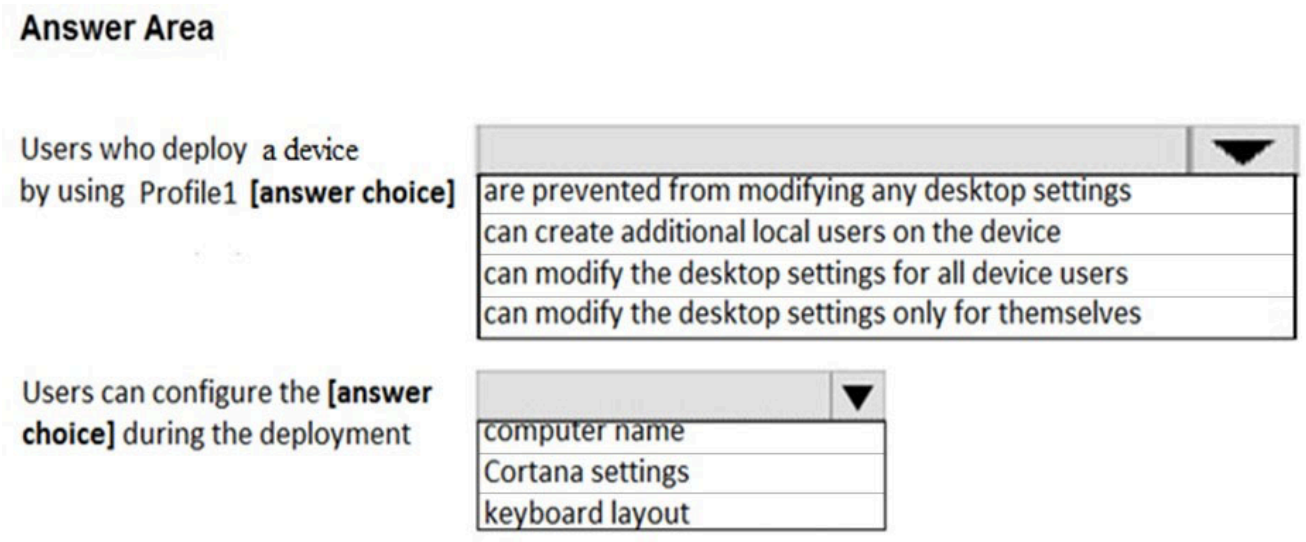
You create the Windows Autopilot deployment profile-shown in the following exhibit.



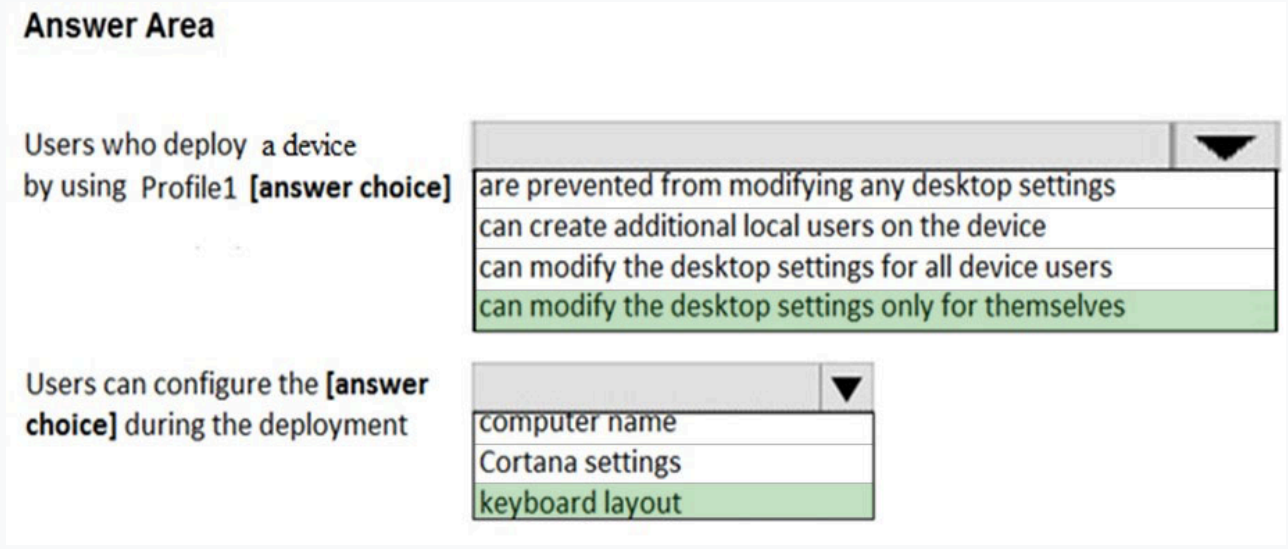

Use the drop-down menus to select the answer choice that completes each statement based on the information presented in the graphic.

NOTE: Each correct selection is worth one point.

Hot Area:



Suggested Answer:




Reference:
https://docs.microsoft.com/en-us/windows/deployment/windows-autopilot/user-driven

**MikeMatt2020** Highly Voted 3 years, 7 months ago
Answer given is correct
upvoted 6 times

**RosalindFranklin** Highly Voted 3 years, 2 months 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** 2 years, 11 months 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

**RodrigoT** 2 years, 9 months ago
Second part wrong, check my answer above, and the demo video.
upvoted 2 times

**camino** 2 years, 10 months 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 3 times

**RodrigoT** 2 years, 9 months 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 6 times

**OnurCJ** Most Recent 11 months, 4 weeks ago
can modify the desktop settings only for themselves - is correct
computer name - is correct
upvoted 1 times

**raduM** 2 years, 4 months ago

correct
upvoted 1 times

**gotrekk** 2 years, 4 months ago
Agree with given answers.
upvoted 1 times

**raduM** 2 years, 4 months 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** 2 years, 9 months ago
is the answer "Can modify the desktop settings only for themselves" because the keyboard option isn't available?
upvoted 1 times

**RodrigoT** 2 years, 9 months 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** 3 years, 6 months ago
all is correct.
upvoted 5 times